



Cisco Nexus 9000 Series NX-OS セキュリティ構成ガイド、リリース 10.6(x)

最終更新：2026 年 2 月 2 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/>

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>. Cisco product warranty information is available at <https://www.cisco.com/c/en/us/products/warranty-listing.html>. US Federal Communications Commission Notices are found here <https://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.



目次

Trademarks ?

はじめに :

はじめに xxxi

対象読者 xxxi

表記法 xxxi

Cisco Nexus 9000 シリーズ スイッチの関連資料 xxxii

マニュアルに関するフィードバック xxxii

通信、サービス、およびその他の情報 xxxiii

Cisco バグ検索ツール xxxiii

マニュアルに関するフィードバック xxxiii

第 1 章

新機能と更新情報 1

新機能と更新情報 1

第 2 章

概要 3

ライセンス要件 4

サポートされるプラットフォーム 4

Authentication, Authorization, and Accounting（認証、許可、およびアカウントティング） 4

RADIUS および TACACS+ セキュリティ プロトコル 5

LDAP 6

SSH および Telnet 6

ユーザ アカウントおよびユーザ ロール 6

IP ACL 6

MAC ACL 7

VACL 7

DHCP スヌーピング	7
ダイナミック ARP インスペクション	8
IP ソース ガード	8
パスワードの暗号化	8
キーチェーン管理	9
コントロールプレーン ポリシング	9
レート制限	9
ソフトウェア イメージ	9
仮想デバイス コンテキスト	10
SGT タグ付きパケット	10
TLS プロトコル サポート	10

第 3 章

FIPS の設定 13

FIPS について	13
FIPS のセルフテスト	13
FIPS エラー状態	14
FIPS の前提条件	15
FIPS の注意事項と制約事項	15
FIPS のデフォルト設定	15
FIPS の設定	16
FIPS モードの有効化	16
FIPS の無効化	17
FIPS 設定の確認	18
2048ビットRSAキーの作成	18
FIPS の設定例	19
FIPS に関する追加情報	19

第 4 章

AAA の設定 21

AAA について	21
AAA セキュリティ サービス	21
AAA を使用する利点	22

リモート AAA サービス	23
AAA サーバグループ	23
AAA サービス設定オプション	23
ユーザ ログインの認証および許可プロセス	25
AES パスワード暗号化およびプライマリ暗号キー	27
AAA の前提条件	27
AAA の注意事項と制約事項	27
AAA のデフォルト設定	29
AAA の設定	29
AAA の設定プロセス	30
コンソール ログイン認証方式の設定	30
デフォルトのログイン認証方式の設定	32
ローカル認証へのフォールバックの無効化	34
AAA 認証のデフォルト ユーザ ロールのイネーブル化	35
ログイン認証失敗メッセージの有効化	36
成功したログイン試行と失敗したログイン試行	37
ユーザごとのログイン ブロックの設定	38
CHAP 認証の有効化	40
MSCHAP または MSCHAP V2 認証の有効化	42
LDAP サーバでの AAA 許可の設定	44
TACACS サーバでの AAA SSH 証明書認証の構成	45
デフォルトの AAA アカウンティング方式の設定	46
Cisco NX-OS デバイスによる AAA サーバの VSA の使用	48
VSA の概要	48
VSA の形式	49
AAA サーバ上での Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータの指定	49
セキュア ログイン機能の設定	50
ログイン パラメータの設定	50
ユーザ ログインセッションの制限	51
パスワードの長さの制限	52
ユーザ名のパスワードプロンプトのイネーブル化	53

RADIUS または TACACS+ の共有秘密の設定	54
RADIUS ログイン情報キャッシュ	55
RADIUS クレデンシャルの処理方法	55
RADIUS クレデンシャルのキャッシングの注意事項と制約事項	56
RADIUS クレデンシャルキャッシングの構成	56
RADIUS ログイン情報キャッシング構成の検証	57
ローカル AAA アカウンティング ログのモニタリングとクリア	58
AAA 設定の確認	58
AAA の設定例	60
ログインパラメータの設定例	60
パスワードプロンプト機能の設定例	61
AAA に関する追加情報	61

第 5 章

RADIUS の設定 63

RADIUS について	63
RADIUS ネットワーク環境	64
RADIUS の動作	64
RADIUS サーバのモニタリング	65
ベンダー固有属性	66
RADIUS 認可変更について	67
セッション再認証	67
セッションの終了	68
RADIUS の前提条件	68
RADIUS の注意事項と制約事項	68
RadSec の注意事項と制約事項	69
RADIUS の認可変更の注意事項と制約事項	70
RADIUS のデフォルト設定	70
RADIUS サーバの設定	71
RADIUS サーバの設定プロセス	71
RADIUS サーバホストの設定	71
グローバル RADIUS キーの設定	73

特定の RADIUS サーバ用のキーの設定	74
RADIUS 属性メッセージ オーセンティケータの構成	76
RadSec の設定	77
DTLS を使用した RADIUS について	79
DTLS を使用する RADIUS の構成	79
RADIUS サーバ グループの設定	81
RADIUS サーバ グループのためのグローバル発信元インターフェイスの設定	83
ログイン時にユーザによる RADIUS サーバの指定を許可	84
グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定	85
サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定	86
RADIUS サーバのアカウンティングおよび認証属性の設定	87
RADIUS サーバのグローバルな定期モニタリングの設定	88
各 RADIUS サーバの定期モニタリングの設定	90
RADIUS デッド タイム間隔の設定	92
ワンタイム パスワードの設定	93
RADIUS サーバまたはサーバ グループの手動モニタリング	93
Dynamic Author Server の有効化または無効化	94
RADIUS 認可変更の設定	94
RADIUS 設定の確認	95
RADIUS 認可変更の設定の検証	96
RADIUS サーバのモニタリング	96
RADIUS サーバ統計情報のクリア	97
RADIUS の設定例	98
RADIUS 認可変更の設定例	98
次の作業	98
RADIUS に関する追加情報	98

第 6 章

TACACS+ の設定	101
TACACS+ について	101
TACACS+ の利点	102
ユーザ ログインにおける TACACS+ の動作	102

デフォルトの TACACS+ サーバ難読化タイプおよび秘密キー	103
TACACS+ サーバのコマンド許可サポート	103
TACACS+ サーバのモニタリング	103
TACACS+ のベンダー固有属性	104
TACACS+ 用の Cisco VSA 形式	104
TACACS+ の前提条件	105
TACACS+ のガイドラインと制約事項	106
TACACS+ のデフォルト設定	107
ワンタイム パスワード サポート	107
TACACS+ の設定	108
TACACS+ サーバの設定プロセス	108
TACACS+ のイネーブル化	108
TACACS+ サーバホストの設定	109
グローバル TACACS+ キーの設定	111
特定の TACACS+ サーバ用のキーの設定	112
TACACS+ サーバグループの設定	113
TACACS+ サーバグループのためのグローバル発信元インターフェイスの設定	115
ユーザによるログイン時の TACACS+ サーバ指定の許可	116
TACACS+ サーバのタイムアウト間隔の設定	117
TCP ポートの設定	118
TACACS+ サーバのグローバルな定期モニタリングの設定	119
各 TACACS+ サーバの定期モニタリングの設定	121
TACACS+ デッド タイム間隔の設定	123
ASCII 認証の設定	124
TACACS+ サーバでのコマンド許可の設定	125
TACACS+ サーバでのコマンド許可のテスト	128
コマンド許可検証のイネーブル化とディセーブル化	128
TACACS サーバーを使用した X.509 証明書ベースの SSH 認証の設定	129
権限ロールのユーザ コマンドの許可または拒否	130
TACACS+ サーバまたはサーバグループの手動モニタリング	132
TACACS+ のディセーブル化	132

TACACS+ サーバのモニタリング	133
TACACS+ サーバ統計情報のクリア	133
TACACS+ の設定の確認	134
TACACS+ の設定例	134
TACACS+ Over TLS の構成	135
TACACS+ Over TLS の構成の確認	137
次の作業	137
TACACS+ に関する追加情報	137

第 7 章

LDAP の設定 139

LDAP について	139
LDAP 認証および許可	140
ユーザ ログインにおける LDAP の動作	140
LDAP サーバのモニタリング	141
LDAP のベンダー固有属性	142
LDAP 用の Cisco VSA 形式	142
LDAP のバーチャライゼーション サポート	142
LDAP の前提条件	142
LDAP の注意事項と制約事項	143
LDAP のデフォルト設定	143
LDAP の設定	144
LDAP サーバの設定プロセス	144
LDAP 機能の有効化	145
LDAP サーバー ホストの構成	146
LDAP サーバの rootDN の設定	147
LDAP サーバ グループの設定	148
グローバルな LDAP タイムアウト間隔の設定	150
LDAP サーバのタイムアウト間隔の設定	151
TCP ポートの設定	152
LDAP 検索マップの構成	153
LDAP サーバの定期的モニタリングの設定	154

LDAP デッドタイム間隔の設定	155
LDAP サーバでの AAA 許可の設定	156
LDAP SSH 公開キー認証の設定	157
LDAP SSH 証明書許可の設定	158
LDAP サーバのモニタリング	159
LDAP サーバ統計情報のクリア	160
LDAP 設定の確認	160
LDAP の設定例	161
次の作業	162
LDAP に関する追加情報	162

第 8 章

SSH および Telnet の設定 163

SSH および Telnet について	163
SSH サーバー	163
SSH クライアント	164
SSH サーバ キー	164
デジタル証明書を使用した SSH 認証	165
ホスト アイデンティティに基づく認証 (HIBA) を使用した SSH 認証	165
HIBA の利点	165
HIBA による SSH 認証の仕組み	166
SSH 認証の HIBA の構成	167
HIBA 構成の確認	170
Telnet サーバ	172
SSH および Telnet の前提条件	172
SSH と Telnet のガイドラインと制約事項	172
SSH および Telnet のデフォルト設定	174
SSH の設定	175
SSH サーバ キーの生成	175
ユーザ アカウント用 SSH 公開キーの指定	176
IETF SECSH 形式による SSH 公開キーの指定	176
OpenSSH 形式の SSH 公開キーの指定	177

SSH ログイン試行の最大回数の設定	178
SSH セッションの開始	179
ブート モードからの SSH セッションの開始	180
SSH のパスワードが不要なファイル コピーの設定	181
SCP サーバと SFTP サーバの設定	183
X.509v3 証明書ベースの SSH 認証の設定	184
TACACS サーバでの SSH 証明書認証の構成	187
SSH 暗号化アルゴリズムのカスタマイズ	187
サポートされるアルゴリズム：FIPモードが有効の場合	192
デフォルトの SSH サーバ ポートの変更	193
SSH ホストのクリア	195
SSH サーバのディセーブル化	195
SSH サーバ キーの削除	196
SSH セッションのクリア	197
Telnet の設定	197
Telnet サーバのイネーブル化	197
リモート デバイスとの Telnet セッションの開始	198
Telnet セッションのクリア	199
SSH および Telnet の設定の確認	199
SSH の設定例	200
SSH のパスワードが不要なファイル コピーの設定例	202
X.509v3 証明書ベースの SSH 認証の設定例	203
SSH および Telnet に関する追加情報	204

第 9 章

PKI の設定 207

PKI の概要 207

CA とデジタル証明書 207

信頼モデル、トラストポイント、アイデンティティ CA 208

CA証明書の階層 208

CA バンドルのインポート 208

PKCS7 形式での CA 証明書バンドルのインポート 209

RSA のキー ペアとアイデンティティ証明書	210
複数の信頼できる CA のサポート	212
PKI の登録のサポート	212
カットアンドペーストによる手動での登録	212
複数の RSA キー ペアとアイデンティティ CA のサポート	213
ピア証明書の検証	213
証明書の取消確認	213
CRL のサポート	214
NDePP : syslog の OCSP	214
証明書と対応するキー ペアのインポートとエクスポート	214
PKI の注意事項と制約事項	214
PKI のデフォルト設定	215
CA の設定とデジタル証明書	215
ホスト名と IP ドメイン名の設定	216
RSA キー ペアの生成	217
ECC キー ペアの生成	218
トラストポイント CA のアソシエーションの作成	219
証明書マッピングのフィルタの設定	221
CA の認証	223
証明書取消確認方法の設定	225
証明書要求の作成	226
アイデンティティ証明書のインストール	228
トラストポイントの設定がリブート後も維持されていることの確認	229
PKCS 12 形式でのアイデンティティ情報のエクスポート	230
PKCS 12または PKCS 7 フォーマットで ID 情報のインポート	231
CRL の設定	232
CA の設定からの証明書の削除	233
Cisco NX-OSデバイスからの RSA キー ペアの削除	235
PKI の設定の確認	236
PKI の設定例	236
Cisco NX-OS デバイスでの証明書の設定	236

CA 証明書のダウンロード	239
アイデンティティ証明書の要求	245
証明書の取り消し	259
CRL の作成と公開	262
CRL のダウンロード	264
CRL のインポート	269
PKI に関する追加情報	272
PKI の関連資料	272
PKI の標準規格	272
Cisco SUDI 証明書チェーンを使用したデバイス構成証明	272
SUDI 証明書チェーン構成証明および署名の仕組み	273
注意事項と制約事項	273
SUDI 証明書チェーンの構成証明と署名の確認	274

第 10 章

ユーザアカウントおよび RBAC の設定	277
ユーザアカウントと RBAC について	277
ユーザアカウント	277
強力なパスワードの特性	278
ユーザ ロール	279
ユーザ ロールのルール	280
ユーザアカウントおよび RBAC の注意事項と制約事項	281
ユーザアカウントおよび RBAC のデフォルト設定	282
パスワードの強度確認のイネーブル化	283
パスワードの連続文字チェックの有効化	284
ユーザアカウントの設定	285
ロールの設定	288
ユーザ ロールおよびルールの作成	288
機能グループの作成	291
ユーザ ロール インターフェイス ポリシーの変更	292
ユーザ ロール VLAN ポリシーの変更	293
ユーザ ロールの VRF ポリシーの変更	294

No Service Password-Recovery について	295
No Service Password-Recovery のイネーブル化	296
ユーザ アカウントおよび RBAC 設定の確認	297
ユーザ アカウントおよび RBAC の設定例	298
ユーザ アカウントおよび RBAC に関する追加情報	299

第 11 章

802.1X の設定 301

802.1X について	301
デバイスのロール	302
認証の開始およびメッセージ交換	303
インターフェイスのオーセンティケータ PAE ステータス	304
許可ステートおよび無許可ステートのポート	304
MAC 認証バイパス	305
MAC-Based Authentication (MAB) に基づくダイナミック VLAN 割り当て	306
RADIUS からの VLAN 割り当て	307
シングル ホストおよびマルチ ホストのサポート	307
サポートされるトポロジ	307
ユーザ単位の DACL について	308
クリティカル認証	308
音声 VLAN 向け 802.1X について	309
音声 VLAN 向け 802.1X の概要	309
音声 VLAN 用 802.1X の機能	309
音声 VLAN の 802.1X のメッセージ交換	309
DACL について	310
802.1X の前提条件	310
802.1X のガイドラインと制約事項	311
音声 VLAN に関連した 802.1X のガイドラインと制限事項	315
802.1X 向け事前ユーザ DACL サポートのガイドラインと制約事項	316
クリティカル認証のガイドラインと制限事項	317
802.1X のデフォルト設定	317
802.1X の設定	318

802.1X の設定プロセス	318
802.1X 機能のイネーブル化	318
802.1X の AAA 認証方式の設定	319
インターフェイスでの 802.1X 認証の制御	320
音声 VLAN 向け 802.1X の構成	322
EAP-TLS の設定	322
インターフェイスでのオーセンティケータ PAE の作成または削除	324
クリティカル認証を有効にする	325
インターフェイスの定期再認証のイネーブル化	327
手動によるサブリカントの再認証	329
インターフェイスの 802.1X 認証タイマーの変更	329
MAC 認証バイパスのイネーブル化	332
デフォルトの 802.1X 認証方法の構成 - MAB	333
ダイナミック アクセス リストの作成	334
ユーザ単位の DACL 設定	335
シングル ホスト モードまたはマルチ ホスト モードのイネーブル化	336
Cisco NX-OS デバイスでの 802.1X 認証の無効化	337
802.1X 機能のディセーブル化	339
802.1X インターフェイス設定のデフォルト値へのリセット	339
インターフェイスでのオーセンティケータとサブリカント間のフレームの最大数の設定	340
802.1X 認証の RADIUS アカウンティングのイネーブル化	341
802.1X の AAA アカウンティング方式の設定	342
インターフェイスでの再認証最大リトライ回数の設定	343
802.1X 設定の確認	344
VXLAN EVPN の 802.1X サポート	346
VXLAN EVPN の 802.1X サポートに関する注意事項と制約事項	346
VXLAN EVPN の 802.1X サポートの設定	347
VXLAN EVPN の 802.1X サポートの確認	348
クリティカル認証の確認	351
802.1X のモニタリング	351

802.1X の設定例	351
ユーザ 1 人あたりの DACL の設定例	352
802.1X に関する追加情報	352

第 12 章

IP ACL の構成 355

ACL について	355
ACL のタイプと適用	356
ACL の適用順序	357
ルールについて	358
IP ACL および MAC ACL のプロトコル	359
送信元と宛先	359
IP ACL および MAC ACL の暗黙ルール	359
その他のフィルタリング オプション	360
シーケンス番号	362
論理演算子と論理演算ユニット	362
ACL ロギング	363
時間範囲	363
ポリシーベース ACL	365
カーネル スタック ACL	366
統計情報と ACL	367
Atomic ACL のアップデート	368
IP ACL に対する Session Manager のサポート	368
ACL TCAM リージョン	368
ACL タイプでサポートされる最大ラベル サイズ	375
IP ACL の前提条件	376
IP ACL の注意事項と制約事項	376
IP ACL のデフォルト設定	389
IP ACL の設定	390
IP ACL の作成	390
IP ACL の変更	392
VTY ACL の作成	394

IP ACL 内のシーケンス番号の変更	396
IP ACL の削除	396
ACL TCAM リージョン サイズの設定	397
テンプレートを使用した ACL TCAM リージョン サイズの設定	409
TCAM カービングの設定	411
UDF ベース ポート ACL の設定	417
ルータ ACL としての IP ACL の適用	420
ポート ACL としての IP ACL の適用	421
IP ACL の VACL としての適用	423
SUP ルールに対する IP ACL ルールの優先順位付けの適用	423
ACL ロギングの設定	424
要求をリダイレクトするための HTTP メソッドによる ACL の設定	427
IPv6 拡張ヘッダーの ACL の設定	430
IP ACL の設定の確認	431
IP ACL の統計情報のモニタリングとクリア	433
IP ACL の設定例	434
システム ACL について	436
TCAM リージョンの分割	437
システム ACL の設定	437
システム ACL の設定および show コマンドの例	437
オブジェクト グループの設定	439
オブジェクト グループに対する Session Manager のサポート	440
IPv4 アドレス オブジェクト グループの作成および変更	440
IPv6 アドレス オブジェクト グループの作成および変更	441
プロトコル ポート オブジェクト グループの作成および変更	442
オブジェクト グループの削除	444
オブジェクト グループの設定の確認	444
時間範囲の設定	445
時間範囲の Session Manager サポート	445
時間範囲の作成	445
時間範囲の変更	446

時間範囲の削除	448
時間範囲のシーケンス番号の変更	448
時間範囲設定の確認	449
IP ACL に関する追加情報	450

第 13 章

MAC ACL の設定	451
MAC ACL について	451
MAC パケット分類	451
MAC ACL の注意事項と制約事項	452
MAC ACL のデフォルト設定	453
MAC ACL の設定	453
MAC ACL の作成	453
UDF ベースの MAC ACL の設定	454
MAC ACL の変更	456
MAC ACL 内のシーケンス番号の変更	458
MAC ACL の削除	458
ポート ACL としての MAC ACL の適用	459
MAC ACL の VACL としての適用	460
MAC パケット分類のイネーブル化または無効化	460
SUP ルールに対する MAC ACL ルールの優先順位付けの適用	462
MAC ACL の設定の確認	463
MAC ACL の統計情報のモニタリングとクリア	464
MAC ACL の設定例	464
MAC ACL に関する追加情報	464

第 14 章

VLAN ACL の設定	465
VLAN ACL について	465
VLAN アクセス マップとエントリ	465
VACL とアクション	466
VACL の統計情報	466
VACL に対する Session Manager のサポート	466

VACL の前提条件	466
VACL の注意事項と制約事項	467
VACL のデフォルト設定	468
VACL の設定	468
VACL の作成または VACL エントリの追加	468
VACL または VACL エントリの削除	470
VACL の VLAN への適用	470
VACL 設定の確認	471
VACL 統計情報のモニタリングとクリア	472
VACL の設定例	472
VACL に関する追加情報	472

第 15 章

ポートセキュリティの設定	473
ポートセキュリティの概要	473
セキュア MAC アドレスの学習	474
スタティック方式	474
ダイナミック方式	474
スティッキ方式	475
ダイナミック アドレスのエージング	475
セキュア MAC アドレスの最大数	476
セキュリティ違反と処理	476
ポートセキュリティとポート タイプ	478
ポートセキュリティとポート チャネルインターフェイス	478
ポート タイプの変更	480
ポートセキュリティの前提条件	481
ポートセキュリティのデフォルト設定	481
ポートセキュリティの注意事項と制約事項	481
vPC 上のポートセキュリティの注意事項と制約事項	482
ポートセキュリティの設定	483
ポートセキュリティのグローバルなイネーブル化またはディセーブル化	483

レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化	484
スティック MAC アドレス ラーニングのイネーブル化またはディセーブル化	485
インターフェイスのスタティック セキュア MAC アドレスの追加	486
インターフェイスのスタティック セキュア MAC アドレスの削除	487
スティック セキュア MAC アドレスの削除	488
ダイナミック セキュア MAC アドレスの削除	490
MAC アドレスの最大数の設定	491
アドレス エージング タイプおよび時間を設定する	492
セキュリティ違反時の処理の設定	493
ポート セキュリティの設定の確認	494
セキュア MAC アドレスの表示	495
ポート セキュリティの設定例	495
vPC ドメインでのポート セキュリティの設定例	495
例：孤立ポートでのポート セキュリティの設定	495
例：vPC レッグ上のポート セキュリティの設定	496
ポート セキュリティに関する追加情報	496
VXLAN EVPN のポート セキュリティ サポート	497
VXLAN EVPN のポート セキュリティ サポートに関する注意事項と制約事項	497
VXLAN EVPN のポート セキュリティ サポートの確認	498

第 16 章

DHCP の設定 501

DHCP スヌーピングについて	502
信頼できる送信元と信頼できない送信元	502
DHCP スヌーピング バインディング データベース	503
vPC 環境での DHCP スヌーピング	503
DHCP スヌーピング バインディング エントリの同期	504
パケット検証	504
DHCP スヌーピングの Option 82 データ挿入	504
DHCP リレー エージェントについて	508
DHCP リレー エージェント	508

DHCP リレー エージェントの Option 82	508
DHCP リレー エージェントに対する VRF サポート	510
DHCP スマート リレー エージェント	511
DHCPv6 リレー エージェントについて	511
DHCPv6 リレー エージェント	511
DHCPv6 リレー エージェントに対する VRF サポート	512
v6 リレー エージェントを介した委任プレフィックスの IPv6 可用性	512
DHCPv6 スマート リレー エージェント	512
DHCPv6 スマート リレーの注意事項と制約事項	513
DHCP クライアントについて	513
DHCP の前提条件	513
DHCP のガイドラインと制約事項	513
DHCP のデフォルト設定	516
DHCP の設定	517
DHCP の最小設定	517
DHCP 機能のイネーブル化またはディセーブル化	518
DHCP スヌーピングの設定	518
DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化	518
VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化	519
DHCP スヌーピングの MAC アドレス検証のイネーブル化またはディセーブル化	520
Option 82 データの挿入および削除の有効化または無効化	521
DHCP パケットの厳密な検証のイネーブル化またはディセーブル化	523
インターフェイスの信頼状態の設定	524
DHCP リレー信頼ポート機能のイネーブル化またはディセーブル化	525
インターフェイスを DHCP リレーの信頼済みまたは信頼できないポートとして設定する	526
すべてのインターフェイスの信頼状態の設定	528
DHCP リレー エージェントのイネーブル化またはディセーブル化	529
DHCP リレー エージェントに対する Option 82 の有効化または無効化	530
DHCP リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化	532
DHCP Server Identifier オーバーライド サブオプション	533

インターフェイスへの DHCP サーバアドレスの設定	533
DHCP リレー送信元インターフェイスの設定	535
DHCP スマート リレーのグローバルなイネーブル化またはディセーブル化	537
レイヤ 3 インターフェイスでの DHCP スマート リレーの有効化または無効化	538
DHCP リレー サブネット選択の設定	539
DHCPv6 の設定	540
DHCPv6 リレー エージェントのイネーブル化またはディセーブル化	540
DHCPv6 リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化	541
DHCPv6 スマート リレーのグローバルな有効化または無効化	543
レイヤ 3 インターフェイスでの DHCPv6 スマート リレーの有効化または無効化	543
インターフェイスへの DHCPv6 サーバアドレスの設定	545
DHCPv6 オプション 79 のイネーブル化	546
DHCPv6 リレー送信元インターフェイスの設定	547
IPv6 RA ガードの設定	548
ローカル ゲスト シェル/Docker でのサーバーへの DHCP リレー	549
ローカル ゲスト シェル/Docker への DHCP リレーの仕組み	550
注意事項と制約事項	550
ローカル ゲスト シェル/Docker への DHCP リレーの構成	551
ローカル ゲスト シェル/Docker への DHCP リレーの確認	552
DHCP クライアントの有効化	553
UDP リレーの設定	554
UDP リレーについて	554
UDP リレーの注意事項と制約事項	555
UDP リレーの設定	556
UDP リレーの設定例	557
UDP リレーの設定の確認	558
DHCP 設定の確認	558
IPv6 RA ガードの統計情報の表示	561
DHCP スヌーピング バインディングの表示	561
DHCP スヌーピング バインディング データベースのクリア	562

DHCP のモニタリング	562
DHCP スヌーピング統計情報のクリア	562
DHCP リレー統計情報のクリア	563
DHCPv6 リレー統計情報のクリア	563
DHCPv6-PD バインドのクリア	563
DHCP の設定例	564
DHCP クライアントの設定例	564
DHCP に関する追加情報	565

第 17 章

IPv6 ファースト ホップ セキュリティの設定	567
ファーストホップセキュリティについて	567
IPv6 グローバル ポリシー	568
IPv6 ファーストホップセキュリティ バインディング テーブル	568
ファーストホップセキュリティの注意事項と制約事項	569
vPC ファーストホップセキュリティ設定について	569
DHCP リレー オンスタック	569
VPC レッグでの DHCP リレー	570
孤立ポートでの DHCP クライアント リレー	571
RA ガード	573
IPv6 RA ガードの概要	573
IPv6 RA ルータ アドバタイズメントとフラグ	573
IPv6 RA ガードの注意事項と制約事項	574
DHCPv6 ガード	574
DHCPの概要 : DHCPv6 ガード	574
DHCPv6 ガードの制限事項	575
IPv6 スヌーピング	575
IGMP スヌーピングの概要	575
IPv6 スヌーピングに関する注意事項と制限事項	576
IPv6 FHS の設定方法	576
デバイスでの IPv6 RA ガード ポリシーの設定	576
インターフェイスの IPv6 RA ガードの設定	579

DHCP の設定 : DHCPv6 ガード	580
IPv6 スヌーピングの設定	582
IPv6 スヌーピングの確認とトラブルシューティング	585
設定例	585
例 : IPv6 RA ガードの設定	585
例 : DHCP—DHCPv6 ガードの設定	586
例 : IPv6 ファーストホップ セキュリティ バインディング テーブルの設定	586
例 : IPv6 スヌーピングの設定	586
IPv6 ファーストホップ セキュリティに関する追加情報	587

第 18 章

ダイナミック ARP インспекションの設定	589
DAI について	589
ARP	589
ARP スプーフィング攻撃	590
DAI および ARP スプーフィング攻撃	591
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	591
DAI パケットのロギング	593
ダイナミック ARP インспекションを使用した DHCP リレー	593
DAI の前提条件	594
DAI の注意事項と制約事項	594
DAI の DHCP リレーの注意事項と制約事項	595
DAI のデフォルト設定	595
DAI の設定	596
VLAN での DAI の有効化と無効化	596
レイヤ 2 インターフェイスの DAI 信頼状態の設定	597
追加検証の有効化または無効化	598
DAI のログ バッファ サイズの設定	599
DAI のログ フィルタリングの設定	600
DAI を使用した DHCP リレーの有効化	601
DAI の設定の確認	602
DAI の統計情報のモニタリングとクリア	602

DAI の設定例 602**DAI をサポートする 2 つのデバイス 602****デバイス A の設定 603****デバイス B の設定 605****DHCP リレーの DAI の例 607****DAI に関する追加情報 608****関連資料 608****標準 608**

第 19 章**IP ソース ガードの設定 609****IP ソース ガードについて 609****IP ソース ガードの前提条件 610****IP ソース ガードの注意事項と制約事項 610****IP ソース ガードのデフォルト設定 611****IP ソース ガードの設定 611****レイヤ 2 インターフェイスに対する IP ソース ガードの有効化または無効化 611****スタティック IP ソース エントリの追加または削除 612****トランク ポート用 IP ソース ガードの設定 613****IP ソース ガード バインディングの表示 614****IP ソース ガードの統計情報のクリア 614****IP ソース ガードの設定例 615****その他の参考資料 615****関連資料 615**

第 20 章**パスワード暗号化の設定 617****AES パスワード暗号化およびプライマリ暗号キーについて 617****パスワード暗号化の注意事項と制約事項 618****パスワード暗号化のデフォルト設定 620****パスワード暗号化の設定 620****プライマリ キーの設定および AES パスワード暗号化機能の有効化 620****既存のパスワードのタイプ 6 暗号化パスワードへの変換 622**

タイプ 6 暗号化パスワードの元の状態への変換	622
MACsec キーでのタイプ 6 暗号化の有効化	622
タイプ 6 暗号化パスワードの削除	624
パスワード暗号化の設定の確認	624
パスワード暗号化の設定例	625

第 21 章

キーチェーン管理の設定 631

キーチェーン管理について	631
キーチェーン管理の前提条件	632
キーチェーン管理の注意事項と制約事項	632
キーチェーン管理のデフォルト設定	633
キーチェーン管理の設定	633
キーチェーンの作成	633
キーチェーンの削除	634
プライマリ キーの設定および AES パスワード暗号化機能の有効化	635
キーのテキストの設定	636
キーの受け入れライフタイムおよび送信ライフタイムの設定	639
OSPFv2 暗号化認証用のキーの設定	641
アクティブなキーのライフタイムの確認	642
キーチェーン管理の設定の確認	642
キーチェーン管理の設定例	642
次の作業	643
キーチェーン管理に関する追加情報	643

第 22 章

トラフィック ストーム制御の設定 645

トラフィック ストーム制御について	645
トラフィック ストーム制御のライセンス要件	647
トラフィック ストーム制御のガイドラインと制約事項	647
トラフィック ストーム制御のデフォルト設定	652
ワンレベルのしきい値のトラフィック ストーム制御の設定	652
CoPP ポリサーよりもストーム制御ポリサーを優先する	653

ツールレベルのしきい値のトラフィック ストーム制御の設定	654
トラフィック ストーム制御の設定の確認	656
トラフィック ストーム制御カウンタのモニタリング	656
トラフィック ストーム制御の設定例	657
トラフィック ストーム制御のシステム ログの例	657
トラフィック ストーム制御に関する追加情報	658

第 23 章

ユニキャスト RPF の設定 659

ユニキャスト RPF について	659
ユニキャスト RPF プロセス	660
ユニキャスト RPF の注意事項と制約事項	661
ユニキャスト RPF のデフォルト設定	664
-R ライン カードを搭載した Cisco Nexus 9500 スイッチのユニキャスト RPF の設定	664
Cisco Nexus 9300 スイッチのユニキャスト RPF の設定	666
ユニキャスト RPF の設定例	668
ユニキャスト RPF の設定の確認	669
ユニキャスト RPF に関する追加情報	670

第 24 章

スイッチポート ブロッキングの設定 671

スイッチポート ブロッキングについて	671
スイッチポート ブロッキングの注意事項および制約事項	671
スイッチポート ブロッキングのデフォルト設定	672
スイッチポート ブロッキングの設定	672
スイッチポート ブロッキング設定の確認	673
スイッチポート ブロッキングの設定例	673

第 25 章

コントロール プレーン ポリシングの設定 675

CoPP について	675
コントロール プレーン保護	677
コントロール プレーンのパケット タイプ	677
CoPP の分類	678

出力 CoPP	678
レート制御メカニズム	678
ダイナミックおよびスタティック CoPP ACL	679
デフォルトのポリシング ポリシー	680
モジュラ QoS コマンドライン インターフェイス	688
CoPP と管理インターフェイス	689
CoPP の注意事項と制約事項	689
CoPP のデフォルト設定	695
CoPP の設定	695
コントロールプレーン クラス マップの設定	695
コントロールプレーン ポリシー マップの設定	697
コントロールプレーン サービス ポリシーの設定	699
ラインカードごとの CoPP のスケール ファクタの設定	701
デフォルトの CoPP ポリシーの変更または再適用	702
CoPP ベスト プラクティス ポリシーのコピー	703
出力 CoPP のプロトコル ACL フィルタリング	703
出力 CoPP の ARP ACL フィルタリングの構成	704
出力 CoPP の IP ACL フィルタリングの構成	706
CoPP の設定の確認	708
CoPP 設定ステータスの表示	711
CoPP 整合性チェッカー	711
CoPP のモニタリング	712
SNMP での CoPP のモニタリング	713
CoPP 統計情報のクリア	713
CoPP の設定例	714
CoPP の設定例	714
セットアップ ユーティリティによるデフォルト CoPP ポリシーの変更または再適用	715
CoPP ポリシー制限の変更	716
CoPP に関する追加情報	717

レート制限について	719
レート制限の注意事項と制約事項	720
レート制限のデフォルト設定	721
レート制限の設定	722
レート制限のモニタリング	724
レート制限統計情報のクリア	724
レート制限の設定の確認	725
レート制限の設定例	725
レート制限に関する追加情報	726

第 27 章

MACsec を構成します	727
MACsec について	727
キー ライフタイムおよびヒットレス キー ロールオーバー	728
フォールバック キー	728
MACsec のライセンス要件	729
MACsec の注意事項と制約事項	729
MACsec の有効化	736
MACsec の無効化	737
MACsec キーチェーンとキーの設定	737
MACsec パケット番号の消耗	740
MACsec フォールバック キーの設定	740
MACsec ポリシーの設定	741
MACsec EAP の構成	744
QKD と MACsec での SKIP の統合	745
QKD と Secure Key Integration Protocol の統合について	746
ポスト量子事前共有キー (PPK)	746
注意事項と制約事項	746
SKIP を使用したポイントツーポイント MACsec リンク暗号化の設定	748
ポスト量子暗号化の有効化	748
MACsec および MKA 機能の有効化	749
量子キー配布プロファイルの設定	749

MACsec および MKA 機能の有効化	750
設定例	750
設定可能な EAPOL の宛先とイーサネット タイプについて	754
EAPOL 設定の有効化	754
EAPOL 設定の無効化	755
MACsec 設定の確認	756
MACsec 統計の表示	758
MACsec の設定例	761
XML の例	765
MIB	773
関連資料	773

第 28 章

Cisco Live Protect による NX- OS のセキュア化	775
Cisco Live Protect	775
Cisco Live Protect の注意事項と制約事項	776
Cisco Live Protect の NXSecure 機能の有効化	776
Cisco Live Protect の NXSecure 設定の確認	777
イベント ログ	777

第 29 章

TCP 認証オプションの設定	779
TCP 認証オプションについて	779
TCP-AO キー チェーン	780
TCP-AO キー ロールオーバー	782
注意事項と制約事項	782
TCP キーチェーンおよびキーの設定	783
TCP キーチェーンの確認	786
TCP キーチェーンの構成例	787



はじめに

この前書きは、次の項で構成されています。

- [対象読者](#) (xxxix ページ)
- [表記法](#) (xxxix ページ)
- [Cisco Nexus 9000 シリーズ スイッチの関連資料](#) (xxxix ページ)
- [マニュアルに関するフィードバック](#) (xxxix ページ)
- [通信、サービス、およびその他の情報](#) (xxxix ページ)

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
<i>italic</i>	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、縦棒で区切って示しています。
{x y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。

例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ (<>) で囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアルセットは、次の URL にあります。

https://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services](#) にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet \[英語\]](#) にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

Cisco バグ検索ツール

[シスコバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 1 章

新機能と更新情報

この章では、Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド、リリース 10.6(x) に記載されている新機能および変更機能について説明します。

- [新機能と更新情報 \(1 ページ\)](#)

新機能と更新情報

表 1: 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
Cisco Live Protect による NX-OS のセキュア化	この機能は、Nexus スイッチをモニタリングモードで保護します。NXSecure 構成を使用して実装されています。	10.6(1)F	Cisco Live Protect による NX-OS のセキュア化 (775 ページ)
Cisco Nexus 9336C-SE1 スイッチの MACsec サポート	Cisco Nexus 9336C-SE1 スイッチの MACsec サポートが追加されました。	10.6(1)F	Cisco Nexus 9336C-SE1 スイッチ上の MACsec のガイドラインと制限事項 (735 ページ)
Cisco Nexus 9336C-SE1 スイッチでのカスタム コントロールプレーン ポリッシング (CoPP) サポート	Cisco Nexus 9336C-SE1 スイッチでカスタム コントロールプレーン ポリッシング (CoPP) サポートを追加しました。	10.6(1)F	Cisco Nexus 9336C-SE1 スイッチ上の CoPP のガイドラインと制限事項 (694 ページ)

特長	説明	変更が行われたリリース	参照先
Cisco Nexus 9336C-SE1 スイッチの ACL サポート	Cisco Nexus 9336C-SE1 スイッチは、次の ACL 機能をサポートしています。 • PACL • L3 インターフェイス、L3 ポート チャネルインターフェイス、サブインターフェイス、および SVI インターフェイスの RACL • PBR ACL	10.6(1)F	IP ACL の注意事項と制約事項 (376 ページ)
TACACS+ over TLS	TACACS+ over TLS を設定するためのサポートが追加されました。	10.6(1)F	TACACS+ のガイドラインと制約事項 (106 ページ) TACACS+ Over TLS の構成 (135 ページ) TACACS+ Over TLS の構成の確認 (137 ページ)
ホスト アイデンティティに基づく認証 (HIBA)	ホスト承認情報を証明書に埋め込むことによる、一元化された SSH 承認管理のサポートが追加されました。	10.6(1)F	ホストアイデンティティに基づく認証 (HIBA) を使用した SSH 認証 (165 ページ) SSH 認証の HIBA の構成 (167 ページ)
冗長な SSH 設定と DSA CLI の廃止	冗長な SSH 設定と DSA CLI を廃止するためのサポートが追加されました。	10.6(1)F	SSH と Telnet のガイドラインと制約事項 (172 ページ) SSH サーバ キーの生成 (175 ページ) SSH のパスワードが不要なファイル コピーの設定 (181 ページ)



CHAPTER 2

概要

Cisco NX-OS ソフトウェアがサポートするセキュリティ機能を利用すると、ネットワークをパフォーマンスの劣化や障害から保護するだけでなく、故意に行われる攻撃や、善意のネットワークユーザの意図しない危険な間違いにより生ずるデータの紛失または毀損に対しても保護できます。

この章は、次の項で構成されています。

- [ライセンス要件 \(4 ページ\)](#)
- [サポートされるプラットフォーム \(4 ページ\)](#)
- [Authentication, Authorization, and Accounting \(認証、許可、およびアカウンティング\) , on page 4](#)
- [RADIUS および TACACS+ セキュリティ プロトコル, on page 5](#)
- [LDAP, on page 6](#)
- [SSH および Telnet, on page 6](#)
- [ユーザ アカウントおよびユーザ ロール, on page 6](#)
- [IP ACL, on page 6](#)
- [MAC ACL, on page 7](#)
- [VACL, on page 7](#)
- [DHCP スヌーピング, on page 7](#)
- [ダイナミック ARP インспекション, on page 8](#)
- [IP ソース ガード, on page 8](#)
- [パスワードの暗号化, on page 8](#)
- [キーチェーン管理, on page 9](#)
- [コントロールプレーン ポリシング, on page 9](#)
- [レート制限, on page 9](#)
- [ソフトウェア イメージ \(9 ページ\)](#)
- [仮想デバイス コンテキスト \(10 ページ\)](#)
- [SGT タグ付きパケット \(10 ページ\)](#)
- [TLS プロトコル サポート \(10 ページ\)](#)

ライセンス要件

Cisco NX-OSを動作させるには、機能とプラットフォームの要件に従って適切なライセンスを取得し、インストールする必要があります。

- 基本（Essential）ライセンスとアドオンライセンスが、さまざまな機能セットに使用できます。
- ライセンスは、製品および購入オプションに応じて、永続的、一時的、または評価可能な場合があります。
- 高度な機能を使用するには、基本ライセンス以外の追加の機能ライセンスが必要です。
- 高度な機能を使用するには、基本ライセンス以外の追加ライセンスが必要です。
- ライセンスの適用と管理は、デバイスのコマンドラインインターフェイス（CLI）を介して行われます。

ハードウェアの取り付け手順の詳細については、[Cisco NX-OS ライセンス ガイド](#) および [Cisco NX-OS ライセンシング オプション ガイド](#) を参照してください。

サポートされるプラットフォーム

Nexus スイッチ プラットフォーム サポート マトリックスには、次のものがリストされています。

- サポートされているCisco Nexus 9000 および 3000 スイッチ モデル
- NX-OS ソフトウェア リリース バージョン

プラットフォームと機能の完全なマッピングについては、[Nexus Switch Platform Support Matrix](#) を参照してください。

Authentication, Authorization, and Accounting（認証、許可、およびアカウンティング）

認証、許可、アカウンティング（AAA）は、3つの独立したセキュリティ機能をまとめて一貫性のあるモジュラ形式で設定するためのアーキテクチャ フレームワークです。

認証

ログイン/パスワードダイアログ、チャレンジ/レスポンス、メッセージングサポート、および暗号化（選択したセキュリティプロトコルに基づく）などによるユーザの識別方法を提供します。認証は、ユーザに対してネットワークとネットワーク サービスへのアクセス

を許可する前に、ユーザの識別を行う方法です。AAA 認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種インターフェイスに適用します。

許可

ワントタイム許可またはサービスごとの許可、ユーザ単位のアカунツリストとプロファイル、ユーザグループサポート、および IP、IPX、ARA、Telnet のサポートなど、リモートアクセスの制御方法を提供します。

RADIUS や TACACS+ などのリモートセキュリティ サーバは、適切なユーザで該当する権利を定義した属性値 (AV) のペアをアソシエートすることによって、ユーザに特定の権限を付与します。AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てることで機能します。これらの属性とデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制限事項が決定されます。

アカウントティング

ユーザ ID、開始時刻と終了時刻、実行コマンド (PPP など)、パケット数、バイト数といった、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信を行う手段を提供します。アカウントティングを使用することで、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。



Note

認証は AAA と別個に設定することができます。ただし RADIUS または TACACS+ を使用する場合や、バックアップの認証方式を設定する場合は、AAA を設定する必要があります。

詳細については、[AAA の設定](#), on page 21 の章を参照してください。

RADIUS および TACACS+ セキュリティ プロトコル

AAA は、セキュリティ機能の管理にセキュリティ プロトコルを使用します。ルータまたはアクセス サーバがネットワーク アクセス サーバとして動作している場合は、ネットワーク アクセス サーバと RADIUS または TACACS+ セキュリティ サーバとの間の通信を確立する手段に、AAA が使用されます。

このマニュアルでは、次のセキュリティ サーバ プロトコルを設定する手順を説明します。

RADIUS

不正アクセスからネットワークを保護する分散型クライアント/サーバ システムです。RADIUS は AAA を使用して実装されます。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

TACACS+

ルータまたはネットワーク アクセス サーバ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+ は AAA を使用して実装されます。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デモンのデータベースで管理されます。TACACS+ では、独立したモジュラ型の認証、許可、アカウントティング機能が提供されます。

詳細については、[TACACS+ の設定, on page 101](#)の章および[RADIUS の設定, on page 63](#)の章を参照してください。

LDAP

Lightweight Directory Access Protocol (LDAP) は、Cisco NX-OS デバイスにアクセスしようとするユーザの検証を集中的に行います。LDAP では、1 台のアクセスコントロールサーバ (LDAP デーモン) で認証と認可を個別に提供できます。

詳細については、[LDAP の設定, on page 139](#)の章を参照してください。

SSH および Telnet

セキュア シェル (SSH) サーバを使用すると、SSH クライアントは、Cisco NX-OS デバイスとの間でセキュアな暗号化された接続を確立できます。SSH は強化暗号化を使用して認証を行います。Cisco NX-OS ソフトウェアの SSH サーバは、市販の一般的な SSH クライアントと相互運用ができます。

Cisco NX-OS ソフトウェアの SSH クライアントは、無償あるいは商用の SSH サーバと関係して動作します。

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。Telnet を使用すると、あるサイトのユーザが別のサイトのログイン サーバと TCP 接続を確立し、キーストロークをデバイス間でやり取りできます。Telnet は、リモートデバイスアドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

詳細については、[SSH および Telnet の設定, on page 163](#)の章を参照してください。

ユーザ アカウントおよびユーザ ロール

ユーザアカウントを作成して管理し、Cisco NX-OS デバイス上で行える操作を制限するロールを割り当てることができます。ロールベースアクセスコントロール (RBAC) を使用すると、割り当てたロールにルールを定義して、ユーザが行える管理操作の権限を制限できます。

詳細については、[ユーザアカウントおよびRBACの設定, on page 277](#)の章を参照してください。

IP ACL

IP ACL は、トラフィックをパケットのレイヤ 3 ヘッダーの IPv4 情報に基づいてフィルタリングするために使用できるルールの順序セットです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。Cisco NX-OS ソフトウェアは、ある IP ACL がパケットに適用されると判断すると、そのすべてのルールの条件にパケットを照合し、テストします。最初の一致によってパケットを許可するか拒否するか判定します。一致するものがない場合、Cisco NX-OS ソフトウェアは適切なデフォルトルールを適用し

ます。Cisco NX-OS ソフトウェアは、許可されたパケットについては処理を続行し、拒否されたパケットはドロップします。

詳細については、[IP ACL の構成, on page 355](#)の章を参照してください。

MAC ACL

MAC ACL は各パケットのレイヤ 2 ヘッダーの情報をを使用してトラフィックをフィルタリングする ACL です。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。Cisco NX-OS ソフトウェアがパケットに MAC ACL を適用することを判定するときは、すべてのルールの条件に照らしてパケットを調べます。最初的一致によってパケットを許可するか拒否するか判定します。一致するものがない場合、Cisco NX-OS ソフトウェアは適切なデフォルトルールを適用します。Cisco NX-OS ソフトウェアは、許可されたパケットについては処理を続行し、拒否されたパケットはドロップします。

VACL

VLAN ACL (VACL) は、IP ACL または MAC ACL の適用例の 1 つです。VACL を設定し、VLAN との間でルーティングされるかまたは VLAN 内でブリッジングされるすべてのパケットに適用できます。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。

詳細については、[VLAN ACL の設定, on page 465](#)の章を参照してください。

DHCP スヌーピング

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバとの間でファイアウォールのような機能を果たします。DHCP スヌーピングでは次のアクティビティを実行します。

- 信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外します。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

ダイナミック ARP インспекション (DAI) および IP ソース ガード (IPSG) も、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た情報を使用します。

ダイナミック ARP インспекション

ダイナミック ARP インспекション (DAI) を使用することで、有効な ARP 要求と応答だけが中継されることを保証できます。DAIが有効になり適切に設定されている場合、Cisco NX-OS デバイスは次のアクティビティを実行します。

- 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。

DAI は DHCP スヌーピング バインディング データベースに保存された有効な IP アドレスと MAC アドレスのバインディングに基づき、ARP パケットの有効性を判断できます。また、このデータベースにはユーザが作成するスタティック エントリも保存できます。ARP パケットを信頼できるインターフェイス上で受信した場合は、デバイスはこのパケットを検査せずに転送します。信頼できないインターフェイス上では、デバイスは有効性を確認できたパケットだけを転送します。

IP ソース ガード

IP ソース ガードは、インターフェイス単位のトラフィック フィルタです。各パケットの IP アドレスと MAC アドレスが、IP と MAC のアドレス バインディングのうち、次に示す 2 つの送信元のどちらかと一致する場合だけ、IP トラフィックを許可します。

- DHCP スヌーピング バインディング テーブル内のエントリ
- 設定したスタティック IP ソース エントリ

信頼できる IP と MAC アドレス バインディングに基づいてフィルタリングするので、有効なホストの IP アドレスのスプーフィングを使用した攻撃の防止に役立ちます。IP ソース ガードを妨ぐためには、攻撃者は有効なホストの IP アドレスと MAC アドレスを両方スプーフィングする必要があります。

パスワードの暗号化

高度暗号化規格 (AES) パスワード暗号化機能では、サポートするアプリケーション (現在は RADIUS および TACACS+) のすべての既存および新規に作成されたクリアテキストパスワードを、堅牢でリバーシブルのタイプ 6 暗号化形式で保存します。プライマリ暗号キーは、パスワードを暗号化および復号化するために使用されます。また、この機能を使用して、暗号化が脆弱な既存のすべてのパスワードをタイプ 6 暗号化パスワードに変換することもできます。

詳細については、[パスワード暗号化の設定, on page 617](#)の章を参照してください。

キーチェーン管理

キーチェーン管理を使用すると、キーチェーンの作成と管理を行えます。キーチェーンはキーのシーケンスを意味します（共有秘密ともいいます）。キーチェーンは、他のデバイスとの通信をキーベース認証を使用して保護する機能と合わせて使用できます。デバイスでは複数のキーチェーンを設定できます。

キーベース認証をサポートするルーティング プロトコルの中には、キーチェーンを使用してヒットレス キー ロールオーバーによる認証を実装できるものがあります。

詳細については、[キーチェーン管理の設定, on page 631](#)の章を参照してください。

コントロール プレーン ポリシング

Cisco NX-OS デバイスは、DoS 攻撃によるパフォーマンスへの影響を防ぐために CoPP を備えています。Cisco NX-OS デバイスのスーパーバイザ モジュールには、マネージメント プレーンとコントロールプレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。スーパーバイザモジュールの動作が途絶するような場合には、重大なネットワークの停止につながります。スーパーバイザに過剰なトラフィックが加わると、スーパーバイザ モジュールが過負荷になり、Cisco NX-OS デバイス全体のパフォーマンスが低下する可能性があります。スーパーバイザ モジュールへの攻撃には、DoS 攻撃のようにコントロール プレーンを流れる IP トラフィック ストリームが非常に高いレートで発生するものなど、さまざまな種類があります。攻撃によってコントロールプレーンはこれらのパケットの処理に大量の時間を費やしてしまい、本来のトラフィック処理が不可能になります。

詳細については、[コントロールプレーン ポリシングの設定, on page 675](#)の章を参照してください。

レート制限

レート制限を行うことで、出力例外のリダイレクトパケットにより、Cisco NX-OS デバイス上のスーパーバイザ モジュールに過剰な負荷がかかるのを回避できます。

詳細については、[レート制限の設定, on page 719](#)の章を参照してください。

ソフトウェア イメージ

Cisco NX-OS ソフトウェアは、1 つの NXOS ソフトウェア イメージで構成されています。

仮想デバイス コンテキスト

Cisco NX-OS では、仮想デバイスをエミュレートする Virtual Device Context (VDCs) に、OS およびハードウェア リソースを分割できます。Cisco Nexus 9000 シリーズ スイッチは、現在のところ、複数の VDC をサポートしていません。すべてのスイッチ リソースはデフォルト VDC で管理されます。

SGT タグ付きパケット

Cisco NX-OS リリース 10.2(2)F 以降、Cisco Nexus 9300-FX/FX2/FX3/GX プラットフォーム スイッチは、SGT タグ付きパケットを転送するための L2 または L3 移行デバイスとして使用できます。Cisco NX-OS N9K は、SGT を削除または変更せずにパケットを渡すことができます。

Cisco NX-OS リリース 10.3(3)F 以降、SGT 転送は N9K-X97160YC-EX ライン カードを搭載した Cisco Nexus 9500 スイッチでサポートされます。



(注) NX-OS N9K は、SGT の適用を行いません。また、パケット内の SGT/DGT 情報を生成または書き換えません。パケットは同じタグで送受信されます。

TLS プロトコル サポート

Transport Layer Security (TLS) プロトコルは、コンピュータ ネットワーク 経由での通信のセキュリティを提供するために設計された、暗号化プロトコルです。

Cisco NX-OS リリース 10.4(3)F 以降、Cisco Nexus アプリケーションは、デフォルトで Transport Layer Security (TLS) バージョン 1.3 をサポートします。

次のアプリケーションは、より高速でセキュアな通信のために TLSv1.3 をサポートしています。

- NX-API : 詳細については、[NX-API 管理コマンド](#)を参照してください。
- gNMI : 詳細については、[gNMI : 管理インターフェイス](#)を参照してください。
- セキュア syslog : 詳細については、[Configuring System Message Logging](#)を参照してください。
- RadSec : 詳細については、[RadSec の注意事項と制約事項 \(69 ページ\)](#)を参照してください。
- コピー ユーティリティ (HTTPS オプション) : 詳細については、[Using the Device File Systems, Directories, and Files](#)を参照してください。
- Callhome : 詳細については、[Configuring Smart Call Home](#)を参照してください。

- スマートライセンシング：詳細については、[Smart Licensing Using Policy](#)を参照してください。
- 802.1x：詳細については、[802.1X のガイドラインと制約事項（311 ページ）](#)を参照してください。
- gRPC エージェント：詳細については、[gRPC エージェント](#)を参照してください。
- LDAP：詳細については、[LDAP の注意事項と制約事項（143 ページ）](#)を参照してください。



第 3 章

FIPS の設定

この章では、Cisco NX-OS デバイスで連邦情報処理標準（FIPS）モードを設定する方法について説明します。

この章は、次の項で構成されています。

- [FIPS について（13 ページ）](#)
- [FIPS の前提条件（15 ページ）](#)
- [FIPS の注意事項と制約事項（15 ページ）](#)
- [FIPS のデフォルト設定（15 ページ）](#)
- [FIPS の設定（16 ページ）](#)
- [FIPS 設定の確認（18 ページ）](#)
- [2048ビットRSAキーの作成（18 ページ）](#)
- [FIPS の設定例（19 ページ）](#)
- [FIPS に関する追加情報（19 ページ）](#)

FIPS について

FIPS 140-2 の刊行物『*Security Requirements for Cryptographic Modules*』には、暗号モジュールに対する米国政府の要件が詳細に記載されています。FIPS 140-2 では、暗号モジュールがハードウェア、ソフトウェア、ファームウェア、または何らかの組み合わせのセットで、暗号機能またはプロセスを実装し、暗号化アルゴリズムおよび任意のキー生成機能を含み、明確に定義された暗号境界の内部に位置しなければならないと定義しています。

FIPS は特定の暗号化アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかを指定しています。

FIPS のセルフテスト

暗号モジュールは、自身の正常な動作を保証するために、電源投入時セルフテストと条件付きセルフテストを実行する必要があります。

電源投入時セルフテストは、デバイスの電源が投入された後に自動的に実行されます。デバイスが FIPS モードになるのは、すべてのセルフテストが正常に完了した後だけです。いずれか

のセルフテストが失敗すると、デバイスはシステムメッセージをログに記録し、エラー状態に移行します。

最小モジュラス サイズが 2048 の「crypto key generate rsa label test exportable modulus」を生成します。キーサイズが 2048 未満の場合は、「FIPS セルフテストまたは FIPS エラー状態」に分類されます。

デバイスは、既知解テスト (KAT) という暗号化アルゴリズムを使用して、デバイス上に実装されている FIPS 140-3 で承認された暗号機能 (暗号化、復号化、認証、および乱数生成) ごとに FIPS モードをテストします。デバイスは、このアルゴリズムを、すでに正しい出力がわかっているデータに対して適用します。次に、計算された出力を、以前に生成された出力と比較します。計算された出力が既知解に等しくない場合は、KAT が失敗します。

適用可能なセキュリティ機能または操作が呼び出された場合は、条件付きセルフテストが自動的に実行されます。電源投入時セルフテストとは異なって、条件付きセルフテストはそれぞれに関連する機能がアクセスされるたびに実行されます。

条件付きセルフテストでは次を含むテストが行われます。

ペアワイズ一貫性テスト

このテストは、公開キーまたは秘密キーのペアが生成されたときに実行されます。

連続乱数ジェネレータ テスト

このテストは、乱数が生成されたときに実行されます。

また、Cisco TrustSec マネージャは、暗号化されたテキストが決してプレーン テキストとして送信されないようにするためにバイパス テストを実行します。



(注) CTS に対応したポート上でバイパス テストが失敗すると、それらの対応するポートのみがシャットダウンされます。バイパス テストは、データ パスの輻輳によって発生したパケットドロップのために失敗することがあります。このような場合は、そのポートを再び立ち上げてみることを推奨します。

FIPS エラー状態

システムが FIPS モードで起動されると、スーパーバイザおよびラインカード モジュール上で FIPS 電源投入時セルフテストが実行されます。これらの起動テストのいずれかが失敗すると、システム全体が FIPS エラー状態に移行されます。この状態では、FIPS の要件に従って、すべての暗号キーが削除され、すべてのラインカードがシャットダウンされます。このモードは、デバッグのみを目的にしています。

スイッチが FIPS エラー状態になった後、ラインカードをリロードすると常に、そのラインカードが障害状態に移行されます。スイッチを FIPS モードに戻すには、再起動する必要があります。ただし、スイッチが FIPS モードになった後、ラインカードのそれ以降のリロードまたは挿入で電源投入時セルフテストが失敗すると常に、そのラインカードにのみ影響を与え、対応するラインカードのみが障害状態に移行されます。

FIPS の前提条件

FIPS には、次の前提条件があります。

- Telnet をディセーブルにする。ユーザのログインはセキュア シェル (SSH) だけで行ってください。
- SNMPv3 に対して設定された、デバイス上の既存ユーザアカウントのいずれについても、認証およびプライバシー用 AES/3DES は SHA で設定されていなければなりません。
- SSH サーバの RSA1 キー ペアすべてを削除してください。
- Cisco TrustSec セキュリティ アソシエーション プロトコル (SAP) ネゴシエーション中に使用する HMAC-SHA1 メッセージ整合性チェック (MIC) をイネーブルにします。そのためには、cts-manual または cts-dot1x モードで **sap hash-algorithm HMAC-SHA-1** コマンドを入力します。

FIPS の注意事項と制約事項

FIPS 設定時の注意事項と制約事項は次のとおりです。

- SSH でサポートされているユーザ認証メカニズムは、ユーザ名とパスワード、公開キー、および X.509 証明書です。
- パスワードは、最小 8 文字の英数字である必要があります。
- FIPS モードがオンの場合は、Radius と TACACS を無効にします。これは、FIPS モードの OpenSSL により適用されます。
- RadSec が有効になっている場合、FIPS が有効になっていても Radius を無効にする必要はありません。
- ASCII リロード後に **fips mode enable** コマンドを実行する場合は、**copy running-config startup-config** コマンドの実行後に Cisco NX-OS スイッチをリロードする必要があります。

FIPS のデフォルト設定

次の表に、FIPS パラメータのデフォルト設定を示します。

表 2: デフォルトの FIPS パラメータ

パラメータ	デフォルト
FIPS モード	無効化

FIPS の設定

ここでは、Cisco NX-OS デバイスで FIPS モードを設定する方法について説明します。

FIPS モードの有効化

Cisco NX-OS リリース 7.0(3)I5(1) 以降では、デバイスの FIPS モードを有効にできます。

始める前に

デフォルト VDC に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 例 : switch# configure terminal switch(config)#	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	fips mode enable 例 : switch(config)# fips mode enable	FIPS モードを有効にします。 (注) fips mode enable はすべての LC がオンラインのときにのみ入力できます。LC がオンラインでないときに入力すると、LC で障害が発生します。
ステップ 3	exit 例 : switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	(任意) show fips status 例 : switch# show fips status FIPS mode is enabled	FIPS モードのステータスを表示します。
ステップ 5	必須: copy running-config startup-config 例 : switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
ステップ 6	必須: reload 例 : <pre>switch# reload</pre>	Cisco NX-OS デバイスをリロードします。 (注) FIPS をイネーブルにすると、システムが FIPS モードで動作するためにリブートが必要です。

FIPS の無効化

デバイスの FIPS モードを無効にできます。

始める前に

デフォルト VDC に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 例 : <pre>switch# configure terminal switch(config)#</pre>	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 fips mode enable 例 : <pre>switch(config)# no fips mode enable</pre>	FIPS モードを無効にします。
ステップ 3	exit 例 : <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	(任意) show fips status 例 : <pre>switch# show fips status FIPS mode is disabled</pre>	FIPS モードのステータスを表示します。
ステップ 5	copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
ステップ 6	reload 例 : switch# reload	Cisco NX-OS デバイスをリロードします。

FIPS 設定の確認

FIPS 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show fips status	FIPS機能のステータスを表示します。

このコマンドの出力フィールドの詳細については、『Cisco Nexus 9000 シリーズ NX-OS セキュリティ コマンドリファレンス』を参照してください。

2048ビットRSAキーの作成

2048ビットRSAキーを作成する手順：

```

• N9k-Switch# conf t
  Enter configuration commands, one per line. End with CNTL/Z.

• N9k-Switch(config)# no feature ssh
  XML interface to system may become unavailable since ssh is disabled

• N9k-Switch(config)# no ssh key rsa

• N9k-Switch(config)# ssh key rsa 2048

• New SSH Key has a bitcount of 2048:
  N9k-Switch(config)# show ssh key

  *****

  rsa Keys generated:Wed Apr 28 13:05:18 2021
  ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDHpxEgZ9LwmbOEjJeJtLwqedmTLkZV7Setxb9D4xgO
  p2o2f6wt/48bPp/vLDGsxTF2PtLRtRSSDFNSQmkw9bg+MXvTpgNivdxWLjxtwo3YpYwPkBiReVmyrFgE
  UuBmV/sDfhJpHXLoH9lR2+y0L5w1OG3cJxMe30TI37O3M8fZPjrAtHgkUubfEpiTbcyEw+aIHf+chyoR
  eDJxcEdnlboiTDFR0/+jMUUM/vMtxd5x5DH3AO7htA/i8lvskrReRlCpXlsOdcshms57EEuEzR9cs+w
  KSftQh6vLD802207T6+J7/+cXMVNQEbq0mCSzeTmOsuIQe8u9ZC24pgYzZ19

  bitcount : 2048

  fingerprint:

```



```

SHA256:Am9861AIq5MzfSPQr4ZXGe0f5M9crnhk7HVZBXhMVBo
*****
could not retrieve dsa key information
*****
could not retrieve ecdsa key information
*****

```

FIPS の設定例

FIPS モードをイネーブルにする例を示します。

```

config terminal
fips mode enable
show fips status
exit
copy running-config startup-config
reload

```

FIPS に関する追加情報

ここでは、FIPS の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『Cisco NX-OS ライセンス ガイド』
コマンド リファレンス	『Cisco Nexus 9000 シリーズ NX-OS セキュリティ コマンド リファレンス』

標準

標準	タイトル
FIPS 140-2	暗号モジュールのセキュリティ要件



第 4 章

AAA の設定

この章では、Cisco NX-OS デバイスで認証、許可、アカウントिंग（AAA）を設定する手順について説明します。

この章は、次の項で構成されています。

- [AAA について, on page 21](#)
- [AAA の前提条件, on page 27](#)
- [AAA の注意事項と制約事項, on page 27](#)
- [AAA のデフォルト設定, on page 29](#)
- [AAA の設定, on page 29](#)
- [ローカル AAA アカウンティング ログのモニタリングとクリア , on page 58](#)
- [AAA 設定の確認, on page 58](#)
- [AAA の設定例, on page 60](#)
- [ログインパラメータの設定例（60 ページ）](#)
- [パスワードプロンプト機能の設定例（61 ページ）](#)
- [AAA に関する追加情報, on page 61](#)

AAA について

ここでは、Cisco NX-OS デバイスの AAA について説明します。

AAA セキュリティ サービス

AAA 機能を使用すると、Cisco NX-OS デバイスを管理するユーザの ID を確認し、ユーザにアクセスを許可し、ユーザの実行するアクションを追跡できます。Cisco NX-OS デバイスは、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control System Plus（TACACS+）プロトコルをサポートします。

Cisco NX-OS は入力されたユーザ ID およびパスワードの組み合わせに基づいて、ローカルデータベースによるローカル認証または許可、あるいは1つまたは複数の AAA サーバによるリモート認証または許可を実行します。Cisco NX-OS デバイスと AAA サーバの間の通信は、事前共

有秘密キーによって保護されます。すべての AAA サーバ用または特定の AAA サーバ専用に通秘密キーを設定できます。

AAA セキュリティは、次のサービスを実行します。

認証

ログインとパスワードのダイアログ、チャレンジとレスポンス、メッセージング サポート、および選択したセキュリティプロトコルに応じた暗号化などを使用してユーザを識別します。

認証は、デバイスにアクセスする人物またはデバイスの ID を確認するプロセスです。この ID の確認は、Cisco NX-OS デバイスにアクセスするエンティティから提供されるユーザ ID とパスワードの組み合わせに基づいて行われます。Cisco NX-OS デバイスでは、ローカル認証（ローカルルックアップデータベースを使用）またはリモート認証（1 台または複数の RADIUS サーバまたは TACACS+ サーバを使用）を実行できます。

許可

アクセス コントロールを提供します。AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てるプロセスです。Cisco NX-OS ソフトウェアでは、AAA サーバからダウンロードされる属性を使用して権限付与が行われます。RADIUS や TACACS+ などのリモートセキュリティサーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。

アカウントティング

情報を収集する、情報をローカルのログに記録する、情報を AAA サーバに送信して課金、監査、レポート作成などを行う方法を提供します。

アカウントティング機能では、Cisco NX-OS デバイスへのアクセスに使用されるすべての管理セッションを追跡し、ログに記録して管理します。この情報を使用して、トラブルシューティングや監査のためのレポートを生成できます。アカウントティングログは、ローカルに保存することもできれば、リモート AAA サーバに送信することもできます。



Note

Cisco NX-OS ソフトウェアでは、認証、許可、およびアカウントティングを個別にサポートしています。たとえば、アカウントティングは設定せずに、認証と許可を設定したりできます。

AAA を使用する利点

AAA は、次のような利点を提供します。

- アクセス設定の柔軟性と制御性の向上
- 拡張性
- 標準化された認証方式（RADIUS、TACACS+ など）
- 複数のバックアップ デバイス

リモート AAA サービス

RADIUS プロトコルおよび TACACS+ プロトコルを介して提供されるリモート AAA サービスには、ローカル AAA サービスと比べて次のような利点があります。

- ファブリック内の各 Cisco NX-OS デバイスのユーザ パスワード リストの管理が容易になります。
- AAA サーバはすでに企業内に幅広く導入されており、簡単に AAA サービスに使用できます。
- ファブリック内のすべての Cisco NX-OS デバイスのアカウンティング ログを中央で管理できます。
- ファブリック内の各 Cisco NX-OS デバイスについてユーザ属性を管理する方が、Cisco NX-OS デバイスのローカル データベースを使用するより簡単です。

AAA サーバグループ

認証、許可、アカウンティングのためのリモート AAA サーバは、サーバグループを使用して指定できます。サーバグループとは、同じ AAA プロトコルを実装した一連のリモート AAA サーバです。サーバグループの目的は、リモート AAA サーバが応答できなくなったときにフェールオーバー サーバを提供することです。グループ内の最初のリモート サーバが応答しなかった場合、いずれかのサーバが応答を送信するまで、グループ内の次のリモートサーバで試行が行われます。サーバグループ内のすべての AAA サーバが応答しなかった場合、そのサーバグループ オプションは障害が発生しているものと見なされます。必要に応じて、複数のサーバグループを指定できます。Cisco NX-OS デバイスは、最初のグループ内のサーバからエラーを受け取った場合、次のサーバグループ内のサーバで試行します。

AAA サービス設定オプション

Cisco NX-OS デバイスの AAA 設定は、サービス ベースです。次のサービスごとに異なった AAA 設定を作成できます。

- User Telnet または Secure Shell (SSH) ログイン認証
- コンソール ログイン認証
- ユーザ管理セッション アカウンティング

次の表に、AAA サービス設定オプションごとに CLI (コマンドライン インターフェイス) の関連コマンドを示します。

Table 3: AAA サービス コンフィギュレーション コマンド

AAA サービス コンフィギュレーション オプション	関連コマンド
Telnet または SSH ログイン	<code>aaa authentication login default</code>

AAA サービス コンフィギュレーション オプション	関連コマンド
コンソール ログイン	aaa authentication login console
ユーザ セッション アカウンティング	aaa accounting default

AAA サービスには、次の認証方式を指定できます。

すべての RADIUS サーバ

RADIUS サーバのグローバル プールを使用して認証を行います。

指定サーバ グループ

設定した特定の RADIUS、TACACS+、または LDAP サーバ グループを使用して認証を行います。

ローカル

ローカルのユーザ名またはパスワード データベースを使用して認証を行います。

なし

AAA 認証が使用されないように指定します。



Note 「指定サーバグループ」方式でなく、「すべての RADIUS サーバ」方式を指定した場合、Cisco NX-OS デバイスは、設定された RADIUS サーバのグローバル プールから設定の順に RADIUS サーバを選択します。このグローバル プールからのサーバは、Cisco NX-OS デバイス上の RADIUS サーバ グループ内で選択的に設定できるサーバです。

次の表に、AAA サービスに対応して設定できる AAA 認証方式を示します。

Table 4: AAA サービスの AAA 認証方式

AAA サービス	AAA の方式
コンソール ログイン認証	サーバグループ、ローカル、なし
ユーザ ログイン認証	サーバグループ、ローカル、なし
ユーザ管理セッションアカウンティング	サーバグループ、ローカル

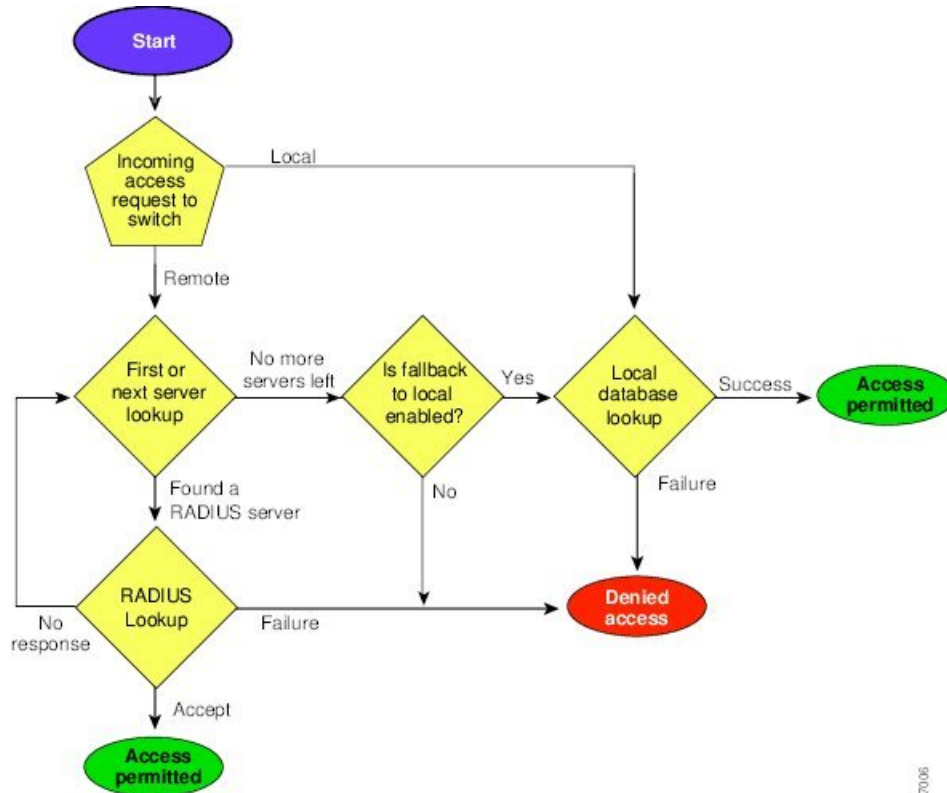


Note コンソール ログイン認証、ユーザ ログイン認証、およびユーザ管理セッションアカウンティングについて、Cisco NX-OS デバイスは各オプションを指定された順序で試行します。その他の設定済みオプションが失敗した場合、ローカルオプションがデフォルト方式です。コンソールまたはデフォルトログインのローカルオプションを無効にするには、**no aaa authentication login {console | default} fallback error local** コマンドを使用します。

ユーザ ログインの認証および許可プロセス

図 1: ユーザ ログインの認証および許可フロー

次の図に、ユーザ ログインの認証および許可プロセスのフローチャートを示します。

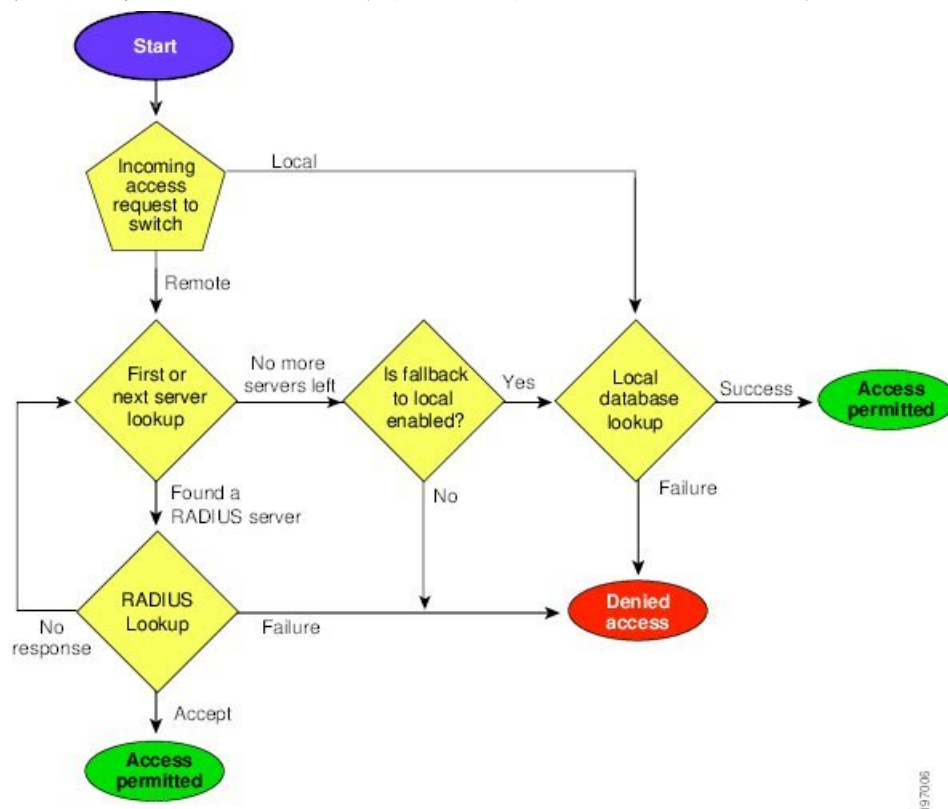


197006

process_workflow

図 2: ユーザ ログインの認証および許可フロー

次の図に、ユーザ ログインの認証および許可プロセスのフローチャートを示します。



次に、このプロセスの動作を示します。

- Telnet、SSH、またはコンソールを使用して Cisco NX-OS デバイスにログインします。
- サーバグループ認証方式を使用して AAA サーバグループを構成します。そして、デバイスは、最初の AAA サーバに要求を送信します。
 - 特定の AAA サーバが応答しなかった場合は、その次の AAA サーバが試行されます。この処理は、リモート サーバが認証要求に応答するまで続けられます。
 - サーバグループのすべての AAA サーバが応答しなかった場合、その次のサーバグループのサーバが試行されます。
 - コンソール ログイン フォールバックが無効で構成されているすべての認証方式が失敗した場合、ローカル データベースを使用して認証が実行されます。
- Cisco NX-OS デバイスがリモート AAA サーバ経由で正常に認証を実行した場合は、これらの可能性が適用する場合があります：
 - AAA サーバ プロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザ ロールがダウンロードされます。

- AAA サーバプロトコルが TACACS+ の場合、シェルのカスタム属性として指定されているユーザ ロールを取得するために、もう 1 つの要求が同じサーバに送信されます。
- ユーザー名とパスワードがローカルで正常に認証された場合は、デバイスにログインでき、ローカル データベース内で構成されているロールが割り当てられます。



(注) 「残りのサーバグループなし」とは、すべてのサーバグループのいずれのサーバからも応答がないということです。「残りのサーバなし」とは、現在のサーバグループ内のいずれのサーバからも応答がないということです。

AES パスワード暗号化およびプライマリ暗号キー

強力で、反転可能な 128 ビットの高度暗号化規格 (AES) パスワード暗号化 (タイプ 6 暗号化ともいう) を有効にすることができます。タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能を有効にし、パスワード暗号化および復号化に使用されるプライマリ暗号キーを設定する必要があります。

AES パスワード暗号化をイネーブルにしてプライマリ キーを設定すると、タイプ 6 パスワード暗号化を無効にしない限り、サポートされているアプリケーション (現在は RADIUS と TACACS+) の既存および新規作成されたクリア テキストパスワードがすべて、タイプ 6 暗号化の形式で保存されます。また、既存の弱いすべての暗号化パスワードをタイプ 6 暗号化パスワードに変換するように Cisco NX-OS を設定することもできます。

AAA の前提条件

リモート AAA サーバには、次の前提条件があります。

- 少なくとも 1 台の RADIUS サーバ、TACACS+ サーバ、または LDAP サーバが IP を使用して到達可能であることを確認します。
- Cisco NX-OS デバイスが、AAA サーバのクライアントとして設定されていること。
- 秘密キーが、Cisco NX-OS デバイスおよびリモート AAA サーバに設定されていることを確認します。
- リモート サーバが Cisco NX-OS デバイスからの AAA 要求に応答することを確認します。

AAA の注意事項と制約事項

AAA に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS リリース 10.2 (1) F 以降では、`cisco-av-pair` の `shell : roles` 属性の前に `SNMPV3` 属性を指定できます。
- LDAP は「`snmpv3`」属性をサポートしていません。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモートユーザアカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザロールではなく、ローカルユーザアカウントのユーザロールをリモートユーザに適用します。
- Cisco Nexus 9000 シリーズスイッチは、TACACS+ でのみ **aaa authentication login ascii-authentication** コマンドをサポートします (RADIUS ではサポートしません)。
- デフォルトのログイン認証方式を (**local** キーワードを使用せずに) 変更すると、コンソールログイン認証方式が設定によって上書きされます。コンソール認証方式を明示的に設定するには、**aaa authentication login console {group group-list [none] | local | none}** コマンドを使用します。
- **login block-for** および **login quiet-mode** コンフィギュレーションモードコマンドは、それぞれ **system login block-for** および **system login quiet-mode** に名前が変更されました。
- **system login quiet-mode access-class QUIET_LIST** コマンドを使用する場合は、指定したトラフィックのみをブロックするようにアクセスリストが正しく定義されていることを確認する必要があります。たとえば、信頼できないホストからのユーザログインのみをブロックする必要がある場合、アクセスリストは、それらのホストからの SSH、Telnet、および HTTP ベースのアクセスに対応するポート 22、23、80、および 443 を指定する必要があります。
- Cisco NX-OS Release 10.2(2)F 以降、新しい非同期化 CLI が導入され、SNMP とセキュリティコンポーネントの間のユーザー同期を無効にするオプションを提供します。詳細については、システム管理構成ガイドの *SNMP の構成* の章を参照してください。

リリース 7.0(3)I7(1) から現在のリリースまでのさまざまな機能をサポートする Cisco Nexus 9000 スイッチの詳細については、[Nexus スイッチプラットフォーム サポート マトリックス](#) を参照してください。
- 非同期 CLI が有効になっている場合、リモートユーザは SNMP データベースに同期されません。
- DCNM (リリース 12.0.1.a 以降 Nexus Dashboard Fabric Controller と呼ばれる) を使用したセキュリティユーザーには、非同期 CLI が有効でないとき、対応する SNMPv3 プロファイルが存在しません。同期が無効になっている場合、セキュリティコンポーネントで作成されたユーザーはスイッチにログインできますが、コントローラはスイッチを検出しません。コントローラは、セキュリティユーザー用に作成された SNMP 構成を使用してスイッチを検出するためです。さらに、SNMP は、userDB の非同期状態のため、作成されたセキュリティユーザーを認識しないので、スイッチを検出できません。したがって、コントローラによってスイッチが検出されるようにするには、SNMP ユーザーを明示的に作成する必要があります。DCNM 機能とともに非同期 CLI を使用することはお勧めしません。詳細については、*Cisco Nexus 9000 NX-OS セキュリティ構成ガイド* を参照してください。

- Cisco NX-OS リリース 10.3(1)F 以降、AAA は Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、AAA は、Cisco Nexus X98900CD-A および X9836DM-A ラインカードを搭載した 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、AAA は、X98900CD-A および X9836DM-A ラインカードを搭載した Cisco Nexus 9804 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(3)F 以降、TACACS+ サーバーを使用した X.509 証明書の SSH ベースの認証が、Cisco Nexus 9000 シリーズプラットフォーム スイッチでサポートされます。この機能は、**aaa authorization ssh-certificate default group tac-group-name** コマンドを使用して有効にできます。詳細については、「[TACACS サーバでの AAA SSH 証明書認証の構成, on page 45](#)」を参照してください。

AAA のデフォルト設定

次の表に、AAA パラメータのデフォルト設定を示します。

Table 5: AAA パラメータのデフォルト設定

パラメータ	デフォルト
コンソール認証方式	ローカル
デフォルト認証方式	ローカル
ログイン認証失敗メッセージ	ディセーブル
CHAP 認証	ディセーブル
MSCHAP 認証	ディセーブル
デフォルト アカウンティング方式	ローカル
アカウンティング ログの表示サイズ	250 KB

AAA の設定

ここでは、Cisco NX-OS デバイスで AAA 機能を設定する手順について説明します。



Note

Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

**Note**

Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、`syslog` エラーが表示されます。

AAA の設定プロセス

AAA 認証およびアカウンティングを設定するには、次の作業を行います。

1. 認証にリモート RADIUS、TACACS+、または LDAP サーバを使用する場合は、Cisco NX-OS デバイス上でホストを設定します。
2. コンソール ログイン認証方式を設定します。
3. ユーザ ログインのためのデフォルトのログイン認証方式を設定します。
4. デフォルト AAA アカウンティングのデフォルト方式を設定します。

コンソール ログイン認証方式の設定

ここでは、コンソール ログインの認証方式を設定する方法を説明します。

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS、TACACS+、または LDAP サーバの指定サブセット
- Cisco NX-OS デバイスのローカル データベース
- ユーザ名のみ (none)

デフォルトの方式はローカルですが、無効にするオプションがあります。

**Note**

`aaa authentication` コマンドの `group radius` および `groupserver-name` 形式は、以前に定義された RADIUS サーバのセットを参照します。ホスト サーバを設定するには、`radius-server host` コマンドを使用します。サーバの名前付きグループを作成するには、`aaa group server radius` コマンドを使用します。

**Note**

リモート認証がイネーブルになっているときにパスワード回復を実行すると、パスワード回復の実行後すぐにコンソールログインのローカル認証がイネーブルになります。そのため、新しいパスワードを使用して、コンソール ポート経由で Cisco NX-OS デバイスにログインできます。ログイン後は、引き続きローカル認証を使用するか、または AAA サーバで設定された管理者パスワードのリセット後にリモート認証をイネーブルにすることができます。パスワード回復プロセスに関する詳細情報については、『Cisco Nexus 9000 シリーズ NX-OS トラブルシューティング ガイド』を参照してください。

Before you begin

必要に応じて RADIUS、TACACS+、または LDAP サーバ グループを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	aaa authentication login console {group group-list [none] local none} Example: <pre>switch(config)# aaa authentication login console group radius</pre>	コンソールのログイン認証方式を設定します。 <i>group-list</i> 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 radius RADIUS サーバのグローバルプールを使用して認証を行います。 named-group RADIUS、TACACS+、または LDAP サーバの指定サブセットを使用して認証を行います。 local 方式は、ローカル データベースを認証に使用します。 none 方式では、AAA 認証が使用されないように指定します。 デフォルトのコンソール ログイン方式は local です。これは、方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られない場合に、コンソール ログインに対して

	Command or Action	Purpose
		ローカルへのフォールバックが無効でない限り、使用されます。
ステップ 3	exit Example: <code>switch(config)# exit</code> <code>switch#</code>	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show aaa authentication Example: <code>switch# show aaa authentication</code>	コンソール ログイン認証方式の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <code>switch# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトのログイン認証方式の設定

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS、TACACS+、または LDAP サーバの指定サブセット
- Cisco NX-OS デバイスのローカル データベース
- ユーザ名だけ

デフォルトの方式はローカルですが、無効にするオプションがあります。

Before you begin

必要に応じて RADIUS、TACACS+、または LDAP サーバ グループを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	aaa authentication login default {group group-list [none] local none}	デフォルト認証方式を設定します。

Command or Action	Purpose
Example: <pre>switch(config)# aaa authentication login default group radius</pre>	<i>group-list</i> 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • radiusRADIUS サーバのグローバルプールを使用して認証を行います。 • named-group : 認証に RADIUS、TACACS+ または LDAP サーバの名前付きサブセットを使用します。 local 方式は、ローカル データベースを認証に使用します。none 方式では、AAA 認証が使用されないように指定します。デフォルトのログイン方式は local です。これは、方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られない場合に、コンソール ログインに対してローカルへのフォールバックがディセーブルでない限り、使用されます。 次のいずれかを設定できます。 • AAA 認証グループ • 認証なしの AAA 認証グループ • ローカル認証 • 認証なし Note local キーワードは、AAA 認証グループを設定するときはサポートされません（必須ではありません）。これは、ローカル認証は、リモートサーバが到達不能の場合のデフォルトであるためです。たとえば、aaa authentication login default group g1 を設定した場合、AAA グループ g1 を使用して認証を行うことができない場合は、ローカル認証が試行されます。これに対し、aaa authentication login default group g1 none を設定した場合、AAA グループ g1 を使用して認証を行うことができない場合は、認証は実行されません。

	Command or Action	Purpose
		Note Cisco NX-OS AAA 認証はハッシュ キーをサポートせず、タイプ 6/7 キーのみをサポートします。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show aaa authentication Example: <pre>switch# show aaa authentication</pre>	デフォルトのログイン認証方式の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ローカル認証へのフォールバックの無効化

デフォルトでは、コンソール ログインまたはデフォルト ログインのリモート認証が設定されている場合、どの AAA サーバにも到達不能なときに（認証エラーになります）、ユーザが Cisco NX-OS デバイスからロックアウトされないように、ローカル認証にフォールバックされます。ただし、セキュリティを向上させるために、ローカル認証へのフォールバックを無効にできます。



Caution

ローカル認証へのフォールバックを無効にすると、Cisco NX-OS デバイスがロックされ、パスワード回復を実行しないとアクセスできなくなることがあります。デバイスからロックアウトされないようにするために、ローカル認証へのフォールバックを無効にする対象は、デフォルト ログインとコンソール ログインの両方ではなく、いずれかだけにすることを推奨します。

Before you begin

コンソール ログインまたはデフォルト ログインのリモート認証を設定します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example:	コンフィギュレーション モードに入ります。

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	no aaa authentication login {console default} fallback error local Example: switch(config)# no aaa authentication login console fallback error local	コンソール ログインまたはデフォルト ログインについて、リモート認証が設定されている場合にどの AAA サーバにも到達不能なときに実行されるローカル認証へのフォールバックを無効にします。 ローカル認証へのフォールバックを無効にすると、次のメッセージが表示されます。 "WARNING!!! Disabling fallback can lock your switch."
ステップ 3	(Optional) exit Example: switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show aaa authentication Example: switch# show aaa authentication	コンソール ログインおよびデフォルト ログイン認証方式の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

AAA 認証のデフォルト ユーザ ロールのイネーブル化

ユーザロールを持たないリモートユーザに、デフォルトのユーザロールを使用して、RADIUS または TACACS+ リモート認証による Cisco NX-OS デバイスへのログインを許可できます。AAA のデフォルトのユーザロール機能をディセーブルにすると、ユーザロールを持たないリモートユーザはデバイスにログインできなくなります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。

	Command or Action	Purpose
ステップ 2	aaa user default-role Example: <pre>switch(config)# aaa user default-role</pre>	AAA 認証のためのデフォルト ユーザ ロールをイネーブルにします。デフォルトではイネーブルになっています。 デフォルト ユーザ ロールの機能をディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show aaa user default-role Example: <pre>switch# show aaa user default-role</pre>	AAA デフォルトユーザロールの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ログイン認証失敗メッセージの有効化

ログイン時にリモート AAA サーバが応答しない場合、そのログインは、ローカルユーザデータベースにロールオーバーして処理されます。このような場合に、ログイン失敗メッセージが有効になっていると、次のメッセージがユーザの端末に表示されます。

```
Remote AAA servers unreachable; local authentication done.
```

```
Remote AAA servers unreachable; local authentication failed.
```

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	aaa authentication login error-enable Example: <pre>switch(config)# aaa authentication login error-enable</pre>	ログイン認証失敗メッセージを有効にします。デフォルトではディセーブルになっています。

	Command or Action	Purpose
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show aaa authentication Example: <pre>switch# show aaa authentication</pre>	ログイン失敗メッセージの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

成功したログイン試行と失敗したログイン試行

成功したログイン試行と失敗したログイン試行をすべて、設定されたsyslogサーバに記録するようにスイッチを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal</pre>	グローバル設定モードを開始します。
ステップ 2	必須: [no] login on-failure log 例 : <pre>switch(config)# login on-failure log</pre>	ロギング レベルが 6 に設定されている場合のみ、失敗した認証に関するすべてのメッセージを設定済みの syslog サーバに記録します。この設定では、ログイン失敗後に次のsyslogメッセージが表示されます。 <pre>AUTHPRIV-3-SYSTEM_MSG : pam_aaa : Authentication failed for user admin from 172.22.00.00</pre> (注) ロギング レベル authpriv が 6 の場合、追加の Linux カーネル認証メッセージが以前のメッセージとともに表示されます。これらの追加のメッセージを無

	コマンドまたはアクション	目的
		視する必要がある場合、authpriv 値を 3 に設定する必要があります。
ステップ 3	必須: [no] login on-success log 例 : <pre>switch(config)# login on-success log switch(config)# logging level authpriv 6 switch(config)# logging level daemon 6</pre>	ロギング レベルが 6 に設定されている場合のみ、成功した認証に関するすべてのメッセージを設定済みの syslog サーバに記録します。この設定では、ログインに成功すると次の syslog メッセージが表示されます。 AUTHPRIV-6-SYSTEM_MSG : pam_aaa : Authentication success for user admin from 172.22.00.00 (注) ロギング レベル authpriv が 6 の場合、追加の Linux カーネル認証メッセージが以前のメッセージとともに表示されます。これらの追加のメッセージを無視する必要がある場合、authpriv 値を 3 に設定する必要があります。
ステップ 4	(任意) show login on-failure log 例 : <pre>switch(config)# show login on-failure log</pre>	失敗した認証メッセージを syslog サーバに記録するようにスイッチが設定されているかどうかを表示します。
ステップ 5	(任意) show login on-successful log 例 : <pre>switch(config)# show login on-successful log</pre>	成功した認証メッセージを syslog サーバに記録するようにスイッチが設定されているかどうかを表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザごとのログイン ブロックの設定

スイッチがグローバル コンフィギュレーション モードになっていることを確認します。

ユーザごとのログインブロック機能を使用すると、Denial of Service (DoS) 攻撃の疑いを検出して、辞書攻撃の影響を緩和することができます。この機能はローカルおよびリモートユーザ

に適用されます。ログインに失敗したユーザをブロックするようにログインパラメータを設定するには、ここに示す手順を実行します。



(注) リリース 9.3(7) 以降では、リモート ユーザのログイン ブロックを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : 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	aaa authentication rejected attemptsinsecondsbanseconds 例 : switch(config)# aaa authentication rejected 3 in 20 ban 300	ユーザをブロックするようにログイン パラメータを設定します。 (注) デフォルトのログイン パラメータに戻すには no aaa authentication rejected コマンドを使用します。
ステップ 3	exit 例 : switch(config)# exit	特権 EXEC モードに戻ります。
ステップ 4	(任意) show running config 例 : switch# show running config	ログイン パラメータを表示します。
ステップ 5	show aaa local user blocked 例 : switch# show aaa local user blocked	ブロックされたローカル ユーザを表示します。
ステップ 6	clear aaa local user blocked {username user all} 例 : switch(config)# switch# clear aaa local user blocked username testuser	ブロックされたローカル ユーザをクリアします。 all : ブロックされたすべてのローカル ユーザをクリアします。
ステップ 7	show aaa user blocked 例 : switch(config)# show aaa user blocked	ブロックされたすべてのローカル ユーザとリモート ユーザを表示します。

	コマンドまたはアクション	目的
ステップ 8	(任意) clear aaa user blocked{username user all} 例 : <pre>switch# clear aaa user blocked username testuser</pre>	ブロックされたすべてのローカル ユーザとリモート ユーザをクリアします。 all : ブロックされたすべてのローカル ユーザとリモート ユーザをクリアします。

例



(注) network-admin および vdc-admin だけが show および clear コマンドを実行できます。

次に、20 秒の間に 3 回のログイン試行が失敗した場合に、300 秒間ユーザをブロックするログイン パラメータを設定する例を示します。

```
switch(config)# aaa authentication rejected 3 in 20 ban 300
switch# show run | i rejected
aaa authentication rejected 3 in 20 ban 300
switch# show aaa local user blocked
Local-user      State
testuser        Watched (till 11:34:42 IST Nov 12 2020)
switch# clear aaa local user blocked username testuser
switch# show aaa user blocked
Local-user      State
testuser        Watched (till 11:34:42 IST Nov 12 2020)
switch# clear aaa user blocked username testuser
```

CHAP 認証の有効化

Cisco NX-OS ソフトウェアは、チャレンジ ハンドシェーク認証プロトコル (CHAP) をサポートしています。このプロトコルは、業界標準の Message Digest (MD5) ハッシュ方式を使用して応答を暗号化する、チャレンジレスポンス認証方式のプロトコルです。リモート認証サーバ (RADIUS または TACACS+) を通じて、Cisco NX-OS スイッチへのユーザ ログインに CHAP を使用できます。

デフォルトでは、Cisco NX-OS デバイスは、Cisco NX-OS デバイスとリモート サーバの間でパスワード認証プロトコル (PAP) 認証を使用します。CHAP が有効の場合は、CHAP ベンダー固有属性 (VSA) を認識するように RADIUS サーバまたは TACACS+ サーバを設定する必要があります。



Note Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、`syslog` エラーが表示されます。次に例を示します。

```
2017 Jun 14 16:14:15 N9K-1 %RADIUS-2-RADIUS_NO_AUTHEN_INFO: ASCII authentication not supported
2017 Jun 14 16:14:16 N9K-1 %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from 192.168.12.34 - dcos_sshd[16804]
```

次の表に、CHAP に必要な RADIUS および TACACS+ VSA を示します。

Table 6: CHAP RADIUS および TACACS+ VSA

ベンダー ID 番号	ベンダータイプ 番号	VSA	説明
311	11	CHAP-Challenge	AAA サーバから CHAP ユーザに送信されるチャレンジを保持します。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。
211	11	CHAP-Response	チャレンジに対する応答として CHAP ユーザが入力した値を保持します。Access-Request パケットだけで使用します。

Before you begin

ログイン用の AAA ASCII 認証を無効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	コンフィギュレーション モードに入ります。
ステップ 2	no aaa authentication login ascii-authentication Example: <code>switch(config)# no aaa authentication login ascii-authentication</code>	ASCII 認証を無効にします。

	Command or Action	Purpose
ステップ 3	aaa authentication login chap enable Example: <pre>switch(config)# aaa authentication login chap enable</pre>	CHAP 認証を有効にします。デフォルトでは無効になっています。 Note Cisco NX-OS デバイスで、CHAP と MSCHAP（または MSCHAP V2）の両方を有効にすることはできません。
ステップ 4	(Optional) exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show aaa authentication login chap Example: <pre>switch# show aaa authentication login chap</pre>	CHAP の設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MSCHAP または MSCHAP V2 認証の有効化

マイクロソフト チャレンジ ハンドシェーク 認証 プロトコル (MSCHAP) は、マイクロソフト版の CHAP です。Cisco NX-OS ソフトウェアは、MSCHAP Version 2 (MSCHAP V2) にも対応しています。リモート認証サーバ (RADIUS または TACACS+) を通じて、Cisco NX-OS スイッチへのユーザ ログインに MSCHAP を使用できます。MSCHAP V2 では、リモート認証 RADIUS サーバを介した Cisco NX-OS デバイスへのユーザ ログインだけがサポートされます。MSCHAP V2 の場合に TACACS+ グループを設定すると、デフォルトの AAA ログイン認証では、次に設定されている方式が使用されます。他のサーバグループが設定されていない場合は、ローカル方式が使用されます。



Note Cisco NX-OS ソフトウェアは、次のメッセージを表示する場合があります。

「Warning: MSCHAP V2 is supported only with Radius.」

この警告メッセージは単なる情報メッセージであり、RADIUS での MSCHAP V2 の動作には影響しません。

デフォルトでは、Cisco NX-OS デバイスは、Cisco NX-OS デバイスとリモート サーバの間でパスワード認証プロトコル (PAP) 認証を使用します。MSCHAP または MSCHAP V2 を有効にする場合は、MSCHAP および MSCHAP V2 ベンダー固有属性 (VSA) を認識するように RADIUS サーバを設定する必要があります。

次の表に、MSCHAP に必要な RADIUS VSA を示します。

Table 7: MSCHAP および MSCHAP V2 RADIUS VSA

ベンダー ID 番号	ベンダー タ イプ番号	VSA	説明
311	11	MSCHAP-Challenge	AAA サーバから MSCHAP または MSCHAP V2 ユーザに送信されるチャレンジを保持します。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。
211	11	MSCHAP-Response	チャレンジに対する応答として MSCHAP または MSCHAP V2 ユーザが入力した値を保持します。Access-Request パケットでしか使用されません。

Before you begin

ログイン用の AAA ASCII 認証を無効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	no aaa authentication login ascii-authentication Example: switch(config)# no aaa authentication login ascii-authentication	ASCII 認証を無効にします。
ステップ 3	aaa authentication login {mschap mschapv2} enable Example: switch(config)# aaa authentication login mschap enable	MSCHAP または MSCHAP V2 認証を有効にします。デフォルトでは無効になっています。 Note

	Command or Action	Purpose
		Cisco NX-OS デバイスで、MSCHAP と MSCHAP V2 の両方を有効にすることはできません。
ステップ 4	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show aaa authentication login {mschap mschapv2} Example: <pre>switch# show aaa authentication login mschap</pre>	MSCHAP または MSCHAP V2 の設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

LDAP サーバでの AAA 許可の設定

LDAP サーバのデフォルトの AAA 許可方式を設定できます。

Before you begin

LDAP を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 authorization ssh-certificate default {group group-list [none] local none} Example: <pre>switch(config)# aaa authorization ssh-certificate default group ldap1 ldap2</pre>	LDAP サーバのデフォルトの AAA 許可方式を設定します。 ssh-certificate キーワードは、証明書認証を使用した LDAP 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して

	Command or Action	Purpose
		許可されたコマンドのリストであるローカル許可です。 <i>group-list</i> 引数には、LDAP サーバグループ名をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。 local 方式では、ローカルデータベースを認証に使用します。 none 方式では、AAA 認証が使用されないように指定します。
ステップ 3	exit Example: switch(config)# exit switch#	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 4	(Optional) show aaa authorization [all] Example: switch# show aaa authorization	AAA 許可設定を表示します。 all キーワードを指定すると、デフォルト値が表示されます。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[TACACS+ のイネーブル化](#) (108 ページ)

TACACS サーバでの AAA SSH 証明書認証の構成

TACACS サーバーに AAA SSH 証明書認証を設定するには、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	configure terminal 例 : switch# configure terminal switch(config)#	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	aaa authorization ssh-certificate default {group group-list [none] local none} 例 : <pre>switch(config)# aaa authorization ssh-certificate default group tac1</pre>	TACACS サーバー グループとして X509 証明書を持つ SSH 要求のデフォルトの AAA 認証方式を設定します。 ssh-certificate キーワードは、証明書認証を使用した TACACS 許可またはローカル許可を構成します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。 <i>group-list</i> 引数には、TACACS サーバグループの名前をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。local 方式では、ローカル データベースを認証に使用します。none 方式では、AAA 認証が使用されないように指定します。
ステップ 3	exit 例 : <pre>switch(config)# exit switch#</pre>	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 4	(任意) show aaa authorization [all] 例 : <pre>switch# show aaa authorization</pre>	AAA 許可設定を表示します。 all キーワードを指定すると、デフォルト値が表示されます。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの AAA アカウンティング方式の設定

Cisco NX-OS ソフトウェアは、アカウンティングに TACACS+ 方式と RADIUS 方式をサポートします。Cisco NX-OS デバイスは、ユーザーのアクティビティを、アカウンティングレコードの形式で TACACS+ または RADIUS セキュリティ サーバーにレポートします。各アカウンティングレコードに、アカウンティング属性値 (AV) のペアが入っており、それが AAA サーバに格納されます。

AAA アカウンティングをアクティブにすると、Cisco NX-OS デバイスは、これらの属性をアカウンティング レコードとして報告します。そのアカウンティング レコードは、セキュリティ サーバ上のアカウンティング ログに格納されます。

特定のアカウンティング方式を定義するデフォルト方式リストを作成できます。次の方式を含めることができます。

RADIUS サーバ グループ

RADIUS サーバのグローバル プールを使用してアカウンティングを行います。

指定されたサーバ グループ

指定された RADIUS または TACACS+ サーバ グループを使用してアカウンティングを行います。

ローカル

ローカルのユーザ名またはパスワードデータベースを使用してアカウンティングを行います。



Note サーバグループが設定されていて、そのサーバグループが応答しない場合、デフォルトではローカルデータベースが認証に使用されます。

Before you begin

必要に応じて RADIUS または TACACS+ サーバ グループを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	aaa accounting default {group group-list local} Example: <pre>switch(config)# aaa accounting default group radius</pre>	デフォルトのアカウンティング方式を設定します。 <i>group-list</i> 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • radius RADIUS サーバのグローバル プールを使用してアカウンティングを行います。 • named-group : TACACS+ サーバまたは RADIUS サーバの名前付きサブセットがアカウンティングに使用されます。

	Command or Action	Purpose
		local 方式はローカル データベースを使用してアカウントिंगを行います。 デフォルトのアカウントिंग方式は、 local です。これはサーバ グループが何も設定されていない場合、または設定されたすべてのサーバ グループから応答が得られなかった場合に使用されます。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show aaa accounting Example: <pre>switch# show aaa accounting</pre>	デフォルトの AAA アカウントिंग方式の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco NX-OS デバイスによる AAA サーバの VSA の使用

ベンダー固有属性（VSA）を使用して、AAA サーバ上での Cisco NX-OS ユーザ ロールおよび SNMPv3 パラメータを指定できます。

VSA の概要

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間での VSA の通信のための方式を規定する標準を作成しています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、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。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き **cisco-av-pair**）です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。**separator** は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

Cisco NX-OS デバイスでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。この許可情報は、VSA で指定されます。

VSA の形式

次の VSA プロトコル オプションが、Cisco NX-OS ソフトウェアでサポートされています。

Shell

ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。

Accounting

accounting-request パケットで使用されるプロトコル。値にスペースが含まれている場合は、二重引用符で囲んでください。

次の属性が、Cisco NX-OS ソフトウェアでサポートされています。

roles

ユーザに割り当てられたすべてのロールの一覧です。値フィールドは、グループ名を空白で区切ったリストの入ったストリングです。たとえば、ユーザが network-operator および network-admin のロールに属している場合、値フィールドは network-operator network-admin となります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、RADIUS サーバから送信されます。この属性は shell プロトコル値とだけ併用できます。次に、ロール属性を使用する例を示します。

```
shell:roles=network-operator network-admin
shell:roles*network-operator network-admin
```

次に、FreeRADIUS でサポートされるロール属性の例を示します。

```
Cisco-AVPair = shell:roles=\network-operator network-admin\
Cisco-AVPair = shell:roles*\network-operator network-admin\
```



Note

VSA を、shell:roles*"network-operator network-admin" または "shell:roles*\network-operator network-admin\" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

accountinginfo

標準の RADIUS アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。この属性が送信されるのは、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分内だけです。この属性は、アカウンティングプロトコル関連の PDU でしか使用できません。

AAA サーバ上での Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータの指定

AAA サーバで VSA cisco-av-pair を使用して、次の形式で、Cisco NX-OS デバイスのユーザ ロール マッピングを指定できます。

```
shell:roles="roleA roleB ..."
```

cisco-av-pair 属性にロール オプションを指定しなかった場合のデフォルトのユーザ ロールは、network-operator です。

SNMPv3属性は、シェル属性の前または後のいずれかにまとめます。次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
snmpv3:auth="SHA" priv="AES-128" shell:roles="network-admin" shell:priv-lvl=15
```

```
shell:roles="network-admin" shell:priv-lvl=15 snmpv3:auth="SHA" priv="AES-128"
```

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と DES です。cisco-av-pair 属性にこれらのオプションを指定しなかった場合のデフォルトの認証プロトコルは、MD5 と DES です。

セキュア ログイン機能の設定

ログインパラメータの設定

可能性のあるサービス妨害（DoS）攻撃が検出された場合に、それ以降のログイン試行を自動的にブロックし、複数回の接続試行の失敗が検出された場合に待機期間を適用することでディクショナリ攻撃を遅らせるように、ログインパラメータを設定できます。



(注) この機能は、システム スイッチオーバーが発生した場合、または AAA プロセスが再起動した場合に再起動します。



(注) **login block-for** および **login quiet-mode** コンフィギュレーションモードコマンドは、それぞれ **system login block-for** および **system login quiet-mode** に名前が変更されました。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : 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	[no] system login block-for seconds attempts tries within seconds 例 : switch(config)# system login block-for 100 attempts 2 within 60	待機モード期間を設定します。すべての引数の範囲は 1 ～ 65535 です。 60 秒以内に 2 回ログイン要求が失敗した場合に 100 秒の待機モードに入るようにスイッチを設定する例を示します。

	コマンドまたはアクション	目的
		このコマンドを入力すると、TelnetまたはSSHを介したすべてのログイン試行は、待機期間中に拒否されます。アクセス コントロール リスト (ACL) も、 system コマンドが入力されます。 (注) 他のログインコマンドを使用する前に、このコマンドを入力する必要があります。
ステップ 3	(任意) [no] system login quiet-mode access-class acl-name 例 : switch(config)# system login quiet-mode access-class myacl	待機モードに切り替わる時に、スイッチに適用される ACL を指定します。スイッチが待機モードになっている間は、すべてのログイン要求が拒否され、使用できる接続はコンソール経由の接続のみになります。
ステップ 4	(任意) show system login [failures] 例 : switch(config)# show system login	ログイン パラメータを表示します。 failures オプションは、失敗したログイン試行に関連する情報のみを表示します。
ステップ 5	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ ログイン セッションの制限

ユーザ 1 人あたりのあたりの同時ログインセッションの最大数を制限することができます。これにより、ユーザが複数の不要なセッションを持つことを防止し、有効なSSHまたはTelnetセッションにアクセスする不正ユーザの潜在的なセキュリティ問題を解決します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : 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	[no] user max-logins max-logins 例 :	ユーザ 1 人あたりの最大同ログイン 時セッション数を制限します。指定できる

	コマンドまたはアクション	目的
	<code>switch(config)# user max-logins 1</code>	範囲は1～7です。最大ログイン制限を1に設定すると、ユーザ1人あたりのTelnet または SSH セッションが1に制限されます。 (注) 設定されたログイン制限は、すべてのユーザに適用されます。個々のユーザに異なる制限を設定することはできません。
ステップ 3	(任意) show running-config all i max-login 例 : <code>switch(config)# show running-config all i max-login</code>	ユーザ1人あたりの最大同時セッション数を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <code>switch(config)# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

パスワードの長さの制限

ユーザパスワードの最小長と最大長を制限できます。この機能を使用すると、ユーザに強力なパスワードの入力を強制することで、システムのセキュリティを強化できます。

始める前に

パスワードの強度の確認を有効にするには、**password strength-check** コマンドを使用する必要があります。パスワードの長さを制限したが、パスワード強度チェックを有効にせず、ユーザが制限された長さの範囲内でないパスワードを入力すると、エラーが表示されますが、ユーザアカウントが作成されます。パスワードの長さを適用し、ユーザアカウントが作成されないようにするには、パスワード強度チェックを有効にし、パスワードの長さを制限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 例 : <code>switch# configure terminal</code>	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	[no] userpassphrase {min-length min-length max-length max-length} 例 : <pre>switch(config)# userpassphrase min-length 8 max-length 80</pre>	ユーザ パスワードの最小長または最大長を制限します。パスワードの最小長は 4 ～ 127 文字にすることができます。パスワードの最大長は 80 ～ 127 文字です。
ステップ 3	(任意) show userpassphrase {length max-length min-length} 例 : <pre>switch(config)# show userpassphrase length</pre>	ユーザ パスワードの最小長と最大長を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ名のパスワード プロンプトのイネーブル化

ユーザによるユーザ名入力後にパスワード入力を要求するように、スイッチを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal</pre>	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	password prompt username 例 : <pre>switch(config)# password prompt username</pre> Password prompt username is enabled. After providing the required options in the username command, press enter. User will be prompted for the username password and password will be hidden. Note: Choosing password key in the same line while configuring user account, password will not be hidden.	password オプションを付けずに username コマンドまたは snmp-server user コマンドが入力された後に、ユーザに対してパスワード入力要求のプロンプトを表示するようスイッチを設定します。ユーザが入力したパスワードは非表示にされます。この機能をディセーブルにするには、このコマンドの no 形式を使用します。 (注) Cisco NX-OS リリース 10.5(2)F 以降、password プロンプトでの SNMP ユーザー削除の構成では、使いやすいよう

	コマンドまたはアクション	目的
		にパスワード関連のプロンプトがスキップされます。
ステップ 3	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

RADIUS または TACACS+ の共有秘密の設定

スイッチとRADIUSまたはTACACS+サーバ間のリモート認証およびアカウンティング用に設定する共有秘密は、機密情報であるため非表示にする必要があります。これらの暗号化された共有秘密の生成には、**radius-server [host] key** および **tacacs-server [host] key** コマンドをそれぞれ使用します。SHA256ハッシュ方式は、暗号化された共有秘密を保存するために使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal</pre>	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	generate type7_encrypted_secret 例 : <pre>switch(config)# generate type7_encrypted_secret Type-7 (Vigenere) Encryption, Use this encrypted secret to configure radius and tacacs shared secret with key type 7. Copy complete secret with double quotes. Enter plain text secret: Confirm plain text secret: Type 7 Encrypted secret is : "fewhg"</pre>	キー タイプ 7 で RADIUS または TACACS+ の共有秘密を設定します。共有秘密の入力を 2 回平文で求められます。秘密は、入力すると非表示になります。次に、暗号化されたバージョンの秘密が表示されます。 (注) プレーン テキストの秘密情報の暗号化バージョンを別途生成しておき、その後で暗号化された共有秘密を設定することができます。その際には、 radius-server [host] key および tacacs-server [host] key を使用します コマンドを発行します。
ステップ 3	(任意) copy running-config startup-config 例 :	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
	<code>switch(config)# copy running-config startup-config</code>	

RADIUS ログイン情報キャッシュ

Cisco NX-OS ソフトウェアは RADIUS ログイン情報のローカル キャッシングをサポートしているため、認証の効率と信頼性がさらに向上します。

Cisco スイッチの RADIUS ログイン情報キャッシング機能は、認証されたユーザー ログイン情報をローカルに保存します。そのため、同じログイン情報をローカルにキャッシュすることで、RADIUS サーバーに何度も認証要求を行う必要がなくなります。これは、同じログイン情報が短時間で繰り返し利用される自動化された環境で特に有利です。

RADIUS ログイン情報のキャッシングの利点

- **パフォーマンスの向上**：RADIUS サーバに送信される認証要求を減らし、パフォーマンスを向上させ、ネットワークの輻輳を軽減します。
- **柔軟性と管理**：管理者が CLI を介してキャッシュ設定を管理することを許可し、スイッチでのユーザー管理が強化します。

RADIUS クレデンシャルの処理方法

process_workflow

1. ログインした時にスイッチは認証のためにお使いのログイン情報を RADIUS サーバーに転送します。
2. 認証されると、Nexus スイッチはログイン情報をローカルにキャッシュします。



- (注) パスワードのハッシュのみがキャッシュに保存され、この目的で最も強力なハッシュタイプの 1 つが使用されます。これにより、キャッシュにアクセスしても元のパスワードを取得できなくなります。

3. 同じクレデンシャルを使用する将来の認証要求については、スイッチは要求をローカルで処理し、RADIUS サーバに対して要求が繰り返されないように防御します。



(注) キャッシュ エントリは、次の場合に自動的に消去されます：

- 機能が無効な場合。
- `clear` コマンドが実行された場合。
- RADIUS または AAA 認証の構成に変更がある場合

RADIUS クレデンシャルのキャッシングの注意事項と制約事項

- キャッシング機能を有効または無効にして、キャッシュタイムアウト値を構成できます。
- キャッシング機能は、RADIUS プロトコル専用です。TACACS や LDAP などの他のプロトコルは、このキャッシング メカニズムではサポートされていません。
- 各キャッシュ エントリはユーザー定義のタイムアウト期間に従い、タイムアウト期間が経過すると、再認証が要求されます。
- 機能が無効になっている場合、`clear` コマンドを実行した場合、またはスイッチの AAA または RADIUS 構成に変更があった場合、キャッシュはクリアされます。
- キャッシュは、次のシナリオで消去されます：
 - 機能が無効な場合
 - `clear` コマンドが実行された場合
 - スwitchの AAA または RADIUS 構成に変更がある場合
- 「管理者」権限を持つユーザーは、キャッシュされたユーザーデータベースをクリアできます。

RADIUS クレデンシャル キャッシングの構成

RADIUS ログイン情報キャッシングを有効にして、Cisco Nexus スイッチでの認証プロセスの効率を向上させることができます。ネットワークパフォーマンスの最適化と認証を効果的に管理するためにこの機能を構成します。Nexus スイッチでこの機能を構成する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	configure terminal 例 : <pre>switch# configure terminal</pre>	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	aaa authentication cache timeout minutes 例 : <pre>switch(config)# aaa authentication cache timeout 10</pre>	RADIUS ログイン情報キャッシングを有効にします。キャッシュ エントリのタイムアウト期間（分単位）を 1 ～ 1,440 の範囲で指定します。

RADIUS ログイン情報キャッシング構成の検証

手順

	コマンドまたはアクション	目的
ステップ 1	show running-config aaa 例 : <pre>Switch(config)# show running-config aaa !Command: show running-config aaa !Running configuration last done at: Thu Jan 30 08:41:11 2025 !Time: Thu Jan 30 08:41:18 2025 version 10.5(3) Bios:version 05.52</pre>	デバイスの実行コンフィギュレーションの一部として、認証、許可、アカウントの詳細を含む現在の AAA コンフィギュレーションの構成を表示します。
ステップ 2	show aaa authentication cache 例 : <pre>Switch# show aaa authentication cache Remote user cache status: enabled Remote user cache timeout: 10</pre>	AAA 認証キャッシュのステータスと構成を表示します。この情報には、キャッシングが有効であるかどうか、およびキャッシュエントリの現在のタイムアウト期間が含まれています。
ステップ 3	（任意） show aaa authentication cache users 例 : <pre>Switch# show aaa authentication cache users Total Users: 4 Username Expiry time ----- bob: Thu Feb 13 06:46:29 2025 UTC bob1: Thu Feb 13 06:46:42 2025 UTC bob2: Thu Feb 13 06:46:55 2025 UTC bob3: Thu Feb 13 06:47:10 2025 UTC</pre>	AAA 認証システムによって現在キャッシュされているユーザーに関する詳細情報を表示します。この情報には、ユーザー名とそれに対応する有効期限のリストが含まれており、各ユーザーのキャッシュ エントリの期限切れを示します。
ステップ 4	clear aaa authentication cache 例 :	キャッシュ済みユーザー データベースのすべてのエントリをクリアします。

	コマンドまたはアクション	目的
	Switch# clear aaa authentication cache	

ローカル AAA アカウンティング ログのモニタリングとクリア

Cisco NX-OS デバイスは、AAA アカウンティング アクティビティのローカル ログを保持しています。このログはモニタリングしたりクリアしたりできます。

Procedure

	Command or Action	Purpose
ステップ 1	show accounting log [<i>size</i> last-index start-seqnum <i>number</i> start-time <i>year month day hh:mm:ss</i>] Example: switch# show accounting log	アカウンティング ログを表示します。 このコマンド出力には、デフォルトで最大 250,000 バイトのアカウンティング ログが表示されます。コマンドの出力を制限する場合は、 <i>size</i> 引数を使用します。指定できる範囲は 0 ～ 250000 バイトです。また、ログ出力の開始シーケンス番号または開始時間を指定できます。開始インデックスの範囲は、1 ～ 1000000 です。アカウンティング ログ ファイルにある最後のインデックス番号の値を表示するには、 last-index キーワードを使用します。
ステップ 2	(Optional) clear accounting log [logflash] Example: switch# clear aaa accounting log	アカウンティング ログの内容をクリアします。 logflash キーワードはログフラッシュに保存されているアカウンティング ログをクリアします。

AAA 設定の確認

AAA の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show aaa accounting	AAA アカウンティングの設定を表示します。

コマンド	目的
show aaa authentication [login {ascii-authentication chap error-enable mschap mschapv2}]	AAA 認証ログイン設定情報を表示します。
show aaa groups	AAA サーバグループの設定を表示します。
show login [failures]	ログイン パラメータを表示します。 failures オプションは、失敗したログイン試行に関連する情報のみを表示します。 Note clear login failures コマンドは、現在の監視期間内のログイン失敗をクリアします。
show login on-failure log	syslog サーバに対して認証失敗メッセージをログ記録するようにスイッチが設定されているか表示します。
show login on-successful log	syslog サーバに対して認証成功メッセージをログ記録するようにスイッチが設定されているか表示します。
show running-config aaa [all]	実行コンフィギュレーションの AAA 設定を表示します。
show running-config all i max-login	ユーザ 1 人あたりの最大同時セッション数を表示します。
show startup-config aaa	スタートアップ コンフィギュレーションの AAA 設定を表示します。
show userpassphrase {length max-length min-length}	ユーザ パスワードの最小長と最大長を表示します。
show userpassphrase sequence alphabet length	ユーザー パスワードの英字シーケンスの最大長を表示します。
show userpassphrase sequence keyboard length	ユーザー パスワードのキーボードシーケンスの最大長を表示します。

AAA の設定例

次に、AAA を設定する例を示します。

```
aaa authentication login default group radius
aaa authentication login console group radius
aaa accounting default group radius
```

ログインパラメータの設定例

次に、60 秒以内に 3 回ログイン要求が失敗した場合に 100 秒の待機モードに入るようにスイッチを設定する例を示します。この例は、ログインの失敗を示しません。

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within 60
switch(config)# show login
```

No Quiet-Mode access list has been configured, default ACL will be applied.

Switch is enabled to watch for login Attacks.
If more than 3 login failures occur in 60 seconds or less,
logins will be disabled for 100 seconds.

Switch presently in Normal-Mode.
Current Watch Window remaining time 45 seconds.
Present login failure count 0.

```
switch(config)# show login failures
*** No logged failed login attempts with the device.***
```

以下に、待機モード ACL の設定例を示します。待機時間中、myacl の ACL からのホスト以外、すべてのログイン要求が拒否されます。この例は、ログインの失敗も示します。

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within 60
switch(config)# login quiet-mode access-class myacl
```

```
switch(config)# show login
```

Switch is enabled to watch for login Attacks.
If more than 3 login failures occur in 60 seconds or less,
logins will be disabled for 100 seconds.

Switch presently in Quiet-Mode.
Will remain in Quiet-Mode for 98 seconds.
Denying logins from all sources.

```
switch(config)# show login failures
Information about last 20 login failure's with the device.
```

Username	Line	SourceIPAddr	Appname	TimeStamp
asd	/dev/pts/0	171.70.55.158	login	Mon Aug 3 18:18:54 2015
qweq	/dev/pts/0	171.70.55.158	login	Mon Aug 3 18:19:02 2015
qwe	/dev/pts/0	171.70.55.158	login	Mon Aug 3 18:19:08 2015

パスワード プロンプト機能の設定例

次の例では、**username** コマンド入力後にユーザ パスワード入力要求のプロンプトを表示し、パスワードが入力されなかった場合にはエラーメッセージを表示するようスイッチを設定する方法を示します。

```
switch# configure terminal
switch(config)# password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password
will not be hidden.
```

```
switch(config)# username user1
Enter password:
Confirm password:
warning: password for user:user1 not set. S/he may not be able to login
```

次の例では、**snmp-server user** コマンド入力後にユーザ パスワード入力要求のプロンプトを表示し、その後、ユーザに提示するプロンプトを表示するようにスイッチを設定する方法を示します。

```
switch# configure terminal
switch(config)# password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password
will not be hidden.
```

```
N9K-1(config)# snmp-server user user1
Enter auth md5 password (Press Enter to Skip):
Enter auth sha password (Press Enter to Skip):
```

AAA に関する追加情報

ここでは、AAA の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	Cisco NX-OS ライセンス ガイド

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
AAA に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 5 章

RADIUS の設定

この章では、Cisco NX-OS デバイスで Remote Access Dial-In User Service (RADIUS) プロトコルを設定する手順について説明します。

この章は、次の項で構成されています。

- [RADIUS について, on page 63](#)
- [RADIUS 認可変更について \(67 ページ\)](#)
- [RADIUS の前提条件, on page 68](#)
- [RADIUS の注意事項と制約事項 \(68 ページ\)](#)
- [RadSec の注意事項と制約事項 \(69 ページ\)](#)
- [RADIUS の認可変更の注意事項と制約事項 \(70 ページ\)](#)
- [RADIUS のデフォルト設定, on page 70](#)
- [RADIUS サーバの設定, on page 71](#)
- [Dynamic Author Server の有効化または無効化 \(94 ページ\)](#)
- [RADIUS 認可変更の設定 \(94 ページ\)](#)
- [RADIUS 設定の確認, on page 95](#)
- [RADIUS 認可変更の設定の検証 \(96 ページ\)](#)
- [RADIUS サーバのモニタリング, on page 96](#)
- [RADIUS サーバ統計情報のクリア, on page 97](#)
- [RADIUS の設定例, on page 98](#)
- [RADIUS 認可変更の設定例 \(98 ページ\)](#)
- [次の作業, on page 98](#)
- [RADIUS に関する追加情報, on page 98](#)

RADIUS について

RADIUS 分散クライアント/サーバシステムを使用すると、不正アクセスからネットワークを保護できます。シスコの実装では、RADIUS クライアントは Cisco NX-OS デバイスで稼働し、すべてのユーザ認証情報およびネットワーク サービスアクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウントिंग要求を送信します。

RADIUS ネットワーク環境

RADIUS は、高度なセキュリティを必要とし、同時にリモート ユーザのネットワーク アクセスを維持する必要があるさまざまなネットワーク環境に実装できます。

RADIUS は、アクセス セキュリティを必要とする次のネットワーク環境で使用します。

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク。たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバベースのセキュリティ データベースを使用できます。
- すでに RADIUS を使用中のネットワーク。RADIUS を使用した Cisco NX-OS デバイスをネットワークに追加できます。この作業は、AAA サーバに移行するときの最初の手順になります。
- リソース アカウンティングが必要なネットワーク。RADIUS アカウンティングは、RADIUS 認証または RADIUS 認可とは個別に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネット サービス プロバイダー（ISP）は、RADIUS アクセスコントロールおよびアカウンティング用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。
- 認証プロファイルをサポートするネットワーク。ネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルを設定アップできます。ユーザごとのプロファイルにより、Cisco NX-OS デバイスは、既存の RADIUS ソリューションを使用してポートを容易に管理できると同時に、共有リソースを効率的に管理してさまざまなサービス レベル契約（SLA）を提供できます。

RADIUS の動作

ユーザが RADIUS を使用して Cisco NX-OS デバイスへのログインおよび認証を試行すると、次のプロセスが実行されます。

- ユーザが、ユーザ名とパスワードの入力を求められ、入力します。
- 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。
- 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

ユーザが認証されました。

REJECT

ユーザは認証されず、ユーザ名とパスワードの再入力を求められるか、アクセスを拒否されます。

CHALLENGE

RADIUS サーバによってチャレンジが発行されます。チャレンジは、ユーザから追加データを収集します。

CHANGE PASSWORD

RADIUS サーバからユーザに、新しいパスワードを選択するよう要求が発行されます。

ACCEPT 応答または REJECT 応答には、EXEC 許可またはネットワーク許可に使用される追加データが含まれています。RADIUS 認可を使用するには、まず RADIUS 認証を完了する必要があります。ACCEPT または REJECT パケットに含まれる追加データの内容は次のとおりです。

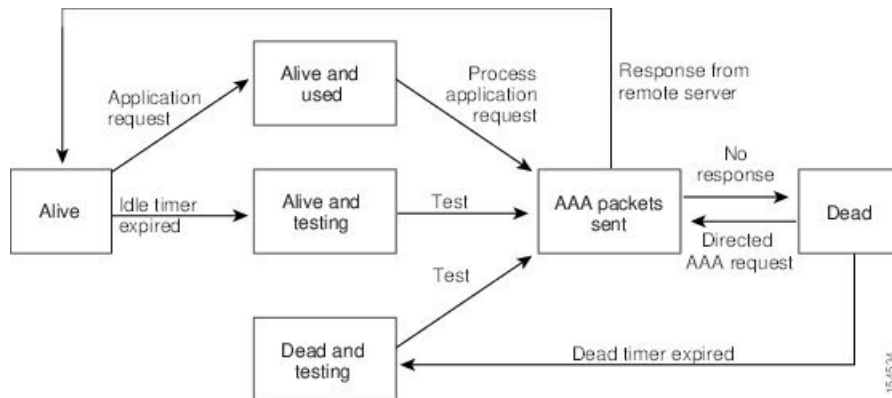
- ユーザがアクセス可能なサービス (Telnet、rlogin、またはローカルエリアトランスポート (LAT) 接続、ポイントツーポイントプロトコル (PPP)、シリアルラインインターネットプロトコル (SLIP)、EXEC サービスなど)
- 接続パラメータ (ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセスリスト、ユーザ タイムアウト)

RADIUS サーバのモニタリング

応答しない RADIUS サーバがあると、AAA 要求の処理が遅れることがあります。AAA 要求の処理時間を節約するために、定期的に RADIUS サーバをモニタリングし、RADIUS サーバが応答を返す (アライブ) かどうかを調べるよう、Cisco NX-OS デバイスを設定できます。Cisco NX-OS デバイスは、応答を返さない RADIUS サーバをデッド (dead) としてマークし、デッド RADIUS サーバには AAA 要求を送信しません。Cisco NX-OS デバイスは定期的にデッド RADIUS サーバをモニタリングし、それらが応答を返したら、アライブ状態に戻します。このモニタリングプロセスでは、実際の AAA 要求が送信される前に、RADIUS サーバが稼働状態であることを確認します。RADIUS サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル (SNMP) トラップが生成され、Cisco NX-OS デバイスによって、障害が発生したことを知らせるエラー メッセージが表示されます。

Figure 3: RADIUS サーバの状態

次の図に、RADIUS サーバ モニタリングの状態を示します。



Note

アライブサーバとデッドサーバのモニタリング間隔は異なります。これらはユーザが設定できます。RADIUS サーバモニタリングを実行するには、テスト認証要求を RADIUS サーバに送信します。

ベンダー固有属性

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間での VSA の通信のための方式を規定する標準を作成しています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、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。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き `cisco-av-pair`）です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

`protocol` は、特定の許可タイプを表すシスコの属性です。`separator` は、必須属性の場合は `=`（等号）、オプションの属性の場合は `*`（アスタリスク）です。

Cisco NX-OS デバイスでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションが、Cisco NX-OS ソフトウェアでサポートされています。

Shell

ユーザ プロファイル情報を提供する `access-accept` パケットで使用されるプロトコル。

Accounting

`accounting-request` パケットで使用されるプロトコル。値にスペースが含まれている場合は、二重引用符で囲む必要があります。

Cisco NX-OS ソフトウェアでは、次の属性がサポートされています。

roles

ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。たとえば、ユーザが `network-operator` および `network-admin` のロールに属している場合、値フィールドは `network-operator network-admin` となります。このサブ属性は `Access-Accept` フレームの VSA 部分に格納され、RADIUS サーバから送信されます。この属性はシェル プロトコル値とだけ併用できます。次に、Cisco Access Control Server（ACS）でサポートされるロール属性の例を示します。

```
shell:roles=network-operator network-admin
```

```
shell:roles*"network-operator network-admin
```

次に、FreeRADIUS でサポートされるロール属性の例を示します。

```
Cisco-AVPair = shell:roles=\network-operator network-admin\
```

```
Cisco-AVPair = shell:roles*\network-operator network-admin\
```




Note VSA を、`shell:roles*"network-operator network-admin"` または `"shell:roles*\network-operator network-admin\""` として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

accountinginfo

標準の RADIUS アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。この属性は、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分だけに送信されます。この属性と共に使用できるのは、アカウンティングのプロトコル データ ユニット (PDU) だけです。

RADIUS 認可変更について

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。Cisco NX-OS ソフトウェアは、プッシュモデルで使用する RFC 5176 で定義された RADIUS Change of Authorization (CoA) 要求をサポートしています。このモデルでは、要求は外部サーバからネットワークに接続されたデバイスへ発信され、外部の認証、認可、およびアカウンティング (AAA) またはポリシー サーバからの動的なセッション再設定が可能になります。

Dot1x が有効の場合、ネットワーク デバイスはオーセンティケータとして機能し、セッションごとのダイナミック COA を処理します。

次の要求がサポートされています。

- セッション再認証
- セッションの終了

セッション再認証

セッションの再認証を開始するには、認証、認可、およびアカウンティング (AAA) サーバは、Cisco VSA および 1 個以上のセッションの ID 属性を含む標準 CoA 要求メッセージを送信します。Cisco VSA は `Cisco:Avpair="subscriber:command=reauthenticate"` の形式です。

次のシナリオでは、現在のセッション状態によって、メッセージに対するデバイスの応答が決まります。

- セッションが現在、IEEE 802.1x によって認証されている場合、デバイスは Extensible Authentication Protocol over LAN (EAPoL) -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、デバイスはサーバにアクセス要求を送信し、初期正常認証で使用するものと同じ ID 属性を渡します。

- デバイスがコマンドを受信する際にセッションの認証が行われている場合、デバイスはプロセスを終了し、認証シーケンスを再起動して、最初に試行されるように設定された方式を開始します。

セッションの終了

CoA 接続解除要求は、ホストポートを無効にせずにセッションを終了します。CoA 接続解除：終了の要求によって、指定し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、ホストのネットワークへのアクセスは制限されません。

セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して Disconnect-NAK メッセージを返します。

セッションが見つかったが、何らかの内部エラーのために NAS がセッションを削除できなかった場合、デバイスは「Session Context Not Removable」エラー コード属性を持つ Disconnect-NAK メッセージを返します。

セッションが見つかった場合、デバイス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ると、デバイスは Disconnect-ACK メッセージを返します。

RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IPv4 または IPv6 アドレスまたはホスト名を取得していること。
- RADIUS サーバからキーを取得すること。
- Cisco NX-OS デバイスが、AAA サーバの RADIUS クライアントとして設定されていること。

RADIUS の注意事項と制約事項

RADIUS には次のガイドラインおよび制限事項があります。

- Cisco NX-OS デバイスに設定できる RADIUS サーバの最大数は 64 です。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- ワンタイム パスワードをサポートするのは RADIUS プロトコルだけです。
- N9K-X9636C-R および N9K-X9636Q-R ラインカードおよび N9K-C9508-FM-R ファブリック モジュールの場合、特殊文字を含むユーザ名の RADIUS 認証は失敗します。

- Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、`syslog` エラーが表示されます。
- Cisco NX-OS リリース 10.3(1)F 以降、RADIUS は Cisco Nexus 9808 プラットフォーム スイッチでサポートされます。
 - Cisco NX-OS リリース 10.4(1)F 以降、RADIUS は、Cisco Nexus X98900CD-A および X9836DM-A ライン カードを搭載した 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、RADIUS は、X98900CD-A および X9836DM-A ライン カードを搭載した Cisco Nexus 9804 スイッチでサポートされます。
- **radius-server key** コマンド および **radius-server hosthostnamekey** コマンドの **key** の値は、引用符の付かないものか（例：secret）、または正しく引用符を付けたもの（例："secret"）である必要があります。以下は許可されません。
 - 先頭または末尾の片方だけに引用符が付いたもの（例：a"、"abc）。
 - 語の途中に引用符が含まれたもの：前後の引用符なし（例：ab"cd）、または前後に引用符あり（例："ab"cd"）。
- Cisco NX-OS リリース 10.4(4) 以降、radius-server CLI では、タイムアウトと再送信のパラメータに値 0 を使用できます。

Cisco NX-OS リリース 10.4(4) 以降では、**show running-config** 出力にもタイムアウトと再送信の値 0 が表示されます。

リリース 10.4(4) と 9.3(11) 以降の間のダウングレード中に、これらの修正を行わないと、タイムアウト値 0 または再送信値 0 を使用する RADIUS サーバー構成が失われるか、機能しない可能性があります。構成の一貫性を確保するために、影響を受けるリリース間での移行時にこれらのパラメータの値として 0 を使用しないでください。または、ソースとターゲットの両方のリリースでこれらの値がサポートされていることを確認してください。

RadSec の注意事項と制約事項

RadSec には、次の注意事項と制約事項があります。

- Cisco NX-OS リリース 10.3(1)F 以降、トランスポート層での RADIUS/TCP ピア間の通信を保護するために、RADIUS Secure（RadSec）サポートが Cisco Nexus スイッチで提供されます。
- RadSec はスイッチ レベルで有効/無効にする必要があります。これは、異なるトランスポート プロトコル（つまり、UDP と TCP-with-TLS）を持つサーバーの組み合わせが不可能であるためです。

- **radius-serverdirected-request** コマンドは、RadSec 機能ではサポートされていません。
- **test aaa server radius** コマンドは RadSec サーバーではサポートされていません。RadSec でサポートされるのは **test aaa group** コマンドだけです。
- Dot1x は RadSec で公式にサポートされていません。
- RADIUS サーバーの監視は、RadSec サーバーではサポートされていません。
- RADIUS サーバーの再送信とタイムアウトは、UDP ベースの RADIUS モードに適用されますが、RadSec サーバーに対してはサポートされません。
- Cisco NX-OS リリース 10.4(3)F 以降、TLS バージョン 1.3 および 1.2 が、Cisco Nexus スイッチでサポートされています。TLS v1.1 は廃止されました。

RADIUS の認可変更の注意事項と制約事項

RADIUS の認可変更に関する注意事項と制約事項は次のとおりです。

- RADIUS の認可変更は FEX によりサポートされています。
- RADIUS の認可変更は VXLAN EVPN によりサポートされています。

RADIUS のデフォルト設定

次の表に、RADIUS パラメータのデフォルト設定を示します。

Table 8: RADIUS パラメータのデフォルト設定

パラメータ	デフォルト
サーバの役割	認証とアカウントティング
デッド タイマー間隔	0 分
再送信回数	1
再送信タイマー間隔	5 秒
認証ポート	1812
アカウントティング ポート	1813
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	テスト

RADIUS サーバの設定

ここでは、Cisco NX-OS デバイスで RADIUS サーバを設定する手順を説明します。

**Note**

Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

**Note**

Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、`syslog` エラーが表示されます。

RADIUS サーバの設定プロセス

1. Cisco NX-OS デバイスと RADIUS サーバとの接続を確立します。
2. RADIUS サーバの RADIUS 秘密キーを設定します。
3. 必要に応じて、AAA 認証方式用に、RADIUS サーバのサブセットを使用して RADIUS サーバグループを設定します。
4. 必要に応じて、次のオプションのパラメータを設定します。
 - デッドタイム間隔
 - ユーザ ログイン時の RADIUS サーバの指定の許可
 - タイムアウト間隔
 - TCP ポート
5. （任意）RADIUS 設定の配布がイネーブルになっている場合は、ファブリックに対して RADIUS 設定をコミットします。

Related Topics

[RADIUS サーバ ホストの設定](#) (71 ページ)

[グローバル RADIUS キーの設定](#) (73 ページ)

RADIUS サーバ ホストの設定

リモートの RADIUS サーバにアクセスするには、RADIUS サーバの IP アドレスまたはホスト名を設定する必要があります。最大 64 の RADIUS サーバを設定できます。



Note RADIUS サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスに設定するとき、デフォルトでは RADIUS サーバはデフォルトの RADIUS サーバ グループに追加されます。RADIUS サーバを別の RADIUS サーバ グループに追加することもできます。

Before you begin

サーバがすでにサーバ グループのメンバーとして設定されていることを確認します。

サーバが RADIUS トラフィックを認証するよう設定されていることを確認します。

Cisco NX-OS デバイスが、AAA サーバの RADIUS クライアントとして設定されていること。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 host {ipv4-address ipv6-address hostname} Example: <pre>switch(config)# radius-server host 10.10.1.1</pre>	認証に使用する RADIUS サーバの IPv4 または IPv6 アドレスまたはホスト名を指定します。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[特定の RADIUS サーバ用のキーの設定](#) (74 ページ)

グローバル RADIUS キーの設定

Cisco NX-OS デバイスで使用するすべてのサーバの RADIUS キーを設定できます。RADIUS キーとは、Cisco NX-OS デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

Before you begin

リモート RADIUS サーバの RADIUS キーの値を取得します。

リモート RADIUS サーバに RADIUS キーを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 [0 6 7] key-value Example: <pre>switch(config)# radius-server key 0 QsEfThUkO</pre> Example: <pre>switch(config)# radius-server key 7 "fewhg"</pre>	すべての RADIUS サーバ用の RADIUS キーを指定します。<i>key-value</i> がクリア テキスト形式 (0) か、タイプ 6 暗号化形式 (6) か、タイプ 7 暗号化形式 (7) かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存する前にクリアテキストのキーを暗号化します。デフォルトの形式はクリア テキストです。最大で 63 文字です。 デフォルトでは、RADIUS キーは設定されません。 Note generate type7_encrypted_secret を使用してすでに共有秘密を設定している場合 コマンドを使用して、二番目の例に示すように引用符に入力します。詳細については、RADIUS または TACACS+ の共有秘密の設定, on page 54を参照してください。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。 Note RADIUS キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された RADIUS キーを表示するには、 show running-config コマンドを使用します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[RADIUS サーバ グループの設定 \(81 ページ\)](#)

[AES パスワード暗号化およびプライマリ暗号キーについて \(617 ページ\)](#)

特定の RADIUS サーバ用のキーの設定

Cisco NX-OS デバイスで、特定の RADIUS サーバ用のキーを設定できます。RADIUS キーは、Cisco NX-OS デバイスと特定の RADIUS サーバとの間で共有する秘密テキスト ストリングです。

Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

リモート RADIUS サーバのキーの値を取得します。

RADIUS サーバにキーを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 host {ipv4-address ipv6-address hostname} key [0 6 7] key-value Example:	特定の RADIUS サーバ用の RADIUS キーを指定します。 <i>key-value</i> がクリア テキスト形式 (0) か、タイプ 6 暗号化形式 (6) か、タイプ 7 暗号化形式 (7)

	Command or Action	Purpose
	<pre>switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg</pre> Example: <pre>switch(config)# radius-server host 10.10.1.1 key 7 "fewhg"</pre>	かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存する前にクリアテキストのキーを暗号化します。デフォルトの形式はクリア テキストです。最大で 63 文字です。 この RADIUS キーが グローバル RADIUS キーの代わりに使用されます。 Note generate type7_encrypted_secret を使用してすでに共有秘密を設定している場合 コマンドを使用して、二番目の例に示すように引用符に入力します。詳細については、RADIUS または TACACS+ の共有秘密の設定, on page 54を参照してください。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。 Note RADIUS キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された RADIUS キーを表示するには、show running-config コマンドを使用します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[RADIUS サーバ ホストの設定 \(71 ページ\)](#)

[AES パスワード暗号化およびプライマリ暗号キーについて \(617 ページ\)](#)

RADIUS 属性メッセージオーセンティケータの構成

Cisco NX-OS スイッチを使用するすべてのサーバに RADIUS 属性メッセージオーセンティケータを構成できます。RADIUS 属性は、Extended Access Protocol (EAP; 拡張アクセス プロトコル) パケットをカプセル化して、スイッチが HMAC-MD5 を使用して EAP 経由でダイヤルイン ユーザを認証できるようにします。



(注) Cisco Fabric Services (CFS) は、RADIUS 属性メッセージオーセンティケータを配信しません。

Cisco NX-OS リリース 10.2(9)M 以降、Cisco Nexus 9000 スイッチでは、**radius-server attribute message-authenticator** コマンドが導入されています。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 attribute message-authenticator 例 : <pre>switch(config)# radius-server attribute message-authenticator</pre>	すべての RADIUS サーバに RADIUS 属性 message-authenticator を指定します。 デフォルトでは、RADIUS 属性の message-authenticator は無効になっています。
ステップ 3	exit 例 : <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(任意) show radius-server 例 : <pre>switch# show radius-server etransmission count:1 timeout value:5 deadtime value:0 message-authenticator attribute:enabled source interface:any available total number of servers:4 following RADIUS servers are configured: 10.10.1.1: available for</pre>	RADIUS サーバの設定を表示します。

	コマンドまたはアクション	目的
	<pre>authentication on port:1812 available for accounting on port:1813 RADIUS shared secret:***** timeout:60</pre>	
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

RadSec の設定

RadSec は、TLS 経由で RADIUS データグラムを転送するためのプロトコルです。

この手順では、スイッチで RadSec を有効または無効にする方法について説明します。

始める前に

- サーバーのクライアント ID 証明書と CA 証明書がスイッチにインストールされていることを確認します。
- サーバー証明書のサブジェクト名が、スイッチで構成されているサーバーのホスト名/IP アドレスと一致していることを確認してください。
- RadSec サーバーを使用するように AAA 認証とアカウンティングを設定する前に、**test aaa group** コマンドを使用して、RadSec 認証が成功することを確認します。
- スイッチからの頻繁な TLS セッションの再試行を避けるために、RadSec サーバーで TLS アイドル タイムアウトを最大値に設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal</pre>	コンフィギュレーション モードに入ります。
ステップ 2	radius-server secure tls 例 : <pre>switch# radius-server secure tls</pre>	グローバル レベルで有効にします。 (注) この CLI は、RadSec に使用されるポート番号を変更または影響しません。

	コマンドまたはアクション	目的
ステップ 3	radius-server host t {ipv4-address ipv6-address hostname} key {key} auth-port 2083 acct-port 2083 authentication accounting 例 : <pre>switch# radius-server host 10.105.222.161 key radsec auth-port 2083 acct-port 2083 authentication accounting</pre>	認証およびアカウントティング ポートとともに共有秘密キーを使用して RadSec サーバーを構成します。 (注) サーバーの場合、認証とアカウントティングのデフォルトの RadSec ポートは「2083」で、キーは「radsec」です。スイッチの場合、RadSec ポートとキーのデフォルト設定はありません。サーバーで定義されているように、この設定を明示的に追加してください。
ステップ 4	radius-server host {ipv4-address ipv6-address hostname} tls client-trustpoint trustpoint 例 : <pre>switch# radius-server host 10.105.222.161 tls client-trustpoint rad1</pre>	クライアント ID 証明書がインストールされている TLS クライアント トラスト ポイントを設定します。
ステップ 5	radius-server host {ipv4-address ipv6-address hostname} tls idle-timeout value 例 : <pre>switch# radius-server host 10.105.222.161 tls idle-timeout 80</pre>	TLS アイドル タイムアウトを設定します。デフォルト値は 600 秒です。 (注) RadSec クライアントからのトランザクションがない場合、サーバーはタイムアウト値に基づいて接続を閉じることができます。クライアントの TLS アイドル タイムアウトは、このリリースではサポートされていません。クライアントは自分自身で接続を閉じません。



- (注) リモートユーザーがログインすると、約 20 秒間のログインの遅延が見られることがあります。つまり、スイッチと RadSec サーバーの間で TLS セッションの確立が初めて行われるときです。TLS セッションが起動すると、連続したリモート ログインで遅延は見られません。



- (注) RadSec クライアントで、証明書が存在しない、または無効な証明書がサーバーと交換されているなどの証明書関連の問題が発生している場合、show run コマンドで遅延が発生する可能性があります。

DTLS を使用した RADIUS について

Cisco NX-OS リリース 10.4(1)F から、DTLS プロトコルを使用した RADIUS が導入されました。このプロトコルは、UDP を使用してセキュア チャネルを介して RADIUS データグラムを転送するためのものです。

RADIUS と DTLS は、トランスポート層での RADIUS ピア間のセキュアな通信を可能にします。このプロトコルは、さまざまな管理ドメインや疑わしい、安全でないネットワークを介してセキュアな RADIUS パケット転送を行いたい場合に役立ちます。

DTLS を使用する RADIUS の構成

始める前に

- スイッチの IP アドレス/DNS ホスト名と同じサブジェクトと代替名を使用してクライアントアイデンティティ証明書を作成してください。トラストポイントを使用して、スイッチにクライアントアイデンティティ証明書をインストールします。
- DTLS/RADIUS に使用される ISE サーバのサーバ証明書がスイッチにインストールされていることを確認します。
- クライアントアイデンティティ証明書の署名に使用される CA 証明書が ISE サーバーの信頼できる証明書ストアにインストールされていることを確認します。
- サーバ証明書のサブジェクト名が、スイッチで構成されているサーバーのホスト名/IP アドレスと同じであることを確認します。
- RADIUS サーバーを使用するように AAA 認証およびアカウントンググループを構成する前に、`test aaa group` コマンドで RADIUS 認証が成功することを確認します。
- スイッチ レベルで RADIUS と DTLS プロトコルを有効にする必要があります。
- DTLS と TLS など、異なるトランスポートプロトコルを使用するように RADIUS サーバーを組み合わせることはサポートされていません。一度に 1 つのプロトコルを構成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	radius-server secure dtls 例 :	スイッチで RADIUS with DTLS プロトコルを有効にします。

	コマンドまたはアクション	目的
	<code>switch(config)# radius-server secure dtls</code>	
ステップ 3	radius-server host {ipv4-address ipv6-address hostname} key {radius/dtls} auth-port 2083 acct-port 2083 authentication accounting 例 : <pre>switch(config)# radius-server host 10.105.222.161 key radius/dtls auth-port 2083 acct-port 2083 authentication accounting</pre>	共有秘密キー、および認証ポートとアカウントティングポートを使用して、RADIUS サーバを構成します。 (注) 認証およびアカウントティングのデフォルトの接続先 DTLS ポートは UDP/2083 です。RFC に従って、DTLS のデフォルトのサーバー キーはありません。サーバーで定義されているように、この構成を明示的に追加してください。ISE サーバーは、その時点で「radius/dtls」キーで事前設定されている必要があります。ISE サーバーで DTLS を構成するときに、Nexus スイッチでキーを確認して追加します。
ステップ 4	radius-server host {ipv4-address ipv6-address hostname} dtls client-trustpoint trustpoint 例 : <pre>switch(config)# radius-server host 10.105.222.161 dtls client-trustpoint rad1</pre>	スイッチ ID 証明書がインストールされているトラストポイントで、DTLS client-trustpoint パラメータを構成します。rad1 は、クライアントアイデンティティ証明書が必要なスイッチ上のトラストポイントです。
ステップ 5	radius-server host {ipv4-address ipv6-address hostname} dtls idle-timeout value 例 : <pre>switch# radius-server host 10.105.222.161 dtls idle-timeout 80</pre>	DTLS アイドルタイムアウトを設定します。デフォルト値は 600 秒です。 (注) RADIUS クライアントからのトランザクションがない場合、サーバは定義されたタイムアウト値に従い接続を閉じます。クライアントの DTLS アイドルタイムアウトは、このリリースではサポートされていません。クライアントは自分自身で接続を閉じません。



- (注)
- リモートユーザーがログインすると、約20秒の遅延が発生することがあります。これは、スイッチとRADIUSサーバの間でTLSセッションが初めて確立されるときに発生します。いったん TLS セッションが確立されれば、後続のリモートログインで遅延は発生しません。
 - RADIUS クライアントで、証明書が存在しない、または無効な証明書がサーバと交換されているなどの証明書関連の問題が発生している場合、`show run` コマンドで遅延が発生する可能性があります。

RADIUS サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによる認証を指定できます。グループのメンバーはすべて、RADIUS プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバ グループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

Before you begin

グループ内のすべてのサーバが RADIUS サーバであることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 group server radius group-name Example: <pre>switch(config)# aaa group server radius RadServer switch(config-radius)#</pre>	RADIUS サーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション サブモードを開始します。<i>group-name</i> 引数は、最大 127 文字の長さの英数字のストリングで、大文字小文字が区別されます。 RADIUS サーバ グループを削除するには、このコマンドの no 形式を使用します。 Note

	Command or Action	Purpose
		デフォルトのシステム生成デフォルトグループ (RADIUS) は削除できません。
ステップ 3	server {ipv4-address ipv6-address hostname} Example: switch(config-radius) # server 10.10.1.1	RADIUS サーバを、RADIUS サーバ グループのメンバーとして設定します。 指定した RADIUS サーバが見つからない場合は、 radius-server host コマンドを実行し、このコマンドを再試行します。
ステップ 4	(Optional) deadtime minutes Example: switch(config-radius) # deadtime 30	モニタリング デッド タイムを設定します。デフォルト値は 0 分です。指定できる範囲は 1 ～ 1440 です。 Note RADIUS サーバグループのデッド タイム間隔が 0 より大きい場合は、この値がグローバルなデッド タイム値より優先されます。
ステップ 5	(Optional) server {ipv4-address ipv6-address hostname} Example: switch(config-radius) # server 10.10.1.1	RADIUS サーバを、RADIUS サーバ グループのメンバーとして設定します。 Tip 指定した RADIUS サーバが見つからない場合は、 radius-server host コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 6	(Optional) use-vrf vrf-name Example: switch(config-radius) # use-vrf vrf1	サーバ グループ内のサーバとの接続に使用する VRF を指定します。
ステップ 7	exit Example: switch(config-radius) # exit switch(config) #	コンフィギュレーション モードを終了します。
ステップ 8	(Optional) show radius-server groups [group-name] Example: switch(config) # show radius-server groups	RADIUS サーバ グループの設定を表示します。

	Command or Action	Purpose
ステップ 9	(Optional) copy running-config startup-config Example: <code>switch(config)# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics[RADIUS デッド タイム間隔の設定](#) (92 ページ)

RADIUS サーバ グループのためのグローバル発信元インターフェイスの設定

RADIUS サーバ グループにアクセスする際に使用する、RADIUS サーバ グループ用のグローバル発信元インターフェイスを設定できます。また、特定の RADIUS サーバ グループ用に異なる発信元インターフェイスを設定することもできます。デフォルトでは、Cisco NX-OS ソフトウェアは、使用可能なあらゆるインターフェイスを使用します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)</code>	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 radius source-interface interface Example: <code>switch(config)# ip radius source-interface mgmt 0</code>	このデバイスで設定されているすべての RADIUS サーバ グループ用のグローバル発信元インターフェイスを設定します。
ステップ 3	exit Example: <code>switch(config)# exit</code> <code>switch#</code>	設定モードを終了します。
ステップ 4	(Optional) show radius-server Example: <code>switch# show radius-server</code>	RADIUS サーバの設定情報を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) copy running-config startup config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[RADIUS サーバ グループの設定](#) (81 ページ)

ログイン時にユーザによる RADIUS サーバの指定を許可

デフォルトでは、Cisco NX-OS デバイスはデフォルトの AAA 認証方式に基づいて認証要求を転送します。VRF と認証要求送信先 RADIUS サーバをユーザが指定できるように Cisco NX-OS デバイスを設定するには、directed-request オプションを有効にします。このオプションを有効にした場合、ユーザは `username@vrfname:hostname` としてログインできます。ここで、`vrfname` は使用する VRF、`hostname` は設定された RADIUS サーバの名前です。



Note directed-request オプションを有効にすると、Cisco NX-OS デバイスでは認証に RADIUS 方式だけを使用し、デフォルトのローカル方式は使用しないようになります。



Note ユーザ指定のログインは Telnet セッションに限りサポートされます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 directed-request Example: <pre>switch(config)# radius-server directed-request</pre>	ログイン時にユーザが認証要求の送信先となる RADIUS サーバを指定できるようにします。デフォルトでは無効になっています。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) show radius-server directed-request Example: switch# show radius-server directed-request	directed request の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定

すべての RADIUS サーバに対するグローバルな再送信リトライ回数とタイムアウト間隔を設定できます。デフォルトでは、Cisco NX-OS デバイスはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。タイムアウト間隔には、Cisco NX-OS デバイスが RADIUS サーバからの応答を待つ時間を指定します。これを過ぎるとタイムアウト エラーになります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 retransmit count Example: switch(config)# radius-server retransmit 3	すべての RADIUS サーバの再送信回数を指定します。デフォルトの再送信回数は 1 で、範囲は 0 ～ 5 です。
ステップ 3	radius-server timeout seconds Example: switch(config)# radius-server timeout 10	RADIUS サーバの送信タイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。
ステップ 4	exit Example: switch(config)# exit switch#	設定モードを終了します。

	Command or Action	Purpose
ステップ 5	(Optional) show radius-server Example: switch# show radius-server	RADIUS サーバの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定

デフォルトでは、Cisco NX-OS デバイスはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。Cisco NX-OS デバイスが、タイムアウトエラーを宣言する前に、RADIUS サーバからの応答を待機するタイムアウト間隔も設定できます。

Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 host {ipv4-address ipv6-address hostname} retransmit count Example: switch(config)# radius-server host server1 retransmit 3	特定のサーバに対する再送信回数を指定します。デフォルトはグローバル値です。 Note 特定の RADIUS サーバに指定した再送信回数は、すべての RADIUS サーバに指定した再送信回数より優先されます。
ステップ 3	radius-server host {ipv4-address ipv6-address hostname} timeout seconds Example: switch(config)# radius-server host server1 timeout 10	特定のサーバの送信タイムアウト間隔を指定します。デフォルトはグローバル値です。 Note 特定の RADIUS サーバに指定したタイムアウト間隔は、すべての RADIUS

	Command or Action	Purpose
		サーバに指定したタイムアウト間隔より優先されます。
ステップ 4	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[RADIUS サーバ ホストの設定](#) (71 ページ)

RADIUS サーバのアカウントिंगおよび認証属性の設定

RADIUS サーバをアカウントング専用、または認証専用に使用するかを指定できます。デフォルトでは、RADIUS サーバはアカウントングと認証の両方に使用されます。また、デフォルトのポートとの競合が発生する場合は、RADIUS アカウントング メッセージと認証 メッセージの送信先である宛先 UDP ポート番号を指定することもできます。

Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	(Optional) radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } acct-port <i>udp-port</i> Example:	RADIUS アカウントングのメッセージに使用する UDP ポートを指定します。デフォルトの UDP ポートは 1813 です。範囲は 0 ～ 65535 です。

	Command or Action	Purpose
	<code>switch(config)# radius-server host 10.10.1.1 acct-port 2004</code>	
ステップ 3	(Optional) radius-server host {ipv4-address ipv6-address hostname} accounting Example: <code>switch(config)# radius-server host 10.10.1.1 accounting</code>	RADIUS サーバをアカウントティングだけに使用することを指定します。デフォルトでは、アカウントティングと認証の両方に使用されます。
ステップ 4	(Optional) radius-server host {ipv4-address ipv6-address hostname} auth-port udp-port Example: <code>switch(config)# radius-server host 10.10.2.2 auth-port 2005</code>	RADIUS 認証メッセージ用の UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。範囲は 0 ～ 65535 です。
ステップ 5	(Optional) radius-server host {ipv4-address ipv6-address hostname} authentication Example: <code>switch(config)# radius-server host 10.10.2.2 authentication</code>	RADIUS サーバを認証だけに使用することを指定します。デフォルトでは、アカウントティングと認証の両方に使用されます。
ステップ 6	exit Example: <code>switch(config)# exit</code> <code>switch#</code>	設定モードを終了します。
ステップ 7	(Optional) show radius-server Example: <code>switch# show radius-server</code>	RADIUS サーバの設定を表示します。
ステップ 8	(Optional) copy running-config startup-config Example: <code>switch# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[RADIUS サーバホストの設定](#) (71 ページ)

RADIUS サーバのグローバルな定期モニタリングの設定

各サーバに個別にテストパラメータを設定しなくても、すべての RADIUS サーバの可用性をモニタリングできます。テストパラメータが設定されていないサーバは、グローバルレベルのパラメータを使用してモニタリングされます。



Note 各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。

グローバル コンフィギュレーション パラメータには、サーバで使用するユーザ名とパスワード、およびアイドル タイマーなどがあります。アイドル タイマーには、RADIUS サーバがどのくらいの期間要求を受信しなかった場合に、Cisco NX-OS デバイスがテスト パケットを送信するかを指定します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。



Note ネットワークのセキュリティを保護するために、RADIUS データベースの既存のユーザ名と同じものを使用しないことを推奨します。



Note デフォルトのアイドル タイマー値は 0 分です。アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

Before you begin

RADIUS をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 test {idle-time minutes password password [idle-time minutes] username name [password password [idle-time minutes]]} Example: <pre>switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3</pre>	グローバルなサーバ モニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 Note RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。

	Command or Action	Purpose
ステップ 3	radius-server deadtime <i>minutes</i> Example: <pre>switch(config)# radius-server deadtime 5</pre>	Cisco NX-OS デバイスが、前回応答しなかった RADIUS サーバをチェックするまでの時間 (分) を指定します。デフォルト値は 0 分です。有効な範囲は 0 ~ 1440 分です。
ステップ 4	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[各 RADIUS サーバの定期モニタリングの設定](#) (90 ページ)

各 RADIUS サーバの定期モニタリングの設定

各 RADIUS サーバの可用性をモニタリングできます。コンフィギュレーション パラメータには、サーバで使用するユーザ名とパスワード、およびアイドルタイマーなどがあります。アイドルタイマーには、RADIUS サーバがどのくらいの期間要求を受信しなかった場合に Cisco NX-OS スイッチがテスト パケットを送信するかを指定します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。



Note

各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。



Note

セキュリティ上の理由から、RADIUS データベース内の既存のユーザ名と同じテストユーザ名を設定しないことを推奨します。



Note デフォルトのアイドル タイマー値は 0 分です。アイドル時間間隔が 0 分の場合、Cisco NX-OS デバイスは、RADIUS サーバの定期的なモニタリングを実行しません。

Before you begin

RADIUS を有効にします。

1 つまたは複数の RADIUS サーバ ホストを追加します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 host {ipv4-address ipv6-address hostname} test {idle-time minutes password password [idle-time minutes] username name [password password [idle-time minutes]]} Example: <pre>switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3</pre>	サーバ モニタリング用のパラメータを個別に指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ~ 1440 分です。 Note RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	radius-server deadtime minutes Example: <pre>switch(config)# radius-server deadtime 5</pre>	Cisco NX-OS デバイスが、前回応答しなかった RADIUS サーバをチェックするまでの時間 (分) を指定します。デフォルト値は 0 分です。有効な範囲は 1 ~ 1440 分です。
ステップ 4	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[RADIUS サーバ ホストの設定](#) (71 ページ)

[RADIUS サーバのグローバルな定期モニタリングの設定](#) (88 ページ)

RADIUS デッドタイム間隔の設定

すべての RADIUS サーバのデッドタイム間隔を設定できます。デッドタイム間隔には、Cisco NX-OS デバイスが、RADIUS サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを確認するためにテスト パケットを送信するまでの間隔を指定します。デフォルト値は 0 分です。



Note デッドタイム間隔が 0 分の場合、RADIUS サーバは、応答を返さない場合でも、デッドとしてマークされません。RADIUS サーバグループに対するデッドタイム間隔を設定できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 deadtime minutes Example: <pre>switch(config)# radius-server deadtime 5</pre>	デッドタイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[RADIUS サーバ グループの設定](#) (81 ページ)

ワンタイムパスワードの設定

RSA SecurID トークン サーバを使用することで、Cisco NX-OS デバイスでワンタイムパスワード (OTP) をサポートできます。この機能を使用すると、ユーザは、暗証番号 (ワンタイムパスワード) とその時点で RSA SecurID トークンに表示されるトークン コードの両方を入力することで、Cisco NX-OS デバイスに対する認証を実行できます。



Note

Cisco NX-OS デバイスにログインするために使用されるトークン コードは、60 秒ごとに変更されます。デバイス検出に関する問題を防ぐために、Cisco Secure ACS 内部データベースに存在する異なるユーザ名を使用することを推奨します。

Before you begin

Cisco NX-OS デバイスで、RADIUS サーバ ホストとデフォルトのリモート ログイン認証を設定します。

次のものがインストールされていることを確認します。

- Cisco Secure Access Control Server (ACS) Version 4.2
- RSA Authentication Manager Version 7.1 (RSA SecurID トークン サーバ)
- RSA ACE Agent/Client

ワンタイムパスワードをサポートするために、Cisco NX-OS デバイスで (RADIUS サーバ ホストとリモート認証以外の) 設定を行う必要はありません。ただし、Cisco Secure ACS を次のように設定する必要があります。

1. RSA SecurID トークン サーバ認証をイネーブルにします。
2. RSA SecurID トークン サーバを不明ユーザ ポリシー データベースに追加します。

RADIUS サーバまたはサーバ グループの手動モニタリング

RADIUS サーバまたはサーバ グループに対し手動でテスト メッセージを送信できます。

Procedure

	Command or Action	Purpose
ステップ 1	test aaa server radius {ipv4-address ipv6-address hostname} [vrf vrf-name] username password Example: <pre>switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH</pre>	RADIUS サーバにテスト メッセージを送信して可用性を確認します。
ステップ 2	test aaa group group-name username password Example: <pre>switch# test aaa group RadGroup user2 As3He3CI</pre>	RADIUS サーバ グループにテスト メッセージを送信して可用性を確認します。

Dynamic Author Server の有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 server radius dynamic-author 例 : <pre>switch(config)# aaa server radius dynamic-author</pre>	RADIUS dynamic author server を有効にします。このコマンドのno形式を使用すれば、RADIUS dynamic author server を無効にできます。

RADIUS 認可変更の設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 :	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
	switch# configure terminal switch(config)#	
ステップ 2	[no] aaa server radius dynamic-author 例 : switch(config)# aaa server radius dynamic-author	スイッチを AAA サーバとして設定し、外部ポリシー サーバとの連携を促進します。このコマンドの no 形式を使用して、RADIUS ダイナミック オーサーと、関連付けられたクライアントを無効にできます。
ステップ 3	[no] client {ip-address hostname } [server-key [0 7] string] 例 : switch(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1	AAA サーバクライアントの IP アドレスまたはホスト名を設定します。オプションの server-key キーワードと string 引数を使用して、「クライアント」レベルでサーバ キーを設定します。クライアント サーバを削除するには、このコマンドの no 形式を使用します。 (注) クライアントレベルでサーバキーを設定すると、グローバル レベルで設定されたサーバ キーが上書きされます。
ステップ 4	[no] port port-number 例 : switch(config-locsvr-da-radius)# port 3799	設定された RADIUS クライアントからの RADIUS 要求をデバイスが受信するポートを指定します。ポート範囲は1～65535です。デフォルトのポートに戻すには、このコマンドの no 形式を使用します。 (注) パケットオブディスコネクトのデフォルト ポートは 1700 です。
ステップ 5	[no] server-key [0 7] string	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。サーバキーを削除するには、このコマンドの no 形式を使用します。

RADIUS 設定の確認

RADIUS の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show radius {status pending pending-diff}	Cisco Fabric Services の RADIUS 設定の配布状況と他の詳細事項を表示します。
show running-config radius [all]	実行コンフィギュレーションの RADIUS 設定を表示します。
show startup-config radius	スタートアップコンフィギュレーションの RADIUS 設定を表示します。
show radius-server [hostname ipv4-address ipv6-address] [directed-request groups sorted statistics]	設定済みのすべての RADIUS サーバのパラメータを表示します。

RADIUS 認可変更の設定の検証

RADIUS 認可変更の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config dot1x	実行コンフィギュレーションの dot1x 設定を表示します。
show running-config aaa	実行コンフィギュレーションの AAA 設定を表示します。
show running-config radius	実行コンフィギュレーションの RADIUS 設定を表示します。
show aaa server radius statistics	ローカルの RADIUS サーバ統計情報を表示します。
show aaa client radius statistics {ip address hostname }	ローカルの RADIUS クライアント統計情報を表示します。
clear aaa server radius statistics	ローカルの RADIUS サーバ統計情報をクリアします。
clear aaa client radius statistics {ip address hostname }	ローカルの RADIUS クライアント統計情報をクリアします。

RADIUS サーバのモニタリング

Cisco NX-OS デバイスが保持している RADIUS サーバのアクティビティに関する統計情報をモニタします。

Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	show radius-server statistics {hostname ipv4-address ipv6-address} Example: switch# show radius-server statistics 10.10.1.1	RADIUS 統計情報を表示します。

Related Topics

[RADIUS サーバ ホストの設定](#) (71 ページ)

[RADIUS サーバ統計情報のクリア](#) (97 ページ)

RADIUS サーバ統計情報のクリア

Cisco NX-OS デバイスが保持している RADIUS サーバのアクティビティに関する統計情報を表示します。

Before you begin

Cisco NX-OS デバイスの RADIUS サーバを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	(Optional) show radius-server statistics {hostname ipv4-address ipv6-address} Example: switch# show radius-server statistics 10.10.1.1	Cisco NX-OS デバイスの RADIUS サーバ統計情報を表示します。
ステップ 2	clear radius-server statistics {hostname ipv4-address ipv6-address} Example: switch# clear radius-server statistics 10.10.1.1	RADIUS サーバ統計情報をクリアします。

Related Topics

[RADIUS サーバ ホストの設定](#) (71 ページ)

RADIUS の設定例

次に、RADIUS を設定する例を示します。

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
```

RADIUS 認可変更の設定例

次に、RADIUS の認可変更を設定する方法の例を示します。

```
radius-server host 10.77.143.170 key 7 "fewhg123" authentication accounting
aaa server radius dynamic-author
    client 10.77.143.170 vrf management server-key 7 "fewhg123"
```

次の作業

これで、サーバグループも含めて AAA 認証方式を設定できるようになります。

RADIUS に関する追加情報

ここでは、RADIUS の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『Cisco NX-OS ライセンス ガイド』
VRF コンフィギュレーション	『Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング設定ガイド』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
RADIUS に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 6 章

TACACS+ の設定

この章では、Cisco NX-OS デバイス上で Terminal Access Controller Access Control System Plus (TACACS+) プロトコルを設定する手順について説明します。

この章は、次の項で構成されています。

- [TACACS+ について, on page 101](#)
- [TACACS+ の前提条件, on page 105](#)
- [TACACS+ のガイドラインと制約事項 \(106 ページ\)](#)
- [TACACS+ のデフォルト設定, on page 107](#)
- [ワンタイム パスワード サポート \(107 ページ\)](#)
- [TACACS+ の設定, on page 108](#)
- [TACACS+ サーバのモニタリング, on page 133](#)
- [TACACS+ サーバ統計情報のクリア, on page 133](#)
- [TACACS+ の設定の確認, on page 134](#)
- [TACACS+ の設定例, on page 134](#)
- [TACACS+ Over TLS の構成 \(135 ページ\)](#)
- [TACACS+ Over TLS の構成の確認 \(137 ページ\)](#)
- [次の作業, on page 137](#)
- [TACACS+ に関する追加情報, on page 137](#)

TACACS+ について

TACACS+ は、Cisco NX-OS デバイス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 プロトコルです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。Cisco NX-OS デバイスに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ では、認証、許可、アカウンティングの各ファシリティを個別に提供します。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利用できる他のサービスを使用できます。

TACACS+ クライアント/サーバー プロトコルでは、トランスポート要件を満たすため TCP (TCP ポート 49) を使用します。Cisco NX-OS デバイスは、TACACS+ プロトコルを使用して集中型の認証を行います。

Cisco NX-OS リリース 10.4(3)F 以降、TACACS+ サーバーを使用した X.509 証明書の SSH ベースの認証は、Cisco Nexus 9000 シリーズ プラットフォーム スイッチで **aaa authorization ssh-certificate default group** コマンドを使用して実行できます。設定の詳細については、[TACACS+ サーバーを使用した X.509 証明書ベースの SSH 認証の設定, on page 129](#)を参照してください。

TACACS+ の利点

TACACS+ には、RADIUS 認証にはない次の利点があります。

- 独立した AAA ファシリティを提供する。たとえば、Cisco NX-OS デバイスは、認証を行わずにアクセスを許可できます。
- AAA クライアントとサーバ間のデータ送信に TCP トランスポートプロトコルを使用しているため、コネクション型プロトコルによる確実な転送を実行します。
- スイッチと AAA サーバ間でプロトコルペイロード全体を難読化して、高度なデータ機密性を実現します。RADIUS プロトコルはパスワードだけを難読化します。

ユーザ ログインにおける TACACS+ の動作

ユーザが TACACS+ を使用して、パスワード認証プロトコル (PAP) によるログインを Cisco NX-OS デバイスに対して試行すると、次のプロセスが実行されます。



Note

TACACS+ では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。通常、デーモンはユーザ名とパスワードを入力するよう求めますが、ユーザの母親の旧姓などの追加項目を求めることもできます。

1. Cisco NX-OS デバイスが接続を確立すると、TACACS+ デーモンにアクセスして、ユーザ名とパスワードを取得します。
2. Cisco NX-OS デバイスは、最終的に TACACS+ デーモンから次のいずれかの応答を受信します。

ACCEPT

ユーザの認証に成功したので、サービスを開始します。Cisco NX-OS デバイスがユーザの許可を要求している場合は、許可が開始されます。

REJECT

ユーザの認証に失敗しました。TACACS+ デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログインシーケンスを再試行するよう要求します。

ERROR

デーモンによる認証サービスの途中でエラーが発生したか、またはデーモンと Cisco NX-OS デバイスの間のネットワーク接続でエラーが発生しました。Cisco NX-OS デバイスが ERROR 応答を受信すると、Cisco NX-OS デバイスは代替方式でユーザ認証を試行します。

認証が終了し、Cisco NX-OS デバイスで許可がイネーブルになっていれば、続いてユーザ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、Cisco NX-OS デバイスは再度 TACACS+ デーモンにアクセスします。デーモンは ACCEPT または REJECT 許可応答を返します。ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT 応答により、ユーザがアクセス可能なサービスが決まります。

この場合のサービスは次のとおりです。

- Telnet、rlogin、ポイントツーポイントプロトコル (PPP)、シリアルラインインターネットプロトコル (SLIP)、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 (IPv4 または IPv6)、アクセスリスト、ユーザタイムアウト)

デフォルトの TACACS+ サーバ難読化タイプおよび秘密キー

スイッチを TACACS+ サーバに対して認証するには、TACACS+ 秘密キーを設定する必要があります。秘密キーとは、Cisco NX-OS デバイスと TACACS+ サーバホスト間の共有秘密テキストストリングです。キーの長さは 63 文字で、出力可能な任意の ASCII 文字を含めることができます (スペースは使用できません)。Cisco NX-OS デバイス上のすべての TACACS+ サーバ設定で使用されるグローバルな秘密キーを設定できます。

グローバルな秘密キーの設定は、個々の TACACS+ サーバの設定時に明示的に **key** オプションを使用することによって上書きできます。

TACACS+ サーバのコマンド許可サポート

デフォルトでは、認証されたユーザがコマンドラインインターフェイス (CLI) でコマンドを入力したときに、Cisco NX-OS ソフトウェアのローカルデータベースに対してコマンド許可が行われます。また、TACACS+ を使用して、認証されたユーザに対して許可されたコマンドを確認することもできます。

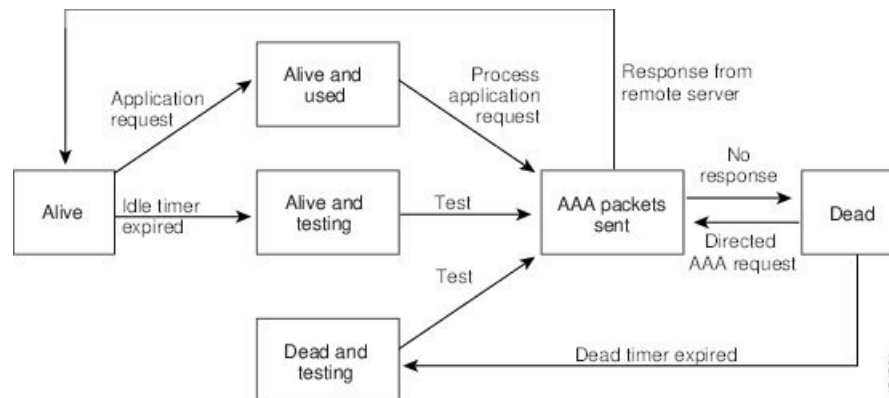
TACACS+ サーバのモニタリング

応答を返さない TACACS+ サーバがあると、AAA 要求の処理に遅延が発生する可能性があります。AAA 要求の処理時間を節約するため、Cisco NX-OS デバイスは定期的に TACACS+ サーバをモニタリングし、TACACS+ サーバが応答を返す (アライブ) かどうかを調べることができます。Cisco NX-OS デバイスは、応答を返さない TACACS+ サーバをデッド (dead) として

マークし、デッド TACACS+ サーバには AAA 要求を送信しません。また、Cisco NX-OS デバイスは、定期的にデッド TACACS+ サーバをモニタリングし、それらが応答を返したら、アライブ状態に戻します。このモニタリングプロセスでは、実際の AAA 要求が送信される前に、TACACS+ サーバが稼働状態であることを確認します。TACACS+ サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル (SNMP) トラップが生成され、Cisco NX-OS デバイスによって、パフォーマンスに影響が出る前に、障害が発生していることを知らせるエラーメッセージが表示されます。

Figure 4: TACACS+ サーバの状態

次の図に、TACACS+ サーバモニタリングのサーバの状態を示します。



Note

アライブサーバとデッドサーバのモニタリング間隔は異なります。これらはユーザが設定できます。TACACS+ サーバモニタリングを実行するには、テスト認証要求を TACACS+ サーバに送信します。

TACACS+ のベンダー固有属性

インターネット技術特別調査委員会 (IETF) ドラフト標準には、ネットワーク アクセスサーバと TACACS+ サーバの間でベンダー固有属性 (VSA) を伝達する方法が規定されています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、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。

TACACS+ 用の Cisco VSA 形式

シスコの TACACS+ 実装では、IETF 仕様で推奨される形式を使用した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、サポートされるオプションのベンダータイプは 1 (名前付き `cisco-av-pair`) です。値は次の形式のストリングです。

protocol : attribute separator value *

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は = (等号)、オプションの属性の場合は * (アスタリスク) です。

Cisco NX-OS デバイスでの認証に TACACS+ サーバを使用した場合、TACACS+ プロトコルは TACACS+ サーバに対し、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションが、Cisco NX-OS ソフトウェアでサポートされています。

Shell

ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。

Accounting

accounting-request パケットで使用されるプロトコル。値にスペースが含まれている場合は、二重引用符で囲む必要があります。

Cisco NX-OS ソフトウェアでは、次の属性がサポートされています。

roles

ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。たとえば、ユーザが network-operator および network-admin のロールに属している場合、値フィールドは network-operator network-admin となります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、TACACS+ サーバから送信されます。この属性はシェル プロトコル値とだけ併用できます。次に、Cisco ACS でサポートされるロール属性の例を示します。

```
shell:roles=network-operator network-admin
```

```
shell:roles*network-operator network-admin
```



Note

VSA を shell:roles*"network-operator network-admin" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

accountinginfo

標準の TACACS+ アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。この属性は、スイッチ上の TACACS+ クライアントから、Account-Request フレームの VSA 部分にだけ格納されて送信されます。この属性と共に使用できるのは、アカウンティングのプロトコル データ ユニット (PDU) だけです。

TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバの IPv4 または IPv6 アドレスまたはホスト名を取得すること。
- TACACS+ サーバから秘密キーを取得すること（ある場合）。
- Cisco NX-OS デバイスが、AAA サーバの TACACS+ クライアントとして設定されていること。

TACACS+ のガイドラインと制約事項

TACACS+ に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS リリース 10.6(2)F 以降、Cisco Nexus 9000 シリーズスイッチは、既存の netstack パスに加えて、Linux カーネル ネットワーク スタック (kstack) を介した TACACS+ (AAA) トラフィックのルーティングをサポートします。
 - TACACS+ サーバーの IP が、選択した VRF でローカル インターフェイス アドレス (理想的にはループバック) として設定されている場合、AAA 要求は kstack を介して送信されます。
 - 外部 TACACS+ サーバー IP の場合、AAA 要求は引き続き netstack を介して送信されます。
 - IPv4 または IPv6 アドレスを使用して設定された TACACS+ サーバーは、kstack を介してサポートされます。ホスト名で構成された TACACS+ サーバーは、kstack を介してサポートされません。ホスト名が使用されている場合、システムは引き続き DNS 解決のために netstack に依存します。
 - この機能は、kstack を介した TACACS-over-TLS 機能をサポートしていません。
 - TACACS+ のみが kstack をサポートします。RADIUS と LDAP は引き続き netstack を使用します。
- Cisco NX-OS リリース 10.6(1)F 以降、ユーザーは TLS を使用してクライアントの TACACS+ サーバーを構成できます。

この機能は、共有キーが有効な場合の AAA 機能をサポートしていません。
- Cisco NX-OS デバイスに設定できる TACACS+ サーバの最大数は 64 です。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- グループ内に 6 台以上のサーバが設定されている場合は、デッドタイム間隔を設定することを推奨します。6 台以上のサーバを設定する必要がある場合は、デッドタイム間隔を 0 より大きな値に設定し、テスト ユーザ名とテスト パスワードを設定することで、デッドサーバのモニタリングを有効にしてください。
- TACACS+ サーバでのコマンド認証は、コンソールと vty セッションに使用できます。コンソール ログインには、テストせずに使用することを推奨します。
- N9K-X9636C-R および N9K-X9636Q-R ラインカードおよび N9K-C9508-FM-R ファブリック モジュールの場合、特殊文字を含むユーザ名の TACACS+ 認証は失敗します。
- Cisco NX-OS リリース 10.3(1)F 以降、TACACS+ は Cisco Nexus 9808 スイッチでサポートされます。

- Cisco NX-OS リリース 10.4(1)F 以降、TACACS+ は Cisco Nexus X98900CD-A および X9836DM-A ラインカードを搭載した Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、TACACS+ は、X98900CD-A および X9836DM-A ラインカードを搭載した Cisco Nexus 9804 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(3)F 以降、TACACS+ サーバーを使用した X.509 証明書の SSH ベースの認証は、Cisco Nexus 9000 シリーズプラットフォーム スイッチで `aaa authorization ssh-certificate default group` コマンドを使用して実行できます。
- Cisco NX-OS スイッチは、ユーザー名/パスワードプロンプトのカスタマイズをサポートしていません。スイッチでカスタムプロンプトを設定した場合、それらは無視されます。

TACACS+ のデフォルト設定

次の表に、TACACS+ パラメータのデフォルト設定値を示します。

Table 9: TACACS+ パラメータのデフォルト設定

パラメータ	デフォルト
TACACS+	ディセーブル
デッド タイマー間隔	0 分
タイムアウト間隔	5 秒
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	テスト
TACACS+ 許可の特権レベル サポート	無効化

ワンタイム パスワード サポート

ワンタイムパスワードサポート (OTP) は、1回のログインセッションまたはトランザクションに有効なパスワードです。OTPは、通常の (スタティック) パスワードに関連する多数の欠点を回避します。OTPは攻撃をリプレイするリスクはありません。すでにサービスへのログインまたは操作の実行に使用された OTP を侵入者が記録しようとしても、OTP は有効ではなくなっているため、悪用されません。

OTP は RADIUS や TACACS プロトコルデーモンに対してのみ適用できます。RADIUS プロトコルデーモンの場合は、ASCII 認証モードを無効にする必要があります。TACACS+プロトコ

ルデーモンの場合は、ASCII 認証モードを有効にする必要があります。TACACS+ サーバでパスワードの ASCII 認証を有効にするには、**aaa authentication login ascii-authentication** コマンドを使用します。

TACACS+ の設定

ここでは、Cisco NX-OS デバイスで TACACS+ サーバを設定する手順を説明します。



Note Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

TACACS+ サーバの設定プロセス

Procedure

- ステップ 1 TACACS+ をイネーブルにします。
- ステップ 2 TACACS+ サーバと Cisco NX-OS デバイスとの接続を確立します。
- ステップ 3 TACACS+ サーバの秘密キーを設定します。
- ステップ 4 必要に応じて、AAA 認証方式用に、TACACS+ サーバのサブセットを使用して TACACS+ サーバグループを設定します。
- ステップ 5 （任意）TCP ポートを設定します。
- ステップ 6 （任意）必要に応じて、TACACS+ サーバの定期モニタリングを設定します。
- ステップ 7 （任意）TACACS+ の配布がイネーブルになっている場合は、ファブリックに対して TACACS+ 設定をコミットします。

Related Topics

[TACACS+ のイネーブル化](#)（108 ページ）

TACACS+ のイネーブル化

デフォルトでは、Cisco NX-OS デバイスの TACACS+ 機能はディセーブルに設定されています。認証に関するコンフィギュレーションコマンドと検証コマンドを使用するには、TACACS+ 機能を明示的にイネーブルにする必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	feature tacacs+ Example: <pre>switch(config)# feature tacacs+</pre>	TACACS+ をイネーブルにします。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバホストの設定

リモートの TACACS+ サーバにアクセスするには、Cisco NX-OS デバイス上でその TACACS+ サーバの IP アドレスかホスト名を設定する必要があります。最大 64 の TACACS+ サーバを設定できます。



Note

TACACS+ サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスに設定するとき、デフォルトでは TACACS+ サーバはデフォルトの TACACS+ サーバ グループに追加されます。TACACS+ サーバは別の TACACS+ サーバ グループに追加することもできます。

Before you begin

TACACS+ を有効にします。

リモート TACACS+ サーバの IP アドレス (IPv4 または IPv6) またはホスト名を取得していること。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	tacacs-server host {ipv4-address ipv6-address hostname} Example: switch(config)# tacacs-server host 10.10.2.2	TACACS+ サーバの IP アドレス (IPv4 または IPv6) 、またはホスト名を指定します。
ステップ 3	(Optional) show tacacs+ {pending pending-diff} Example: switch(config)# show tacacs+ pending	配布するために保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) tacacs+ commit Example: switch(config)# tacacs+ commit	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。
ステップ 5	exit Example: switch(config)# exit switch#	設定モードを終了します。
ステップ 6	(Optional) show tacacs-server Example: switch# show tacacs-server	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[TACACS+ のイネーブル化](#) (108 ページ)

[TACACS+ サーバグループの設定](#) (113 ページ)

グローバル TACACS+ キーの設定

Cisco NX-OS デバイスで使用するすべてのサーバについて、グローバルレベルで秘密 TACACS+ キーを設定できます。秘密キーとは、Cisco NX-OS デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

Before you begin

TACACS+ を有効にします。

リモート TACACS+ サーバの秘密キーの値を取得します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	tacacs-server key [0 6 7] key-value Example: <pre>switch(config)# tacacs-server key 0 QsEfThUkO</pre> Example: <pre>switch(config)# tacacs-server key 7 "fewhg"</pre>	すべての TACACS+ サーバ用の TACACS+ キーを指定します。 <i>key-value</i> がクリアテキスト形式 (0) か、タイプ 6 暗号化形式 (6) か、タイプ 7 暗号化形式 (7) かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存する前にクリアテキストのキーを暗号化します。デフォルトの形式はクリアテキストです。最大で 63 文字です。 デフォルトでは、秘密キーは設定されていません。 Note generate type7_encrypted_secret を使用してすでに共有秘密を設定している場合 コマンドを使用して、二番目の例に示すように引用符に入力します。詳細については、RADIUS または TACACS+ の共有秘密の設定, on page 54を参照してください。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) show tacacs-server Example: <pre>switch# show tacacs-server</pre>	TACACS+サーバの設定を表示します。 Note 秘密キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された秘密キーを表示するには、 show running-config コマンドを使用します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[TACACS+ のイネーブル化](#) (108 ページ)

[AES パスワード暗号化およびプライマリ暗号キーについて](#) (617 ページ)

特定の TACACS+ サーバ用のキーの設定

TACACS+サーバの秘密キーを設定できます。秘密キーとは、Cisco NX-OS デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

Before you begin

TACACS+ を有効にします。

リモート TACACS+ サーバの秘密キーの値を取得します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	tacacs-server host {ipv4-address ipv6-address host-name} key [0 6 7] key-value Example: <pre>switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg</pre>	特定の TACACS+サーバの秘密キーを指定します。 <i>key-value</i> がクリア テキスト形式 (0) か、タイプ 6 暗号化形式 (6) か、タイプ 7 暗号化形式 (7) かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存

	Command or Action	Purpose
	Example: <pre>switch(config)# tacacs-server host 10.10.1.1 key 7 "fewhg"</pre>	する前にクリア テキストのキーを暗号化します。デフォルトの形式はクリア テキストです。最大で 63 文字です。 グローバル秘密キーではなく、この秘密キーが使用されます。 Note generate type7_encrypted_secret を使用してすでに共有秘密を設定している場合 コマンドを使用して、二番目の例に示すように引用符に入力します。詳細については、RADIUS または TACACS+ の共有秘密の設定, on page 54を参照してください。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show tacacs-server Example: <pre>switch# show tacacs-server</pre>	TACACS+ サーバの設定を表示します。 Note 秘密キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された秘密キーを表示するには、show running-config コマンドを使用します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[AES パスワード暗号化およびプライマリ暗号キーについて](#) (617 ページ)

TACACS+ サーバグループの設定

サーバグループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバーはすべて、TACACS+ プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバグループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

Before you begin

TACACS+ を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 group server tacacs+ group-name Example: switch(config)# aaa group server tacacs+ TacServer switch(config-tacacs+)#	TACACS+サーバグループを作成し、そのグループのTACACS+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 3	server {ipv4-address ipv6-address hostname} Example: switch(config-tacacs+)# server 10.10.2.2	TACACS+ サーバを、TACACS+ サーバグループのメンバーとして設定します。 指定した TACACS+サーバが見つからない場合は、 tacacs-server host コマンドを使用して、このコマンドを再試行します。
ステップ 4	exit Example: switch(config-tacacs+)# exit switch(config)#	TACACS+サーバグループ コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show tacacs-server groups Example: switch(config)# show tacacs-server groups	TACACS+サーバグループの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[TACACS+ のイネーブル化](#) (108 ページ)

[リモート AAA サービス](#) (23 ページ)

[TACACS+ サーバ ホストの設定 \(109 ページ\)](#)[TACACS+ デッド タイム間隔の設定 \(123 ページ\)](#)

TACACS+サーバグループのためのグローバル発信元インターフェイスの設定

TACACS+ サーバグループにアクセスする際に使用する、TACACS+ サーバグループ用のグローバル発信元インターフェイスを設定できます。また、特定のTACACS+サーバグループ用に異なる発信元インターフェイスを設定することもできます。デフォルトでは、Cisco NX-OS ソフトウェアは、使用可能なあらゆるインターフェイスを使用します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)</pre>	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 tacacs source-interface interface Example: <pre>switch(config)# ip tacacs source-interface mgmt 0</pre>	このデバイスで設定されているすべての TACACS+サーバグループ用のグローバル発信元インターフェイスを設定します。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show tacacs-server Example: <pre>switch# show tacacs-server</pre>	TACACS+サーバの設定情報を表示します。
ステップ 5	(Optional) copy running-config startup config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[TACACS+ のイネーブル化 \(108 ページ\)](#)[TACACS+ サーバグループの設定 \(113 ページ\)](#)

ユーザによるログイン時の TACACS+ サーバ指定の許可

スイッチ上で `directed-request`（誘導要求）オプションを有効にすることにより、認証要求の送信先の TACACS+ サーバをユーザが指定できるようになります。デフォルトでは、Cisco NX-OS デバイスはデフォルトの AAA 認証方式に基づいて認証要求を転送します。このオプションを有効にすると、ユーザは `username@vrfname:hostname` としてログインできます。ここで `vrfname` は使用する VRF で、`hostname` は設定された TACACS+ サーバの名前です。



Note `directed-request` オプションをイネーブルにすると、Cisco NX-OS デバイスでは認証に TACACS+ 方式だけを使用し、デフォルトのローカル方式は使用しないようになります。



Note ユーザ指定のログインは Telnet セッションに限りサポートされます。

Before you begin

TACACS+ をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	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	tacacs-server directed-request Example: <code>switch(config)# tacacs-server directed-request</code>	ログイン時にユーザが認証要求の送信先となる TACACS+ サーバを指定できるようにします。デフォルトでは無効になっています。
ステップ 3	(Optional) show tacacs+ {pending pending-diff} Example: <code>switch(config)# show tacacs+ pending</code>	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) tacacs+ commit Example: <code>switch(config)# tacacs+ commit</code>	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。
ステップ 5	exit Example:	設定モードを終了します。

	Command or Action	Purpose
	switch(config)# exit switch#	
ステップ 6	(Optional) show tacacs-server directed-request Example: switch# show tacacs-server directed-request	TACACS+ の directed request の設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[TACACS+ のイネーブル化](#) (108 ページ)

TACACS+ サーバのタイムアウト間隔の設定

Cisco NX-OS デバイスが、タイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機するタイムアウト間隔を設定できます。タイムアウト間隔には、Cisco NX-OS デバイスが TACACS+ サーバからの応答を待つ時間を指定します。これを過ぎるとタイムアウトエラーになります。

Before you begin

TACACS+ をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	tacacs-server host {ipv4-address ipv6-address hostname} timeout seconds Example: switch(config)# tacacs-server host server1 timeout 10	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 Note 特定の TACACS+ サーバに指定したタイムアウト間隔は、すべての TACACS+ サーバに指定したタイムアウト間隔より優先されます。

	Command or Action	Purpose
ステップ 3	(Optional) show tacacs+ {pending pending-diff} Example: <code>switch(config)# show tacacs+ pending</code>	配布するために保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) tacacs+ commit Example: <code>switch(config)# tacacs+ commit</code>	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。
ステップ 5	exit Example: <code>switch(config)# exit</code> <code>switch#</code>	設定モードを終了します。
ステップ 6	(Optional) show tacacs-server Example: <code>switch# show tacacs-server</code>	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: <code>switch# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics
[TACACS+ のイネーブル化](#) (108 ページ)

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、TACACS+ サーバ用に別の TCP ポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての TACACS+ 要求にポート 49 を使用します。

Before you begin

TACACS+ を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	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

	Command or Action	Purpose
ステップ 2	tacacs-server host {ipv4-address ipv6-address hostname} port tcp-port Example: switch(config)# tacacs-server host 10.10.1.1 port 2	サーバに送る TACACS+ メッセージに使用する TCP ポートを指定します。デフォルトの TCP ポートは 49 です。値の範囲は 1 ～ 65535 です。
ステップ 3	(Optional) show tacacs+ {pending pending-diff} Example: switch(config)# show tacacs+ distribution pending	配布するために保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) tacacs+ commit Example: switch(config)# tacacs+ commit	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。
ステップ 5	exit Example: switch(config)# exit switch#	設定モードを終了します。
ステップ 6	(Optional) show tacacs-server Example: switch# show tacacs-server	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[TACACS+ のイネーブル化](#) (108 ページ)

TACACS+ サーバのグローバルな定期モニタリングの設定

各サーバに個別にテストパラメータを設定しなくても、すべての TACACS+ サーバの可用性をモニタリングできます。テストパラメータが設定されていないサーバは、グローバルレベルのパラメータを使用してモニタリングされます。



Note

各サーバ用に設定されたテストパラメータは、グローバルのテストパラメータより優先されます。

グローバル コンフィギュレーション パラメータには、サーバで使用するユーザ名とパスワード、およびアイドルタイマーなどがあります。アイドルタイマーには、TACACS+サーバがどのくらいの期間要求を受信しなかった場合に、Cisco NX-OS デバイスがテストパケットを送信するかを指定します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。



Note テストパラメータは、すべてのスイッチに配布されます。ファブリック内に旧リリースが稼働しているスイッチが 1 つでもある場合は、ファブリック内のすべてのスイッチにテストパラメータが配布されなくなります。



Note ネットワークのセキュリティ保護のため、TACACS+ データベース内の既存のユーザ名と同じユーザ名を使用しないことを推奨します。



Note デフォルトのアイドル タイマー値は 0 分です。アイドル タイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。

Before you begin

TACACS+ を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	tacacs-server test {idle-time minutes password password [idle-time minutes] username name [password password [idle-time minutes]]} Example: <pre>switch(config)# tacacs-server test username user1 password Ur2Gd2BH idle-time 3</pre>	グローバルなサーバモニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ~ 1440 分です。 Note TACACS+ サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。

	Command or Action	Purpose
ステップ 3	tacacs-server dead-time <i>minutes</i> Example: <pre>switch(config)# tacacs-server dead-time 5</pre>	Cisco NX-OS デバイスが、前回応答しなかった TACACS+ サーバをチェックするまでの時間（分）を指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。
ステップ 4	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) show tacacs-server Example: <pre>switch# show tacacs-server</pre>	TACACS+ サーバの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[各 TACACS+ サーバの定期モニタリングの設定](#) (121 ページ)

各 TACACS+ サーバの定期モニタリングの設定

各 TACACS+ サーバの可用性をモニタリングできます。コンフィギュレーションパラメータには、サーバで使用するユーザ名とパスワード、およびアイドルタイマーなどがあります。アイドルタイマーには、TACACS+ サーバがどのくらいの期間要求を受信しなかった場合に、Cisco NX-OS デバイスがテスト パケットを送信するかを指定します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。



Note

各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。



Note

ネットワークのセキュリティ保護のため、TACACS+ データベース内の既存のユーザ名と同じユーザ名を使用しないことを推奨します。



Note デフォルトのアイドル タイマー値は 0 分です。アイドル タイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。



Note テスト パラメータは、すべてのスイッチに配布されます。テスト パラメータは、ファブリック内のスイッチには配信されません。

Before you begin

TACACS+ をイネーブルにします。

1 つまたは複数の TACACS+ サーバ ホストを追加します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	tacacs-server host {ipv4-address ipv6-address hostname} test {idle-time minutes password password [idle-time minutes] username name [password password [idle-time minutes]]} Example: <pre>switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3</pre>	サーバ モニタリング用のパラメータを個別に指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 Note TACACS+ サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	tacacs-server dead-time minutes Example: <pre>switch(config)# tacacs-server dead-time 5</pre>	Cisco NX-OS デバイスが、前回応答しなかった TACACS+サーバをチェックするまでの時間 (分) を指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。
ステップ 4	exit Example:	設定モードを終了します。

	Command or Action	Purpose
	switch(config)# exit switch#	
ステップ 5	(Optional) show tacacs-server Example: switch# show tacacs-server	TACACS+ サーバの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[TACACS+ サーバ ホストの設定](#) (109 ページ)

[TACACS+ サーバのグローバルな定期モニタリングの設定](#) (119 ページ)

TACACS+ デッド タイム間隔の設定

すべての TACACS+ サーバのデッドタイム間隔を設定できます。デッドタイム間隔には、Cisco NX-OS デバイスが TACACS+ サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを判断するためにテスト パケットを送信するまでの間隔を指定します。



Note デッドタイム間隔が 0 分の場合、TACACS+ サーバは、応答を返さない場合でも、デッドとしてマークされません。デッド タイマーはグループ単位で設定できます。

Before you begin

TACACS+ をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	tacacs-server deadtime minutes Example: switch(config)# tacacs-server deadtime 5	グローバルなデッド タイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。

	Command or Action	Purpose
ステップ 3	(Optional) show tacacs+ {pending pending-diff} Example: <code>switch(config)# show tacacs+ pending</code>	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) tacacs+ commit Example: <code>switch(config)# tacacs+ commit</code>	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。
ステップ 5	exit Example: <code>switch(config)# exit</code> <code>switch#</code>	設定モードを終了します。
ステップ 6	(Optional) show tacacs-server Example: <code>switch# show tacacs-server</code>	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: <code>switch# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ASCII 認証の設定

TACACS+ サーバで ASCII 認証をイネーブルにできます。

Before you begin

TACACS+ をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	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。

	Command or Action	Purpose
ステップ 2	aaa authentication login ascii-authentication Example: <pre>switch(config)# aaa authentication login ascii-authentication</pre>	ASCII 認証をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	(Optional) show tacacs+ {pending pending-diff} Example: <pre>switch(config)# show tacacs+ pending</pre>	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) tacacs+ commit Example: <pre>switch(config)# tacacs+ commit</pre>	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。
ステップ 5	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 6	(Optional) show tacacs-server Example: <pre>switch# show tacacs-server</pre>	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバでのコマンド許可の設定

TACACS+ サーバでコマンド許可を設定できます。



Caution

コマンド許可では、デフォルト ロールを含むユーザのロールベース許可コントロール (RBAC) がディセーブルになります。



Note コンソールを使用してサーバにログインすると、コマンド認可はディセーブルになります。認証は、非コンソールセッションとコンソールセッションの両方に使用できます。デフォルトでは、コマンド許可はデフォルト（非コンソール）セッション用に設定されていますが、コンソールセッションに対してディセーブルです。コンソールセッションでコマンド許可をイネーブルにするには、コンソールの AAA グループを明示的に設定する必要があります。



Note デフォルトでは、状況依存ヘルプおよびコマンドのタブ補完に表示されるのは、割り当てられたロールでユーザに対するサポートが定義されているコマンドだけです。コマンド許可をイネーブルにすると、Cisco NX-OS ソフトウェアでは、ユーザに割り当てられているロールに関係なく、状況依存ヘルプおよびタブ補完にすべてのコマンドが表示されるようになります。

Before you begin

TACACS+ を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 authorization {commands config-commands} {console default} {group group-list [local] local} Example: <pre>switch(config)# aaa authorization commands default group TacGroup Per command authorization will disable RBAC for all users. Proceed (y/n)?</pre>	TACACS+サーバの特定の役割にコマンド許可方式を設定します。 commands キーワードを使用するとすべての EXEC コマンドの許可ソースを設定でき、config-commands キーワードを使用するとすべてのコンフィギュレーション コマンドの許可ソースを設定できます。 console キーワードは、コンソールセッションのコマンド許可を設定し、default キーワードは、非コンソールセッションのコマンド許可を設定します。 group-list 引数には、TACACS+ サーバグループの名前をスペースで区切ったリストを指定します。このグループに属しているサーバに対して、コマンド許可のためのアクセスが行われます。local 方

	Command or Action	Purpose
		式では、許可にローカル ロールベース データベースが使用されます。 local 方式は、設定されたすべてのサーバ グループから応答が得られなかった場合に、local をフォールバック方式として設定しているときにだけ使用されます。デフォルトの方式は local です。 TACACS+サーバグループの方式のあとにフォールバック方式を設定していないと、すべてのサーバ グループから応答が得られなかった場合は許可に失敗します。 確認プロンプトで Enter キーを押した場合のデフォルトのアクションは n です。
ステップ 3	(Optional) show tacacs+ {pending pending-diff} Example: <pre>switch(config)# show tacacs+ pending</pre>	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) tacacs+ commit Example: <pre>switch(config)# tacacs+ commit</pre>	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。
ステップ 5	exit Example: <pre>switch(config)# exit switch#</pre>	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 6	(Optional) show aaa authorization [all] Example: <pre>switch(config)# show aaa authorization</pre>	AAA 許可設定を表示します。 all キーワードを指定すると、デフォルト値が表示されます。
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[TACACS+ のイネーブル化](#) (108 ページ)

[TACACS+ サーバでのコマンド許可のテスト](#) (128 ページ)

TACACS+ サーバでのコマンド許可のテスト

TACACS+ サーバで、ユーザに対するコマンド許可をテストできます。



Note 許可の正しいコマンドを送信しないと、結果の信頼性が低くなります。



Note `test` コマンドでは許可に、コンソール方式ではなくデフォルト（非コンソール）方式を使用します。

Before you begin

TACACS+ をイネーブルにします。

TACACS+ サーバにコマンド許可が設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	test aaa authorization command-type {commands config-commands} user username command command-string Example: <pre>switch# test aaa authorization command-type commands user TestUser command reload</pre>	TACACS+サーバで、コマンドに対するユーザの許可をテストします。 commands キーワードはEXEC コマンドだけを指定し、config-commands キーワードはコンフィギュレーション コマンドだけを指定します。 Note <code>command-string</code> 引数にスペースが含まれる場合は、二重引用符 (") で囲みます。

Related Topics

[TACACS+ のイネーブル化](#)（108 ページ）

[TACACS+ サーバでのコマンド許可の設定](#)（125 ページ）

[ユーザ アカウントおよび RBAC の設定](#)（277 ページ）

コマンド許可検証のイネーブル化とディセーブル化

デフォルトのユーザー セッションまたは別のユーザー一名に対して、コマンドライン インターフェイス（CLI）でコマンド許可検証を有効にしたり、無効にしたりすることができます。



(注) 許可検証をイネーブルにした場合は、コマンドは実行されません。

手順

	コマンドまたはアクション	目的
ステップ 1	terminal verify-only [username username] 例 : <pre>switch# terminal verify-only</pre>	コマンド許可検証をイネーブルにします。このコマンドを入力すると、入力したコマンドが許可されているかどうかは Cisco NX-OS ソフトウェアによって示されます。
ステップ 2	terminal no verify-only [username username] 例 : <pre>switch# terminal no verify-only</pre>	コマンド許可検証をディセーブルにします。

TACACS サーバーを使用した X.509 証明書ベースの SSH 認証の設定

Cisco NX-OS リリース 10.4(3)F 以降では、Cisco Nexus スイッチの TACACS+ サーバーを使用して、x509v3 証明書の SSH ベースの認証を設定できます。

TACACS+ サーバーを使用して X.509 証明書ベースの SSH 認証を設定するには、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 例 : <pre>switch# configure terminal switch(config)#</pre>	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 authorization ssh-certificate default group tacacs-group-name 例 : <pre>switch(config)# aaa authorization ssh-certificate default group tac</pre>	TACACS+ サーバーのデフォルトの AAA 許可方式を設定します。 ssh-certificate キーワードは、証明書認証を使用した TACACS 許可またはローカル許可を構成します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。

	コマンドまたはアクション	目的
		(注) • aaa group server tacacs+ <i>tacacs-group-name</i> コマンドを使用して、TACACS サーバー構成で <i>tacacs-group-name</i> が構成されていることを確認します。 • SSH 証明書ベースの認証をサポートするには、暗号トラストポイントを設定し、ルート CA をインストールします。詳細については、PKI の設定 (207 ページ) のセクションを参照してください。
ステップ 3	exit 例 : <pre>switch(config)# exit switch#</pre>	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 4	(任意) show aaa authorization [all] 例 : <pre>switch# show aaa authorization</pre>	AAA 許可設定を表示します。 all キーワードを指定すると、デフォルト値が表示されます。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

権限ロールのユーザ コマンドの許可または拒否

ネットワーク管理者は、権限ロールを変更して、ユーザが特定のコマンドを実行できるようにしたり実行できなくなったりすることができます。

権限ロールのルールを変更する場合は、次の注意事項に従う必要があります。

- priv-14 ロールと priv-15 ロールは変更できません。
- 拒否ルールは priv-0 ロールにだけ追加できます。
- priv-0 ロールでは以下のコマンドは常に許可されます。**configure**、**copy**、**dir**、**enable**、**ping**、**show**、**ssh**、**telnet**、**terminal**、**traceroute**、**end**、**exit**。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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] role name priv-<i>n</i> Example: switch(config)# role name priv-5 switch(config-role)#	権限ロールをイネーブルまたはディセーブルにして、ロール コンフィギュレーション モードを開始します。 <i>n</i> 引数には、特権レベルを 0 ～ 13 の数値で指定します。
ステップ 3	rule number {deny permit} command command-string Example: switch(config-role)# rule 2 permit command pwd	権限ロールのユーザ コマンド ルールを設定します。これらのルールで、ユーザによる特定のコマンドの実行を許可または拒否します。ロールごとに最大 256 のルールを設定できます。ルール番号によって、ルールが適用される順序が決まります。ルールは降順で適用されます。たとえば、1 つのロールが 3 つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。 <i>command-string</i> 引数には、空白スペースを含めることができます。 Note 必要な規則の数だけこのコマンドを繰り返します。
ステップ 4	exit Example: switch(config-role)# exit switch(config)#	ロール コンフィギュレーション モードを終了します。
ステップ 5	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[ユーザ ロールおよびルールの作成](#) (288 ページ)

TACACS+ サーバまたはサーバグループの手動モニタリング

TACACS+ サーバまたはサーバグループに、手動でテストメッセージを送信できます。

Before you begin

TACACS+ をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	test aaa server tacacs+ {ipv4-address ipv6-address hostname} [vrf vrf-name] username password Example: <pre>switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH</pre>	TACACS+ サーバにテストメッセージを送信して可用性を確認します。
ステップ 2	test aaa group group-name username password Example: <pre>switch# test aaa group TacGroup user2 As3He3CI</pre>	TACACS+ サーバグループにテストメッセージを送信して可用性を確認します。

Related Topics

[TACACS+ サーバホストの設定](#) (109 ページ)

[TACACS+ サーバグループの設定](#) (113 ページ)

TACACS+ のディセーブル化

TACACS+ をディセーブルにできます。



Caution

TACACS+ をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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。

	Command or Action	Purpose
ステップ 2	no feature tacacs+ Example: <pre>switch(config)# no feature tacacs+</pre>	TACACS+ をディセーブルにします。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバのモニタリング

Cisco NX-OS デバイスが保持している TACACS+ サーバのアクティビティに関する統計情報をモニタできます。

Before you begin

Cisco NX-OS デバイスの TACACS+ サーバを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	show tacacs-server statistics {hostname ipv4-address ipv6-address} Example: <pre>switch# show tacacs-server statistics 10.10.1.1</pre>	TACACS+ 統計情報を表示します。

Related Topics

[TACACS+ サーバ ホストの設定](#) (109 ページ)

[TACACS+ サーバ統計情報のクリア](#) (133 ページ)

TACACS+ サーバ統計情報のクリア

Cisco NX-OS デバイスが保持している TACACS+ サーバのアクティビティに関する統計情報を表示します。

Before you begin

Cisco NX-OS デバイスの TACACS+ サーバを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	(Optional) show tacacs-server statistics {hostname ipv4-address ipv6-address} Example: switch# show tacacs-server statistics 10.10.1.1	Cisco NX-OS デバイスの TACACS+ サーバ統計情報を表示します。
ステップ 2	clear tacacs-server statistics {hostname ipv4-address ipv6-address} Example: switch# clear tacacs-server statistics 10.10.1.1	TACACS+ サーバ統計情報をクリアします。

Related Topics

[TACACS+ サーバ ホストの設定](#) (109 ページ)

TACACS+ の設定の確認

TACACS+ の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show tacacs+ { status pending pending-diff }	Cisco Fabric Services の TACACS+ 設定の配布状況と他の詳細事項を表示します。
show running-config tacacs [all]	実行コンフィギュレーションの TACACS+ 設定を表示します。
show startup-config tacacs	スタートアップ コンフィギュレーションの TACACS+ 設定を表示します。
show tacacs-server [host-name ipv4-address ipv6-address] [directed-request groups sorted statistics]	設定済みのすべての TACACS+ サーバのパラメータを表示します。

TACACS+ の設定例

次に、TACACS+ サーバ ホストおよびサーバ グループを設定する例を示します。

```
feature tacacs+
tacacs-server key 7 "ToIkLhPgG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
aaa group server tacacs+ TacServer
server 10.10.2.2
```

次に、コマンド許可検証を設定して使用する例を示します。

```
switch# terminal verify-only
switch# show interface ethernet 7/2 brief
%Success
switch# terminal no verify-only
switch# show interface ethernet 7/2 brief
```

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed	Port Ch #
Eth7/2	1	eth	access	down	SFP not inserted	auto (D)	--

次に、priv-5 以上のロールを持つすべてのユーザが **pwd** コマンドを実行できるようにする例を示します。

```
switch# configure terminal
switch(config)# role name priv-5
switch(config-role)# rule 1 permit command pwd
```

次に、priv-5 未満のロールを持つすべてのユーザが **show running-config** コマンドを実行できないようにする例を示します。まず、このコマンドを実行する権限を priv-0 ロールから削除する必要があります。次に、ロール **priv-5** でこのコマンドを許可し、priv-5 以上のロールを持つユーザにこのコマンドを実行する権限が付与されるようにする必要があります。

```
switch# configure terminal
switch(config)# role name priv-0
switch(config-role)# rule 2 deny command show running-config
switch(config-role)# exit
switch(config)# role name priv-5
switch(config-role)# rule 3 permit command show running-config
switch(config-role)# exit
```

TACACS+ Over TLS の構成

Cisco NX-OS リリース 10.6(1)F 以降、TACACS+ クライアントは、事前に指定されたポートで、TLS 対応 TACACS+ サーバーへの TCP 接続を開始できます。TCP 接続が確立されると、クライアントは TACACS+ データを送信する前に TLS ネゴシエーションを開始します。ピアは、

TLS 証明書を使用して相互に認証。各ピアでは、他のピアの証明書パスの検証（失効チェックを含む）を確認する必要があります。ピア証明書の検証が成功すると、接続が許可されます。

TLS 接続が確立されると、すべての TACACS+ データはスイッチの TACACS+ 構成に従って交換され、TLS 暗号化アプリケーションデータとして送信されます。TLS 接続は、TACACS+ 接続が閉じられるまでアクティブなままです。TLS エラーによって終了した場合、TACACS+ セッションは無効になります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	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	feature tacacs+ 例： <pre>switch(config)# feature tacacs+</pre>	TACACS+ をイネーブルにします。
ステップ 3	tacacs-server secure tls 例： <pre>switch(config)# tacacs-server secure tls</pre>	パラメータで構成されたすべての TACACS+ サーバーへの接続に対して TLS1.3 をグローバルにイネーブルにします。
ステップ 4	tacacs-server host tacacs-server-name port port-number 例： <pre>switch(config)# tacacs-server host 10.0.0.1 port 449</pre>	接続先の接続先 TACACS+ サーバーおよび TCP ポート番号を定義します。 TACACS+ サーバーが同じポートでリスンするように構成されていること。 TSL 接続の場合は、AAA サーバーで TACACS TLS 用に設定されたポートを使用します。
ステップ 5	tacacs-server host tacacs-server-name tls client-trustpoint trustpoint-name 例： <pre>switch(config)# tacacs-server host 10.0.0.1 tls client-trustpoint trusttplus</pre>	指定の TACACS+ サーバーで認証するときに使用するクライアント証明書を含む トラスト ポイントを指定します。
ステップ 6	aaa group server tacacs+ server-pool-name 例： <pre>switch(config)# aaa group server tacacs+ tac1</pre>	AAA TACACS+ サーバーのプールを定義します。

	コマンドまたはアクション	目的
ステップ 7	server tacacs-server-name 例 : switch(config-tacacs+) # server 10.0.0.1	定義したサーバーをAAA サーバー プールに追加します。
ステップ 8	use-vrf vrf-name 例 : switch(config-tacacs+) # use-vrf management	VRF メンバーを構成します。

TACACS+ Over TLS の構成の確認

TACACS+ over TLS 機能が有効されていることを確認するには、次のコマンドを使用します。

```
!Command: show running-config tacacs+
!Running configuration last done at: Wed Apr 23 00:21:38 2025
!Time: Wed Apr 23 00:21:43 2025

version 10.6(1) Bios:version 05.52
feature tacacs+

tacacs-server secure tls
tacacs-server host 10.0.0.1 port 449
tacacs-server host 10.0.0.1 tls client-trustpoint trusttplus
aaa group server tacacs+ tac1
    server 10.0.0.1
    use-vrf management
```

次の作業

これで、サーバグループも含めて AAA 認証方式を設定できるようになります。

TACACS+ に関する追加情報

ここでは、TACACS+ の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『Cisco NX-OS ライセンス ガイド』
VRF コンフィギュレーション	『Cisco NX-OS 9000 Series NX-OS Unicast Routing Configuration Guide』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
TACACS+に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 7 章

LDAP の設定

この章では、Cisco NX-OS デバイス上で Lightweight Directory Access Protocol (LDAP) を設定する方法について説明します。次の項が含まれています。

- [LDAP について \(139 ページ\)](#)
- [LDAP の前提条件 \(142 ページ\)](#)
- [LDAP の注意事項と制約事項 \(143 ページ\)](#)
- [LDAP のデフォルト設定 \(143 ページ\)](#)
- [LDAP の設定 \(144 ページ\)](#)
- [LDAP サーバのモニタリング \(159 ページ\)](#)
- [LDAP サーバ統計情報のクリア \(160 ページ\)](#)
- [LDAP 設定の確認 \(160 ページ\)](#)
- [LDAP の設定例 \(161 ページ\)](#)
- [次の作業 \(162 ページ\)](#)
- [LDAP に関する追加情報 \(162 ページ\)](#)

LDAP について

Lightweight Directory Access Protocol (LDAP) は、Cisco NX-OS デバイスにアクセスしようとするユーザの検証を集中的に行います。LDAP サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する LDAP デーモンのデータベースで管理されます。Cisco NX-OS デバイスに設定した LDAP 機能を使用可能にするには、LDAP サーバにアクセスして設定しておく必要があります。

LDAP では、認証と認可のファシリティが別々に提供されます。LDAP では、1 台のアクセスコントロールサーバ (LDAP デーモン) で各サービス認証と認可を個別に提供できます。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。

LDAP クライアント/サーバプロトコルでは、トランスポート要件を満たすために、TCP (ポート 389) を使用します。Cisco NX-OS デバイスは、LDAP プロトコルを使用して集中型の認証を行います。

LDAP 認証および許可

クライアントは、簡易バインド（ユーザ名とパスワード）を使用して LDAP サーバとの TCP 接続および認証セッションを確立します。許可プロセスの一環として、LDAP サーバはそのデータベースを検索し、ユーザ プロファイルやその他の情報を取得します。

バインドしてから検索する（認証を行ってから許可する）か、または検索してからバインドするように、バインド操作を設定できます。デフォルトでは、検索してからバインドする方式が使用されます。

検索してからバインドする方式の利点は、baseDN の前にユーザ名（cn 属性）を追加することで認定者名（DN）を形成するのではなく、検索結果で受け取った DN をバインディング時にユーザ DN として使用できることです。この方式は、ユーザ DN がユーザ名と baseDN の組み合わせとは異なる場合に特に役立ちます。ユーザ バインドのために、bindDN が baseDN + append-with-baseDN として構成されます。ここで、append-with-baseDN は cn=\$userid のデフォルト値です。



(注) バインド方式の代わりに、比較方式を使用して LDAP 認証を確立することもできます。比較方式では、サーバでユーザ入力の属性値を比較します。たとえば、ユーザパスワード属性を比較して認証を行うことができます。デフォルトのパスワード属性タイプは userPassword です。

ユーザ ログインにおける LDAP の動作

LDAP を使用する Cisco NX-OS デバイスに対して、ユーザがパスワード認証プロトコル（PAP）ログインを試みると、次の処理が行われます。

1. Cisco NX-OS デバイスは接続が確立されると、ユーザ名とパスワードを取得するために LDAP デーモンに接続します。
2. Cisco NX-OS デバイスは、最終的に LDAP デーモンから次のいずれかの応答を得ます。
 - **ACCEPT** : ユーザの認証に成功したので、サービスを開始します。Cisco NX-OS デバイスがユーザ許可を必要とする場合は、許可処理が始まります。
 - **REJECT** : ユーザ認証は失敗します。LDAP デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン操作を再試行するように要求します。
 - **ERROR** : デーモンによる認証サービスの途中でエラーが発生したか、またはデーモンと Cisco NX-OS デバイスの間のネットワーク接続でエラーが発生しました。Cisco NX-OS デバイスは ERROR 応答を受信した場合、別の方法でユーザの認証を試行します。

認証が終了し、Cisco NX-OS デバイスで許可がイネーブルになっていれば、続いてユーザの許可フェーズに入ります。LDAP 許可に進むには、まず LDAP 認証を正常に終了する必要があります。

3. LDAP 許可が必要な場合、Cisco NX-OS デバイスは再び LDAP デーモンに接続し、デーモンから ACCEPT または REJECT 応答が返されます。ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT

応答により、ユーザがアクセス可能なサービスが決まります。この場合のサービスは次のとおりです。

- Telnet、rlogin、ポイントツーポイントプロトコル（PPP）、シリアルラインインターネットプロトコル（SLIP）、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（IPv4 または IPv6）、アクセスリスト、ユーザタイムアウト）



(注) LDAP では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。通常、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、他の項目を求めることもできます。

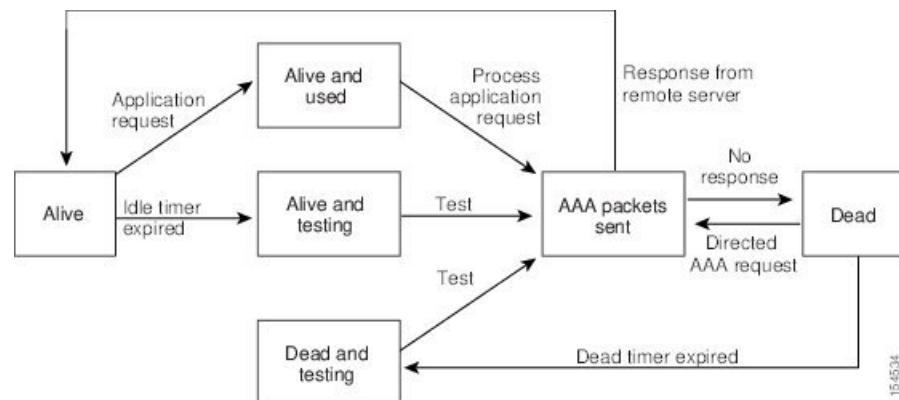


(注) LDAP では、認証の前に許可を行うことができます。

LDAP サーバのモニタリング

応答を返さない LDAP サーバがあると、AAA 要求の処理に遅延が発生することがあります。AAA 要求の処理時間を短縮するために、LDAP サーバを定期的にモニタして LDAP サーバが応答している（アライブ）かどうかを調べることができます。Cisco NX-OS デバイスは、応答の遅い LDAP サーバをデッド（dead）としてマークし、デッド LDAP サーバには AAA 要求を送信しません。Cisco NX-OS デバイスはデッド LDAP サーバを定期的にモニタし、応答があればアライブ状態に戻します。このモニタリングプロセスでは、実際の AAA 要求が送信される前に、LDAP サーバが稼働状態であることを確認します。LDAP サーバがデッドまたはアライブの状態が変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco NX-OS デバイスは、パフォーマンスに影響が出る前に、障害が発生していることをエラーメッセージで表示します。次の図に、LDAP サーバモニタリングのサーバの状態を示します。

図 5: LDAP サーバの状態





- (注) 稼働中のサーバと停止中のサーバのモニタリング間隔はそれぞれ別で、ユーザが設定できません。LDAP サーバ モニタリングを実行するには、テスト認証要求を LDAP サーバに送信します。

LDAP のベンダー固有属性

Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) ドラフト標準には、ネットワーク アクセス サーバと LDAP サーバ間での Vendor-Specific Attribute (VSA; ベンダー固有属性) の通信方法が規定されています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、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。

LDAP 用の Cisco VSA 形式

シスコの LDAP 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダータイプは 1 (名前付き `cisco-av-pair`) です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

`protocol` は、特定の許可タイプを表すシスコの属性です。`separator` は、必須属性の場合は `=` (等号)、オプションの属性の場合は `*` (アスタリスク) です。Cisco NX-OS デバイス上の認証に LDAP サーバを使用した場合、LDAP では LDAP サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。この許可情報は、VSA で指定されます。Cisco NX-OS ソフトウェアでは、次の VSA プロトコル オプションをサポートしています。

- `shell` : ユーザ プロファイル情報を提供する `access-accept` パケットで使用するプロトコル。

Cisco NX-OS ソフトウェアは、次の属性をサポートしています。

- `roles` : ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。

LDAP のバーチャライゼーション サポート

Cisco NX-OS デバイスは、仮想ルーティング/転送 (VRF) インスタンスを使用して LDAP サーバにアクセスします。VRF の詳細情報については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

LDAP の前提条件

LDAP の前提条件は次のとおりです。

- LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得すること
- Cisco NX-OS デバイスが AAA サーバの LDAP クライアントとして設定されていること

LDAP の注意事項と制約事項

LDAP に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイス上には最大 64 の LDAP サーバを設定できます。
- Cisco NX-OS は LDAP バージョン 3 だけをサポートします。
- Cisco NX-OS は次の LDAP サーバだけをサポートします。
 - OpenLDAP
 - Microsoft Active Directory
- Secure Sockets Layer (SSL) 上の LDAP は、SSL バージョン 3 および Transport Layer Security (TLS) バージョン 1.2 のみをサポートします。
- Cisco NX-OS リリース 10.4(3)F 以降、Secure Sockets Layer (SSL) を介した LDAP は、Cisco Nexus スイッチで TLS バージョン 1.3 および 1.2 をサポートします。TLS v1.1 は廃止されました。
- LDAP over SSL の場合、LDAP クライアント設定では、LDAP サーバ証明書のサブジェクトとしてホスト名を含める必要があります。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- Cisco NX-OS リリース 10.3(1)F 以降、LDAP は Cisco Nexus 9808 スイッチでサポートされます。
 - Cisco NX-OS リリース 10.4(1)F 以降、LDAP は、Cisco Nexus X98900CD-A および X9836DM-A ラインカードを搭載した Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、LDAP は Cisco Nexus 9804 スイッチ、Cisco Nexus X98900CD-A および X9836DM-A ラインカードでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、構成の置換機能は Cisco NX-OS デバイスの LDAP でサポートされます。

LDAP のデフォルト設定

次の表に、LDAP パラメータのデフォルト設定を示します。

パラメータ	デフォルト
LDAP	ディセーブル

パラメータ	デフォルト
LDAP 認証方式	検索してからバインド
LDAP 認証メカニズム	プレーン
デッドタイム間隔	0 分
タイムアウト間隔	5 秒
アイドル タイマー間隔	60 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	Cisco

LDAP の設定

ここでは、Cisco NX-OS デバイスで LDAP を設定する手順を説明します。

LDAP サーバの設定プロセス

process_workflow

次の設定プロセスに従って、LDAP サーバを設定できます。

1. LDAP をイネーブルにします。
2. LDAP サーバと Cisco NX-OS デバイスの接続を確立します。
3. 必要に応じて、AAA 認証方式用に、LDAP サーバのサブセットを使用して LDAP サーバグループを設定します。
4. (任意) TCP ポートを設定します。
5. (任意) LDAP サーバにデフォルト AAA 認証方式を設定します。
6. (任意) LDAP 検索マップを設定します。
7. (任意) 必要に応じて、LDAP サーバの定期モニタリングを設定します。

関連トピック

- [LDAP 機能の有効化](#) (145 ページ)
- [LDAP サーバー ホストの構成](#) (146 ページ)
- [LDAP サーバの rootDN の設定](#) (147 ページ)
- [LDAP サーバグループの設定](#) (148 ページ)
- [TCP ポートの設定](#) (152 ページ)
- [LDAP 検索マップの構成](#) (153 ページ)

[LDAP サーバの定期的モニタリングの設定](#) (154 ページ)

LDAP 機能の有効化

LDAP は最初は NX-OS デバイス上で無効です。認証に関するコンフィギュレーション コマンドと検証コマンドを使用するには、LDAP 機能を明示的に有効にする必要があります。

LDAP 機能を有効にするには、次の手順を実行します。

手順

ステップ 1 **configure terminal** コマンドでグローバル コンフィギュレーション モードに入ります。

例：

```
switch# configure terminal
```

ステップ 2 **feature ldap** コマンドで LDAP を有効にします。これを無効化するには、このコマンドの **no** 形式を入力します。

例：

```
switch(config)# feature ldap
```

(注)

LDAP を無効化にすると、関連するすべての構成が削除されます。

ステップ 3 **copy running-config startup-config** で実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

例：

```
switch(config)# copy running-config startup-config
```

LDAP 機能が有効になり、認証コンフィギュレーション コマンドが利用可能になります。

関連トピック

[LDAP サーバの設定プロセス](#) (144 ページ)

[LDAP サーバー ホストの構成](#) (146 ページ)

[LDAP サーバの rootDN の設定](#) (147 ページ)

[LDAP サーバ グループの設定](#) (148 ページ)

[グローバルな LDAP タイムアウト間隔の設定](#) (150 ページ)

[LDAP サーバのタイムアウト間隔の設定](#) (151 ページ)

[TCP ポートの設定](#) (152 ページ)

[LDAP 検索マップの構成](#) (153 ページ)

[LDAP サーバの定期的モニタリングの設定](#) (154 ページ)

[LDAP デッド タイム間隔の設定](#) (155 ページ)

[LDAP サーバでの AAA 許可の設定](#) (156 ページ)

LDAP サーバー ホストの構成

Cisco NX-OS デバイスがユーザー認証を目的としてリモート LDAP サーバーにアクセスできるように、LDAP サーバー ホストを構成します。LDAP サーバーの IP またはホスト名を追加し、必要に応じてセキュアな通信のために SSL を有効にするには、次の手順を活用します。



(注) デフォルトでは、LDAP サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスで設定すると、LDAP サーバがデフォルトの LDAP サーバグループに追加されます。LDAP サーバを別の LDAP サーバグループに追加することもできます。

LDAP サーバー ホストを構成するには、次の手順を実行します：

始める前に

- デバイスの LDAP を有効にします。
- LDAP サーバーの IPv4 または IPv6 アドレスまたはホスト名を取得します。
- SSL を有効にする場合は、デバイスで LDAP サーバー証明書が手動で構成されていることを確認します。

手順

ステップ 1 **configure terminal** コマンドを使用して、グローバル構成モードを開始します。。

例：

```
switch# configure terminal
switch(config)#
```

ステップ 2 次のコマンドを使用して、LDAP サーバーの IP アドレスまたはホスト名を指定します：

ldap-server host。

- オプションで、**enable-ssl** キーワードを使用して通信を暗号化します。
- オプションで、**referral-disable** キーワードを使用して参照リンクを無効にします。

例：

```
switch(config)# switch(config)# ldap-server host 10.10.2.2 enable-ssl
```

ステップ 3 (オプション) **show ldap-server** を使用して LDAP サーバーの構成を確認します。 コマンドを使用します。

例：

```
switch(config)# show ldap-server
```


ステップ 4 `copy running-config startup-config` コマンドを使用して構成を保存します。

例 :

```
switch(config)# copy running-config startup-config
```

LDAP サーバー ホストが構成され、認証操作を行える状態になっています。

関連トピック

- [LDAP サーバの設定プロセス](#) (144 ページ)
- [LDAP 機能の有効化](#) (145 ページ)
- [LDAP サーバ グループの設定](#) (148 ページ)
- [LDAP サーバの rootDN の設定](#) (147 ページ)
- [LDAP サーバ グループの設定](#) (148 ページ)
- [LDAP サーバの定期的モニタリングの設定](#) (154 ページ)
- [LDAP サーバのモニタリング](#) (159 ページ)
- [LDAP サーバ統計情報のクリア](#) (160 ページ)

LDAP サーバの rootDN の設定

LDAP サーバデータベースのルート指定名 (DN) を設定できます。rootDN は、LDAP サーバにバインドしてそのサーバの状態を確認するために使用します。

始める前に

LDAP を有効にします。

リモートの LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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] ldap-server host {ipv4-address ipv6-address hostname} rootDN root-name [password password [port tcp-port [timeout seconds] timeout seconds]] 例 : <pre>switch(config)# ldap-server host 10.10.1.1 rootDN cn=manager,dc=acme,dc=com password Ur2Gd2BH timeout 60</pre>	LDAP サーバデータベースの rootDN を指定し、ルートのパスワードをバインドします。 任意で、サーバに送る LDAP メッセージに使用する TCP ポートを指定します。有効な範囲は 1 ～ 65535 です。デフォルトの TCP ポートはグローバル値です (グローバル値が設定されていない場合は

	コマンドまたはアクション	目的
		389)。また、サーバのタイムアウト間隔も指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。
ステップ 3	(任意) show ldap-server 例： switch(config)# show ldap-server	LDAP サーバの設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

[LDAP サーバの設定プロセス](#) (144 ページ)

[LDAP 機能の有効化](#) (145 ページ)

[LDAP サーバ ホストの構成](#) (146 ページ)

LDAP サーバグループの設定

サーバグループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバはすべて、LDAP を使用するよう設定する必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバグループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

Before you begin

LDAP を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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] aaa group server ldap group-name Example:	LDAP サーバグループを作成し、そのグループの LDAP サーバグループ コ

	Command or Action	Purpose
	<pre>switch(config)# aaa group server ldap LDAPServer1 switch(config-ldap)#</pre>	イ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] server {<i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i>} Example: <pre>switch(config-ldap)# server 10.10.2.2</pre>	LDAP サーバを、LDAP サーバグループのメンバとして設定します。 指定した LDAP サーバが見つからなかった場合は、ldap-server host コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	(Optional) [no] authentication {bind-first append-with-baseDN <i>DNstring</i> compare [password-attribute <i>password</i>]} Example: <pre>switch(config-ldap)# authentication compare password-attribute TyuL8r</pre>	バインド方式または比較方式を使用して LDAP 認証を実行します。デフォルトの LDAP 認証方式は、検索してからバインドするバインド方式です。
ステップ 5	(Optional) [no] enable user-server-group Example: <pre>switch(config-ldap)# enable user-server-group</pre>	グループ検証を有効にします。LDAP サーバでグループ名を設定する必要があります。ユーザは、ユーザ名が LDAP サーバで設定されたこのグループのメンバとして示されている場合にだけ、公開キー認証を通じてログインできます。
ステップ 6	(Optional) [no] enable Cert-DN-match Example: <pre>switch(config-ldap)# enable Cert-DN-match</pre>	ユーザプロファイルでユーザ証明書のサブジェクト DN がログイン可能と示されている場合にだけユーザがログインできるようにします。
ステップ 7	(Optional) no [use-vrf <i>vrf-name</i>] Example: <pre>switch(config-ldap)# use-vrf vrf1</pre>	サーバグループ内のサーバとの接続に使用する VRF を指定します。
ステップ 8	exit Example: <pre>switch(config-ldap)# exit switch(config)#</pre>	LDAP サーバグループ コンフィギュレーション モードを終了します。
ステップ 9	(Optional) show ldap-server groups Example: <pre>switch(config)# show ldap-server groups</pre>	LDAP サーバグループの設定を表示します。

	Command or Action	Purpose
ステップ 10	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Related Topics

[LDAP サーバの設定プロセス](#) (144 ページ)

[LDAP サーバー ホストの構成](#) (146 ページ)

[LDAP 機能の有効化](#) (145 ページ)

[LDAP サーバー ホストの構成](#) (146 ページ)

グローバルな LDAP タイムアウト間隔の設定

Cisco NX-OS デバイスがすべての LDAP サーバからの応答を待つ時間を決定するグローバル タイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

始める前に

LDAP 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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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] ldap-server timeout seconds 例 : <pre>switch(config)# ldap-server timeout 10</pre>	LDAP サーバのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。
ステップ 3	(任意) show ldap-server 例 : <pre>switch(config)# show ldap-server</pre>	LDAP サーバの設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

[LDAP 機能の有効化](#) (145 ページ)[LDAP サーバのタイムアウト間隔の設定](#) (151 ページ)[LDAP サーバのタイムアウト間隔の設定](#) (151 ページ)

LDAP サーバのタイムアウト間隔の設定

Cisco NX-OS デバイスが LDAP サーバからの応答を待つ時間を決定するタイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

始める前に

LDAP 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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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] ldap-server host {ipv4-address ipv6-address hostname} timeout seconds 例 : <pre>switch(config)# ldap-server host server1 timeout 10</pre>	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 (注) 特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。
ステップ 3	(任意) show ldap-server 例 : <pre>switch(config)# show ldap-server</pre>	LDAP サーバの設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

[グローバルな LDAP タイムアウト間隔の設定](#) (150 ページ)

[LDAP 機能の有効化](#) (145 ページ)

[グローバルな LDAP タイムアウト間隔の設定](#) (150 ページ)

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、LDAPサーバ用に別のTCPポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての LDAP 要求に対しポート 389 を使用します。

始める前に

LDAP 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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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] ldap-server host {ipv4-address ipv6-address hostname} port tcp-port [timeout seconds] 例 : <pre>switch(config)# ldap-server host 10.10.1.1 port 200 timeout 5</pre>	サーバに送る LDAP メッセージに使用する TCP ポートを指定します。デフォルトの TCP ポートは 389 です。有効な範囲は 1 ～ 65535 です。 任意でサーバのタイムアウト間隔を指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。 （注） 特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。
ステップ 3	（任意） show ldap-server 例 : <pre>switch(config)# show ldap-server</pre>	LDAP サーバの設定を表示します。
ステップ 4	（任意） copy running-config startup-config 例 :	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
	<code>switch(config)# copy running-config startup-config</code>	

関連トピック

[LDAP サーバの設定プロセス](#) (144 ページ)

[LDAP 機能の有効化](#) (145 ページ)

LDAP 検索マップの構成

検索クエリーを LDAP サーバーに送信するように LDAP 検索マップを構成できます。サーバはそのデータベースで、検索マップで指定された基準を満たすデータを検索します。

始める前に

LDAP 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	configure terminal 例 : <code>switch# configure terminal</code> <code>switch(config)#</code>	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	ldap search-map map-name 例 : <code>switch(config)# ldap search-map map1</code> <code>switch(config-ldap-search-map)#</code>	LDAP 検索マップを設定します。
ステップ 3	(任意) [userprofile trustedCert CRLLookup user-certdn-match user-pubkey-match user-switch-bind] attribute-name attribute-name search-filter filter base-DN base-DN-name 例 : <code>switch(config-ldap-search-map)#</code> <code>userprofile attribute-name att-name</code> <code>search-filter</code> <code>(&(objectClass=inetOrgPerson)(cn=\$userid))</code> <code>base-DN dc=acme,dc=com</code>	ユーザ プロファイル、信頼できる証明書、CRL、証明書 DN 一致、公開キー一致、または user-switchgroup ルックアップ検索操作の属性名、検索フィルタ、およびベース DN を設定します。これらの値は、検索クエリーを LDAP サーバに送信するために使用されます。 <i>Attribute-name</i> 引数は Nexus ロール定義を含む LDAP サーバ属性の名前です。
ステップ 4	(任意) exit 例 : <code>switch(config-ldap-search-map)# exit</code> <code>switch(config)#</code>	LDAP 検索マップ 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	(任意) show ldap-search-map 例 : switch(config)# show ldap-search-map	設定された LDAP 検索マップを表示します。
ステップ 6	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

[LDAP サーバの設定プロセス \(144 ページ\)](#)[LDAP 機能の有効化 \(145 ページ\)](#)

LDAP サーバの定期的モニタリングの設定

LDAP サーバの可用性をモニタリングできます。設定パラメータには、サーバに対して使用するユーザ名とパスワード、サーバにバインドして状態を確認するための rootDN、およびアイドル タイマーがあります。アイドル タイマーには、LDAP サーバで何の要求も受信されない状態の時間を指定します。これを過ぎると Cisco NX-OS デバイスはテスト パケットを送信します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。



(注) ネットワークのセキュリティを保護するために、LDAP データベースの既存のユーザ名と同じものを使用しないことを推奨します。

始める前に

LDAP 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	configure terminal 例 : switch# configure terminal switch(config)#	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	必須: [no] ldap-server host {ipv4-address ipv6-address hostname} test rootDN root-name [idle-time minutes password	サーバ モニタリング用のパラメータを指定します。デフォルトのユーザ名は

	コマンドまたはアクション	目的
	<code>password [idle-time minutes] username name [password password [idle-time minutes]]]</code> 例 : <pre>switch(config)# ldap-server host 10.10.1.1 test rootDN root1 username user1 password Ur2Gd2BH idle-time 3</pre>	test、デフォルトのパスワードは Cisco です。アイドル タイマーのデフォルト値は 60 分です。有効な範囲は 1 ～ 1,440 分です。 (注) LDAP サーバデータベースの既存のユーザでないユーザを指定することを推奨します。
ステップ 3	<code>[no] ldap-server deadtime minutes</code> 例 : <pre>switch(config)# ldap-server deadtime 5</pre>	以前に応答の遅かった LDAP サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。デフォルト値は 0 分です。そして、有効な範囲は 0 ～ 60 分です。
ステップ 4	(任意) <code>show ldap-server</code> 例 : <pre>switch(config)# show ldap-server</pre>	LDAP サーバの設定を表示します。
ステップ 5	(任意) <code>copy running-config startup-config</code> 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

[LDAP サーバの設定プロセス](#) (144 ページ)

[LDAP 機能の有効化](#) (145 ページ)

[LDAP サーバー ホストの構成](#) (146 ページ)

LDAP デッド タイム間隔の設定

すべての LDAP サーバのデッド タイム間隔を設定できます。デッド タイム間隔では、Cisco NX-OS デバイスが LDAP サーバをデッドであると宣言した後、そのサーバがアライブになったかどうかを確認するためにテスト パケットを送信するまでの時間を指定します。



(注) デッド タイム間隔に 0 分を設定すると、LDAP サーバは、応答を返さない場合でも、デッドとしてマークされません。デッド タイム間隔はグループ単位で設定できます。

始める前に

LDAP 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	configure terminal 例 : switch# configure terminal switch(config)#	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] ldap-server deadtime minutes 例 : switch(config)# ldap-server deadtime 5	グローバルなデッド タイム間隔を設定します。デフォルト値は0分です。範囲は 0 ～ 60 分です。
ステップ 3	(任意) show ldap-server 例 : switch(config)# show ldap-server	LDAP サーバの設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

[LDAP 機能の有効化](#) (145 ページ)

LDAP サーバでの AAA 許可の設定

LDAP サーバのデフォルトの AAA 許可方式を設定できます。

始める前に

LDAP を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 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
	switch# configure terminal switch(config)#	
ステップ 2	aaa authorization {ssh-certificate ssh-publickey} default {group group-list local} 例 : <pre>switch(config)# aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2</pre>	LDAP サーバのデフォルトの AAA 許可方式を設定します。 ssh-certificate キーワードは証明書認証を使用した LDAP 許可またはローカル許可を設定し、ssh-publickey キーワードは SSH 公開キーを使用した LDAP 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。 <i>group-list</i> 引数には、LDAP サーバグループ名をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。local 方式はローカルデータベースを使用して許可を行います。
ステップ 3	(任意) show aaa authorization [all] 例 : <pre>switch(config)# show aaa authorization</pre>	AAA 許可設定を表示します。 all キーワードを指定すると、デフォルト値が表示されます。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

[LDAP 機能の有効化](#) (145 ページ)

LDAP SSH 公開キー認証の設定

AAA 認証は、LDAP サーバのユーザーエントリに保存されているユーザーの公開キーを使用して、LDAP サーバを介して実行されます。

LDAP SSH 公開キー認証を設定する前に、次の点を考慮したことを確認してください。

- ユーザーの公開キーをユーザー属性として LDAP サーバに保存します。
- SSH クライアントからの秘密キーを使用してサインインします。



- (注) SSH サインイン時に提示した秘密キーは、LDAP サーバーに保存されている公開キーを使用して検証されます。

次の例は、サンプルの LDAP クライアントの設定を示しています。

次の例では、ユーザーの公開キーが、**user-pubkey-match** 構成で指定された属性（以下の場合には **sshPublicKeys** 属性）で LDAP サーバーに保存されます。

```
ldap-server host fully qualified domain name.com rootDN
"CN=ucsadmin1,CN=Users,DC=PI-Sec-DT,DC=com" password 7 password1
ldap search-map Map1
  userprofile attribute-name "description" search-filter "(cn=$userid)" base-DN
  "DC=PI-Sec-DT,DC=com"
  user-pubkey-match attribute-name "sshPublicKeys" search-filter "(cn=$userid)" base-DN
  "DC=PI-Sec-DT,DC=com"
aaa group server ldap ldap1
  server fully qualified domain name.com
  use-vrf management
  ldap-search-map Map1

aaa authorization ssh-publickey default group ldap1
```

次に、ユーザの SSH クライアント秘密キーを使用して、スイッチ管理 IP アドレスにサインインする例を示します。

```
ssh ldapuser@10.0.0.1 -i ldap_pub_key_test
```

LDAP SSH 証明書許可の設定

AAA 許可は、LDAP サーバーのユーザー属性に保存されている証明書と証明書の DN を使用して、LDAP サーバーを介して実行されます。

LDAP SSH 証明書の許可中に、次のことが処理されます。

- スイッチにインストールされている CA 証明書を使用して、SSH クライアントを介して提示されたユーザー証明書の検証。
- **enable cert-dn-match** 設定はデフォルトで有効になっているため、証明書を検証するための、LDAP サーバーに保存されている DN との **cert-DN-match** は、自動的に処理されます。

次の例は、サンプルの LDAP クライアントの設定を示しています。

- 次の例は、**user-certdn-match** 構成で指定された特定の属性の下で LDAP サーバーに証明書 DN を保存する方法を示しています。

形式は「x509v3-sign-rsa DN /DC=com, DC=PI-Sec-DT, CN=Users, CN=username1」です。

```
ldap-server host fully qualified domain name.com rootDN
"CN=ucsadmin1,CN=Users,DC=PI-Sec-DT,DC=com" password 7 password1
ldap search-map Map24
  userprofile attribute-name "description" search-filter "(cn=$userid)" base-DN
  "DC=PI-Sec-DT,DC=com"
  user-certdn-match attribute-name <attribute> search-filter "(cn=$userid)" base-DN
  "DC=PI-Sec-DT,DC=com"
```

```
aaa group server ldap ldap24
  server fully qualified domain name.com
  enable Cert-DN-match
  use-vrf management
  ldap-search-map Map24
```

```
aaa authorization ssh-certificate default group ldap24
```

- 次の show コマンドは、ボックスにインストールされている rootCA 証明書の詳細を表示します。

```
switch# show crypto ca certificates
Trustpoint: ldap
CA certificate 0:
subject=C = IN, ST = KAR, L = BGL, O = Cisco, OU = DCBG-Cert, CN = RootCA
issuer=C = IN, ST = KAR, L = BGL, O = Cisco, OU = DCBG-Cert, CN = RootCA
serial=82EE7603BF7E74A9
notBefore=May 29 07:12:30 2023 GMT
notAfter=May 26 07:12:30 2033 GMT
SHA1 Fingerprint=D5:AE:75:8E:A1:4F:79:1E:80:3E:5E:67:C5:42:44:10:13:C6:F7:1D
purposes: sslserver sslclient
```

```
n7700-DE#
```

- 次の例は、SSH クライアントからユーザー サインインを実行する方法を示しています。
 - SSHクライアントでは、入力証明書には秘密キーとユーザー証明書の両方が含まれており、結合されて「<user>.crt」という単一のファイルになっています。
 - rootCA.crt は rootCA 証明書ファイルです。
 - IP アドレスはスイッチの管理 IP アドレスです。

```
ssh username1@10.0.0.1 -i username1.crt -vvv -oCACertificateFile=rootCA.crt
```

LDAP サーバのモニタリング

Cisco NX-OS デバイスが保持している LDAP サーバのアクティビティに関する統計情報をモニタリングできます。

始める前に

Cisco NX-OS デバイスに LDAP サーバを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	show ldap-server statistics {hostname ipv4-address ipv6-address} 例 : <pre>switch# show ldap-server statistics 10.10.1.1</pre>	LDAP サーバの統計情報を表示します。

関連トピック

[LDAP サーバー ホストの構成](#) (146 ページ)

[LDAP サーバ統計情報のクリア](#) (160 ページ)

[LDAP サーバ統計情報のクリア](#) (160 ページ)

LDAP サーバ統計情報のクリア

Cisco NX-OS デバイスが保持している LDAP サーバのアクティビティに関する統計情報を表示します。

始める前に

Cisco NX-OS デバイスに LDAP サーバを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	(任意) show ldap-server statistics {hostname ipv4-address ipv6-address} 例 : <pre>switch# show ldap-server statistics 10.10.1.1</pre>	LDAP サーバの統計情報を表示します。
ステップ 2	clear ldap-server statistics {hostname ipv4-address ipv6-address} 例 : <pre>switch# clear ldap-server statistics 10.10.1.1</pre>	LDAP サーバ統計情報をクリアします。

関連トピック

[LDAP サーバのモニタリング](#) (159 ページ)

[LDAP サーバー ホストの構成](#) (146 ページ)

[LDAP サーバのモニタリング](#) (159 ページ)

LDAP 設定の確認

LDAP 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show running-config ldap [all]	実行コンフィギュレーションの LDAP 設定を表示します。

コマンド	目的
show startup-config ldap	スタートアップコンフィギュレーションの LDAP 設定を表示します。
show ldap-server	LDAP 設定情報を表示します。
show ldap-server groups	LDAP サーバグループの設定情報を表示します。
show ldap-server statistics {hostname ipv4-address ipv6-address}	LDAP 統計情報を表示します。
show ldap-search-map	設定されている LDAP 属性マップに関する情報を表示します。

LDAP の設定例

次に、LDAP サーバ ホストおよびサーバ グループを設定する例を示します。

```
feature ldap
ldap-server host 10.10.2.2 enable-ssl
aaa group server ldap LdapServer
server 10.10.2.2
exit
show ldap-server
show ldap-server groups
```

次に、LDAP 検索マップを設定する例を示します。

```
ldap search-map s0
userprofile attribute-name att-name search-filter "
(&(objectClass=Person)(sAMAccountName=$userid))" base-DN dc=acme,dc=com
exit
show ldap-search-map
```

次に、LDAP サーバに対する証明書認証を使用して AAA 許可を設定する例を示します。

```
aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
exit
show aaa authorization
```

次の例は、認証を検証する方法を示しています。

```
failing
test aaa group LdapServer user <user-password>
user has failed authentication

! working
test aaa group LdapServer user <user-password>
user has been authenticated
```

次の作業

これで、サーバグループも含めて AAA 認証方式を設定できるようになります。

LDAP に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『Cisco NX-OS ライセンス ガイド』
VRF コンフィギュレーション	『Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング設定ガイド』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
LDAPに関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 8 章

SSH および Telnet の設定

この章では、Cisco NX-OS デバイス上でセキュア シェル（SSH）プロトコルおよび Telnet を設定する手順について説明します。

この章は、次の項で構成されています。

- [SSH および Telnet について, on page 163](#)
- [SSH および Telnet の前提条件, on page 172](#)
- [SSH と Telnet のガイドラインと制約事項（172 ページ）](#)
- [SSH および Telnet のデフォルト設定, on page 174](#)
- [SSH の設定, on page 175](#)
- [Telnet の設定, on page 197](#)
- [SSH および Telnet の設定の確認, on page 199](#)
- [SSH の設定例, on page 200](#)
- [SSH のパスワードが不要なファイル コピーの設定例, on page 202](#)
- [X.509v3 証明書ベースの SSH 認証の設定例（203 ページ）](#)
- [SSH および Telnet に関する追加情報, on page 204](#)

SSH および Telnet について

ここでは、SSH および Telnet について説明します。

SSH サーバー

SSH サーバを使用すると、SSH クライアントは Cisco NX-OS デバイスとの間でセキュアな暗号化された接続を確立できます。SSH は強化暗号化を使用して認証を行います。Cisco NX-OS ソフトウェアの SSH サーバは、市販の一般的な SSH クライアントと相互運用ができます。

SSH がサポートするユーザ認証メカニズムには、Remote Authentication Dial-In User Service（RADIUS）、TACACS+、LDAP、およびローカルに格納されたユーザ名とパスワードを使用した認証があります。

SSH クライアント

SSH クライアントは、SSH プロトコルで稼働しデバイス認証および暗号化を提供するアプリケーションです。Cisco NX-OS デバイスは、SSH クライアントを使用して、別の Cisco NX-OS デバイスまたは SSH サーバの稼働する他のデバイスとの間で暗号化された安全な接続を確立できます。この接続は、暗号化されたアウトバウンド接続を実現します。認証と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

Cisco NX-OS ソフトウェアの SSH クライアントは、無償あるいは商用の SSH サーバと関係して動作します。

SSH サーバキー

SSH では、Cisco NX-OS とのセキュアな通信を行うためにサーバキーが必要です。SSH サーバキーは、次の SSH オプションに使用できます。

- Rivest, Shamir, and Adelman (RSA) 公開キー暗号化を使用した SSH バージョン 2
- Digital System Algorithm (DSA) を使用した SSH バージョン 2
- 楕円曲線デジタル署名アルゴリズム (ECDSA) を使用した SSH バージョン 2

SSH サービスをイネーブルにする前に、適切なバージョンの SSH サーバキーペアを取得してください。使用中の SSH クライアントバージョンに応じて、SSH サーバキーペアを生成します。SSH サービスでは、SSH バージョン 2 に対応する以下の 2 通りのキーペアを使用できます。

- **dsa** オプションでは、SSH バージョン 2 プロトコル用の DSA キーペアを作成します。
- **rsa** オプションでは、SSH バージョン 2 プロトコル用の RSA キーペアを作成します。
- **ecdsa** オプションでは、SSH バージョン 2 プロトコル用の ECDSA キーペアを作成します。

デフォルトでは、Cisco NX-OS ソフトウェアは 1024 ビットの RSA キーを生成します。

SSH は、次の公開キー形式をサポートします。

- OpenSSH
- IETF SSH (SECSH)
- Privacy-Enhanced Mail (PEM) の公開キー証明書

**Caution**

SSH キーをすべて削除すると、SSH サービスを開始できません。

デジタル証明書を使用した SSH 認証

Cisco NX-OS デバイスでの SSH 認証では、ホスト認証用に X.509 デジタル証明書をサポートしています。X.509 デジタル証明書は、メッセージの出所と整合性を保証するデータ項目です。これには安全な通信のための暗号化されたキーが含まれています。また、発信者のアイデンティティを証明するために信頼できる認証局（CA）によって署名されています。X.509 デジタル証明書のサポートにより、認証に DSA と RSA のいずれかのアルゴリズムを使用します。

証明書のインフラストラクチャでは、Secure Socket Layer（SSL）に対応し、セキュリティインフラストラクチャによってクエリーまたは通知を通じて最初に返される証明書が使用されます。証明書が信頼できる CA のいずれかで設定されており、無効にされたり期限が切れたりしていなければ、証明書の検証は成功します。

X.509 証明書を使用する SSH 認証用にデバイスを設定できます。認証に失敗した場合は、パスワードの入力が求められます。

X.509v3 証明書（RFC 6187）を使用する SSH 認証を設定できます。X.509v3 証明書ベースの SSH 認証では、スマートカードと組み合わせた証明書を使用して、シスコ デバイスへのアクセスの 2 要素認証を有効にします。SSH クライアントは、シスコパートナーの Pragma Systems によって提供されます。

ホスト アイデンティティに基づく認証（HIBA）を使用した SSH 認証

ホストベース認証は、サーバーの `known_hosts` ファイルでクライアントのホスト公開キーを確認することにより、クライアントのホストをサーバー（Cisco Nexus 9000 スイッチ）に対して認証する SSH 認証方式です。これは、ユーザーまたはホストを認証ために認証局（CA）によって署名されたデジタル証明書を使用する SSH 証明書ベースの認証とは異なります。

ホストアイデンティティベースの認証（HIBA）は、証明書にホスト承認情報を埋め込むことによって SSH 承認管理を一元化する方式です。

- ホスト承認情報は、ホスト証明書に組み込まれています。
- ユーザー証明書には、アクセス許可を指定する「付与」が含まれています。
- 認証は、認証局（CA）によって一元的に管理されます。

HIBA は SSH アクセス制御を簡素化し、管理オーバーヘッドを削減し、承認のための外部 AAA サーバーへの依存を排除します。

HIBA の利点

HIBA には、従来の SSH キー管理に比べて次のような利点があります。

HIBA の主なメリットは以下のとおりです：

- **管理の簡素化**：証明書ベースのアイデンティティによる一元化された承認により、管理が簡素化されます。
- **拡張性**：大規模で複雑な環境での SSH アクセスの管理が簡素化されます。

- **依存関係の軽減**：承認に関する外部 AAA サーバーへの依存性を排除し、最終手段としてのアクセスに適したものにします。
- **セキュリティの強化**：短期間の証明書を使用した一時的なアクセスと特権アクセスの制御を向上させます。

HIBA による SSH 認証の仕組み

このプロセスでは、HIBA が構成されている場合に SSH 認証がどのように行われるかについて説明します。

process_summary

SSH サーバーは、HIBA 承認モジュールを呼び出し、認証中にユーザー証明書を処理します。アクセスは、構成されたホストアイデンティティと付与に対して HIBA モジュールがユーザーの証明書を正常に検証した場合に付与されます。HIBA 検証が失敗した場合、SSH サーバーは、構成に応じて、他の認証方法にフォールバックする場合があります。

process_workflow

次の段階で、HIBA を使用した SSH 認証プロセスについて説明します。

1. **[SSH 接続試行 (SSH Connection Attempt)]**：ユーザーは、SSH でスイッチへの接続を試行します。
2. **[証明書の提示 (Certificate Presentation)]**：SSH クライアントは、スイッチ上の SSH サーバーにユーザーの証明書を提示します。
3. **[HIBA モジュール呼び出し (HIBA Module Invocation)]**：SSH サーバーは、その構成 (AuthorizedPrincipalsCommand) に基づいて、HIBA 承認モジュールを呼び出します。
4. **[証明書の検証 (Certificate Validation)]**：HIBA モジュールは、次の検証を実行します：
 - 構成された HIBA CA と照合してユーザー証明書の署名を確認します。
 - ホスト証明書からホスト アイデンティティを抽出します。
 - ホストアイデンティティと一致するユーザー証明書内の有効な「付与」をチェックします。
5. **[アクセス決定 (Access Decision)]**：HIBA モジュールの検証に基づいて、次のいずれかが行われます：

属性...	結合できるフィールド	次の操作	結合できるフィールド
ユーザー証明書が HIBA モジュールによって正常に検証されました。	ターゲット ホストの有効な付与がユーザー証明書にあります。	ユーザーにアクセス権が付与されます。	SSH セッションが実行されます。

属性...	結合できるフィールド	次の操作	結合できるフィールド
ユーザー証明書が無効であるか、検証できません。	ユーザー証明書に有効な付与が見つかりませんでした。	HIBA モジュールによってアクセスが拒否されました。	SSH サーバーは、他の認証方法にフォールバックする場合があります（構成されている場合）。

SSH 認証の HIBA の構成

この手順では、SSH ホスト アイデンティティ ベースの認可（HIBA）の構成について説明します。

この構成では、SSH サーバー キーの生成、HIBA CA のトラストポイントの構成、SSH ホスト証明書の登録、認証に HIBA を使用するための SSH サーバーの構成を行います。



- (注) 初めて HIBA を構成する場合、ローカル ユーザー アカウントやその他の構成済み AAA サーバーなど、従来の SSH 認証方式を使用してスイッチにログインできます。HIBA を有効にしても、既存のローカル SSH ユーザーは、明示的にアカウントを削除しない限り、削除またはブロックされません。

始める前に

HIBA を構成する前に、次の点を確認してください：

- 認証局（CA）を含む、機能する PKI インフラストラクチャ。
- CA サーバーへの接続。

手順

ステップ 1 configure terminal

例：

```
switch# configure terminal
```

グローバル構成モードを開始します。

ステップ 2 ssh key ecdsa bits

例：

```
switch(config)# ssh key ecdsa 384
```

スイッチの ECDSA キーペアを生成します。この例では、384 ビットの ECDSA キーが使用されています。セキュリティ ポリシーとプラットフォームでサポートされるキー サイズを使用します。

ステップ 3 **ssh key export bootflash:file_name ecdsa**

例：

```
switch(config)# ssh key export bootflash:host_key ecdsa
Enter Passphrase:
```

SSH ホスト ECDSA キーをブートフラッシュにエクスポートします。必要に合わせて file_name を置き換えます。

エクスポート後、SFTP を使用して host_key および host_key.pub ファイルを CA マシンに転送します：

```
switch(config)# feature sftp-server
# On CA machine:
sftp admin@<switch_ip>
sftp> get host_key .
sftp> get host_key.pub .
```

ステップ 4 **crypto ca trustpoint openssh-ca type ssh**

例：

```
switch(config)# crypto ca trustpoint openssh-ca type ssh
```

HIBA CA のトラストポイントを作成します。一貫性を保つために、**openssh-ca** という名前を使用します。

ステップ 5 **crypto ca authenticate openssh-ca type ssh ecdsa-sha2-nistp384 public_key**

例：

```
switch(config-trustpoint)# crypto ca authenticate openssh-ca type ssh ecdsa-sha2-nistp384
AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAABmlzdHAzODQAAABhBBPiMs3fwftVUoMT...
/home/admin/.hiba-ca CA
```

CA 公開キーをインポートして HIBA CA を認証します。キー文字列を実際の CA 公開キーに置き換えます。

ステップ 6 **crypto ca enroll openssh-ca type ssh host-certificate ecdsa-sha2-nistp384-cert-v01@openssh.com certificate_content**

例：

```
switch(config)# crypto ca enroll openssh-ca type ssh host-certificate
ecdsa-sha2-nistp384-cert-v01@openssh.com
-----BEGIN SSH HOST KEY CERTIFICATE-----
root@switch
```

CA によって署名された SSH ホスト証明書を登録します。Google HIBA CA Wiki の手順に従って生成された証明書のコンテンツを使用します。

設定例：Linux での HIBA SSH クライアント



重要 次に、Linux システムで HIBA SSH クライアントを設定するための例として、次の手順を示します。正確な手順と出力は、クライアントオペレーティングシステムと SSH のバージョンによって異なる場合があります。確実な手順については、システムの公式な SSH ドキュメントを参照してください。

この手順では、SSH でホストアイデンティティベースの認証（HIBA）を使用するためのクライアント側の設定について説明します。



(注) 「HIBA サーバー」という用語は、Cisco Nexus 9000 スイッチで実行され、HIBA を使用するよう設定された SSH サーバーを指します。

始める前に

HIBA SSH クライアントを設定する前に、次を確認してください。

- ホストに `openssh-client` が有効にインストールされていること。
- CA 公開キー (`ca.pub`)。
- ユーザー秘密キーおよび有効な HIBA 拡張との一致証明書。
- ユーザー公開キー (`key_rsa.pub` または同等のもの)。

手順

ステップ 1 `$ cat /etc/ssh/ssh_config`

例：

```
$ cat /etc/ssh/ssh_config
# Enable host key checking
StrictHostKeyChecking yes
# Declare our trusted CA
GlobalKnownHostsFile /etc/ssh/known_hosts
```

SSH クライアント設定の構成

`/etc/ssh/ssh_config` を編集して、厳密なホストキーのチェックを有効にし、SSH 証明書の検証用の CA 公開キーを含む `GlobalKnownHostsFile` を指定します。

ステップ 2 `$ echo "@cert-authority * $(cat /etc/ssh/ca.pub)" > /etc/ssh/known_hosts`

例：

```
$ echo "@cert-authority * $(cat /etc/ssh/ca.pub)" > /etc/ssh/known_hosts
```

known_hosts に CA 公開キーを入力します

@cert-authority ディレクティブを使用して、known_hosts ファイルに CA 公開キーを追加します。この手順によって、SSH クライアントがこの CA によって署名されたホスト証明書を信頼できるようになります。

ステップ 3 \$ cat ~/.ssh/key_rsa.pub

例：

```
$ cat ~/.ssh/key_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAQE... user@host
```

公開キーの表示

ユーザー公開キーファイルの内容を表示します。このキーは証明書ベースの認証に必要であり、秘密キーおよび証明書に対応している必要があります。

(注)

キーの名前や場所が異なる場合は、それに応じてパスを調整します。

ステップ 4 \$ ssh -i <path_to_private_key> <user>@<hiba_server_ip>

例：

```
$ ssh -i <path_to_private_key> <user>@<hiba_server_ip>
```

HIBA 対応 SSH サーバーへの接続

自分の秘密キー（および必要な場合は秘密キーとそれに一致する証明書）を使用して、SSH サーバーに接続します。

(注)

-i オプションは、ユーザーの秘密キー（アイデンティティ ファイル）を指定します。

正しく設定されている場合、SSH 接続は HIBA 証明書ベースの認証を使用して確立され、CA 公開キーに対するホストの検証が成功します。公開キーがサーバーの authorized_keys に存在する場合、パスワードレス ログインが可能になります。

HIBA 構成の確認

手順

ステップ 1 show crypto ca certificates type ssh

例：

```
switch(config)# show crypto ca certificates type ssh
trustpoint: openssh-ca
CA Public Key:
ecdsa-sha2-nistp384
-----BEGIN PUBLIC KEY-----
MIGbMBAGByqGSM4iAgECCgEBDAEwAwQAAQ==
```



```

/home/admin/.hiba-ca CA
Finger Print:
384 SHA256:ZcJws/mPrts6twB29OoZU/c3AMAL0x3mUp00YxwSRmk /home/admin/.hiba-ca
CA (ECDSA)

Host Certificate:
Type: ecdsa-sha2-nistp384-cert-v01@openssh.com host certificate
Public key: ECDSA-CERT SHA256:bZkNWnvxyUK1DHRwqayWivobGUwA25GRGkUMNEd/Ujw
Signing CA: ECDSA SHA256:ZcJws/mPrts6twB29OoZU/c3AMAL0x3mUp00YxwSRmk (using
ecdsa-sha2-nistp384)
Key ID: "cisco_nexus_9000"
Serial: 1
Valid: from 2025-06-05T04:34:00 to 2025-08-28T04:35:39
Principals:
cisco_nexus_9000
Critical Options: (none)
Extensions:
identity@hibassh.dev

HIBA Info:
certificate 'cisco_nexus_9000' (1 principal) contains 1 HIBA grant
principal: 'cisco_nexus_9000'
identity@hibassh.dev (v2):
[0] domain = 'google.com'

```

SSH 証明書を表示し、ホスト証明書が登録済みで、正しいトラストポイント (openssh-ca) に関連付けられていることを確認します。

[想定される出力 (Expected Output)] : 出力には、HIBA 付与を示す「HIBA Info」セクションを含む、SSH ホスト証明書の詳細が表示される必要があります。

ホスト証明書と HIBA 情報が正しく表示されれば、証明書の登録は成功です。

ステップ 2 show crypto ca trustpoints type ssh

例 :

```

switch(config)# show crypto ca trustpoints type ssh
trustpoint: openssh-ca

```

SSH トラストポイントを表示し、HIBA CA トラストポイント (openssh-ca) が存在することを確認します。

[想定される出力 (Expected Output)] : 出力には、タイプ ssh のトラストポイント名が一覧表示されます。

HIBA CA トラストポイントが出力に表示される場合、トラストポイントは正常に構成されています。

ステップ 3 ssh -i path_to_private_key <user>@<switch_ip>

例 :

```

ssh -i /home/admin/.hiba-ca/users/google-user admin@10.126.67.44

```

CA によって署名された HIBA 対応証明書を持つユーザーを使用して、スイッチに SSH で接続します。

注：-i オプションは、ユーザーの秘密キー（アイデンティティ ファイル）へのパスを指定します。HIBA 拡張は、この秘密キーとペアになる証明書に含める必要があり、CA 公開キーはスイッチによって信頼されている必要があります。秘密キーファイルが安全に保たれていることを確認してください。

パスワードの入力を求めずに、SSH 接続が正常に確立されます（パスワード認証が無効になっている場合）。

Telnet サーバ

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。Telnet を使用すると、あるサイトのユーザが別のサイトのログイン サーバと TCP 接続を確立し、キーストロークをデバイス間でやり取りできます。Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

デフォルトでは、Telnet サーバが Cisco NX-OS デバイス上でディセーブルになっています。

SSH および Telnet の前提条件

レイヤ 3 インターフェイス上で IP、mgmt 0 インターフェイス上でアウトバンド、またはイーサネット インターフェイス上でインバンドを設定していることを確認します。

SSH と Telnet のガイドラインと制約事項

SSH および Telnet に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS ソフトウェアは、SSH バージョン 2（SSHv2）だけをサポートしています。
- Cisco NX-OS リリース 10.4(3)F 以降、Cisco Nexus 9000 シリーズ スイッチは、TACACS+ サーバを介し、X.509 証明書を使用した SSH 認証をサポートしています。この機能は、RADIUS ではサポートされていません。
- **no feature ssh feature** コマンドを使用すると、ポート 22 はディセーブルになりません。ポート 22 は常にオープンで、すべての着信外部接続を拒否する拒否ルールがプッシュされます。
- Poodle の脆弱性により、SSLv3 はサポートされなくなりました。
- IPSG は、次のものではありません。
 - Cisco Nexus 9372PX、9372TX、および 9332PQ スイッチの最後の 6 個の 40 Gb 物理ポート
 - Cisco Nexus 9396PX、9396TX、および 93128TX スイッチのすべての 40G 物理ポート

- X.509 証明書を使用する SSH 認証用にデバイスを設定できます。認証に失敗した場合は、パスワードの入力が求められます。
- SFTP サーバー機能は、通常の SFTP の **chown** および **chgrp** コマンドをサポートしません。
- SFTP サーバーが有効になっている場合は、admin ユーザだけが SFTP を使用してデバイスにアクセスできます。
- SSH パスワードレス ファイルコピーを目的として AAA プロトコル (RADIUS や TACACS+ など) を介してリモート認証されたユーザ アカウントにインポートされた SSH 公開キーと秘密キーは、同じ名前のローカル ユーザ アカウントでない限り、Nexus デバイスがリロードされると保持されません。リモート ユーザ アカウントは、SSH キーがインポートされる前にデバイスで設定されます。
- SSH のタイムアウト時間は、tac-pac の生成時間よりも長くする必要があります。そうでないと、VSH ログに %VSHD-2-VSHD_SYSLOG_EOL_ERR エラーが記録されることがあります。理想的には、tac-pac または showtech を収集する前に 0 (無限) に設定します。
- Cisco NX-OS リリース 10.4(3)F 以降、**show running-config all** コマンドは次のコマンドの詳細を表示しません：
 - no feature telnet
 - no feature nxdb
 - no feature scp-server
 - no feature sftp-server



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

- Cisco NX-OS Release 10.2(2)F 以降、新しい非同期化 CLI が導入され、SNMP とセキュリティ コンポーネントの間のユーザー同期を無効にするオプションを提供します。詳細については、システム管理構成ガイドの *SNMP* の構成の章を参照してください。

リリース 7.0(3)I7(1)から現在のリリースまでのさまざまな機能をサポートする Cisco Nexus 9000 スイッチの詳細については、[Nexus スイッチ プラットフォーム サポート マトリックス](#)を参照してください。

- 非同期 CLI が有効になっている場合、リモート ユーザーは SNMP データベースに同期されません。
- DCNM (リリース 12.0.1.a 以降 Nexus Dashboard Fabric Controller と呼ばれる) を使用したセキュリティ ユーザーには、非同期 CLI が有効でないとき、対応する SNMPv3 プロファイルが存在しません。同期が無効になっている場合、セキュリティ コンポーネントで作成されたユーザーはスイッチにログインできますが、コントローラはスイッチを検出しません。コントローラは、セキュリティ ユーザー用に作成された SNMP 構成を使用してスイッチを検出するためです。さらに、SNMP は、userDB の非同期状態のため、作成されたセ

セキュリティユーザーを認識しないので、スイッチを検出できません。したがって、コントローラによってスイッチが検出されるようにするには、SNMP ユーザーを明示的に作成する必要があります。DCNM 機能とともに非同期 CLI を使用することはお勧めしません。詳細については、*Cisco Nexus 9000 NX-OS セキュリティ構成ガイド*を参照してください。

- Cisco NX-OS リリース 10.6(1)F 以降、次の DSA アルゴリズムとすべての DSA 関連の SSH CLI コマンドは廃止されています：
 - **show ssh key dsa**
 - **[no] ssh key dsa**
 - **[no] username username keypair generate {dsa [force]}**
 - **username username keypair export {bootflash:filename | volatile:filename} {dsa} [force]**
 - **username username keypair import {bootflash:filename | volatile:filename} {dsa} [force]**
 - **username user-id ssh-cert-dn dn-name {dsa}**
 - **[no] ssh cipher-mode weak**
 - **ssh ciphers aes256-gcm** : このコマンドを実行すると、「未定義のアルゴリズム名 (Undefined algorithm name)」という警告が表示されます。



(注) 廃止された DSA および暗号モード CLI の場合、CLI 構成の置換、デュアルステージコミット、および Netconf 操作中に、廃止の警告は表示されません。セキュリティを強化するため、SSH 認証と管理に RSA キーまたは ECDSA キーを生成して使用します。

- Cisco NX-OS リリース 10.6(2)F 以降、Cisco Nexus 9000 シリーズスイッチは、既存の netstack パスに加えて、Linux カーネル ネットワークスタック (kstack) を介した SSH 接続の受け入れをサポートしています。

SSH および Telnet のデフォルト設定

次の表に、SSH および Telnet パラメータのデフォルト設定を示します。

Table 10: デフォルトの SSH および Telnet パラメータ

パラメータ	デフォルト
SSH サーバ	イネーブル
SSH サーバ キー	1024 ビットで生成された RSA キー
RSA キー生成ビット数	1024

パラメータ	デフォルト
Telnet サーバ	無効化
Telnet ポート番号	23
SSH ログインの最大試行回数	3
SCP サーバ	ディセーブル
SFTP サーバ	無効化

SSH の設定

ここでは、SSH の設定方法について説明します。

SSH サーバ キーの生成

セキュリティ要件に基づいて SSH サーバ キーを生成できます。デフォルトの SSH サーバ キーは、1024 ビットで生成される RSA キーです。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 feature ssh Example: switch(config)# no feature ssh	SSH を無効にします。
ステップ 3	ssh key export export-host-keypath {rsa ecdsa} [force] Example: switch(config)# ssh key rsa export bootflash:host_key rsa Enter Passphrase:	SSH サーバ キーをエクスポートします。 SSH サーバ キーを既存のファイル パスにエクスポートする場合は、 force キーワードを使用します。
ステップ 4	ssh rekey max-data max-data max-time max-time Example: switch(config)# ssh rekey max-data 1K max-time 1M	キー再生成パラメータを設定します。

	Command or Action	Purpose
ステップ 5	feature ssh Example: switch(config)# feature ssh	SSH を有効にします。
ステップ 6	exit Example: switch(config)# exit switch#	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 7	(Optional) show ssh key [dsa rsa ecdsa] [md5] Example: switch# show ssh key	SSH サーバ キーを表示します。 このコマンドは、デフォルトで SHA256 形式でフィンガープリントを表示します。SHA256 は、以前のデフォルトの MD5 形式よりも安全です。ただし、フィンガープリントを MD5 形式で表示する必要がある場合の下位互換性のために、 md5 オプションが追加されています。 Note Cisco NX-OS リリース 10.6(1)F 以降、 dsa キーワードは非表示になっています。フル コマンドを入力すると、NX-OS は廃止の警告を出しますが、それを受け入れます。
ステップ 8	show run security all	
ステップ 9	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ アカウント用 SSH 公開キーの指定

SSH 公開キーを設定すると、パスワードを要求されることなく、SSH クライアントを使用してログインできます。SSH 公開キーは、次のいずれかの形式で指定できます。

- OpenSSH 形式
- Internet Engineering Task Force (IETF) SECSH 形式

IETF SECSH 形式による SSH 公開キーの指定

ユーザ アカウント用に IETF SECSH 形式で SSH 公開キーを指定できます。

Before you begin

IETF SCHSH 形式の SSH 公開キーを作成します。

Procedure

	Command or Action	Purpose
ステップ 1	copy server-file bootflash:filename Example: <pre>switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub</pre>	サーバから IETF SECSH 形式の SSH キーを含むファイルをダウンロードします。サーバは FTP、Secure Copy (SCP)、Secure FTP (SFTP)、または TFTP のいずれかを使用できます。
ステップ 2	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 username sshkey file bootflash:filename Example: <pre>switch(config)# username User1 sshkey file bootflash:secsh_file.pub</pre>	IETF SECSH 形式の SSH 公開キーを設定します。
ステップ 4	exit Example: <pre>switch(config)# exit switch#</pre>	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 5	(Optional) show user-account Example: <pre>switch# show user-account</pre>	ユーザアカウントの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

OpenSSH 形式の SSH 公開キーの指定

ユーザアカウントに OpenSSH 形式の SSH 公開キーを指定できます。

Before you begin

OpenSSH 形式の SSH 公開キーを作成します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	username username sshkey ssh-key Example: switch(config)# username User1 sshkey ssh-rsa AAAENaCly2ZWWF5WMP419FQZ19G3fXsK0W4H7MjUyA50v7gSP h0EmsidAKuInIf/QJm+LNgP/60v7to+IMRFY/G4LNQ89ig30d6t Xm+Njn1LB7ihpVh7dcdMOWQXhYshVrSiH3UD/KyziB5S4tpLx8=	OpenSSH 形式の SSH 公開キーを設定します。
ステップ 3	exit Example: switch(config)# exit switch#	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 4	(Optional) show user-account Example: switch# show user-account	ユーザアカウントの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH ログイン試行の最大回数の設定

SSH ログイン試行の最大回数を設定できます。許可される試行の最大回数を超えると、セッションが切断されます。



Note

ログイン試行の合計回数には、公開キー認証、証明書ベースの認証、およびパスワードベースの認証を使用した試行が含まれます。イネーブルにされている場合は、公開キー認証が優先されます。証明書ベースとパスワードベースの認証だけがイネーブルにされている場合は、証明書ベースの認証が優先されます。これらすべての方法で、ログイン試行の設定された数を超えると、認証失敗回数を超過したことを示すメッセージが表示されます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	ssh login-attempts number Example: <pre>switch(config)# ssh login-attempts 5</pre>	ユーザが SSH セッションへのログインを試行できる最大回数を設定します。ログイン試行のデフォルトの最大回数は3です。値の範囲は 1 ～ 10 です。 Note このコマンドの no 形式を使用すると、以前のログイン試行の値が削除され、ログイン試行の最大回数がデフォルト値の 3 に設定されます。
ステップ 3	(Optional) show running-config security all Example: <pre>switch(config)# show running-config security all</pre>	SSH ログイン試行の設定された最大回数を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SSH セッションの開始

Cisco NX-OS デバイスから IPv4 または IPv6 を使用して SSH セッションを開始し、リモートデバイスと接続します。

Before you begin

リモートデバイスのホスト名を取得し、必要なら、リモートデバイスのユーザ名も取得します。

リモートデバイスの SSH サーバを有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	ssh [username@]{ipv4-address hostname} [vrf vrf-name] Example: switch# ssh 10.10.1.1	IPv4 を使用してリモート デバイスとの SSH IPv4 セッションを作成します。デフォルトの VRF はデフォルト VRF です。
ステップ 2	ssh6 [username@]{ipv6-address hostname} [vrf vrf-name] Example: switch# ssh6 HostA	IPv6 を使用してリモート デバイスとの SSH IPv6 セッションを作成します。

ブートモードからの SSH セッションの開始

SSH セッションは、リモート デバイスに接続する Cisco NX-OS デバイスのブートモードから開始できます。

Before you begin

リモート デバイスのホスト名を取得し、必要なら、リモート デバイスのユーザ名も取得します。

リモート デバイスの SSH サーバを有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	ssh [username@]hostname Example: switch(boot)# ssh user1@10.10.1.1	リモート デバイスへの SSH セッションを、Cisco NX-OS デバイスのブートモードから作成します。デフォルト VRF が常に使用されます。
ステップ 2	exit Example: switch(boot)# exit	ブートモードを終了します。
ステップ 3	copy scp://[username@]hostname/filepath directory Example: switch# copy scp://user1@10.10.1.1/users abc	セキュア コピー プロトコル (SCP) を使用して、ファイルを Cisco NX-OS デバイスからリモート デバイスへコピーします。デフォルト VRF が常に使用されます。

SSH のパスワードが不要なファイル コピーの設定

Cisco NX-OS デバイスから Secure Copy (SCP) サーバまたは Secure FTP (SFTP) サーバに、パスワードなしでファイルをコピーすることができます。これを行うには、SSH による認証用の公開キーと秘密キーで構成される RSA または DSA のアイデンティティを作成する必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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] username username keypair generate {rsa [bits [force]] dsa [force]} Example: <pre>switch(config)# username user1 keypair generate rsa 2048 force</pre>	SSH の公開キーと秘密キーを生成し、指定したユーザの Cisco NX-OS デバイスのホーム ディレクトリ (\$HOME/.ssh) に格納します。Cisco NX-OS デバイスでは、これらのキーを使用してリモート マシンの SSH サーバと通信します。 <i>bits</i> 引数には、キーの生成に使用するビット数を指定します。有効な範囲は 768 ~ 4096 です。デフォルト値は 1024 です。 既存のキーを置き換える場合は、force キーワードを使用します。force キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーは生成されません。 Note Cisco NX-OS リリース 10.6(1)F 以降、dsa キーワードは非表示になっています。フル コマンドを入力すると、NX-OS は廃止の警告を出しますが、それを受け入れます。
ステップ 3	(Optional) show username username keypair Example: <pre>switch(config)# show username user1 keypair</pre>	指定したユーザの公開キーを表示します。 Note セキュリティ上の理由から、このコマンドで秘密キーは表示されません。

	Command or Action	Purpose
ステップ 4	Required: username <i>username</i> keypair export {bootflash:<i>filename</i> volatile:<i>filename</i>} {rsa dsa} [force] Example: <pre>switch(config)# username user1 keypair export bootflash:key_rsa rsa</pre>	Cisco NX-OS デバイスのホーム ディレクトリから、指定したブートフラッシュ ディレクトリまたは一時ディレクトリに、公開キーと秘密キーをエクスポートします。 既存のキーを置き換える場合は、force キーワードを使用します。force キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーはエクスポートされません。 生成したキー ペアをエクスポートするとき、秘密キーを暗号化するパスフレーズを入力するように求められます。秘密キーは、指定したファイルとしてエクスポートされ、公開キーは、同じファイル名に .pub 拡張子を付けてエクスポートされます。これで、このキー ペアを任意の Cisco NX-OS デバイスにコピーし、SCP または SFTP を使用してサーバのホーム ディレクトリに公開キー ファイル (*.pub) をコピーできるようになります。 Note セキュリティ上の理由から、このコマンドはグローバル コンフィギュレーション モードでしか実行できません。 Note Cisco NX-OS リリース 10.6(1)F 以降、dsa キーワードは非表示になっています。フル コマンドを入力すると、NX-OS は廃止の警告を出しますが、それを受け入れます。
ステップ 5	Required: username <i>username</i> keypair import {bootflash:<i>filename</i> volatile:<i>filename</i>} {rsa dsa} [force] Example: <pre>switch(config)# username user1 keypair import bootflash:key_rsa rsa</pre>	指定したブートフラッシュ ディレクトリまたは一時ディレクトリから、Cisco NX-OS デバイスのホーム ディレクトリに、エクスポートした公開キーと秘密キーをインポートします。 Note Cisco NX-OS リリース 10.6(1)F 以降、dsa キーワードは非表示になっています。

	Command or Action	Purpose
		フル コマンドを入力すると、NX-OS は廃止の警告を出しますが、それを受け入れます。 既存のキーを置き換える場合は、force キーワードを使用します。force キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーはインポートされません。 生成したキー ペアをインポートするとき、秘密キーを復号化するパスフレーズを入力するように求められます。秘密キーは指定したファイルとしてインポートされ、公開キーは同じファイル名に .pub 拡張子を付けてインポートされます。 Note セキュリティ上の理由から、このコマンドはグローバル コンフィギュレーション モードでしか実行できません。 Note パスワードなしでサーバにアクセスできるのは、サーバでキーが設定されているユーザのみです。

What to do next

SCP サーバまたは SFTP サーバで、次のコマンドを使用して、*.pub ファイル（たとえば、key_rsa.pub）に格納された公開キーを authorized_keys ファイルに追加します。

```
$ cat key_rsa.pub >> $HOME/.ssh/authorized_keys
```

これで、標準の SSH コマンドおよび SCP コマンドを使用してパスワードを指定しなくても、Cisco NX-OS デバイスからサーバにファイルをコピーできます。

SCP サーバと SFTP サーバの設定

リモートデバイスとの間でファイルをコピーできるように、Cisco NX-OS デバイスで SCP サーバまたは SFTP サーバを設定できます。SCP サーバまたは SFTP サーバをイネーブルにした後、Cisco NX-OS デバイスとの間でファイルをコピーするために、リモート デバイスで SCP または SFTP コマンドを実行できます。



Note arcfour および blowfish cipher オプションは SCP サーバではサポートされません。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] feature scp-server Example: switch(config)# feature scp-server	Cisco NX-OS デバイス上で SCP サーバをイネーブルまたはディセーブルにします。
ステップ 3	Required: [no] feature sftp-server Example: switch(config)# feature sftp-server	Cisco NX-OS デバイス上で SFTP サーバをイネーブルまたはディセーブルにします。
ステップ 4	Required: exit Example: switch(config)# exit switch#	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 5	(Optional) show running-config security Example: switch# show running-config security	SCP サーバと SFTP サーバの設定ステータスを表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

X.509v3 証明書ベースの SSH 認証の設定

X.509v3 証明書を使用する SSH 認証を設定できます。

始める前に

リモート デバイスの SSH サーバ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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	username user-id [password [0 5] password] 例 : <pre>switch(config)# username jsmith password 4Ty18Rnt</pre>	ユーザ アカウントを設定します。 user-id 引数は、大文字と小文字が区別される英数字で、最大 28 文字です。これはローカルおよびリモートユーザーの両方に当てはまります。指定できる文字は、A ～ Z の英大文字、a ～ z の英小文字、0 ～ 9 の数字、ハイフン (-)、ピリオド (.)、アンダースコア (_)、プラス符号 (+)、および等号 (=) です。アットマーク (@) はリモートユーザ名では使用できますが、ローカル ユーザ名では使用できません。 ユーザ名の先頭は英数字で始まる必要があります。 デフォルトパスワードは定義されていません。オプションの 0 は、パスワードがクリア テキストであり、5 はパスワードが暗号化されていることを意味します。デフォルトは 0 (クリア テキスト) です。 (注) パスワードを指定しなかった場合、ユーザは Cisco NX-OS デバイスにログインできません。 (注) 暗号化パスワードオプションを使用してユーザアカウントを作成する場合、対応する SNMP ユーザは作成されません。 (注) 非同期 CLI が有効になっている場合、ユーザーアカウントを作成しても、対

	コマンドまたはアクション	目的
		応する SNMP ユーザーは作成されません。
ステップ 3	username user-id ssh-cert-dn dn-name {dsa rsa} 例 : <pre>switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa</pre>	既存のユーザアカウント認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。識別名は最大 512 文字で、例に示す形式に従う必要があります。電子メールアドレスと状態がそれぞれ emailAddress と ST に設定されていることを確認します。
ステップ 4	[no] crypto ca trustpoint trustpoint 例 : <pre>switch(config)# crypto ca trustpoint winca switch(config-trustpoint)#</pre>	トラストポイントを設定します。 (注) このコマンドの no 形式を使用してトラストポイントを削除する前に、まず delete crl および delete ca-certificate コマンドを使用して、CRL および CA 証明書を削除する必要があります。
ステップ 5	crypto ca authenticate trustpoint 例 : <pre>switch(config-trustpoint)# crypto ca authenticate winca</pre>	トラストポイントの CA 証明書を設定します。 (注) CA 証明書を削除するには、トラストポイントコンフィギュレーションモードで delete ca-certificate コマンドを入力します。
ステップ 6	(任意) crypto ca crl request trustpoint bootflash:static-crl.crl 例 : <pre>switch(config-trustpoint)# crypto ca crl request winca bootflash:crllist.crl</pre>	この項はオプションですが、強く推奨されます。トラストポイントの証明書失効リスト (CRL) を設定します。CRL ファイルは、トラストポイントによって失効した証明書のリストのスナップショットです。このスタティック CRL リストは、認証局 (CA) からデバイスに手動でコピーされます。 (注) スタティック CRL は、サポートされている唯一の失効チェック方式です。 (注) CRL を削除するには、 delete crl コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 7	(任意) show crypto ca certificates 例 : <pre>switch(config-trustpoint)# show crypto ca certificates</pre>	設定されている証明書またはチェーンと、関連付けられているトラストポイントを表示します。
ステップ 8	(任意) show crypto ca crt trustpoint 例 : <pre>switch(config-trustpoint)# show crypto ca crt winca</pre>	指定したトラストポイントの CRL リストの内容を表示します。
ステップ 9	(任意) show user-account 例 : <pre>switch(config-trustpoint)# show user-account</pre>	設定されたユーザアカウントの詳細を表示します。
ステップ 10	(任意) show users 例 : <pre>switch(config-trustpoint)# show users</pre>	デバイスにログオンしているユーザが表示されます。
ステップ 11	(任意) copy running-config startup-config 例 : <pre>switch(config-trustpoint)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

TACACS サーバでの SSH 証明書認証の構成

Cisco NX-OS リリース 10.4(3)F 以降、Cisco Nexus 9000 シリーズ スイッチは、TACACS+ サーバを介し、X.509 証明書を使用した SSH 認証をサポートしています。この機能は、RADIUS ではサポートされていません。この機能は、**aaa authorization ssh-certificate default group tac-group-name** コマンドを使用して有効にできます。設定の詳細については、[TACACS サーバでの AAA SSH 証明書認証の構成 \(45 ページ\)](#) を参照してください。

SSH 暗号化アルゴリズムのカスタマイズ

Cisco Nexus 9000 スイッチは、デフォルトで強力なアルゴリズムをサポートします。Cisco Product Security Baseline (PSB) で定義されている強力なアルゴリズムのみを有効にするデフォルトモードのままにするか、サポートされているすべてのアルゴリズムを許可するかを選択できます。これらのアルゴリズムは、着信サーバー接続に適用できることに注意してください。SSH キー交換アルゴリズム、メッセージ認証コード (MAC)、キー タイプ、および暗号のサポートを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal</pre>	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	(任意) ssh kexalgos [all key-exchangealgorithm-name] 例 : <pre>switch(config)# ssh kexalgos ecdhsha2-nistp384</pre>	接続ごとのキーの生成に使用されるキー交換方式である、サポートされているすべての KexAlgorithm を有効にするには、all キーワードを使用します。 サポートされる KexAlgorithm は次のとおりです。 • curve25519-sha256 • curve25519-sha256@libssh.org • diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256 • diffie-hellman-group16-sha512 • ecdh-sha2-nistp256 • ecdh-sha2-nistp521 サポートされない KexAlgorithm は次のとおりです。 • diffie-hellman-group1-sha1 • diffie-hellman-group-exchange-sha256 ecdh-sha2-nistp384 KexAlgorithm のみを有効にするには、ecdh-sha2-nistp384 キーワードを使用します。 (注) Cisco NX-OS リリース 10.4(2) 以降では、サポートされている任意の KexAlgorithm を設定できます。このリリースから、ecdh-sha2-nistp384 キーワードは廃止されました。
ステップ 3	(任意) ssh macs [all mac-name] 例 :	トラフィック変更の検出に使用されるメッセージ認証コードである、サポート

	コマンドまたはアクション	目的
	<pre>switch(config)# ssh macs hmacsha2-256-etm@openssh.com</pre>	されているすべての MAC を有効にします。 サポートされる MAC は次のとおりです。 • hmac-sha1 • hmac-sha2-256 • hmac-sha2-512 • hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • hmac-sha1-etm@openssh.com (注) Cisco NX-OS リリース 10.4(2)F 以降では、サポートされている任意の MAC を設定できます。
ステップ 4	(任意) ssh ciphers [all cipher-name] 例 : <pre>switch(config)# ssh ciphers aes192-ctr</pre>	サポートされているすべての暗号を有効にして接続を暗号化するには、all キーワードを使用します。 サポート対象の暗号方式 : • aes128-cbc • aes192-cbc • aes256-cbc • aes128-ctr • aes192-ctr • aes256-ctr • aes128-gcm@openssh.com • chacha20-poly1305@openssh.com (注) Cisco NX-OS リリース 10.4(2)F 以降では、サポートされている任意の暗号を設定できます。このリリースから、aes256-gcm キーワードは廃止されました。 (注)

	コマンドまたはアクション	目的
		Cisco NX-OS リリース 10.6(1) 以降、 <code>ssh ciphers aes256-gcm</code> コマンドは廃止され、サポートされなくなりました。このコマンドが設定に存在する場合、設定の置換 (CR) と ISSU は失敗します。アップグレードする前に設定からコマンドを削除してください。
ステップ 5	(任意) <code>ssh keytypes [all keytype-string]</code> 例 : <pre>switch(config)# ssh keytypes ecdsa-sha2-nistp256</pre>	サーバーがクライアントに対して自身を認証するために使用できる公開キー アルゴリズムである、サポートされているすべての <code>PubkeyAcceptedKeyType</code> を有効にします。 サポートされるキー タイプは次のとおりです。 • <code>ecdsa-sha2-nistp256</code> • <code>ecdsa-sha2-nistp384</code> • <code>ecdsa-sha2-nistp521</code> • <code>ecdsa-sha2-nistp256-cert-v01@openssh.com</code> • <code>ecdsa-sha2-nistp384-cert-v01@openssh.com</code> • <code>ecdsa-sha2-nistp521-cert-v01@openssh.com</code> • <code>ssh-dss</code> • <code>rsa-sha2-256</code> • <code>ssh-rsa-cert-v01@openssh.com</code> • <code>ssh-rsa</code> (注) Cisco NX-OS リリース 10.4(2)F 以降では、サポートされている任意のキータイプを設定できます。 (注) <code>rsa</code>、<code>dsa</code>、および <code>ecdsa</code> キータイプを有効にするには、対応する SSH ホストキーを生成する必要があります。 設定例 : <pre>switch(config)# ssh key rsa 2048 switch(config)# ssh key dsa</pre>

	コマンドまたはアクション	目的
		switch(config)# ssh key ecdsa 256

例

show ssh [ciphers | macs | keytypes | kexalogs | version] コマンドを使用して、サポートされているアルゴリズムを確認できます。

show ssh ciphers

Cipher	Status	FIPS
-----	-----	-----
aes128-ctr	permitted	yes
aes192-ctr	denied	yes
aes256-ctr	permitted	yes
aes128-cbc	denied	yes
aes192-cbc	denied	yes
aes256-cbc	denied	yes
aes256-gcm@openssh.com	permitted	yes
aes128-gcm@openssh.com	permitted	yes
chacha20-poly1305@openssh.com	permitted	no

show ssh macs

MAC	Status	FIPS
-----	-----	-----
hmac-sha2-256-etm@openssh.com	permitted	no
hmac-sha2-512-etm@openssh.com	permitted	no
hmac-sha1-etm@openssh.com	permitted	no
hmac-sha2-256	permitted	yes
hmac-sha2-512	permitted	yes
hmac-sha1	permitted	yes
hmac-sha1-96	unsupported	no
hmac-md5	unsupported	no
hmac-md5-96	unsupported	no
umac-64@openssh.com	unsupported	no
umac-128@openssh.com	unsupported	no
hmac-sha1-96-etm@openssh.com	unsupported	no
hmac-md5-etm@openssh.com	unsupported	no
umac-64-etm@openssh.com	unsupported	no
umac-128-etm@openssh.com	unsupported	no

show ssh keytypes

Keytype	Status	FIPS
-----	-----	-----
ecdsa-sha2-nistp256-cert-v01@openssh.com	permitted	no <<Currently not supported>>
ecdsa-sha2-nistp384-cert-v01@openssh.com	permitted	no <<Currently not supported>>
ecdsa-sha2-nistp521-cert-v01@openssh.com	permitted	no <<Currently not supported>>
ssh-rsa-cert-v01@openssh.com	permitted	no
ecdsa-sha2-nistp256	permitted	yes
ecdsa-sha2-nistp384	permitted	yes
ecdsa-sha2-nistp521	permitted	no
rsa-sha2-256	permitted	no
ssh-rsa	permitted	yes
ssh-dss	denied	no
ssh-ed25519	unsupported	no
ssh-ed25519-cert-v01@openssh.com	unsupported	no
ssh-dss-cert-v01@openssh.com	unsupported	no

サポートされるアルゴリズム：FIPモードが有効の場合

```

show ssh kexalgos
KexAlgorithm                               Status      FIPS
-----
curve25519-sha256                          permitted   no
curve25519-sha256@libssh.org               permitted   no
ecdh-sha2-nistp256                         permitted   yes
ecdh-sha2-nistp384                         permitted   yes
ecdh-sha2-nistp521                         permitted   yes
diffie-hellman-group16-sha512              permitted   yes
diffie-hellman-group14-sha1                permitted   yes
diffie-hellman-group14-sha256              permitted   no

show ssh version
CiscoSSH 1.9.29, OpenSSH_8.3p1, CiscoSSL 1.1.1t.7.2.500

```

サポートされるアルゴリズム：FIPモードが有効の場合

FIP モードが有効な場合にサポートされるアルゴリズムのリストは次のとおりです。

表 11: サポートされるアルゴリズム：FIPモードが有効の場合

アルゴリズム	サポート対象	サポート対象外
ciphers	• aes128-ctr • aes256-ctr • aes256-gcm@openssh.com • aes128-gcm@openssh.com • chacha20-poly1305@openssh.com	• aes192-ctr • aes128-cbc • aes192-cbc • aes256-cbc
hmac	• hmac-sha2-256 • hmac-sha2-512 • hmac-sha1 • hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • hmac-sha1-etm@openssh.com	-

アルゴリズム	サポート対象	サポート対象外
kexalgo	• ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group16-sha512 • diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256 • curve25519-sha256@libssh.org • curve25519-sha256	-
keytypes	• ecdsa-sha2-nistp256-cert-v01@openssh.com • ecdsa-sha2-nistp384-cert-v01@openssh.com • ecdsa-sha2-nistp521-cert-v01@openssh.com • ssh-rsa-cert-v01@openssh.com • rsa-sha2-256 • ssh-rsa • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521	• ssh-dss

デフォルトの SSH サーバポートの変更

Cisco NX-OS Cisco リリース 9.2(1) 以降では、SSHv2 のポート番号をデフォルトのポート番号 22 から変更できます。デフォルトの SSH ポートの変更時に使用される暗号化により、より強力なプライバシーとセッション整合性をサポートする接続が実現します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	no feature ssh 例 : <pre>switch(config)# no feature ssh</pre>	SSH を無効にします。
ステップ 3	show sockets local-port-range 例 : <pre>switch(config)# show sockets local port range (15001 - 58000) switch(config)# local port range (58001 - 63535) and nat port range (63536 - 65535) switch# show sockets local-port-range Kstack local port range (15001 - 22002) Netstack local port range (22003 - 65535)</pre>	使用可能なポート範囲を表示します。
ステップ 4	ssh port local-port 例 : <pre>switch(config)# ssh port 58003</pre>	ポートを設定します。 (注) 以前のリリースからリリース 9.3(1) 以降のリリースにアップグレードする場合は、ユーザ定義の SSH ポートを使用する機能が次の範囲内にあることを確認してください。 - リリース 9.3(1) およびリリース 9.3(2) の場合 : Kstack ローカルポートの範囲は 15001 ～ 58000、netstack ローカルポートの範囲は 58001 ～ 63535、nat ポートの範囲は 63536 ～ 65535 - リリース 9.3(3) 以降 : Kstack ローカルポートの範囲は 15001 ～ 58000、netstack ローカルポートの範囲は 58001 ～ 60535、nat ポートの範囲は 60536 ～ 65535
ステップ 5	feature ssh 例 : <pre>switch(config)# feature ssh</pre>	SSH を有効にします。
ステップ 6	exit 例 : <pre>switch(config)# exit switch#</pre>	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。

	コマンドまたはアクション	目的
ステップ 7	(任意) show running-config security all 例 : switch# ssh port 58003	セキュリティの設定を表示します。
ステップ 8	(任意) copy running-config startup-config 例 : switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH ホストのクリア

サーバから SCP または SFTP を使用してファイルをダウンロードする場合、またはこのデバイスからリモート ホストに SSH セッションを開始する場合には、そのサーバと信頼できる SSH 関係が確立されます。ユーザ アカウントの、信頼できる SSH サーバのリストはクリアすることができます。

Procedure

	Command or Action	Purpose
ステップ 1	clear ssh hosts Example: switch# clear ssh hosts	SSH ホスト セッションおよび既知のホスト ファイルをクリアします。

SSH サーバのディセーブル化

Cisco NX-OS では、デフォルトで SSH サーバがイネーブルになっています。SSH サーバをディセーブルにすると、SSH でスイッチにアクセスすることを防止できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 feature ssh Example: switch(config)# no feature ssh	SSH を無効にします。

	Command or Action	Purpose
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	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 4	(Optional) show ssh server Example: <pre>switch# show ssh server</pre>	SSH サーバの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH サーバ キーの削除

SSH サーバをディセーブルにした後、Cisco NX-OS デバイス上の SSH サーバ キーを削除できます。



Note SSH を再度イネーブルにするには、まず、SSH サーバ キーを生成する必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 feature ssh Example: <pre>switch(config)# no feature ssh</pre>	SSH を無効にします。
ステップ 3	no ssh key[dsa rsa ecdsa] Example: <pre>switch(config)# no ssh key rsa</pre>	SSH サーバ キーを削除します。 デフォルトでは、すべての SSH キーが削除されます。
ステップ 4	exit Example:	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。

	Command or Action	Purpose
	switch(config)# exit switch#	
ステップ 5	(Optional) show ssh key Example: switch# show ssh key	SSH サーバ キーの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics
[SSH サーバ キーの生成](#) (175 ページ)

SSH セッションのクリア

Cisco NX-OS デバイスから SSH セッションをクリアできます。

Procedure

	Command or Action	Purpose
ステップ 1	show users Example: switch# show users	ユーザ セッション情報を表示します。
ステップ 2	clear line vty-line Example: switch(config)# clear line pts/12	ユーザ SSHセッションをクリアします。

Telnet の設定

ここでは、Cisco NX-OS デバイスで Telnet を設定する手順を説明します。

Telnet サーバのイネーブル化

Cisco NX-OS デバイス上で Telnet サーバをイネーブルにできます。デフォルトでは、Telnet はディセーブルです。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	feature telnet Example: <pre>switch(config)# feature telnet</pre>	Telnet サーバをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	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 4	(Optional) show telnet server Example: <pre>switch# show telnet server</pre>	Telnet サーバの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

リモート デバイスとの Telnet セッションの開始

Cisco NX-OS デバイスから SSH セッションを開始して、リモート デバイスと接続できます。IPv4 または IPv6 のいずれかを使用して Telnet セッションを開始できます。

Before you begin

リモート デバイスのホスト名または IP アドレスと、必要な場合はリモート デバイスのユーザ名を取得します。

Cisco NX-OS デバイス上で Telnet サーバを有効にします。

リモート デバイス上で Telnet サーバを有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	telnet { <i>ipv4-address</i> <i>host-name</i> } [<i>port-number</i>] [vrf <i>vrf-name</i>] Example: switch# telnet 10.10.1.1	IPv4 を使用してリモート デバイスとの Telnet セッションを開始します。デフォルトのポート番号は 23 です。値の範囲は 1 ～ 65535 です。デフォルトの VRF はデフォルト VRF です。
ステップ 2	telnet6 { <i>ipv6-address</i> <i>host-name</i> } [<i>port-number</i>] [vrf <i>vrf-name</i>] Example: switch# telnet6 2001:0DB8::ABCD:1 vrf management	IPv6 を使用してリモート デバイスとの Telnet セッションを開始します。デフォルトのポート番号は 23 です。値の範囲は 1 ～ 65535 です。デフォルトの VRF はデフォルト VRF です。

Related Topics

[Telnet サーバのイネーブル化](#) (197 ページ)

Telnet セッションのクリア

Cisco NX-OS デバイスから Telnet セッションをクリアできます。

Before you begin

Cisco NX-OS デバイス上で Telnet サーバをイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	show users Example: switch# show users	ユーザ セッション情報を表示します。
ステップ 2	clear line vty-line Example: switch(config)# clear line pts/12	ユーザ Telnet セッションをクリアします。

SSH および Telnet の設定の確認

SSH および Telnet の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ssh key [<i>dsa</i> <i>rsa</i>] [<i>md5</i>]	SSH サーバ キーを表示します。 Cisco NX-OS リリース 7.0(3)I4(6) および 7.0(3)I6(1) 以降のリリースでは、このコマンドはデフォルトで SHA256 形式でフィンガープリントを表示します。SHA256 は、以前のデフォルトの MD5 形式よりも安全です。ただし、フィンガープリントを MD5 形式で表示する必要がある場合の下位互換性のために、 md5 オプションが追加されています。
show running-config security [<i>all</i>]	実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。 all キーワードを指定すると、SSH およびユーザ アカウントのデフォルト値が表示されます。
show ssh server	SSH サーバの設定を表示します。
show telnet server	Telnet サーバの設定を表示します。
show username <i>username</i> <i>keypair</i>	指定したユーザの公開キーを表示します。
show user-account	設定されたユーザ アカウントの詳細を表示します。
show users	デバイスにログオンしているユーザが表示されます。
show crypto ca certificates	X.509v3 証明書ベースの SSH 認証に設定された CA 証明書および関連するトラストポイントを表示します。
show crypto ca crl <i>trustpoint</i>	指定したトラストポイントの CRL リストの内容を表示します。

SSH の設定例

次の例は、OpenSSH キーを使用して SSH を設定する方法を示しています。

Procedure

ステップ 1 SSH サーバをディセーブルにします。

Example:

```
switch# configure terminal
switch(config)# no feature ssh
```

ステップ 2 SSH サーバ キーを生成します。

Example:

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
generated rsa key
```

ステップ 3 SSH サーバをイネーブルにします。

Example:

```
switch(config)# feature ssh
```

ステップ 4 SSH サーバ キーを表示します。

Example:

```
switch(config)# show ssh key
could not retrieve dsa key information
*****
rsa Keys generated:Tue Mar 14 13:13:47 2017

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDh4+DZboQJbJt10nJhgKBYL5l0lhsFM2oZRi9+JqEU
GA44I9ej+E5NIRZ1x8ohIt6Vx9Et5csO7Pw72rjUwR3UPmuAm79k7I/SyLGEP3WUL7sqbLvNF5GqKXph
oqMT075WUdbGWphorA2g0tTObrRrFIQBJVQ0SSBh3oEaaALqYUQ==

bitcount:1024
fingerprint:
SHA256:V6KAeLAiKRRUPBZmlYq3rl6JW7Eo7vhLi6CXYxnD/+Y
*****
*****

switch(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2013

ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr
+MZm99n2U0ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39
HmXL6VgprVn1XQFiBwn4na+Hld3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
*****
could not retrieve dsa key information
*****
```

ステップ 5 OpenSSH 形式の SSH 公開キーを指定します。

Example:

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIWAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50r
v7gsEPjhOBYmsi6PAVKui1nIf/DQhum+1JNqJP/eLowb7ubO+1VKRXFY/G+1JNlIQ
W3g9igG30c6k6+XVn+Njn1lB7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyzIEh5
4Tplx8=
```

ステップ 6 設定を保存します。

Example:

```
switch(config)# copy running-config startup-config
```

SSH のパスワードが不要なファイルコピーの設定例

次に、Cisco NX-OS デバイスから Secure Copy (SCP) サーバまたは Secure FTP (SFTP) サーバに、パスワードなしでファイルをコピーする例を示します。

Procedure

ステップ 1 SSH の公開キーと秘密キーを生成し、指定したユーザの Cisco NX-OS デバイスのホーム ディレクトリに格納します。

Example:

```
switch# configure terminal
switch(config)# username admin keypair generate rsa
generating rsa key(1024 bits).....
generated rsa key
```

ステップ 2 指定したユーザの公開キーを表示します。

Example:

```
switch(config)# show username admin keypair

*****

rsa Keys generated: Thu Jul  9 11:10:29 2013

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcVnrMbx2BmD0P8boZE1TfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoaJzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
*****

could not retrieve dsa key information
*****
```

ステップ 3 Cisco NX-OS デバイスのホーム ディレクトリから、指定したブートフラッシュ ディレクトリに、公開キーと秘密キーをエクスポートします。

Example:

```
switch(config)# username admin keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
```



```

.
.
.
951      Jul 09 11:13:59 2013  key_rsa
221      Jul 09 11:14:00 2013  key_rsa.pub
.
.

```

ステップ 4 これら 2 つのファイルを他の Cisco NX-OS デバイスへコピーした後、**copy scp** または **copy sftp** コマンドを使用して、Cisco NX-OS デバイスのホーム ディレクトリにインポートします。

Example:

```

switch(config)# username admin keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# show username admin keypair
*****

rsa Keys generated: Thu Jul  9 11:10:29 2013

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZE1TfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
*****

could not retrieve dsa key information
*****
switch(config)#

```

ステップ 5 SCP サーバまたは SFTP サーバで、key_rsa.pub に格納されている公開キーを authorized_keys ファイルに追加します。

Example:

```
$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys
```

これで、標準の SSH コマンドおよび SCP コマンドを使用してパスワードを指定しなくても、Cisco NX-OS デバイスからサーバにファイルをコピーできます。

ステップ 6 (Optional) DSA キーについてこの手順を繰り返します。

X.509v3 証明書ベースの SSH 認証の設定例

次の例は、X.509v3 証明書を使用する SSH 認証の設定方法を示しています。



- (注) Cisco NX-OS リリース 10.4(3)F 以降、Cisco Nexus 9000 シリーズ スイッチは、TACACS+ サーバを介し、X.509 証明書を使用した SSH 認証をサポートしています。この機能は、RADIUS ではサポートされていません。

```

configure terminal
username jsmith password 4Ty18Rnt
username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith"
  rsa
crypto ca trustpoint tp1
crypto ca authenticate tp1
crypto ca crt request tp1 bootflash:crl1.crl

show crypto ca certificates
Trustpoint: tp1
CA certificate 0:
subject= /CN=SecDevCA
issuer= /CN=SecDevCA
serial=01AB02CD03EF04GH05IJ06KL07MN
notBefore=Jun 29 12:36:26 2016 GMT
notAfter=Jun 29 12:46:23 2021 GMT
SHA1 Fingerprint=47:29:E3:00:C1:C1:47:F2:56:8B:AC:B2:1C:64:48:FC:F4:8D:53:AF
purposes: sslserver sslclient

show crypto ca crt tp1
Trustpoint: tp1 CRL: Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /CN=SecDevCA
  Last Update: Aug 8 20:03:15 2016 GMT
  Next Update: Aug 16 08:23:15 2016 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:30:43:AA:80:10:FE:72:00:DE:2F:A2:17:E4:61:61:44:CE:78:FF:2A

show user-account
user:user1
  this user account has no expiry date
  roles:network-operator
  ssh cert DN : /C = US, ST = New York, L = Metropolis, O = cisco , OU = csg, CN
= user1; Algo: x509v3-sign-rsa

show users
NAME      LINE      TIME      IDLE      PID      COMMENT
user1     pts/1     Jul 27 18:43 00:03     18796    (10.10.10.1) session=ssh

```

SSH および Telnet に関する追加情報

ここでは、SSH および Telnet の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	Cisco NX-OS ライセンス ガイド
VRF コンフィギュレーション	『Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング 設定ガイド』

RFC

RFC	タイトル
RFC 6187	セキュアシェル認証用のX.509v3証明書

MIB

MIB	MIB のリンク
SSH および Telnet に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 9 章

PKI の設定

この章では、Cisco NX-OS での公開キー インフラストラクチャ（PKI）のサポートについて説明します。PKI を使用すると、ネットワーク上で通信を安全に行うためのデジタル証明書をデバイスが入手して使用できるようになり、セキュアシェル（SSH）の管理性と拡張性も向上します。

この章は、次の項で構成されています。

- [PKI の概要, on page 207](#)
- [PKI の注意事項と制約事項（214 ページ）](#)
- [PKI のデフォルト設定, on page 215](#)
- [CA の設定とデジタル証明書, on page 215](#)
- [PKI の設定の確認, on page 236](#)
- [PKI の設定例, on page 236](#)
- [PKI に関する追加情報, on page 272](#)
- [Cisco SUDI 証明書チェーンを使用したデバイス構成証明（272 ページ）](#)

PKI の概要

ここでは、PKI について説明します。

CA とデジタル証明書

証明機関（CA）は証明書要求を管理して、ホスト、ネットワーク デバイス、ユーザなどの参加エンティティに証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

デジタル署名は、公開キー暗号法に基づいて、デバイスや個々のユーザをデジタル的に認証します。RSA 暗号化システムなどの公開キー暗号法では、各デバイスやユーザはキー ペアを持ち、これには秘密キーと公開キーが含まれています。秘密キーは秘密裡に保管し、これを知っているのは所有するデバイスまたはユーザだけです。一方、公開キーは誰もが知っているものです。これらのキーの一方で暗号化されたものは、他方のキーで復号化できます。署名は、送信者の秘密キーを使用してデータを暗号化したときに作成されます。受信側は、送信側の公開

キーを使用してメッセージを復号化することで、シグニチャを検証します。このプロセスは、受信者が送信者の公開キーのコピーを持っていて、これが本当に送信者のものであり、送信者を騙る他人のものではないことを高い確実性を持って知っていることを基盤としています。

デジタル証明書は、デジタル署名と送信者を結び付けるものです。デジタル証明書には、名前、シリアル番号、企業、部署または IP アドレスなど、ユーザまたはデバイスを特定する情報を含んでいます。また、エンティティの公開キーのコピーも含んでいます。証明書に署名する CA は、受信者が明示的に信頼する第三者機関であり、アイデンティティの正当性を立証し、デジタル証明書を作成します。

CA のシグニチャを検証するには、受信者は、CA の公開キーを認識する必要があります。一般的にはこのプロセスはアウトオブバンドか、インストール時に行われる操作によって処理されます。たとえば、通常の Web ブラウザでは、デフォルトで、複数の CA の公開キーが設定されています。

信頼モデル、トラストポイント、アイデンティティ CA

PKI の信頼モデルは、設定変更が可能な複数の信頼できる CA によって階層化されています。信頼できる CA のリストを使用して各参加デバイスを設定して、セキュリティプロトコルの交換の際に入手したピアの証明書がローカルに信頼できる CA のいずれかで発行されていた場合には、これを認証できるようにすることができます。Cisco NX-OS ソフトウェアでは、信頼できる CA の自己署名ルート証明書（または下位 CA の証明書チェーン）をローカルに保存しています。信頼できる CA のルート証明書（または下位 CA の場合には全体のチェーン）を安全に入手するプロセスを、CA 認証と呼びます。

信頼できる CA について設定された情報をトラストポイントと呼び、CA 自体もトラストポイント CA と呼びます。この情報は、CA 証明書（下位 CA の場合は証明書チェーン）と証明書取消確認情報で構成されています。

Cisco NX-OS デバイスは、トラストポイントに登録して、アイデンティティ証明書を入手し、キーペアと関連付けることができます。このトラストポイントをアイデンティティ CA と呼びます。

CA 証明書の階層

セキュアサービスの場合、通常は複数の信頼できる CA があります。CA は通常、すべてのホストにバンドルとしてインストールされます。NX-OS PKI インフラストラクチャは、証明書チェーンのインポートをサポートします。ただし、現在の CLI では、一度に 1 つのチェーンをインストールできます。インストールする CA チェーンが複数ある場合、この手順は面倒です。これには、複数の中間 CA とルート CA を含む CA バンドルをダウンロードする機能が必要です。

CA バンドルのインポート

crypto CA trustpoint コマンドは、CA 証明書、CRL、アイデンティティ証明書、およびキーペアを名前付きラベルにバインドします。これらの各エンティティに対応するすべてのファイルは、NX-OS certstore ディレクトリ（/isan/etc/certstore）に保存され、トラストポイントラベルでタグ付けされます。

CA証明書にアクセスするには、SSLアプリケーションは標準のNX-OS証明書ストアをポイントし、SSL初期化中にCAパスとして指定するだけです。CAがインストールされているトラストポイントラベルを認識する必要はありません。

クライアントがアイデンティティ証明書にバインドする必要がある場合は、トラストポイントラベルをバインディングポイントとして使用する必要があります。

`import pkcs` コマンドは、トラストポイントラベルの下にCA証明書をインストールするように拡張されています。CAバンドルをインストールするようにさらに拡張できます。`import` コマンド構造が変更され、`pkcs7`形式のCAバンドルファイルを提供するために使用される`pkcs7`オプションが追加されました。

Cisco NX-OS リリース 10.1(1) 以降、CA バンドルを解凍し、独自のラベルの下に各 CA チェーンをインストールするために、`pkcs7` ファイル形式がサポートされています。ラベルは、メイントラストポイントラベルにインデックスを追加することによって形成されます。

一度インストールすると、バンドルへのすべてのCAチェーンの論理バインディングはありません。

PKCS7 形式での CA 証明書バンドルのインポート

複数の独立した証明書チェーンで構成される CA 証明書バンドルのインポートをサポートするために、`'pkcs7'` のオプションが `crypto import` コマンドに導入されました。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 ca import <baselabel> pkcs7 <uri0> force	コマンドには2つの入力引数があります。Ca バンドルファイルであるソースファイルは、<code><uri0></code>、入力ファイルは <code>pkcs7</code> 形式である必要があります。これは <code>cabundle</code> ファイルであることを示します。 複数の証明書チェーンが <code>cabundle</code> から抽出されます。このコマンドは、CA証明書チェーンが接続された複数のトラストポイントを生成します。<code>import</code> コマンドは、グローバルCAバンドル構成と、生成された各トラストポイントごとのCAバンドル下位構成の、2つの構成を生成します。

	コマンドまたはアクション	目的
		force オプションを指定すると、CA バンドルおよび関連するトラストポイント構成が削除され、同じバンドル名を持つ新しい CA バンドルがインポートされ、その CA バンドルに関連する新しいトラストポイント構成が生成されます。
ステップ 3	crypto ca cabundle <bundle-name>	bundle-name は、インポートの場合の baselabel と同じです。このコマンドの no 形式を使用すると、CA バンドル、トラストポイント、および関連する証明書チェーンを削除できます。 特定のベースラベル名で CA バンドルをインポートし、すべてのトラストポイントを生成した後、ユーザーが同じベースラベル名で import コマンドを再度実行しようとする、CA バンドルがすでに存在するというエラーがスローされます。ユーザーは force オプションを使用して、既存の CA バンドルを変更できます。 サポートされる CA バンドルの最大数は 20 です。
ステップ 4	exit 例 : <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(任意) show crypto ca certificates 例 : <pre>switch# show crypto ca certificates</pre>	CA 証明書を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

RSA のキー ペアとアイデンティティ証明書

アイデンティティ証明書を入手するには、1 つまたは複数の RSA キー ペアを作成し、各 RSA キー ペアと Cisco NX-OS デバイスが登録しようとしているトラストポイント CA を関連付けま

す。Cisco NX-OS デバイスは、CA ごとにアイデンティティを 1 つだけ必要とします。これは CA ごとに 1 つのキー ペアと 1 つのアイデンティティ証明書で構成されています。

Cisco NX-OS ソフトウェアでは、設定変更が可能なキーのサイズ（またはモジュラス）で RSA キー ペアを作成できます。デフォルトのキーのサイズは 512 です。また、RSA キー ペアのラベルも設定できます。デフォルトのキーラベルは、デバイスの完全修飾ドメイン名（FQDN）です。

トラストポイント、RSA キー ペア、およびアイデンティティ証明書の関係を要約したものを次に示します。

- トラストポイントとは、Cisco NX-OS デバイスが、あらゆるアプリケーション（SSH など）のピア証明書用に信頼する特定の CA です。
- Cisco NX-OS デバイスでは、デバイス上に多くのトラストポイントを置くことができ、デバイス上のすべてのアプリケーションは、任意のトラストポイント CA によって発行されたピア証明書を信頼できます。
- トラストポイントは特定のアプリケーション用に限定されません。
- Cisco NX-OS デバイスは、トラストポイントに対応する CA に登録して、アイデンティティ証明書を入手します。デバイスは複数のトラストポイントに登録できます。これは、各トラストポイントから異なるアイデンティティ証明書を入手できることを意味します。アイデンティティ証明書は、発行する CA によって証明書に指定されている目的に応じてアプリケーションで使用します。証明書の目的は、証明書の拡張機能として証明書に保存されます。
- トラストポイントに登録するときには、証明を受ける RSA キー ペアを指定する必要があります。このキーペアは、登録要求を作成する前に作成されていて、トラストポイントに関連付けられている必要があります。トラストポイント、キーペア、およびアイデンティティ証明書との間のアソシエーション（関連付け）は、証明書、キーペア、またはトラストポイントが削除されて明示的になくなるまで有効です。
- アイデンティティ証明書のサブジェクト名は、Cisco NX-OS デバイスの完全修飾ドメイン名です。
- デバイス上には 1 つまたは複数の RSA キー ペアを作成でき、それぞれを 1 つまたは複数のトラストポイントに関連付けることができます。しかし、1 つのトラストポイントに関連付けられるキー ペアは 1 だけです。これは 1 つの CA からは 1 つのアイデンティティ証明書しか入手できないことを意味します。
- Cisco NX-OS デバイスが複数のアイデンティティ証明書を（それぞれ別の CA から）入手する場合は、アプリケーションがピアとのセキュリティプロトコルの交換で使用する証明書は、アプリケーション固有のものになります。
- 1 つのアプリケーションに 1 つまたは複数のトラストポイントを指定する必要はありません。証明書の目的がアプリケーションの要件を満たしていれば、どのアプリケーションもあらゆるトラストポイントで発行されたあらゆる証明書を使用できます。
- あるトラストポイントから複数のアイデンティティ証明書を入手したり、あるトラストポイントに複数のキー ペアに関連付ける必要はありません。ある CA はあるアイデンティ

ティ（または名前）を1回だけ証明し、同じ名前で複数の証明書を発行することはありません。ある CA から複数のアイデンティティ証明書を入手する必要があり、またその CA が同じ名前で複数の証明書の発行を許可している場合は、同じ CA 用の別のトラストポイントを定義して、別のキー ペアを関連付け、証明を受ける必要があります。

複数の信頼できる CA のサポート

Cisco NX-OS デバイスは、複数のトラストポイントを設定して、それぞれを別の CA に関連付けることにより、複数の CA を信頼できるようになります。信頼できる CA が複数あると、ピアに証明書を発行した特定の CA にデバイスを登録する必要がなくなります。代わりに、ピアが信頼する複数の信頼できる CA をデバイスに設定できます。すると、Cisco NX-OS デバイスは設定されている信頼できる CA を使用して、ピアから受信した証明書で、ピア デバイスの ID で定義されている CA から発行されたものではないものを検証できるようになります。

PKI の登録のサポート

登録とは、SSHなどのアプリケーションに使用するデバイス用のアイデンティティ証明書を入手するプロセスです。これは、証明書を要求するデバイスと、認証局の間で生じます。

Cisco NX-OS デバイスでは、PKI 登録プロセスを実行する際に、次の手順を取ります。

- デバイスで RSA の秘密キーと公開キーのペアを作成します。
- 標準の形式で証明書要求を作成し、CA に送ります。



Note 要求が CA で受信されたとき、CA サーバでは CA アドミニストレータが登録要求を手動で承認しなくてはならない場合があります。

- 発行された証明書を CA から受け取ります。これは CA の秘密キーで署名されています。
- デバイスの不揮発性のストレージ領域（ブートフラッシュ）に証明書を書き込みます。

カットアンドペーストによる手動での登録

Cisco NX-OS ソフトウェアでは、手動でのカットアンドペーストによる証明書の取得と登録をサポートしています。カットアンドペーストによる登録とは、証明書要求をカットアンドペーストして、デバイスと CA 間で認証を行うことを意味します。

手動による登録プロセスでカットアンドペーストを使用するには、次の手順を実行する必要があります。

- 証明書登録要求を作成します。これは Cisco NX-OS デバイスで base64 でエンコードされたテキスト形式として表示されます。

- エンコードされた証明書要求のテキストを E メールまたは Web フォームにカットアンドペーストし、CA に送ります。
- 発行された証明書（base64 でエンコードされたテキスト形式）を CA から E メールまたは Web ブラウザによるダウンロードで受け取ります。
- 証明書のインポート機能を使用して、発行された証明書をデバイスにカットアンドペーストします。

複数の RSA キー ペアとアイデンティティ CA のサポート

複数のアイデンティティ CA を使用すると、デバイスが複数のトラストポイントに登録できるようになり、その結果、別々の CA から複数のアイデンティティ証明書が発行されます。この機能によって、Cisco NX-OS デバイスは複数のピアを持つ SSH およびアプリケーションに、これらのピアに対応する CA から発行された証明書を使用して参加できるようになります。

また複数の RSA キー ペアの機能を使用すると、登録している各 CA ごとの別々のキー ペアをデバイスで持てるようになります。これは、他の CA で指定されているキーの長さなどの要件と競合することなく、各 CA のポリシー要件に適合させることができます。デバイスでは複数の RSA キー ペアを作成して、各キー ペアを別々のトラストポイントに関連付けることができます。したがって、トラストポイントに登録するときには、関連付けられたキー ペアを証明書要求の作成に使用します。

ピア証明書の検証

PKI では、Cisco NX-OS デバイスでのピア証明書の検証機能をサポートしています。Cisco NX-OS では、SSH などのアプリケーションのためのセキュリティ交換の際にピアから受け取った証明書を検証します。アプリケーションはピア証明書の正当性を検証します。Cisco NX-OS ソフトウェアでは、ピア証明書の検証の際に次の手順を実行します。

- ピア証明書がローカルの信頼できる CA のいずれかから発行されていることを確認します。
- ピア証明書が現在時刻において有効であること（期限切れでない）ことを確認します。
- ピア証明書が、発行した CA によって取り消されていないことを確認します。

取消確認については、Cisco NX-OS ソフトウェアでは証明書失効リスト（CRL）をサポートしています。トラストポイント CA ではこの方法を使用して、ピア証明書が取り消されていないことを確認できます。

証明書の取消確認

Cisco NX-OS ソフトウェアでは、CA 証明書の取消のステータスを確認できます。アプリケーションでは、指定した順序に従って取消確認メカニズムを使用できます。CRL、NDcPP:OCSP for Syslog、なし、またはこれらの方式の組み合わせを指定できます。

CRL のサポート

CA では証明書失効リスト (CRL) を管理して、有効期限前に取り消された証明書についての情報を提供します。CA では CRL をリポジトリで公開して、発行したすべての証明書の中にダウンロード用の公開 URL 情報を記載しています。ピア証明書を検証するクライアントは、発行した CA から最新の CRL を入手して、これを使用して証明書が取り消されていないかどうかを確認できます。クライアントは、自身の信頼できる CA のすべてまたは一部の CRL をローカルにキャッシュして、その CRL が期限切れになるまで必要に応じて使用することができます。

Cisco NX-OS ソフトウェアでは、先にダウンロードしたトラストポイントについての CRL を手動で設定して、これをデバイスのブートフラッシュ (cert-store) にキャッシュすることができます。ピア証明書の検証の際、Cisco NX-OS ソフトウェアは、CRL がすでにローカルにキャッシュされていて、取消確認でこの CRL を使用するよう設定されている場合にだけ、発行した CA からの CRL をチェックします。それ以外の場合、Cisco NX-OS ソフトウェアでは CRL チェックを実行せず、他の取消確認方式が設定されている場合を除き、証明書は取り消されていないと見なします。

NDcPP : syslog の OCSP

Online Certificate Status Protocol (OCSP) は、ピアがこの失効情報を取得し、それを検証して証明書失効ステータスを確認する必要がある場合に、証明書失効をチェックする方法です。この方式では、クラウドを介して OCSP レスポンダに到達するピアの機能、または証明書失効情報を取得する証明書送信者のパフォーマンスによって、証明書失効ステータスが制限されます。

リモート syslog サーバが OCSP レスポンダ URL を持つ証明書を共有すると、クライアントはサーバ証明書を外部 OCSP レスポンダ (CA) サーバに送信します。CA サーバはこの証明書を検証し、有効な証明書か失効した証明書かを確認します。この場合、クライアントは失効した証明書リストをローカルに保持する必要はありません。

証明書と対応するキー ペアのインポートとエクスポート

CA 認証と登録のプロセスの一環として、下位 CA 証明書 (または証明書チェーン) とアイデンティティ証明書を標準の PEM (base64) 形式でインポートできます。

トラストポイントでのアイデンティティ情報全体を、パスワードで保護される PKCS#12 標準形式でファイルにエクスポートできます。このファイルは、後で同じデバイス (システムクラッシュの後など) や交換したデバイスにインポートすることができます。PKCS#12 ファイル内の情報は、RSA キー ペア、アイデンティティ証明書、および CA 証明書 (またはチェーン) で構成されています。

PKI の注意事項と制約事項

PKI に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイスに設定できるキー ペアの最大数は 16 です。

- Cisco NX-OS デバイスで宣言できるトラスト ポイントの最大数は 16 です。
- Cisco NX-OS デバイスに設定できるアイデンティティ証明書の最大数は 16 です。
- CA 証明書チェーン内の証明書の最大数は 10 です。
- ある CA に対して認証できるトラストポイントの最大数は 10 です。
- 設定のロールバックでは PKI の設定はサポートしていません。
- Cisco NX-OS リリース 9.3 (5) 以降では、Cisco NX-OS ソフトウェアは NDCPP: OCSP for Syslog をサポートしています。
- Cisco NX-OS リリース 10.3(3)F 以降、Cisco Nexus スイッチで証明書を生成およびインポートするために、楕円曲線暗号 (ECC) キー ペアのサポートが提供されます。



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

PKI のデフォルト設定

次の表に、PKI パラメータのデフォルト設定を示します。

Table 12: PKI パラメータのデフォルト値

パラメータ	デフォルト
トラスト ポイント	なし
RSA キー ペア	なし
RSA キー ペアのラベル	デバイスの FQDN
RSA キー ペアのモジュール	512
RSA キー ペアのエクスポートの可否	イネーブル
取消確認方式	CRL

CA の設定とデジタル証明書

ここでは、Cisco NX-OS デバイス上で CA とデジタル証明書が相互に連携して動作するようにするために、実行が必要な作業について説明します。

ホスト名と IP ドメイン名の設定

デバイスのホスト名または IP ドメイン名をまだ設定していない場合は、設定する必要があります。これは、Cisco NX-OS ソフトウェアでは、アイデンティティ証明書のサブジェクトとして完全修飾ドメイン名 (FQDN) を使用するためです。また、Cisco NX-OS ソフトウェアでは、キーの作成の際にラベルが指定されていないと、デバイスの FQDN をデフォルトのキー ラベルとして使用します。たとえば、DeviceA.example.com という名前の証明書は、DeviceA というデバイスのホスト名と example.com というデバイスの IP ドメイン名に基づいています。



Caution

証明書を作成した後にホスト名または IP ドメイン名を変更すると、証明書が無効になります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 Example: switch(config)# hostname DeviceA	デバイスのホスト名を設定します。
ステップ 3	ip domain-name name [use-vrf vrf-name] Example: DeviceA(config)# ip domain-name example.com	デバイスの IP ドメイン名を設定します。VRF 名が指定されていないと、このコマンドではデフォルトの VRF を使用します。
ステップ 4	exit Example: switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show hosts Example: switch# show hosts	IP ドメイン名を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

RSA キー ペアの生成

RSA キー ペアは、アプリケーション向けのセキュリティプロトコルの交換時に、セキュリティペイロードの署名、暗号化、および復号化のために作成します。デバイスのための証明書を取得する前に、RSA キー ペアを作成する必要があります。

Cisco NX-OS リリース 9.3(3) 以降では、Cisco NX-OS デバイスをトラスト ポイント CA に関連付ける前に、明示的に RSA キー ペアを生成する必要があります。Cisco NX-OS リリース 9.3(3) よりも前では、使用できない場合、RSA キー ペアは自動生成されます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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-string] [exportable] [modulus size] Example: <pre>switch(config)# crypto key generate rsa exportable</pre>	RSA キー ペアを生成します。デバイスに設定できるキー ペアの最大数は 16 です。 ラベル文字列には、大文字と小文字を区別して、最大 64 文字の英数字で値を指定します。デフォルトのラベル文字列は、ピリオド文字 (.) で区切ったホスト名と FQDN です。 有効なモジュラスの値は 512、768、1024、1536、2048、3072 および 4096 です。デフォルトのモジュラスのサイズは 512 です。 Note 適切なキーのモジュラスを決定する際には、Cisco NX-OS デバイスと CA（登録を計画している対象）のセキュリティポリシーを考慮する必要があります。 デフォルトでは、キーペアはエクスポートできません。エクスポート可能なキーペアだけ、PKCS#12 形式でエクスポートできます。 Caution キー ペアのエクスポートの可否は変更できません。

	Command or Action	Purpose
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show crypto key mypubkey rsa Example: <pre>switch# show crypto key mypubkey rsa</pre>	作成したキーを表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ECC キー ペアの生成

ECC キーペアは、アプリケーション向けのセキュリティプロトコルの交換時に、セキュリティペイロードの署名、暗号化、および復号化のために作成します。デバイスのための証明書を取得する前に、ECC キー ペアを作成する必要があります。ECC キーは、同じ長さの場合、RSA キーと比較して強力です。

Cisco NX-OS リリース 10.3(3)F リリース以降、ECC キー ペアを生成して、Cisco NX-OS デバイスをトラストポイント CA に関連付けることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 ecc [label ecc-key-label] [exportable] [modulus size] 例 : <pre>switch(config)# crypto key generate ecc exportable modulus 224</pre>	ECC キーペアを生成します。デバイスに設定できるキー ペアの最大数は 16 です。 ラベル文字列には最大 64 文字の英数字で値を指定します。大文字と小文字は区別されます。デフォルトのラベル文字列は、ピリオド文字 (.) で区切ったホスト名と FQDN です。

	コマンドまたはアクション	目的
		有効なモジュラス値は、224、384、および 521 です。デフォルトのモジュラスのサイズは 224 です。 (注) 適切なキーのモジュラスを決定する際には、Cisco NX-OS デバイスと CA（登録を計画している対象）のセキュリティポリシーを考慮する必要があります。 デフォルトでは、キーペアはエクスポートできません。エクスポート可能なキーペアだけ、PKCS#12 形式でエクスポートできます。 注意 キー ペアのエクスポートの可否は変更できません。
ステップ 3	no crypto key generate ecc [label ecc-key-label] 例 : <pre>switch(config)# no crypto key generate ecc label label-name</pre>	ECC キーを削除します。
ステップ 4	exit 例 : <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(任意) show crypto key mypubkey ecc 例 : <pre>switch# show crypto key mypubkey ecc</pre>	作成した ECC キーを表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

トラストポイント CA のアソシエーションの作成

Cisco NX-OS デバイスとトラスト ポイント CA を関連付ける必要があります。

Before you begin

RSA キー ペアを作成します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	crypto ca trustpoint name Example: <pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	デバイスが信頼するトラストポイント CA を宣言し、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。 Note 設定できるトラストポイントの最大数は 50 です。
ステップ 3	cabundle baselabel Example: <pre>switch(config-trustpoint)# cabundle test</pre>	特定の CA バンドル下でトラストポイントをグループ化します。このコマンドの No 形式を使用すると、CA バンドルからトラストポイントが切り離されます。このコマンドは、トラストポイントを既存の CA バンドルに関連付けます。新しい CA バンドルは設定しません。
ステップ 4	enrollment terminal Example: <pre>switch(config-trustpoint)# enrollment terminal</pre>	手動でのカットアンドペーストによる証明書の登録をイネーブルにします。デフォルトではイネーブルになっていません。 Note Cisco NX-OS ソフトウェアでは、手動でのカットアンドペースト方式による証明書の登録だけをサポートしています。
ステップ 5	rsakeypair label Example: <pre>switch(config-trustpoint)# rsakeypair SwitchA</pre>	RSA キー ペアのラベルを指定して、このトラストポイントを登録用に関連付けます。 Note CA ごとに 1 つの RSA キー ペアだけを指定できます。

	Command or Action	Purpose
ステップ 6	exit Example: <pre>switch(config-trustpoint)# exit switch(config)#</pre>	トラストポイントコンフィギュレーション モードを終了します。
ステップ 7	(Optional) show crypto ca trustpoints Example: <pre>switch(config)# show crypto ca trustpoints</pre>	トラストポイントの情報を表示します。
ステップ 8	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[RSA キー ペアの生成](#) (217 ページ)

証明書マッピングのフィルタの設定

認証に使用される CA 証明書を検証するためのマッピングのフィルタを設定できます。マッピングのフィルタは、CA 証明書をユーザ名と照合するために使用されます。

Cisco NX-OS は次の証明書マッピングのフィルタをサポートします。

- %username% : ユーザのログイン名が代入されます。
- %hostname% : ピアのホスト名が代入されます。

始める前に

証明書認証の cert-store を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 certificatemap mapname map-name 例 :	新しいフィルタ マップを作成します。

	コマンドまたはアクション	目的
ステップ 3	<pre>switch(config)# crypto certificatemap mapname filtermap1</pre> filter [subject-name <i>subject-name</i> altname-email <i>e-mail-ID</i> altname-upn <i>user-principal-name</i>] 例 : <pre>switch(config-certmap-filter)# filter altname-upn %username%@cisco.com</pre>	フィルタ マップ内で証明書マッピングのフィルタを 1 つまたは複数設定します。これらの証明書のフィールド属性は、フィルタでサポートされています。証明書は、マップで設定されたすべてのフィルタを通過した場合に検証にパスします。 • subject-name : 必要なサブジェクト名です。LDAP の認定者名 (DN) 文字列の形式で指定します。次に例を示します。 <pre>filter subject-name CN=%username%</pre> または <pre>filter subject-name /C=IN/ST=KA/L=BIR/O=CISCO/OU=ABC/OU=%username%</pre> • altname-email : サブジェクト名の代わりに証明書に含まれている必要がある E メールアドレスです。次に例を示します。 <pre>filter altname-email %username%@cisco.com</pre> • altname-upn : サブジェクト名の代わりに証明書に含まれている必要があるプリンシパル名です。次に例を示します。 <pre>filter altname-upn %username%@%hostname%</pre> 証明書は、マップで設定されたすべてのフィルタを通過した場合に検証にパスします。
ステップ 4	exit 例 : <pre>switch(config-certmap-filter)# exit switch(config)#</pre>	証明書マッピングのフィルタ コンフィギュレーション モードを終了します。
ステップ 5	(任意) crypto cert ssh-authorize [default issuer-CAname] [map map-name1 [map-name2]]	セキュア シェル (SSH) プロトコル用の証明書マッピングのフィルタを設定します。SSH 認証用のデフォルトのフィ

	コマンドまたはアクション	目的
	例 : <pre>switch(config)# crypto cert ssh-authorize default map filtermap1</pre>	ルタマップを使用するか、CA 証明書の発行元を指定できます。デフォルトのマップを使用しない場合は、認証用のフィルタマップを 1 つまたは 2 つ指定できます。 CA 証明書の発行元を指定した場合、ユーザアカウントにバインドされた証明書が検証され、設定されたマップのいずれかを通過すると検証にパスします。
ステップ 6	(任意) show crypto certificatemap 例 : <pre>switch(config)# show crypto certificatemap</pre>	証明書マッピングのフィルタを表示します。
ステップ 7	(任意) show crypto ssh-auth-map 例 : <pre>switch(config)# show crypto ssh-auth-map</pre>	SSH 認証用に設定されたマッピングのフィルタを表示します。
ステップ 8	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

CA の認証

CA が Cisco NX-OS デバイスに対して認証されると、CA を信頼するプロセスの設定が完了します。まず、PEM 形式の CA の自己署名証明書を入手し、Cisco NX-OS デバイスを CA に対して認証する必要があります。この証明書には、CA の公開キーが含まれています。この CA の証明書は自己署名（CA が自身の証明書に署名したもの）であるため、CA の公開キーは、CA アドミニストレータに連絡し、CA 証明書のフィンガープリントを比較して手動で認証する必要があります。



Note

認証する CA が他の CA の下位 CA である場合、認証する CA は自己署名 CA ではありません。その上位の CA がさらに別の CA の下位である場合もあります。最終的には自己署名 CA に到達します。このタイプの CA 証明書を、認証する CA の CA 証明書チェーンと呼びます。この場合は、CA 認証の際に、証明書チェーン内のすべての CA の CA 証明書の完全なリストを入力する必要があります。CA 証明書チェーン内の証明書の最大数は 10 です。

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 ca authenticate name pemfile uri0 Example: <pre>switch(config)# crypto ca authenticate admin-ca input (cut & paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : -----BEGIN CERTIFICATE----- MIIChCAAgAwIBAgIQWDSiaYQZFRSLjk0ZejABgJchkiC9wDQYJKoZIhvcNAQELBQAQ MBEjBgkqhkiG9w0BCQEWFzRFRmVlbnRlcnRlZjAxbjIyLTAxMDUyMTYtMTA0MRItEAMQ OQIEWILXUuPazE8ejaCBNEACIUhhichGyzIEOMAGALE CMVQZlZz8ezARBNvEStfclHnOb3UzUEjaCBNEMICUWwKUMSE QAFwONAIMDMjQ2cGFwONAIMDMjUIMicMICQSAHgCKZihndi AQEFPhWUZ3LQSpC2MinNdiEMKALUBMSUwejaCBNEAGIUh cmfrdFYIESMBALEBMQRZZFsb3UuMAVDQQEWdAnjoETMBEQ ALUCMMonUc3RcmFrZIESMBALEBMQRZhmENEMwDQKfKZihndi AQEFND3AAABAW/b3HXEBsiHziLnNdN87pyzwcsNZOXpeRXI CzePgIXIZASRUOLiHMRO/4lj8PwwKysAvFAaOBzCBDAIBGNH8 BMAcwDMDAPACH/EUAwEB/zABNMHQERQUuyjRdmrNR2oRoQ GsVHEwMDR0BGWjaucYgoicaFOdbz3ZZSwOCZYXOR5bzs IOFWXUSUjMNEnNjDawOGjLYzhmsZibvLxc3ULTAMENlcRbmJy hgCQBcmfrJULQBLG3BMFGCSGAQbjzAQDTAgFAAGCSGSib3QEP BUAPFAH6QH8E39TfwfEGCGyNLicNgIHARCOBjyt/MGPzsf9EA NBG7EOOn66zexOEOfGLVs6mXpl//w== -----END CERTIFICATE----- END OF INPUT Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12 Do you accept this certificate? [yes/no]: yes</pre>	CA の証明書をカットアンドペーストするようプロンプトが表示されます。CA を宣言したときに使用した名前と同じ名前を使用します。 また、CA チェーンを検証し、指定されたトラストポイントに直接接続します。 ある CA に対して認証できるトラストポイントの最大数は 10 です。 Note 下位 CA の認証の場合、Cisco NX-OS ソフトウェアでは、自己署名 CA に到達する CA 証明書の完全なチェーンが必要になります。これは証明書の検証や PKCS#12 形式でのエクスポートに CA チェーンが必要になるためです。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show crypto ca trustpoints Example: <pre>switch# show crypto ca trustpoints</pre>	トラストポイント CA の情報を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[トラストポイント CA のアソシエーションの作成](#) (219 ページ)

証明書取消確認方法の設定

クライアント（SSH ユーザなど）とのセキュリティ交換の際に、Cisco NX-OS デバイスは、クライアントから送られたピア証明書の検証を実行します。検証プロセスには、証明書の取消状況の確認が含まれます。

CA からダウンロードした CRL を確認するよう、デバイスに設定できます。CRL のダウンロードとローカルでの確認では、ネットワーク上にトラフィックは発生しません。しかし、証明書がダウンロードとダウンロードの途中で取り消され、デバイス側ではその取り消しに気付かない場合も考えられます。

Before you begin

CA を認証します。

CRL チェックを使用する場合は、CRL が設定済みであることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	crypto ca trustpoint name Example: <pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	トラストポイント CA を指定し、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	revocation-check {crl [none] none} Example: <pre>switch(config-trustpoint)# revocation-check none</pre>	証明書取消確認方法を設定します。デフォルトの方式は crl です。 Cisco NX-OS ソフトウェアでは、指定した順序に従って証明書取消方式を使用します。

	Command or Action	Purpose
ステップ 4	exit Example: <pre>switch(config-trustpoint)# exit switch(config)#</pre>	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ます。
ステップ 5	(Optional) show crypto ca trustpoints Example: <pre>switch(config)# show crypto ca trustpoints</pre>	トラストポイント CA の情報を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Related Topics

[CA の認証](#) (223 ページ)

[CRL の設定](#) (232 ページ)

証明書要求の作成

使用する各デバイスの RSA キーペア用に、対応するトラストポイント CA からアイデンティティ証明書を入手するために、要求を作成する必要があります。その後、表示された要求を CA 宛の E メールまたは Web サイトのフォームにカットアンドペーストします。

Before you begin

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	crypto ca enroll name Example: <pre>switch(config)# crypto ca enroll admin-ca</pre>	認証した CA に対する証明書要求を作成します。 Note

	Command or Action	Purpose
	Create the certificate request .. Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password:nbv123 The subject name in the certificate will be: DeviceA.cisco.com Include the switch serial number in the subject name? [yes/no]: no Include an IP address in the subject name [yes/no]: yes ip address:172.22.31.162 The certificate request will be displayed... <pre>-----BEGIN CERTIFICATE REQUEST----- MIByCQRQOQWHEaBgAIEFAAEMM5jANjy5j20gZ8DQY KZlhdNQEHQdGOMIGPoGFA8YUA2NC7UJD6SMNig2k8r14IK 0U8vN4q48AMZSIL4UjZw8LDKtYsjuOG7owj0Eh/y5IT9y E2NU8omqShvZgC7sVPMKqzh3pjhzgZHG9LXK4W4SC248S VgHDBAgBAGjZ4BkchdGw0BQxCMGm2MTzMDGCSgS1b3QET DjMCoQDRFQCHBsGZRMvM5jANjy5j22H4WH6LWQY KZlhdNQEHQdGMAK6KFRQ8nj0sDZHSFZh86HDe3Gc89GLEvt PftNBUE/pwH4yQl2T3eqVei2H15L33EF2k4BdI6U188HIDjgIMfja8 8a23NpS8dkwA8WkV18UZFKdjfngBNZaCU8ZqfMetH4U0+ -----END CERTIFICATE REQUEST-----</pre>	チャレンジパスワードを記憶しておいてください。このパスワードは設定と一緒に保存されません。証明書を取り消す必要がある場合には、このパスワードを入力する必要があります。
ステップ 3	exit Example: <pre>switch(config-trustpoint)# exit switch(config)#</pre>	トラストポイントコンフィギュレーション モードを終了します。
ステップ 4	(Optional) show crypto ca certificates Example: <pre>switch(config)# show crypto ca certificates</pre>	CA 証明書を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[トラストポイント CA のアソシエーションの作成](#) (219 ページ)

アイデンティティ証明書のインストール

アイデンティティ証明書は、CA から E メールまたは Web ブラウザ経由で base64 でエンコードされたテキスト形式で受信できます。CA から入手したアイデンティティ証明書を、エンコードされたテキストをカットアンドペーストしてインストールする必要があります。

Before you begin

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	crypto ca import name certificate Example: <pre>switch(config)# crypto ca import admin-ca certificate input (cut & paste) certificate in PEM format: -----BEGIN CERTIFICATE----- MIEFAOC6gawIEPgIKCj0oQAAAAcDABgkchidGwBQEAADCBgB4G CSgSib3DQEPFRFWLhtrZLBJeXjy5j20xCABgNBAYTAdONRtEAYD VQJIEwILYXUj2a2BxjAQBgMFAcUUhndhG9ZIRMAcAUECHMQ2Iz Y28wZARBgMFAStQ6lchNob3JhZ2MEjAQBgMFAmUkFwXUShQAPeR0v NIEBMTWZyNDhBw0NjBMTWMEjADABwGjABgNBAMIEVZlZ2ZlUEU Y2IyZ3A29hMIGMA0GCSqGSIb3DQEBAQAAQADCBiQBgQ/GNAQIjQ4IC dQlWcjgSICqjLk5eBhNQjQpacKsZEXjE2biyeCE8yindjwGE08x47 glxr42/sI9IRIb/8ud/cj9jSSBk56ca/MWA8ndE8jMChIM9lA/cpofQb x7RiId0dRfZBgsL7/Elash9LxwIQABo4ICEzCPg8wQMDRFRQH/Bsw GTRWwM2MMS5jaXjy5j22HwWH6wHQDAFOEBMEFKLi+2sqwEfgR bhwNlyc9jngMIFBgNH3BgQwGCAKcc8aD8w7IEANjskUBolFpxxcGW plCMIQMSwHjyKZLhxdNQBBhHwRZ3LQNPc2NurNubIEMAGAUe HMCsAkJAQBgMFAgIUthorGndGPHYIESMFAUEBMTqrLZ2F83JMQ4w DAVDQJkEWdANjoeIIMBGAUECMKorVOC3RcmFRZIESMFAUEPMQ8h orfhIENBjAFYKChQZIE9EiWMRLdVcGALU4HwRMGwLqsoCgGdHA6 Iy8a2UMDgQ2VycUu983c9BcGjbnEIMjE0S5jcmwMAucQ/G4tq3bU6 Ly8xXNz30wCEIXXORV5jb2s8EwXUjUSUMNEnNjdiBiqZlWwBBQU AQRFjBMDsCCsGAUEBzChl9odRwCi8xc3NlU4I0NlorFbnJkGwc3Nl U4A0RwXUjUSUMNEnNjclA9BgrBjRQwA0vZmlsZlZlLkcc3NlU4 XENlorFbnJkGcc3NlU4A0RwXUjUSUMNEnNjclANBgqchidGwBQAU AAFAADG8be7GNI9eCIMBNbr240623JdOdzUllgpridjPyejtsyflw E36cI2u4WsExREqxbTk8ycx7V5o= -----END CERTIFICATE-----</pre>	admin-ca という名前の CA に対するアイデンティティ証明書をカットアンドペーストするよう、プロンプトが表示されます。 デバイスに設定できるアイデンティティ証明書の最大数は 16 です。
ステップ 3	exit Example:	設定モードを終了します。

	Command or Action	Purpose
	switch(config)# exit switch#	
ステップ 4	(Optional) show crypto ca certificates Example: switch# show crypto ca certificates	CA 証明書を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[トラストポイント CA のアソシエーションの作成](#) (219 ページ)

トラストポイントの設定がリブート後も維持されていることの確認

トラストポイントの設定が、Cisco NX-OS デバイスのリブート後も維持されていることを確認できます。

トラストポイントの設定は、通常の Cisco NX-OS デバイスの設定であり、スタートアップ コンフィギュレーションに確実にコピーした場合にだけ、システムのリブート後も維持されます。トラストポイント設定をスタートアップ コンフィギュレーションにコピーしておけば、トラストポイントに関連する証明書、キー ペア、および CRL が自動的に保持されます。逆に、トラストポイントがスタートアップ コンフィギュレーションにコピーされていないと、証明書、キーペア、および関連 CRL は保持されません。リブート後に、対応するトラストポイント設定が必要になるからです。設定した証明書、キー ペア、および CRL を確実に保持するために、必ず、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてください。また、証明書またはキーペアを削除した後は実行コンフィギュレーションを保存して、削除が永続的に反映されるようにしてください。

トラストポイントに関連付けられた証明書と CRL は、そのトラストポイントがすでにスタートアップ コンフィギュレーションに保存されていれば、インポートした時点で（つまりスタートアップ コンフィギュレーションにコピーしなくても）維持されるようになります。

パスワードで保護したアイデンティティ証明書のバックアップを作成して、これを外部のサーバに保存することを推奨します。



Note コンフィギュレーションを外部サーバにコピーすると、証明書およびキー ペアも保存されます。

Related Topics

[PKCS 12 形式でのアイデンティティ情報のエクスポート](#) (230 ページ)

PKCS 12 形式でのアイデンティティ情報のエクスポート

アイデンティティ証明書を、トラストポイントの RSA キーペアや CA 証明書（または下位 CA の場合はチェーン全体）と一緒に PKCS#12 ファイルにバックアップ目的でエクスポートすることができます。デバイスのシステムクラッシュからの復元の際や、スーパーバイザモジュールの交換の際には、証明書や RSA キーペアをインポートすることができます。



Note エクスポートの URL を指定するときには使用できるのは、`bootflash:filename` という形式だけです。

Before you begin

CA を認証します。

アイデンティティ証明書をインストールします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 ca export name pkcs12 bootflash:filename password Example: <pre>switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre>	アイデンティティ証明書と、トラストポイント CA の対応するキーペアと CA 証明書をエクスポートします。パスワードには、大文字と小文字を区別して、最大 128 文字の英数字で値を指定します。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	copy bootflash:filename scheme://server/ [url /]filename Example: <pre>switch# copy bootflash:adminid.p12 tftp:adminid.p12</pre>	PKCS#12 形式のファイルをリモート サーバにコピーします。 scheme 引数に対しては、 tftp: 、 ftp: 、 scp: 、または sftp: を入力できます。 server 引数は、リモートサーバのアドレスまたは名前であり、 url 引数はリモートサーバにあるソース ファイルへのパスです。

	Command or Action	Purpose
		<i>server</i> 、 <i>url</i> 、および <i>filename</i> の各引数は、大文字小文字を区別して入力します。

Related Topics

[RSA キー ペアの生成](#) (217 ページ)

[CA の認証](#) (223 ページ)

[アイデンティティ証明書のインストール](#) (228 ページ)

PKCS 12または PKCS 7 フォーマットで ID 情報のインポート

デバイスのシステム クラッシュからの復元の際や、スーパーバイザ モジュールの交換の際には、証明書や RSA キー ペアをインポートすることができます。



Note インポートの URL を指定するときに使用できるのは、`bbootflash:filename f` という形式だけです。

Before you begin

CA 認証によってトラストポイントに関連付けられている RSA キー ペアがないこと、およびトラストポイントに関連付けられている CA がいないことを確認して、トラストポイントが空であるようにします。

Procedure

	Command or Action	Purpose
ステップ 1	copy scheme:// server/[url /]filename bootflash:filename Example: <pre>switch# copy tftp:adminid.p12 bootflash:adminid.p12</pre>	PKCS#12 形式のファイルをリモートサーバからコピーします。 <i>scheme</i> 引数に対しては、 tftp: 、 ftp: 、 scp: 、または sftp: を入力できます。 <i>server</i> 引数は、リモートサーバのアドレスまたは名前であり、 <i>url</i> 引数はリモートサーバにあるソース ファイルへのパスです。 <i>server</i> 、 <i>url</i> 、および <i>filename</i> の各引数は、大文字小文字を区別して入力します。
ステップ 2	configure terminal Example:	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

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 3	crypto ca import name [pkcs12 pkcs7] bootflash:filename Example: switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123	アイデンティティ証明書と、トラストポイント CA の対応するキーペアと CA 証明書をインポートします。
ステップ 4	exit Example: switch(config)# exit switch#	設定モードを終了します。
ステップ 5	(Optional) show crypto ca certificates Example: switch# show crypto ca certificates	CA 証明書を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

CRL の設定

トラストポイントからダウンロードした CRL を手動で設定することができます。Cisco NX-OS ソフトウェアでは、CRL をデバイスのブートフラッシュ (cert-store) にキャッシュします。ピア証明書の検証の際、Cisco NX-OS ソフトウェアが発行した CA からの CRL をチェックするのは、CRL をデバイスにダウンロードしていて、この CRL を使用する証明書取消確認を設定している場合だけです。

Before you begin

証明書取消確認がイネーブルになっていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	copy scheme:[//server/[url /]]filename bootflash:filename Example: switch# copy tftp:adminca.crl bootflash:adminca.crl	リモートサーバから CRL をダウンロードします。 <i>scheme</i> 引数に対しては、 tftp: 、 ftp: 、 scp: 、または sftp: を入力できます。 <i>server</i> 引数は、リモートサーバのアドレ

	Command or Action	Purpose
		スまたは名前であり、<i>url</i> 引数はリモートサーバにあるソース ファイルへのパスです。 <i>server</i>、<i>url</i>、および <i>filename</i> の各引数は、大文字小文字を区別して入力します。
ステップ 2	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 ca crt request name bootflash:filename Example: <pre>switch(config)# crypto ca crt request admin-ca bootflash:adminca.crl</pre>	ファイルで指定されている CRL を設定するか、現在の CRL と置き換えます。
ステップ 4	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show crypto ca crt name Example: <pre>switch# show crypto ca crt admin-ca</pre>	CA の CRL 情報を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

CA の設定からの証明書の削除

トラストポイントに設定されているアイデンティティ証明書や CA 証明書を削除できます。最初にアイデンティティ証明書を削除し、その後で CA 証明書を削除します。アイデンティティ証明書を削除した後で、RSA キー ペアとトラストポイントの関連付けを解除できます。証明書の削除は、期限切れになった証明書や取り消された証明書、破損した（あるいは破損したと思われる）キー ペア、現在は信頼されていない CA を削除するために必要です。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	crypto ca trustpoint name Example: <pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	トラストポイント CA を指定し、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	delete ca-certificate Example: <pre>switch(config-trustpoint)# delete ca-certificate</pre>	CA 証明書または証明書チェーンを削除します。
ステップ 4	delete certificate [force] Example: <pre>switch(config-trustpoint)# delete certificate</pre>	アイデンティティ証明書を削除します。 削除しようとしているアイデンティティ証明書が証明書チェーン内の最後の証明書である場合や、デバイス内の唯一のアイデンティティ証明書である場合は、force オプションを使用する必要があります。この要件は、証明書チェーン内の最後の証明書や唯一のアイデンティティ証明書を誤って削除してしまい、アプリケーション（SSH など）で使用する証明書がなくなってしまうことを防ぐために設けられています。
ステップ 5	exit Example: <pre>switch(config-trustpoint)# exit switch(config)#</pre>	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ます。
ステップ 6	(Optional) show crypto ca certificates [name] Example: <pre>switch(config)# show crypto ca certificates admin-ca</pre>	CA の証明書情報を表示します。

	Command or Action	Purpose
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco NX-OSデバイスからの RSA キー ペアの削除

RSA キー ペアが何らかの理由で破損し、現在は使用されていないと見られるときには、その RSA キー ペアを Cisco NX-OS デバイスから削除することができます。



Note

デバイスから RSA キー ペアを削除した後、CA アドミニストレータに、その CA にあるこのデバイスの証明書を取り消すよう依頼します。その証明書を最初に要求したときに作成したチャレンジ パスワードを入力する必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 zeroize rsa label Example: <pre>switch(config)# crypto key zeroize rsa MyKey</pre>	RSA キー ペアを削除します。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show crypto key mypubkey rsa Example: <pre>switch# show crypto key mypubkey rsa</pre>	RSA キー ペアの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[証明書要求の作成](#) (226 ページ)

PKI の設定の確認

PKI 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
<code>show crypto key mypubkey rsa</code>	Cisco NX-OS デバイスで作成された RSA 公開キーの情報を表示します。
<code>show crypto ca certificates</code>	CA とアイデンティティ証明書についての情報を表示します。
<code>show crypto ca crt</code>	CA の CRL についての情報を表示します。
<code>show crypto ca trustpoints</code>	CA トラストポイントについての情報を表示します。

PKI の設定例

ここでは、Microsoft Windows Certificate サーバを使用して Cisco NX-OS デバイスで証明書と CRL を設定する作業の例について説明します。

**Note**

デジタル証明書の作成には、どのようなタイプのサーバでも使用できます。Microsoft Windows Certificate サーバに限られることはありません。

Cisco NX-OS デバイスでの証明書の設定

Cisco NX-OS デバイスで証明書を設定するには、次の手順に従ってください。

Procedure

ステップ 1 デバイスの FQDN を設定します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# hostname Device-1
```

```
Device-1(config)#
```

ステップ 2 デバイスの DNS ドメイン名を設定します。

```
Device-1(config)# ip domain-name cisco.com
```

ステップ 3 トラストポイントを作成します。

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key:
revocation methods:  crt
```

ステップ 4 このデバイス用の RSA キー ペアを作成します。

```
Device-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Device-1(config)# show crypto key mypubkey rsa
key label: myKey
key size: 1024
exportable: yes
```

ステップ 5 RSA キー ペアとトラストポイントに関連付けます。

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# rsakeypair myKey
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key: myKey
revocation methods:  crt
```

ステップ 6 Microsoft Certificate Service の Web インターフェイスから CA をダウンロードします。

ステップ 7 トラストポイントに登録する CA を認証します。

```
Device-1(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPRI1jK0ZejaNBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1O
MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBGNVBACTCUJhbmdbG9yZTEOMAwGA1UE
ChMFQ21zY28xZzARBGNVBASTCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFWYXJuYSBD
QTAEfw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFWFuZGt1QGNpc2NvLmNvbTELMakGA1UEBhMCSU4xEjAQBGNVBAGTCUth
cm5hdGFrYTESMBAGA1UEBxMjQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVdaXNjbzETMBEG
A1UECXMkbnV0c3RvcnFnZTESMBAGA1UEAxMjQXBhcm5hIENBMFwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUowQliDM8rO/41jf8RxxvYKvysCAwEAaA0BvzCBvDALBGNVHQ8E
BAMCAYDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYYSUyMENBLmNybDAwOC6gLIYqZmlsZTovL1xc3N1LTA4XEN1cnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsbAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAAHv6UQ+8nE399Tww+KaGr0g0NIJaQNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y
```

```
Device-1(config)# show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May  3 22:46:37 2005 GMT
notAfter=May  3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

ステップ 8 トラストポイントに登録するために使用する証明書要求を作成します。

```
Device-1(config)# crypto ca enroll myCA
Create the certificate request ..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password: nbv123
The subject name in the certificate will be: Device-1.cisco.com
Include the switch serial number in the subject name? [yes/no]: no
Include an IP address in the subject name [yes/no]: yes
ip address: 10.10.1.1
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBGGA1UEAxMRVnYXNjb20wZGZ8wDQYJ
KoZIHvNAQEBAQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVA5MqNigJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAAGTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCsGSIb3DQEJ
DjEpMCCwJQYDVR0RAQH/BBswGYIRVnYXNjb20wZGZ8wDQYJ
KoZIHvNAQEBAQADgYEAkt60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PfrNcWUE/pw6HayfQ12T3ecgNwel2d15133YBF2bktExiI6U18nTOjg1XMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbJfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

ステップ 9 Microsoft Certificate Service の Web インターフェイスからアイデンティティ証明書を要求します。

ステップ 10 アイデンティティ証明書をインポートします。

```
Device-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBAkDEgMBAG
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjb20wZGZ8wDQYJ
KoZIHvNAQEBAQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVA5MqNigJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAAGTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCsGSIb3DQEJ
DjEpMCCwJQYDVR0RAQH/BBswGYIRVnYXNjb20wZGZ8wDQYJ
KoZIHvNAQEBAQADgYEAkt60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PfrNcWUE/pw6HayfQ12T3ecgNwel2d15133YBF2bktExiI6U18nTOjg1XMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbJfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE-----
```

```

DAYDVQQKEwVDAxNjBzETMBEGA1UECzMKBmV0c3RvcnFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYnKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGiWlqAsOCqGKGh0dHA6
Ly9zc2UtdGvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKMZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3N1LTA4L0N1cnRfbnJvbGwvc3N1
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3N1LTA4
XEN1cnRfbnJvbGwvc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADBGBGSe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
Device-1(config)# exit
Device-1#

```

ステップ 11 証明書の設定を確認します。

ステップ 12 証明書の設定をスタートアップ コンフィギュレーションに保存します。

Related Topics

[CA 証明書のダウンロード](#) (239 ページ)

[アイデンティティ証明書の要求](#) (245 ページ)

CA 証明書のダウンロード

Microsoft Certificate Service の Web インターフェイスから CA 証明書をダウンロードする手順は、次のとおりです。

Procedure

ステップ 1 Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation task] をクリックし、[Next] をクリックします。

Microsoft Certificate Services -- Aparna CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and encrypt data depending upon the type of certificate you request.

Select a task:

- ☒ Retrieve the CA certificate or certificate revocation list
- ☐ Request a certificate
- ☐ Check on a pending certificate

ステップ 2 表示されたリストから、ダウンロードする CA 証明書ファイルを選択します。[Base 64 encoded] をクリックし、[Download CA certificate] をクリックします。

Microsoft Certificate Services -- Aparna CA

Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from t

It is not necessary to manually install the CA certification path if you request and install a
CA certification path will be installed for you automatically.

Choose file to download:

CA Certificate: **Current [Aparna CA]**

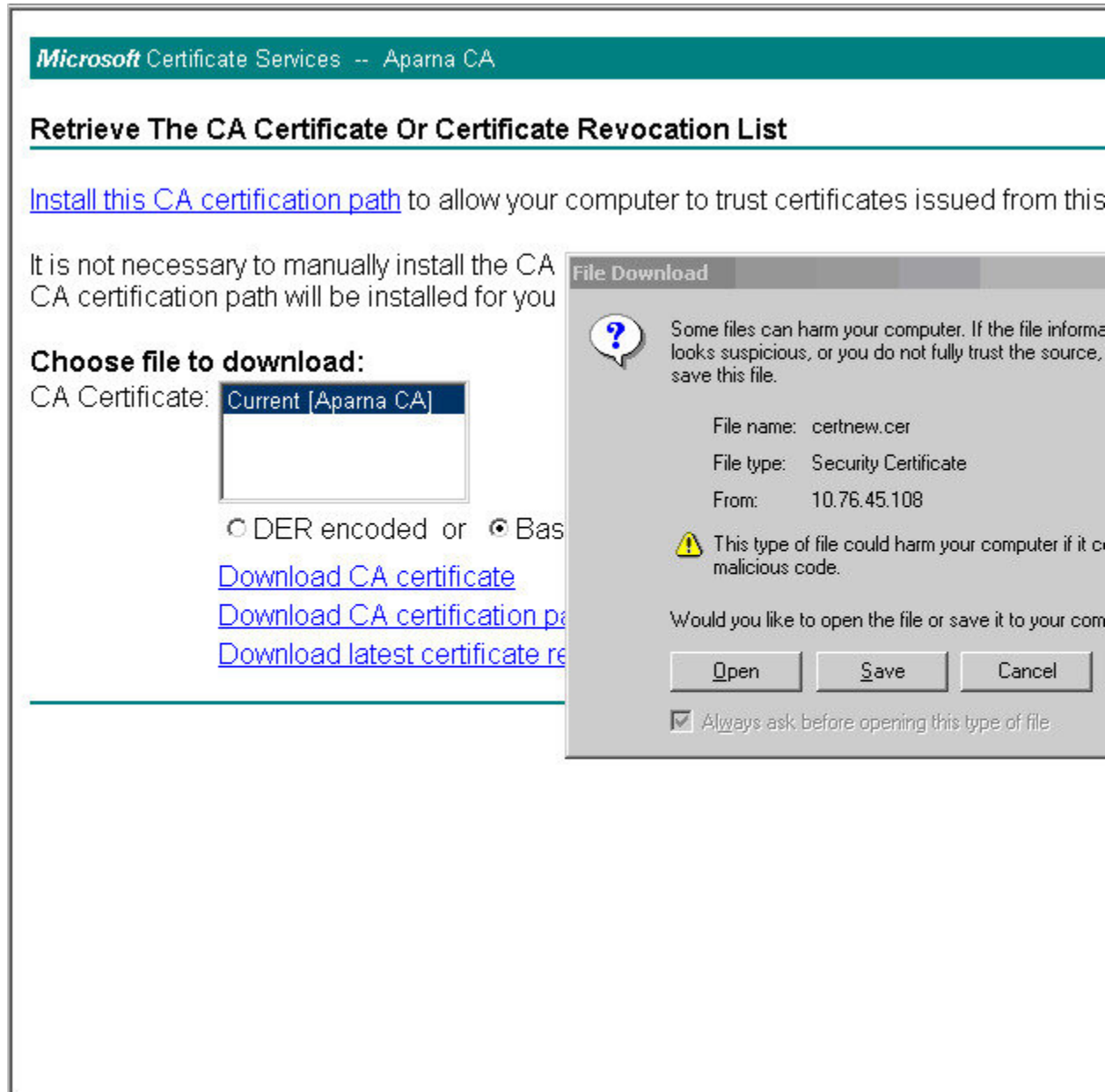
☐ DER encoded or ☒ Base 64 encoded

[Download CA certificate](#)

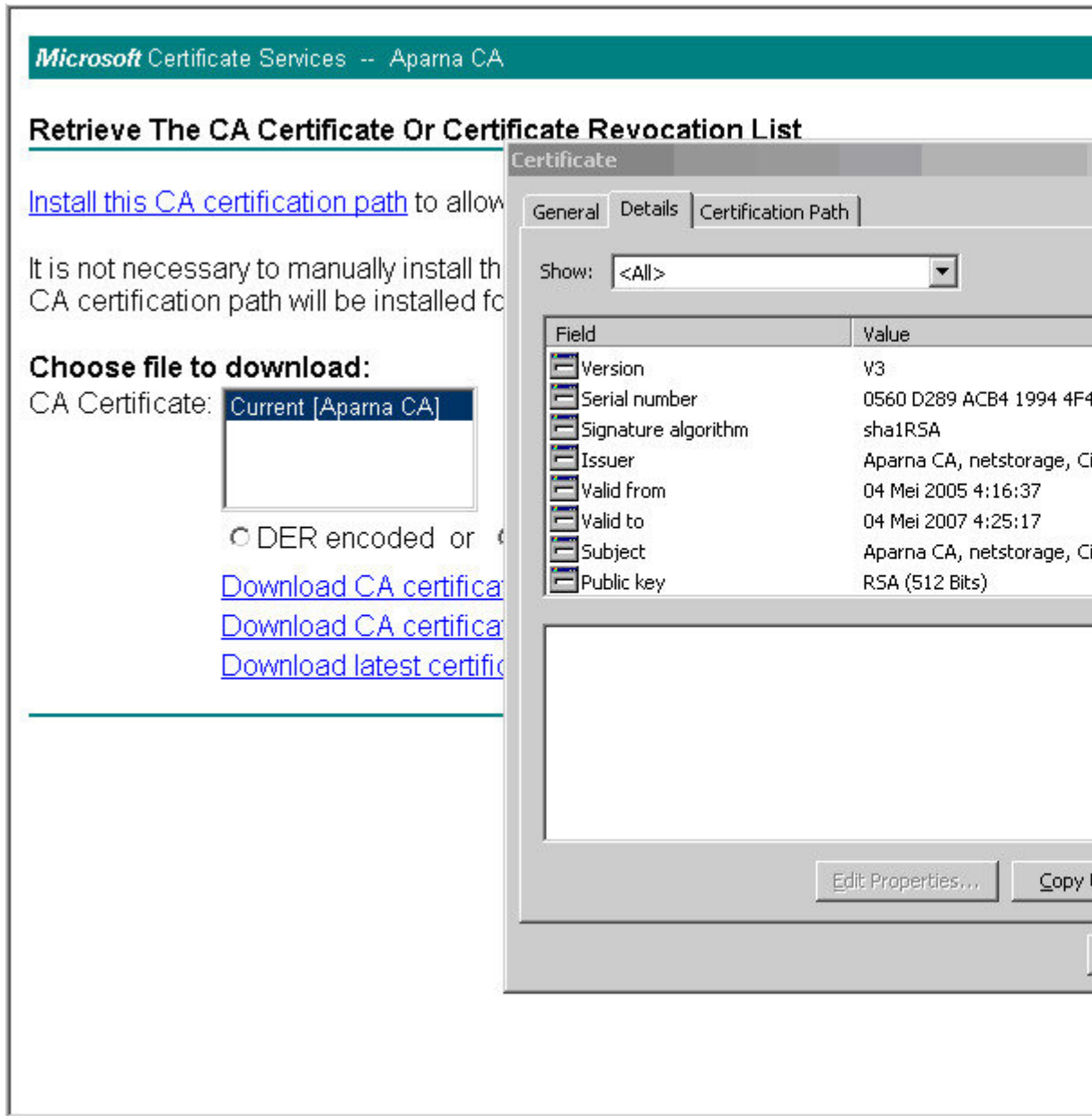
[Download CA certification path](#)

[Download latest certificate revocation list](#)

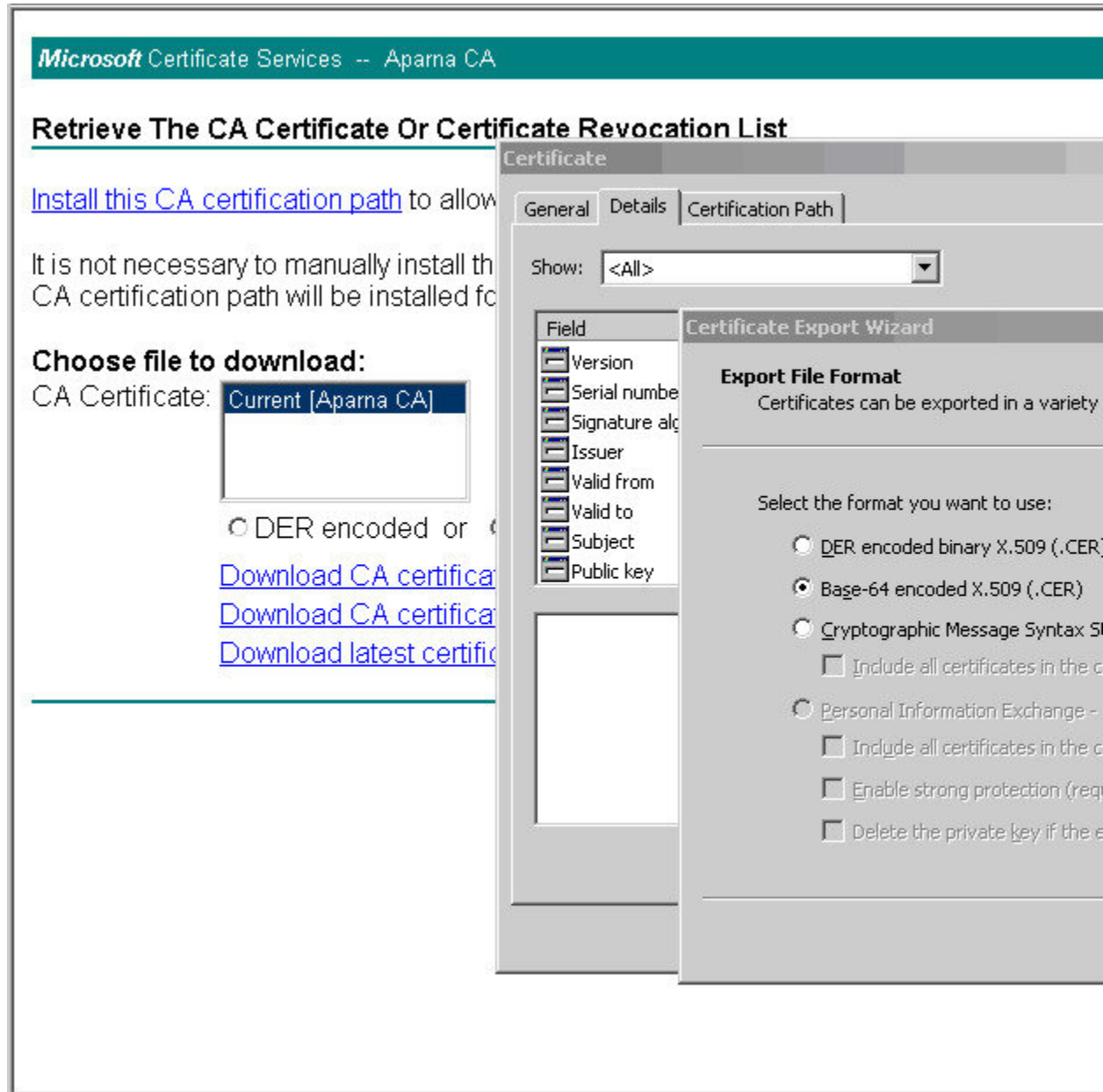
ステップ 3 [File Download] ダイアログボックスにある [Open] をクリックします。



ステップ 4 [Certificate] ダイアログボックスにある [Copy to File] をクリックし、[OK] をクリックします。



ステップ 5 [Certificate Export Wizard] ダイアログボックスから [Base-64 encoded X.509 (.CER)] を選択し、[Next] をクリックします。



ステップ 6 [Certificate Export Wizard] ダイアログボックスにある [File name:] テキストボックスに保存するファイル名を入力し、[Next] をクリックします。

ステップ 7 [Certificate Export Wizard] ダイアログボックスで、[Finish] をクリックします。

- ステップ 8 Microsoft Windows の type コマンドを入力して、Base-64 (PEM) 形式で保存されている CA 証明書を表示します。

```
C:\WINNT\system32\cmd.exe

D:\testcerts>type aparnaCA.cer
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWD5iaY0GZRPSRI1jK0ZeJANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjb3Y5LjB20xCzAJBgNVBAYTAk10
MRIwEAYDUQIIEwLLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdbbG9yZTEOMAwGA1UE
ChMFQ21zY28xEzARBgNVBAstCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAEFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIQMSAwHgYJKoZIhvcN
AQkBFHhFhbWFuZGt1QGNpc2NvLmNvbnRlMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDUQKewUDaXNjbzETMBEG
A1UECXMkbnU0c3RvcnFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsiHHZluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxyYKvysCAwEAAaOBuzCBuDALBgNUHQSE
BAMCAcYwDwYDUR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDUR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYXUyMENBLmNybDAwOjC6gLIYqZmlsZTovL1xccc3N1LTA4XENlcuRFbnJv
bGxcQXBhcm5hJT1wQ0EuY3JsMBAGCSsGAQQBgjcUAQQAgaEAMAGCSqGSIb3DQEB
BQUAA0EAAHv6UQ+8nE399Tww+KaGr0g0NIJagNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Us6mXp1//w==
-----END CERTIFICATE-----

D:\testcerts>
```

アイデンティティ証明書の要求

PKCS#12 証明書署名要求 (CSR) を使用して Microsoft Certificate サーバにアイデンティティ証明書を要求するには、次の手順に従ってください。

Procedure

- ステップ 1** Microsoft Certificate Services の Web インターフェイスから、[証明書の要求 (Request a certificate)] をクリックし、[次へ (Next)] をクリックします。

Microsoft Certificate Services -- Apama CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and encrypt data depending upon the type of certificate you request.

Select a task:

- ☐ Retrieve the CA certificate or certificate revocation list
- ☒ Request a certificate
- ☐ Check on a pending certificate

ステップ 2 [詳細な要求 (Advanced request)] をクリックし、[次へ (Next)] をクリックします。

Microsoft Certificate Services -- Apama CA

Choose Request Type

Please select the type of request you would like to make:

☐ User certificate request:

- Web Browser Certificate
- E-Mail Protection Certificate

☒ Advanced request

ステップ 3 [Base64 エンコード済み PKCS#10 を使用する証明書要求または base64 エンコード済み PKCS#7 ファイルを使用する更新要求を送信する (Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file)] をクリックし、[次へ

(Next)] をクリックします。

Microsoft Certificate Services -- Apama CA

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. The certification authority (CA) will determine the certificates that you can obtain.

- ☐ Submit a certificate request to this CA using a form.
- ☒ Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request.
- ☐ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Wizard.
You must have an enrollment agent certificate to submit a request for another user.

ステップ 4 [保存済みの要求 (Saved Request)] テキストボックスに、base64 の PKCS#10 証明書要求をペーストし、**[次へ (Next)]** をクリックします。証明書要求が Cisco NX-OS デバイスのコンソール

からコピーされます。

Microsoft Certificate Services -- Aparna CA

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request (server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded
Certificate Request
(PKCS #10 or #7):

```
VqyHOvEvAgMBAAAGTzAVBgkqhkiG9w0BCQexCBMG  
DjEpMCcwJQYDVRORAQH/BBswGYIRVmVnYXMtMS5j  
KoZIhvcNAQEEBQADgYEAkT6OKER6Qo8nj0sDXZVH  
PftrNcWUE/pw6HayfQ12T3ecgNwe12d15133YBF2  
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPN  
-----END CERTIFICATE REQUEST-----
```

[Browse](#) for a file to insert.

Additional Attributes:

Attributes:

ステップ 5 CA アドミニストレータから証明書が発行されるまで、1 ～ 2 日間待ちます。

Microsoft Certificate Services -- Apama CA

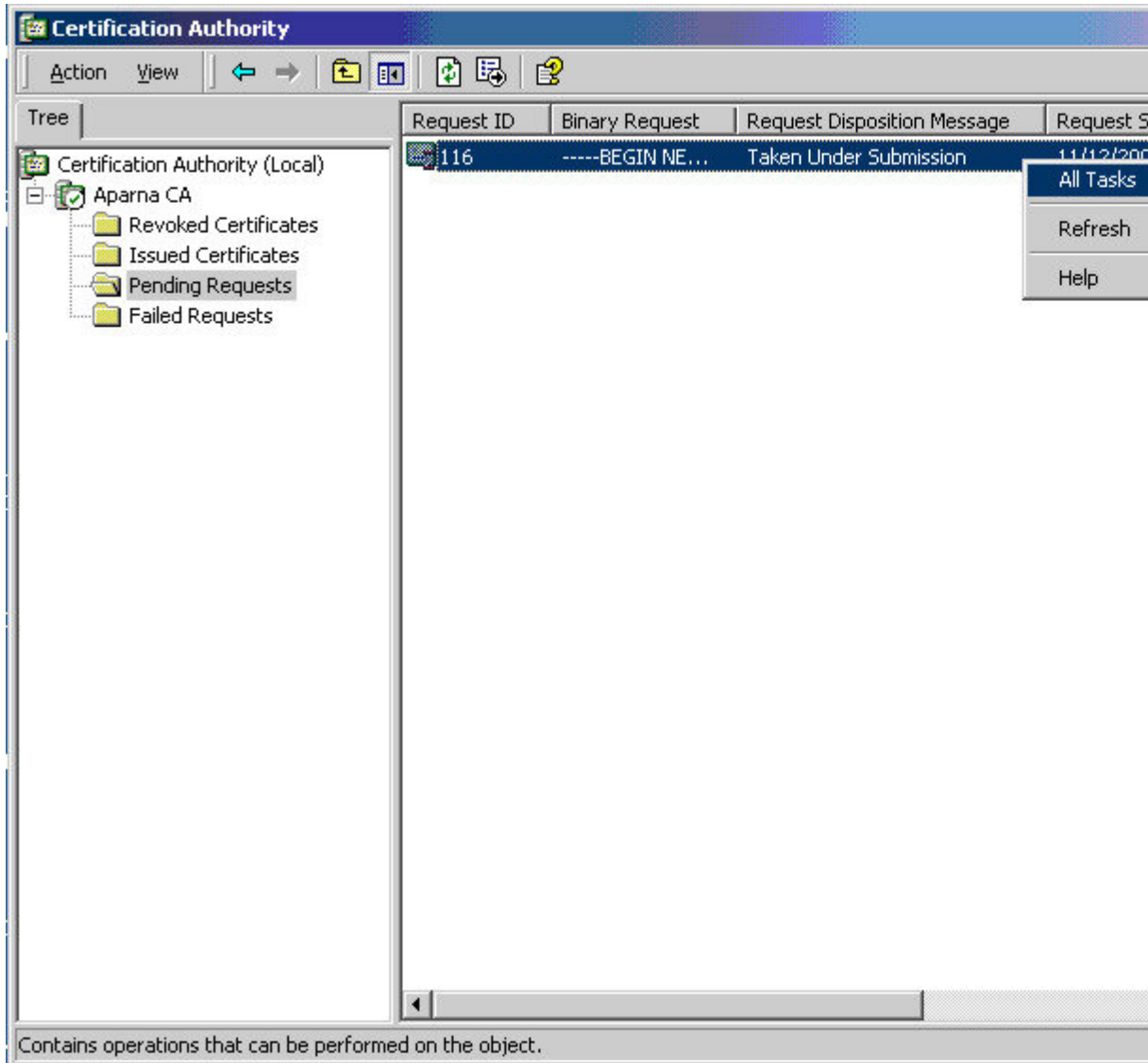
Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to approve your request.

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with **this** web browser within 10 days to retrieve your certificate

ステップ 6 CA アドミニストレータが証明書要求を承認するのを確認します。



- ステップ 7 Microsoft Certificate Services の Web インターフェイスから、[保留中の証明書をチェックする (Check on a pending certificate)] をクリックし、[次へ (Next)] をクリックします。

Microsoft Certificate Services -- Apama CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and encrypt data depending upon the type of certificate you request.

Select a task:

- ☐ Retrieve the CA certificate or certificate revocation list
- ☐ Request a certificate
- ☒ Check on a pending certificate

ステップ 8 チェックする証明書要求を選択して、**[次へ (Next)]** をクリックします。

Microsoft Certificate Services -- Aparna CA

Check On A Pending Certificate Request

Please select the certificate request you want to check:

Saved-Request Certificate (12 Nopember 2005 20:30:22)

- ステップ 9 [Base 64 エンコード済み (Base 64 encoded)] をクリックして、[CA 証明書のダウンロード (Download CA certificate)] をクリックします。

Microsoft Certificate Services -- Aparna CA

Certificate Issued

The certificate you requested was issued to you.

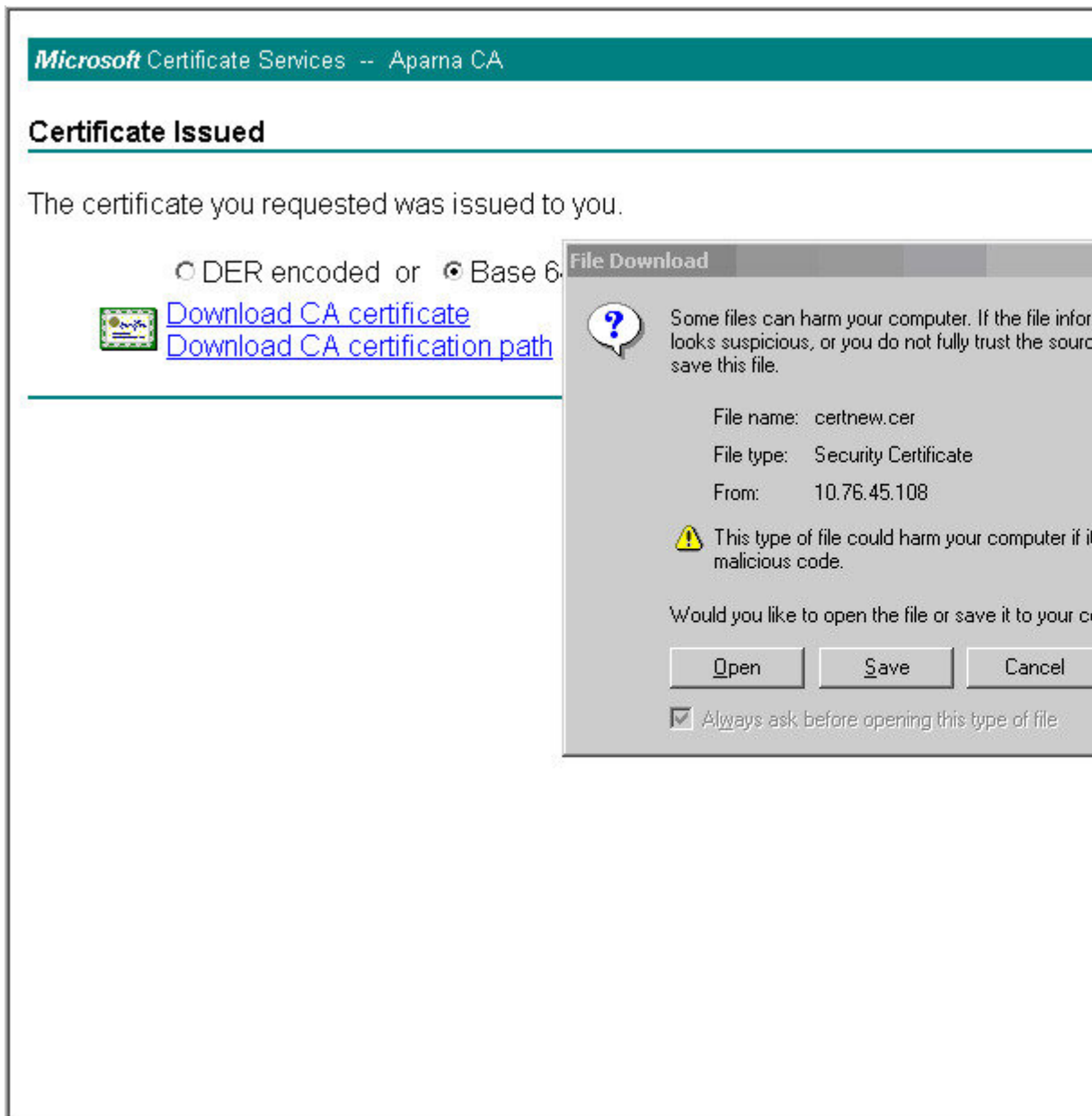
☐ DER encoded or ☒ Base 64 encoded



[Download CA certificate](#)

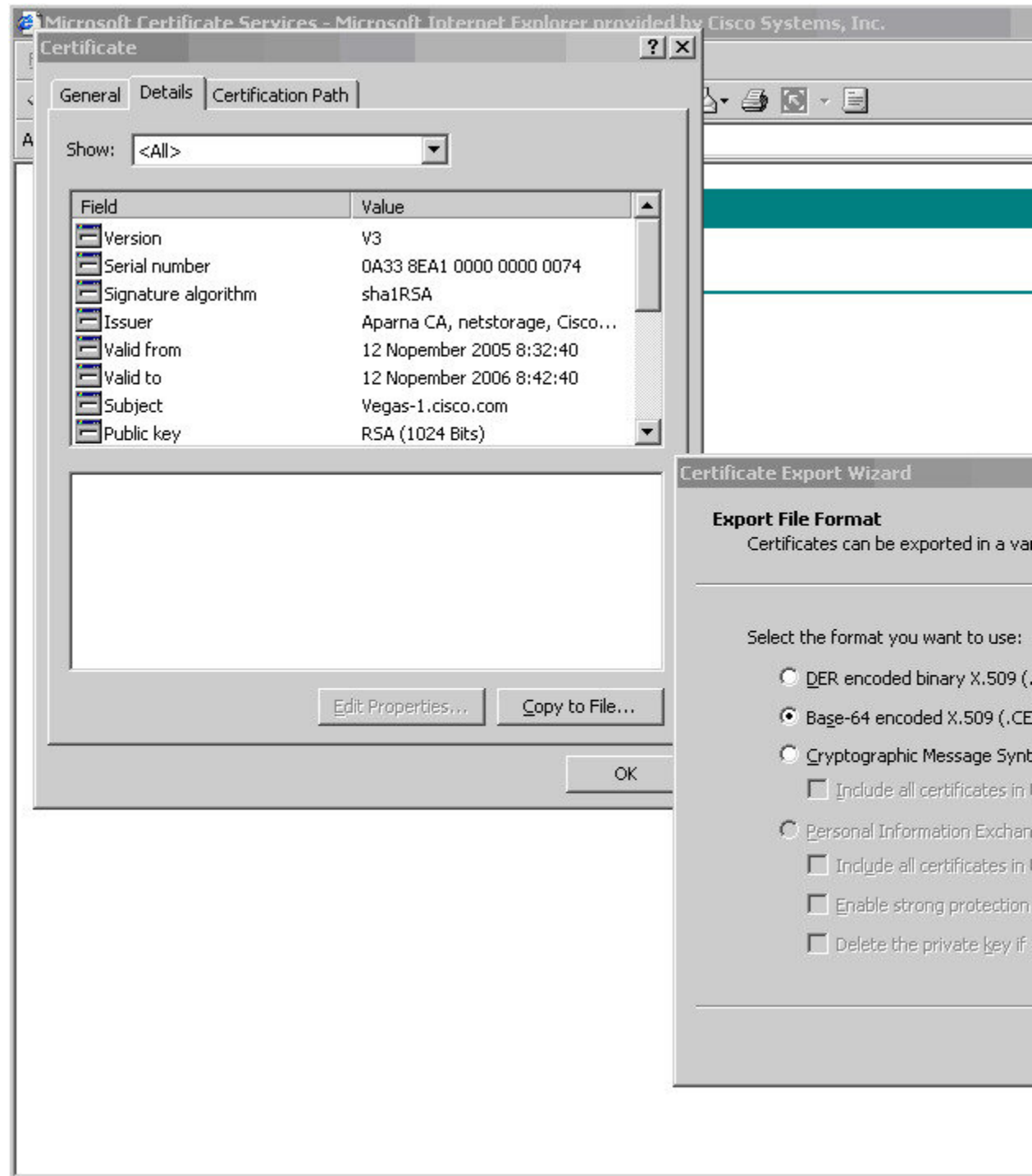
[Download CA certification path](#)

- ステップ 10** [ファイルのダウンロード (File Download)] ダイアログボックスで、**[開く (Open)]** をクリックします。



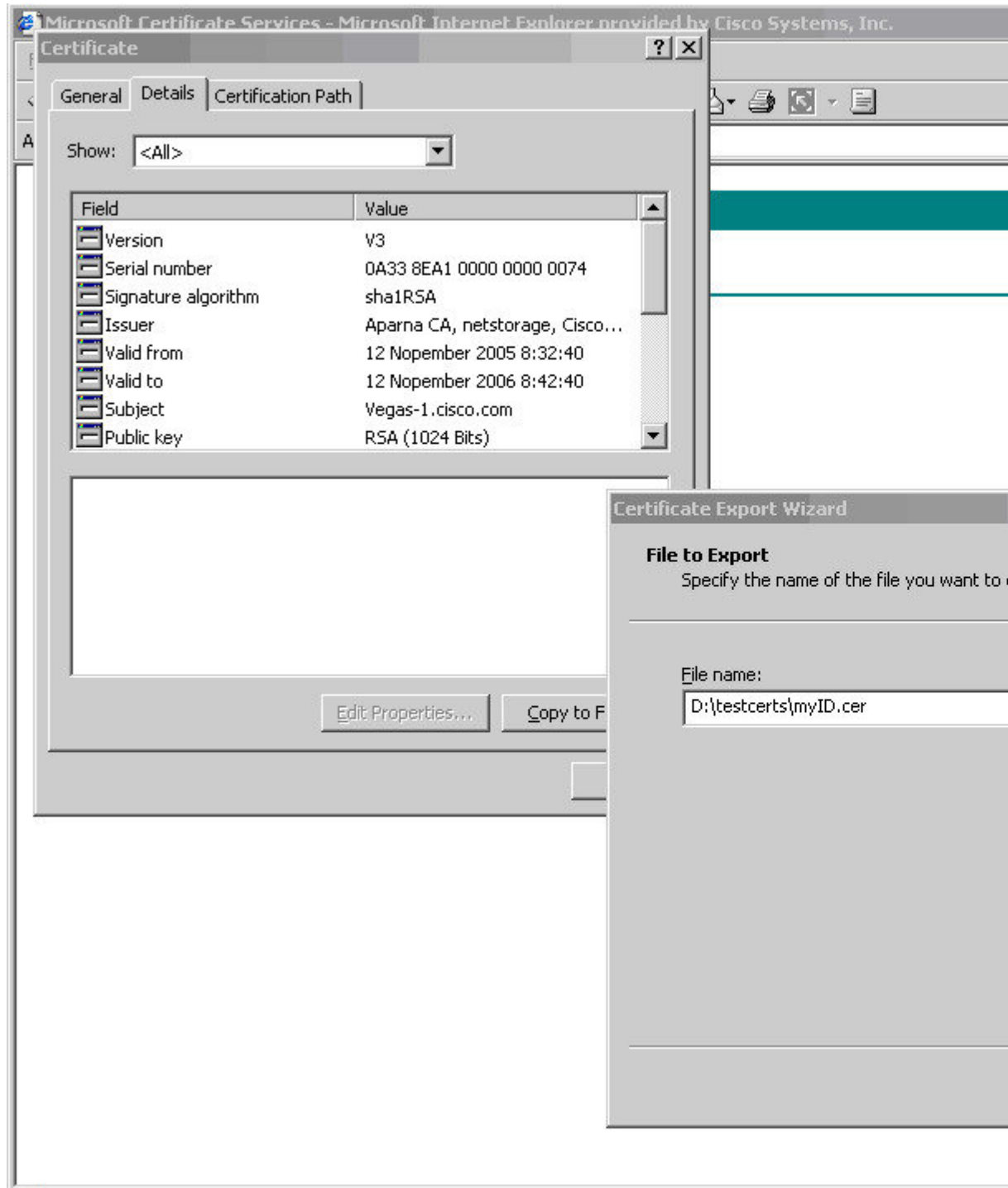
- ステップ 11** [Certificate] ボックスで、**[Details]** タブをクリックし、**[Copy to File...]** をクリックします。[証明書のエクスポート ダイアログ (Certificate Export Dialog)] ボックスで、**[Base-64 エンコード済み X.509 (.CER) (Base-64 encoded X.509 (.CER))]** をクリックし、**[次へ (Next)]** をクリック

クします。

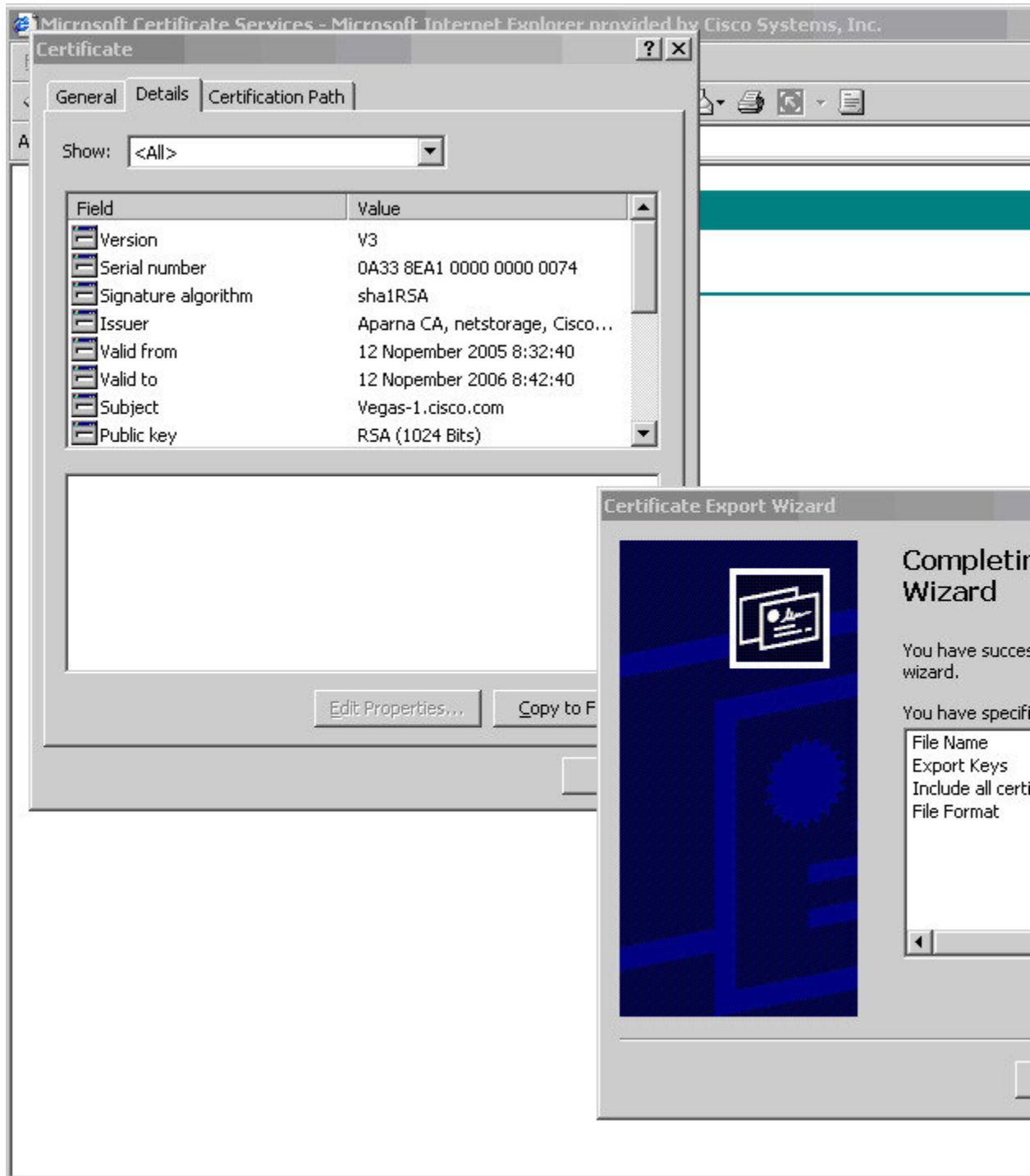


ステップ 12 [証明書エクスポートウィザード (Certificate Export Wizard)] ダイアログボックスにある [ファイル名 : (File name:)] テキスト ボックスに保存するファイル名を入力し、[次へ (Next)] を

クリックします。



ステップ 13 [完了 (Finish)] をクリックします。




```
C:\WINNT\system32\cmd.exe
```

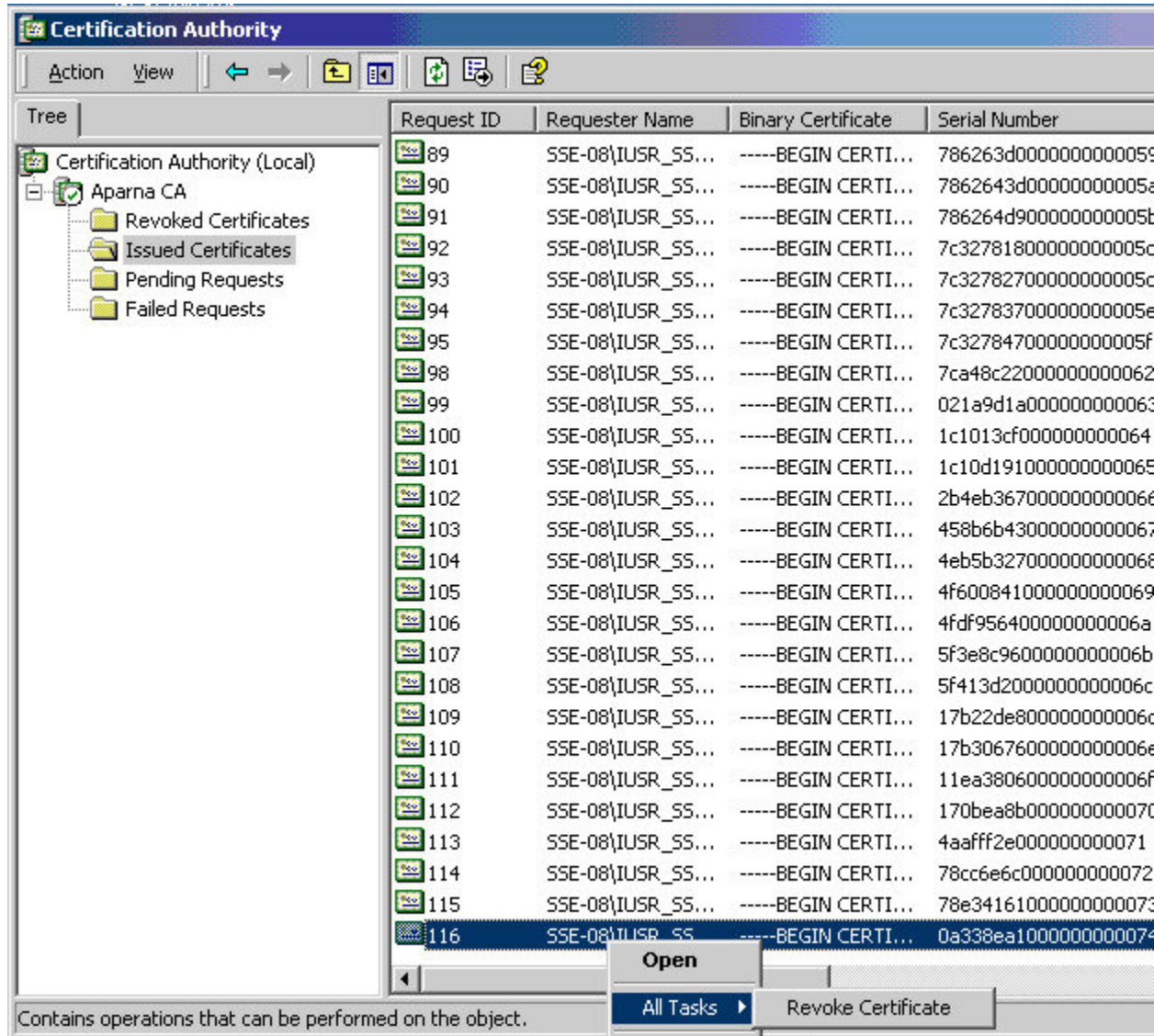
```
D:\testcerts>type myID.cer  
-----BEGIN CERTIFICATE-----  
MIIEADCCA6ggAwIBAgIKCj00oQAAAAAAdDANBgkqhkiG9w0BAQUFADCbkDEgMBAGCSqGSIb3DQEJARYRYWV1hbmrZUBjaXNjb3Y5LjB2b0xzc2ZAJBgNUBAYTAkLOMRIwEAYDVQQIEWlLYXJuYXRha2ExEJAQBGNVBACICUJhhmdhbgG9yZTEOMAWGA1UEChMPQ2lzY28xEzARBGNVBAsTCm5ldHN0b3JhZ2UxEJAQBGNVBAMT CUFwYXJuYYSBDQTAEfW0wNTExMTIwMzA5NDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNUBAMTEUVZL2Z2LTLeuY2LzY28uY29tMiGfMA0GCsqGISIb3DQEBAQUAA4GNADCBiQKBgcQC/GNUvACdjq4u41CdQ1WkJKJSICdpLfK5eJSmNCQujGpzcuKsZPFxfJ2UoiyeCYE8ylncWgw5E08rJ47glxr42/sI9IRIh/8udU/cj9jSSfKK56koa7xWYAuu8rDfz8jMCnIM4W1ay/q2q4Gb x7RifdU06ufqFZEgs17/Elash9LxLwIDAQABo4ICEZCCAg8wJQYDUVR0RAQH/BBSwGYIRUMUnYXmtMS5jaXNjb3Y5LjB2HBKMMH6IwhQYDUR0BBVEFKCLi+2sspwEfgrRbhWmlUyo9jngMIHMBGNVHSMEGcQwgCGAFCCo8kaDG6wjTEUNjskYUBoLFmxoxoYGWpIGTMIQM5AwhgYJKoZIhvcNAQkBKFPhfbWPUZGT LQGNpc2NuLmNmVhTELMAkGA1UEBHMCSU4xEJAQBGNVBAGTCUthcm5hdGFrfYTESEMBA GA1UEBxMJMQmFuZ2Fsh3JlMQ4wDAYDUQQKEWJDAXNjb3ETBMBEAGA1UECxMKbWU0c3RucmFnZTESMBA GA1UEAxMJQXBhcml5cm5hIENBghAFYNKJRlQZLE9JEiWMRR16MGsGA1UdHwRkMGIlwLQfAsOCqCKGH0dHA6Ly9zc2U0MDguQ2UydEUucm9sb3B9BcGFybmlElmjBDQS5jcmmwMKAuoCyGKmZpbGU6Ly9cXHNzZS0wbGFzZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNydhDCBigYIKwYBBQUH AQEEfjB8MDZGCCJAQUBFAChi9odHRwOi8vc3NllTA4L0NlcnRFbnJubGwoc3NlLTA4X0FwYXJuYSUyMENBLmNyddA9BggrBgEFBQcwAoYxZmlsZTovL1xc3NllTA4XENlc nRFbnJubGwcc3NllTA4X0FwYXJuYSUyMENBLmNyddANBgkqhkiG9w0BAQUFAANBADbGBGsbe7GNLh9xeOTWBnbm24U69ZSuDDcOcUZUUTgrpntqUpPyejtsyf lwE36ciZu4WsEXREqxbTk8ycx7U5o=  
-----END CERTIFICATE-----  
  
D:\testcerts>
```

[証明書要求の作成 \(226 ページ\)](#)
[Cisco NX-OS デバイスでの証明書の設定 \(236 ページ\)](#)

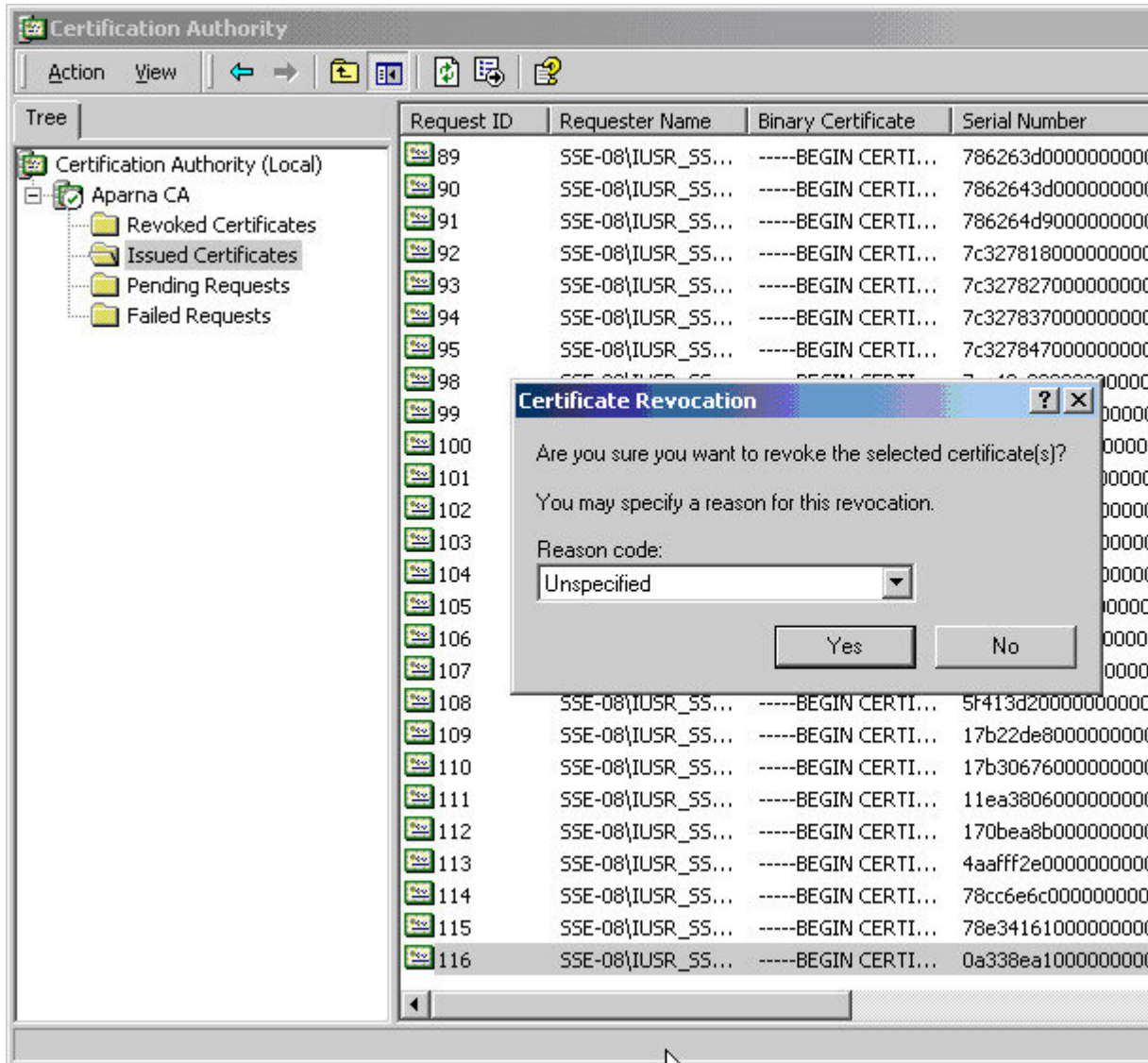
Microsoft CA 管理者プログラムを使用して証明書を取り消す手順は、次のとおりです。

ステップ1 [Certification Authority] ツリーから、[Issued Certificates] フォルダをクリックします。リストから、取り消す証明書を右クリックします。

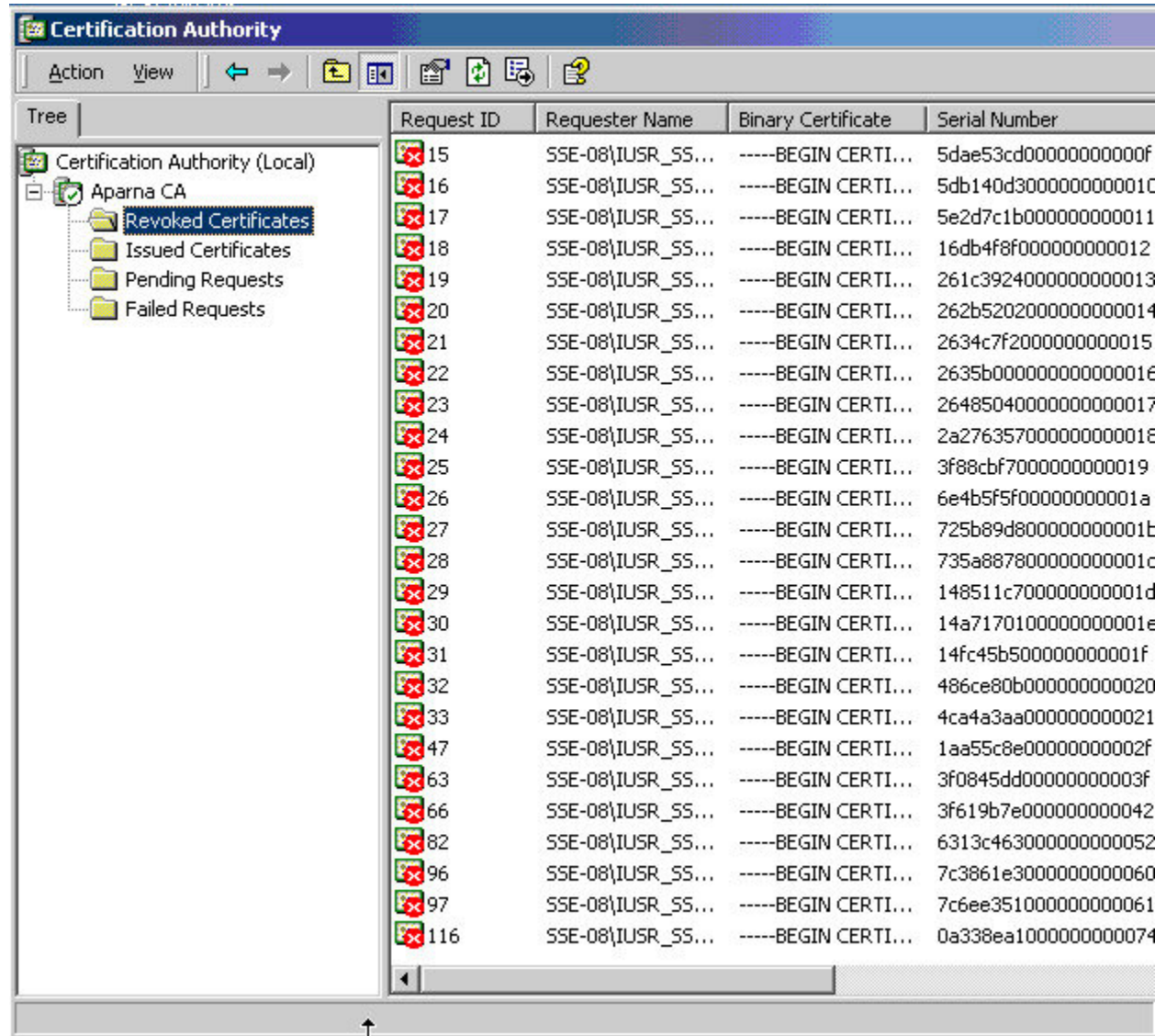
ステップ 2 [All Tasks] > [Revoke Certificate] の順に選択します。



ステップ3 [Reason code] ドロップダウン リストから取り消しの理由を選択し、[Yes] をクリックします。



ステップ 4 [Revoked Certificates] フォルダをクリックして、証明書の取り消しを表示および確認します。

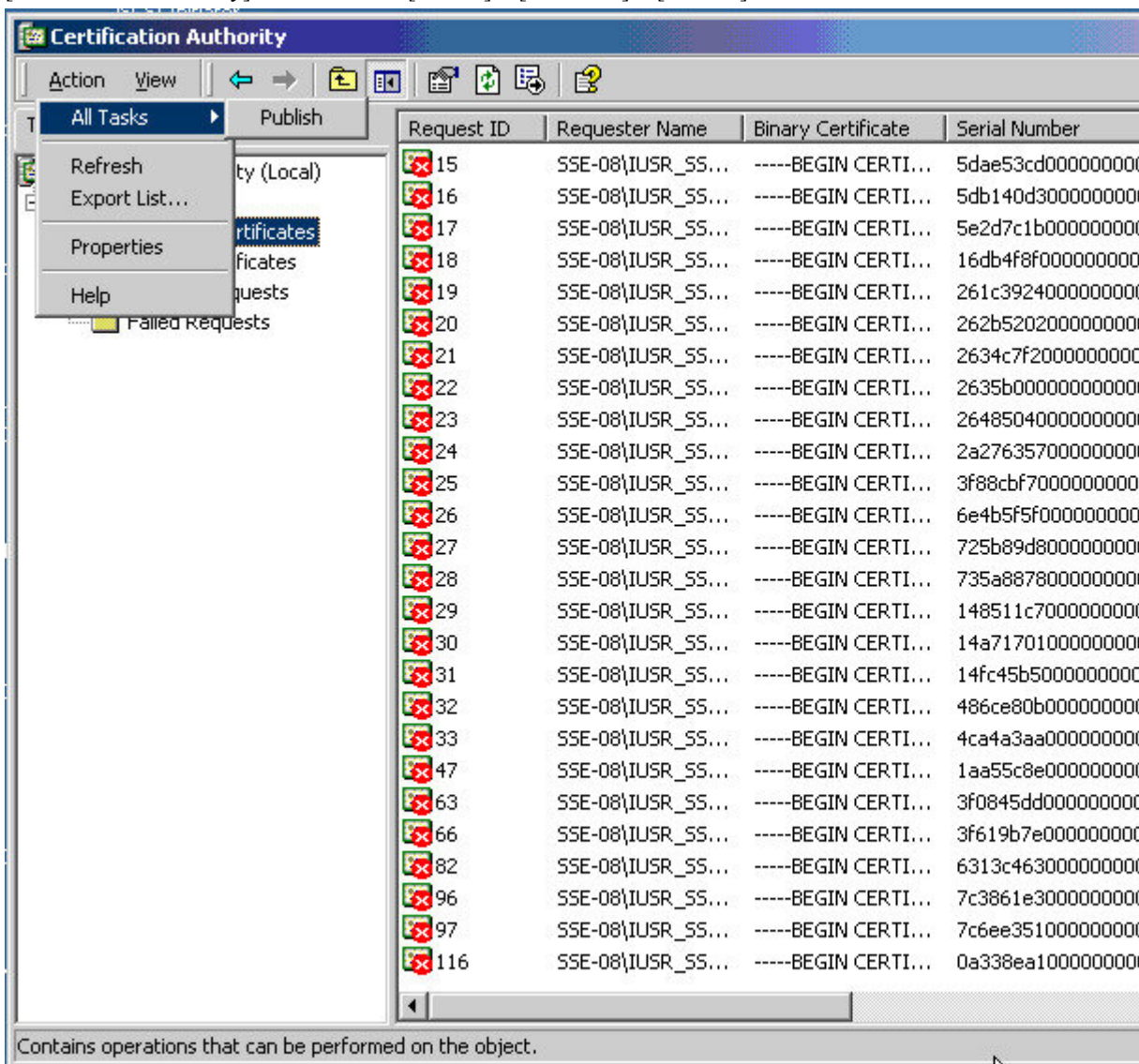


CRL の作成と公開

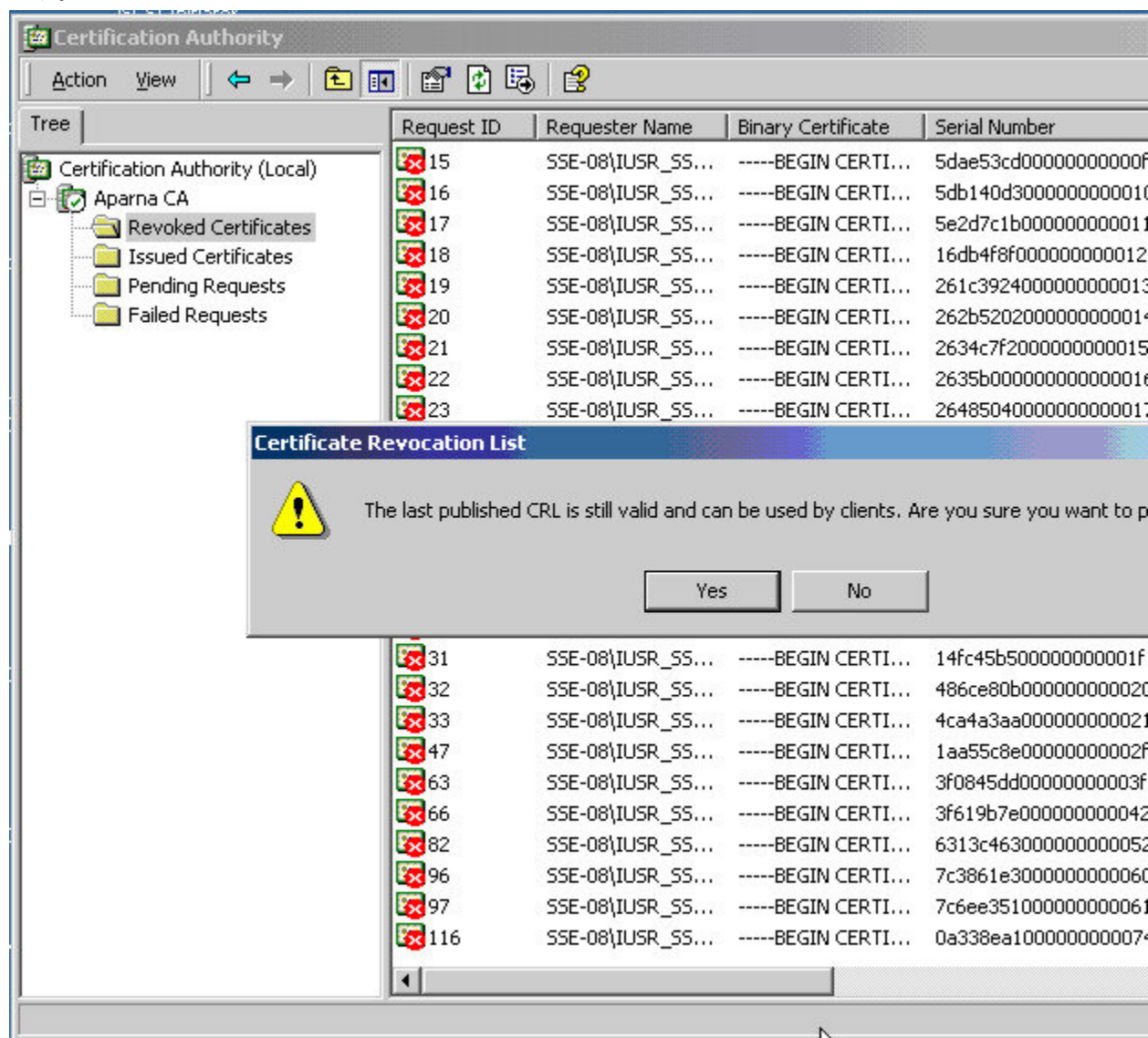
Microsoft CA 管理者プログラムを使用して CRL を作成および公開する手順は、次のとおりです。

Procedure

ステップ 1 [Certification Authority] の画面から、[Action] > [All Tasks] > [Publish] の順に選択します。



ステップ 2 [Certificate Revocation List] ダイアログボックスで、[Yes] をクリックして最新の CRL を公開します。



CRL のダウンロード

Microsoft 社の CA の Web サイトから CRL をダウンロードする手順は、次のとおりです。

Procedure

- ステップ 1** Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation list] をクリックし、[Next] をクリックします。

Microsoft Certificate Services -- Aparna CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other application. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and so on, depending upon the type of certificate you request.

Select a task:

- ☒ Retrieve the CA certificate or certificate revocation list
- ☐ Request a certificate
- ☐ Check on a pending certificate

ステップ 2 [Download latest certificate revocation list] をクリックします。

Microsoft Certificate Services -- Apama CA

Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this

It is not necessary to manually install the CA certification path if you request and install a c
CA certification path will be installed for you automatically.

Choose file to download:

CA Certificate: **Current [Apama CA]**

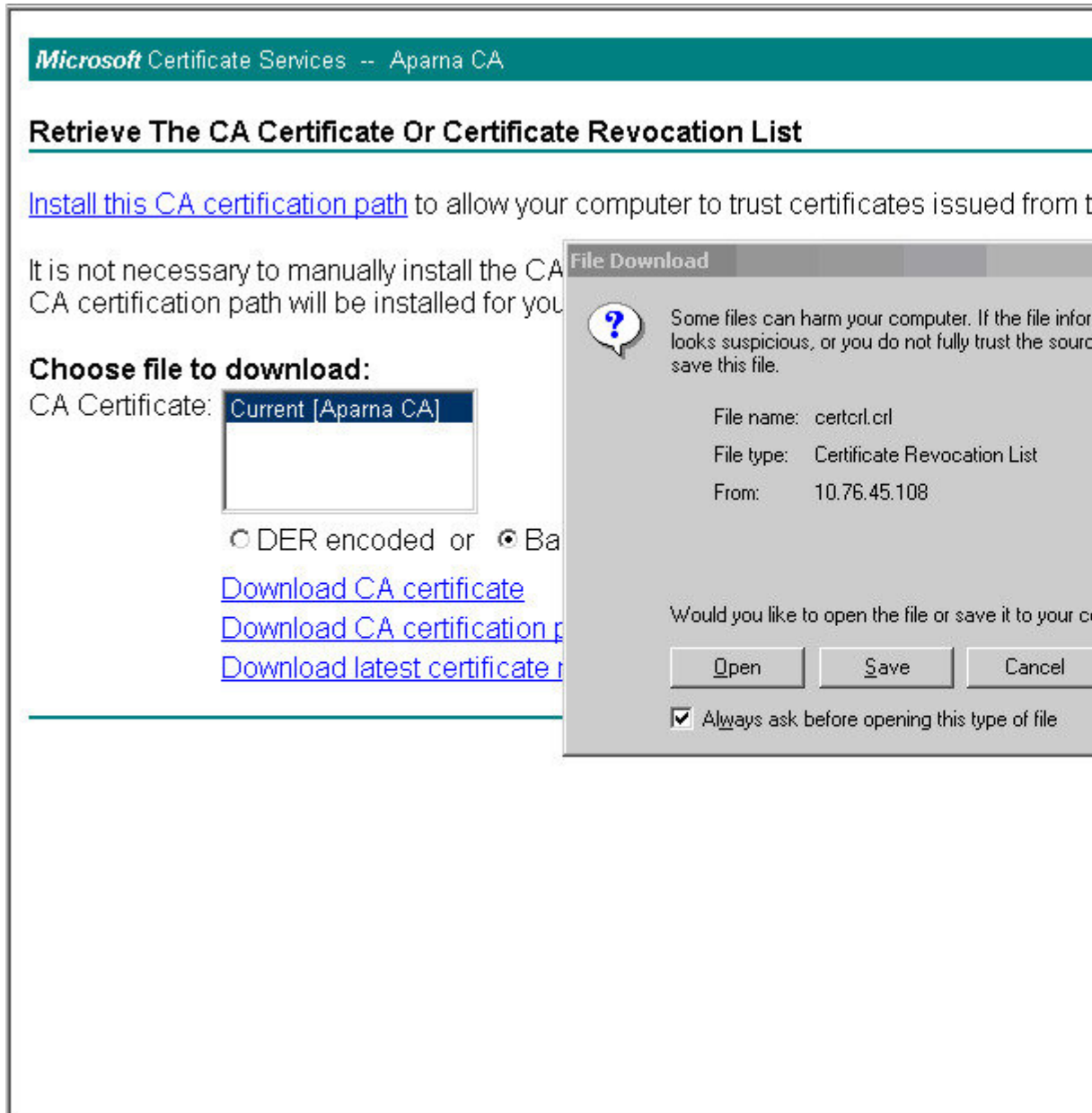
☐ DER encoded or ☒ Base 64 encoded

[Download CA certificate](#)

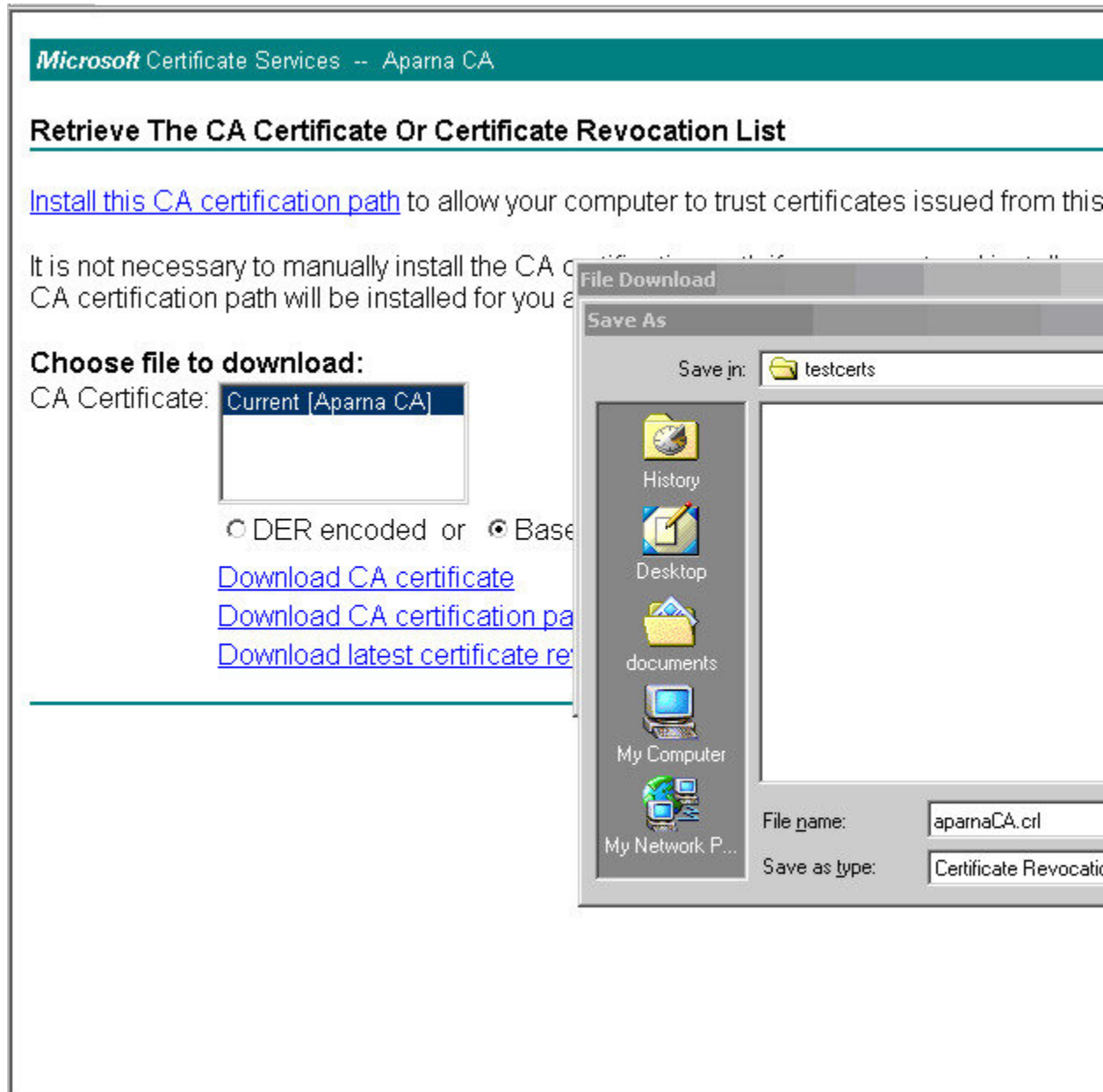
[Download CA certification path](#)

[Download latest certificate revocation list](#)

ステップ 3 [File Download] ダイアログボックスで、[Save] をクリックします。



ステップ 4 [Save As] ダイアログボックスで、保存するファイル名を入力して、[Save] をクリックします。



ステップ5 Microsoft Windows の type コマンドを入力して、CRL を表示します。

```
C:\WINNT\system32\cmd.exe

D:\testcerts>type aparnaCA.crl
-----BEGIN X509 CRL-----
MIIGBTCCBa8CAQEWdQYJKoZIhvcNAQEFBQAwwGZANIDAEBgkqhkiG9w0BCQEWEFt
YW5ka2YAY2IzY28uYyY29tMQswCQYDUQAGEwJJTjESMBAGA1UECBMJS2FybmF0YWt
hMRIwEAYDUQHEw1CYW5nYWxvcmlzLjAMBGBUBoTBUNpcc2NuMRMwEQYDUQQLLwpu
ZXRzdG9yYVdlMlRIwEAYDUQDEw1BcGFybmEgQ0EXDTA1MTEExMjA0MzYwNFoXDTA1
MTEExOTE2NTYwNFowggSxMBsCCmEhCaEAAAAAAAAAIXDTA1MDgxNjI1xNTI1xOUowGwIK
TN5GTgAAAAAAAAcNMDUwODE2MjE1MjI1WjAbaGppM/CtCAAAAAAAAAEFw0wNTA4MTYy
MTUyYNDFAAMBsCCmcpnsIAAAAAAAAAUJDTA1MDgxNjI1xNTI1MlMowGwIKhM993AAAAA
BhcNMDUwNjA4MDAxMjA0WjAbaGppwzE//AAAAAAAAAHFw0wNTA4MTYyYMTUzMTUaMBsC
Ck2bERYAAAAAAAAgXDTA1MDgxNjI1xNTMxNUowKQIKUggCAAAAAAAAAACRcNMDUwNjI3
MjM0NzA2WjAMMAoGA1UdFQDDCgECMCKCCINJrUYAAAAAAAAAoXDTA1MDYyNzIzNDcy
MlMowDDAKBgNUHRUEAwBoBAjapagpTvrC8AAAAAAAAALFw0wNTA3MDQxODA0MDFaMAww
CgYDUROUBAMKAQYwGwIKWR56zgAAAAAAAAADBCNMDUwODE2MjE1MzE1WjAbaGppdP9Uu
AAAAAAAAANFw0wNTA2MjkyMjA3MjUaMAwwCgYDUROUBAMKAQEWGwIKXat3EwAAAAAA
DhcNMDUwNzE0MDA4ZmZU2WjAbaGppdrLPNAAAAAAAAAFw0wNTA4MTYyYMTUzMTUaMBsC
C12xQNMAAAAAAAAABAZDTA1MDgxNjI1xNTMxNUowKQIKX1I8GwAAAAAAERcNMDUwNzA2
MjExMjEwWjAMMAoGA1UdFQDDCgEFMBsCCChbBT48AAAAAAAAABIXDTA1MDgxNjI1xNTMx
NUowGwIKJhw5JAAAAAAAAEXcNMDUwODE2MjE1MzE1WjAbaGomKI1CAAAAAAAAAAFw0w
NTA3MTQwMDMzMtBAMBsCCiY0x/IAAAAAAAAABUXDTA1MDcxNDAxMzI1OwGwIKJjWw
AAAAAAAAAFhcNMDUwNzE0MDA4ZmZU2WjAbaGomSFBAAAAAAAAAAFw0wNTA3MTQwMDMw
MjUaMBsCCionY1CAAAAAAAAAABgXDTA1MDgxNjI1xNTMxNUowGwIKP4jL9wAAAAAAGRCn
MDUwODE2MjE1MzE1WjAbaGppuS19fAAAAAAAAaFw0wNTA4MTYyYMTUzMTUaMBsCCnJb
idgAAAAAAAABsXDTA1MDgxNjI1xNTMxNUowGwIKc1qleAAAAAAAAAHBcNMDUwODE2MjE1
MzE1WjAbaGoUhtRHMAAAAAAAAAAFw0wNTA4MTYyYMTUzMTUaMBsCCChSnFwEAAAAAAAAB4X
DTA1MDgxNjI1xNTMxNUowGwIKFPpFtQAAAAAAHxcNMDUwODE3MTg2MDQyWjAbaGppI
bOgLAAAAAAAAAGFw0wNTA4MTcxODMwNDNaMBsCCkyko6oAAAAAAAAACEXDTA1MDgxNzE4
MzA0M1owGwIKGqUcJgAAAAAAAAALxcNMDUwOTA1MTcwnZa2WjAbaGo/CEXAAAAAAAA/
Fw0wNTA5MDgyUDIMZJAMBsCCj9hm34AAAAAAAAEIXDTA1MDkwODI1xNDA0OFowGwIK
YxPEYwAAAAAAUHCNMDUwOTE5MTcxZmZlWjAbaGpp8OGHjAAAAAAAABgFw0wNTA5MjA5MjA
NzUyNTZAMBsCCnxu41EAAAAAAAAGEXDTA1MDkyMDE4NTIzMFowGwIKCj00oQAAAAAA
dBCNMDUxMTEyMDQzNDQyWQA1MDMwHwYDUROjBBgwFoAUJyYyRoMhrCNMRU20yRhQ
GgsWbHEwEAYJKwYBBAAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEFBQAwdQQAly91DCrhi
hOCUBm9NgwYjJjEjEjUu168CuaacFP3rkM8YyZYpu1c32R/UuU6aSxgrAC/SbsEa
nXPJt5xYJNdy
-----END X509 CRL-----

D:\testcerts>
```

Related Topics

[証明書取消確認方法の設定](#) (225 ページ)

CRL のインポート

CRL を CA に対応するトラストポイントにインポートする手順は、次のとおりです。

Procedure

ステップ1 CRL ファイルを Cisco NX-OS デバイスのブートフラッシュにコピーします。

```
Device-1# copy tftp:aparnaCA.crl bootflash:aparnaCA.crl
```

ステップ 2 CRL を設定します。

```
Device-1# configure terminal
Device-1(config)# crypto ca crl request myCA bootflash:aparnaCA.crl
Device-1(config)#
```

ステップ 3 CRL の内容を表示します。

```
Device-1(config)# show crypto ca crl myCA
Trustpoint: myCA
CRL:
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
Yourcompany/OU=netstorage/CN=Aparna CA
  Last Update: Nov 12 04:36:04 2005 GMT
  Next Update: Nov 19 16:56:04 2005 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1
      1.3.6.1.4.1.311.21.1:
        ...
  Revoked Certificates:
    Serial Number: 611B09A100000000000002
      Revocation Date: Aug 16 21:52:19 2005 GMT
    Serial Number: 4CDE464E00000000000003
      Revocation Date: Aug 16 21:52:29 2005 GMT
    Serial Number: 4CFC2B4200000000000004
      Revocation Date: Aug 16 21:52:41 2005 GMT
    Serial Number: 6C699EC200000000000005
      Revocation Date: Aug 16 21:52:52 2005 GMT
    Serial Number: 6CCF7DDC00000000000006
      Revocation Date: Jun 8 00:12:04 2005 GMT
    Serial Number: 70CC4FFF00000000000007
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 4D9B111600000000000008
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 52A8023000000000000009
      Revocation Date: Jun 27 23:47:06 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        CA Compromise
    Serial Number: 5349AD460000000000000A
      Revocation Date: Jun 27 23:47:22 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        CA Compromise
    Serial Number: 53BD173C0000000000000B
      Revocation Date: Jul 4 18:04:01 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        Certificate Hold
    Serial Number: 591E7ACE0000000000000C
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E0000000000000D
      Revocation Date: Jun 29 22:07:25 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        Key Compromise
    Serial Number: 5DAB77130000000000000E
```

```

        Revocation Date: Jul 14 00:33:56 2005 GMT
Serial Number: 5DAE53CD00000000000F
        Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 5DB140D30000000000010
        Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 5E2D7C1B0000000000011
        Revocation Date: Jul  6 21:12:10 2005 GMT
CRL entry extensions:
    X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 16DB4F8F0000000000012
        Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 261C39240000000000013
        Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 262B52020000000000014
        Revocation Date: Jul 14 00:33:10 2005 GMT
Serial Number: 2634C7F20000000000015
        Revocation Date: Jul 14 00:32:45 2005 GMT
Serial Number: 2635B0000000000000016
        Revocation Date: Jul 14 00:31:51 2005 GMT
Serial Number: 264850400000000000017
        Revocation Date: Jul 14 00:32:25 2005 GMT
Serial Number: 2A2763570000000000018
Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 3F88CBF70000000000019
        Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 6E4B5F5F000000000001A
        Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 725B89D8000000000001B
        Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 735A8878000000000001C
        Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 148511C7000000000001D
        Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 14A71701000000000001E
        Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 14FC45B5000000000001F
        Revocation Date: Aug 17 18:30:42 2005 GMT
Serial Number: 486CE80B0000000000020
        Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 4CA4A3AA0000000000021
        Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 1AA55C8E000000000002F
        Revocation Date: Sep  5 17:07:06 2005 GMT
Serial Number: 3F0845DD000000000003F
        Revocation Date: Sep  8 20:24:32 2005 GMT
Serial Number: 3F619B7E0000000000042
        Revocation Date: Sep  8 21:40:48 2005 GMT
Serial Number: 6313C4630000000000052
        Revocation Date: Sep 19 17:37:18 2005 GMT
Serial Number: 7C3861E30000000000060
        Revocation Date: Sep 20 17:52:56 2005 GMT
Serial Number: 7C6EE3510000000000061
        Revocation Date: Sep 20 18:52:30 2005 GMT
Serial Number: 0A338EA10000000000074    <-- Revoked identity certificate
        Revocation Date: Nov 12 04:34:42 2005 GMT
Signature Algorithm: sha1WithRSAEncryption
0b:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32:
44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96:
29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1:
1a:9f:1a:49:b7:9c:58:24:d7:72

```

Note

取り消されたデバイスのアイデンティティ証明書（シリアル番号は 0A338EA10000000000074）が最後に表示されています。

PKI に関する追加情報

ここでは、PKI の実装に関する追加情報について説明します。

PKI の関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	Cisco NX-OS ライセンス ガイド
VRF コンフィギュレーション	『Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング 設定ガイド』

PKI の標準規格

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

Cisco SUDI 証明書チェーンを使用したデバイス構成証明

Cisco NX-OS リリース 10.6(2) 以降、Cisco Nexus 9000 スイッチは、Cisco Secure Unique Device Identifier (SUDI) 証明書チェーンの構成証明と署名をサポートします。この機能により、スイッチは SUDI 証明書チェーンを表示し、ユーザーが提供するナンスに基づいて署名を生成でき、デバイス本人確認と外部システムとの統合をサポートします。

SUDI 証明書チェーン証明書の利点

この機能は、複数の利点を提供します：

- デバイス本人確認（Device identity verification）：管理者および自動システムは、SUDI 証明書チェーンと署名を取得してスイッチのアイデンティティを検証できます。
- バックエンドシステムとの統合：スイッチは、CLI コマンドを使用して SUDI 証明書チェーンと署名を表示できます。出力は自動化してバックエンドサーバーが使用するために JSON 形式で利用できます。

- 自動化および規則遵守ワークフローのサポート：JSONでのCLI出力により、証明書チェーンと署名の取得と処理の自動化が可能になり、既存の顧客システムとの統合が促進されます。
- セキュアなオンボーディングとゼロ トラスト ワークフローのサポート：重要なインフラインフラストラクチャへのアクセスを許可する前に、デバイスの信頼性が必要な環境でデバイス アイデンティティの証明を有効にします。

SUDI 証明書チェーン構成証明および署名の仕組み

Cisco NX-OSリリース 10.6 (2) により、Cisco Nexus 9000 スイッチはセキュアな固有デバイス識別子 (SUDI) 証明書チェーンを表示し、デバイス構成証明の署名を生成できます。このプロセスにより、ユーザーは標準規格のCLI コマンドを介して証明書チェーンと署名を確認することで、スイッチを認証します。

process_summary

このプロセスにより、ユーザーは SUDI 証明書チェーンを取得し、スイッチ CLI を使用してデバイス構成証明の署名を生成できます。

process_workflow

SUDI 証明書の構成証明と署名のプロセスには、次の手順が含まれます：

1. ユーザーは CLI を介してスイッチにアクセスし、SUDI 証明書チェーンを取得するか、または指定された値 (nonce) を使用して署名付き応答を生成する要求を開始します。
2. スイッチは、セキュア ストレージから SUDI 証明書チェーンを取得します。
3. ナンスが指定されている場合、スイッチは証明書チェーンとナンスを使用して署名を生成します。
4. スイッチは、証明書チェーンと、該当する場合は、選択した出力形式で署名を表示します。
5. ユーザーは、表示された情報をデバイスの検証や外部システムとの統合に使用できます。

注意事項と制約事項

- この機能は、必要なセキュアなストレージと関連サービスを提供するプラットフォームでのみサポートされます。必要なハードウェアまたはサービスがない場合、機能は利用できません。
- SUDI 証明書チェーンと署名機能には、スイッチのコマンドライン インターフェイスからのみアクセスできます。
- 署名を生成するために、ユーザーが提供するナンスが必要です。ナンスが指定されていない場合は、証明書チェーンのみが表示されます。

- 出力は標準規格または JSON 形式で表示できるため、手動での確認と自動処理の両方が可能になります。
- この機能は、デバイス認証、構成証明、または自動検証ワークフローが必要な環境を対象としています。

SUDI 証明書チェーンの構成証明と署名の確認

次のコマンドを使用して、デバイスの SUDI 証明書チェーンの構成証明および署名機能を確認します。

SUDI 証明書チェーンを表示し、ナンスを使用して署名を生成し、自動化のために JSON 形式での出力を表示できます。

このタスクでは、デバイスによって提供される構成証明および署名情報にアクセスして確認する方法を示します。

手順

- ステップ 1** このコマンドを使用し、ユーザー指定のナンス値を使用して、SUDI 証明書チェーンの署名を生成します（<hex_nonce> は 16 進のナンス文字列で置き換えます）。

例：

```
sh platform security certificate sudi nonce <hex_nonce>

switch# sh platform security certificate sudi nonce abc123
----- Node location: SUP
----- Nonce: abc123 Certificate name: Cisco SUDI Root
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBGNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODA5 ... -----END
CERTIFICATE----- Certificate name: Cisco SUDI CA -----BEGIN CERTIFICATE-----
MIEEZzCCA0+gAwIBAgIJCmRlUkzYYXxiMA0GCSqGSIb3DQEBCwUAMC0xDjAMBGNV ... -----END
CERTIFICATE----- Certificate name: Cisco SUDI -----BEGIN CERTIFICATE-----
MIID2DCCAsCgAwIBAgIKCINlGmUgRgUJpTANBgkqhkiG9w0BAQsFADAxMR8wHQYD ... -----END
CERTIFICATE----- signature:
33a3639c5d994e40f6a99740d18c3caw/MFEP22%45a6c040s3kzQvYUJmcmV2Sjpm05Dm1m9gASARce7mmVX5p6SjpmWm8e=
signature_version: 2
```

SUDI 証明書チェーンおよび指定されたナンス値で生成された署名を表示します。出力には、ノードの場所、ナンス、証明書、署名、および署名バージョンが含まれます。

ノードの場所、ナンス、証明書チェーン、および署名が出力に表示されます。

- ステップ 2** JSON 形式の出力を表示します。自動化やスクリプトまたは外部システムとの統合のために、「|json-pretty」オプションをコマンドに追加します。

例：

```
sh platform security certificate sudi <hex_nonce> | json-pretty

switch# sh platform security certificate sudi nonce abc123 | json-pretty
{ "system-certificates": { "TABLE_system-certificates": { "ROW_system-certificates": {
"node-location": "SUP", "nonce": "YWJjMTIz", "certificates": { "TABLE_certificate": {
```



```
"ROW_certificate": [ { "name": "Cisco SUDI Root",  
"value": "MIIDICAgAwIwPgAFAgEAAQAGCSGSIb3DQEBCwUAMC0xDjAMBGAIBNpc2NmRsgQYDQQExTANhjoBSZ90...END CERTIFICATE-----"  
}, { "name": "Cisco SUDI CA", "value": "  
"MIIIEZzCCA0+gAwIBAgIJCmRlUKzYYXxiMA0GCsgGSib3DQEBCwUAMC0xDjAMBGAIBNBAoTBUNpc2Nv...END  
CERTIFICATE-----" }, { "name": "Cisco SUDI", "value": "  
"MIID2DCCAsCgAwIBAgIKCINigmUgRjUJpTANBgkqhkiG9w0BAQAQSFADAXMR8WHQYD...END CERTIFICATE-----"  
} ] } }, "signature": "  
"3d3djgssyMM2S0Vnq7ZKf8ScFpmW/LmZPH2V2+namOWH9vde-zWYUjUimdm2PbaSpyn+edgUSL47Cn/B6W/AKxPSnpWmPhd,"  
"signature_version": "2" } } }
```

自動化と統合のために、JSON 形式で SUDI 証明書チェーンと署名を提供します。出力には、ノードの場所、ナンス（Base64 エンコード）、証明書、署名、および署名バージョンが含まれます。

JSON 出力には、ノードの場所、ナンス、証明書チェーン、および署名が含まれます。



第 10 章

ユーザ アカウントおよび RBAC の設定

この章では、Cisco NX-OS デバイス上でユーザ アカウントおよびロールベース アクセス コントロール (RBAC) を設定する手順について説明します。

この章は、次の項で構成されています。

- ユーザ アカウントと RBAC について, [on page 277](#)
- ユーザ アカウントおよび RBAC の注意事項と制約事項 (281 ページ)
- ユーザ アカウントおよび RBAC のデフォルト設定, [on page 282](#)
- パスワードの強度確認のイネーブル化, [on page 283](#)
- パスワードの連続文字チェックの有効化 (284 ページ)
- ユーザ アカウントの設定, [on page 285](#)
- ロールの設定, [on page 288](#)
- No Service Password-Recovery について (295 ページ)
- No Service Password-Recovery のイネーブル化 (296 ページ)
- ユーザ アカウントおよび RBAC 設定の確認, [on page 297](#)
- ユーザ アカウントおよび RBAC の設定例, [on page 298](#)
- ユーザ アカウントおよび RBAC に関する追加情報, [on page 299](#)

ユーザ アカウントと RBAC について

ユーザ アカウントを作成して管理し、Cisco NX-OS で行える操作を制限するロールを割り当てることができます。RBAC は、ユーザが実行する必要がある管理操作の許可を制限するロールの割り当てのルールを定義することを可能にします。

ユーザーアカウント

最大 256 のユーザ アカウントを作成できます。デフォルトでは、明示的に期限を指定しない限り、ユーザ アカウントは無期限に有効です。expire オプションを使用すると、ユーザ アカウントをディセーブルにする日付を設定できます。

次の語は予約済みであり、ユーザ設定に使用できません。bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、gopher、ftp、nobody、nscd、mailnull、root、rpc、rpcuser、xfs、gdm、mtuser、ftuser、man、および sys。

**Note**

ユーザのパスワードは、設定ファイルでは表示されません。

**Caution**

ユーザ名は、先頭が英数字で始まる必要があり、その他に使用できる特殊文字は (+ = . _ \ -)。#, @ および ! 記号はサポートされていません。ユーザ名に許可されていない文字が含まれている場合、指定したユーザはログインできません。

強力なパスワードの特性

強力なパスワードは、次の特性を持ちます。

**Note**

Cisco Nexus デバイスのパスワードには、ドル記号 (\$) やパーセント記号 (%) などの特殊文字を使用できます。

- 長さが 8 文字以上である
- 複数の連続する文字（「abcd」など）を含んでいない
- 複数の同じ文字の繰返し（「aaabbb」など）を含んでいない
- 辞書に載っている単語を含んでいない
- 正しい名前を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

強力なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21



Note

クリアテキストのパスワードでは、パスワードの先頭に引用符 (" または ')、縦棒 (|)、大なり記号 (>) などの特殊文字を含めることはできません。パスワードの強度確認をイネーブルにすると、パスワードが単純である場合（短く、簡単に解読されるパスワードなど）に、Cisco NX-OS ソフトウェアによってパスワード設定が拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードでは大文字と小文字が区別されます。



Note

出力可能なすべての ASCII 文字は、引用符で囲めば、パスワード文字列でサポートされます。

Related Topics

[パスワードの強度確認のイネーブル化](#) (283 ページ)

ユーザロール

ユーザロールには、そのロールを割り当てられたユーザが実行できる操作を定義するルールが含まれています。各ユーザロールに複数のルールを含めることができ、各ユーザが複数のロールを持つことができます。たとえば、ロール 1 では設定操作の実行だけが許可されており、ロール 2 ではデバッグ操作の実行だけが許可されている場合、ロール 1 とロール 2 の両方に属するユーザは、設定操作とデバッグ操作を実行できます。また、特定の仮想ルーティング/転送 (VRF) インスタンス、VLAN、およびインターフェイスへのアクセスも制限できます。

Cisco NX-OS ソフトウェアには、次のユーザロールが用意されています。

- **network-admin** : Cisco NX-OS デバイス全体への完全な読み取り/書き込みアクセス権
- **network-operator** または **vdc-operator** : Cisco NX-OS デバイス全体への完全な読み取りアクセス権



Note

- Cisco Nexus 9000 シリーズスイッチは複数の VDC をサポートしていません。ただし、**vdc-operator** ロールは使用可能で、**network-operator** ロールと同じ権限と制限があります。
- Cisco Nexus 9000 シリーズスイッチは、VDC 管理者がネットワーク管理者と同じ権限と制限を持つような、単一の VDC をサポートします。



Note

ユーザロールは変更できません。



Note 一部の **show** コマンドは、**network-operator** ユーザには表示されないようにすることができます。加えて、一部の **show** 以外のコマンド (**telnet** など) を、このユーザロールで使用できるようにすることができます。

デフォルトでは、管理者のロールがないユーザアカウントでは**show**、**exit**、**end**、および **configure terminal** コマンドにしかアクセスできません。ルールを追加して、ユーザが機能を設定できるようにすることが可能です。



Note 複数のロールに属するユーザは、そのロールで許可されるすべてのコマンドの組み合わせを実行できます。コマンドへのアクセス権は、コマンドへのアクセス拒否よりも優先されます。たとえば、ユーザが、コンフィギュレーション コマンドへのアクセスが拒否されたロール A を持っていたとします。しかし、同じユーザが ロール B も持ち、このロールではコンフィギュレーション コマンドにアクセスできるとします。この場合、このユーザはコンフィギュレーション コマンドにアクセスできます。

ユーザロールのルール

ルールは、ロールの基本要素です。ルールは、そのロールがユーザにどの操作の実行を許可するかを定義します。ルールは次のパラメータで適用できます。

コマンド

正規表現で定義されたコマンドまたはコマンド グループ

機能

正規表現で定義されたコマンドまたはコマンド グループ

機能グループ

機能のデフォルト グループまたはユーザ定義グループ

OID

SNMP オブジェクト ID (OID)。

command、**feature**、および **feature group** の各パラメータにより、階層的な関係が作成されます。最も基本的な制御パラメータはコマンドです。次の制御パラメータは機能です。これは、その機能にアソシエートされているすべてのコマンドを表します。最後の制御パラメータが、機能グループです。機能グループは、関連する機能を組み合わせたものです。機能グループによりルールを簡単に管理できます。**Cisco NX-OS** ソフトウェアは、使用可能な事前定義済み機能グループもサポートしています。

SNMP OID は **RBAC** でサポートされています。**SNMP OID** に読み取り専用ルールまたは読み取り/書き込みルールを設定できます。

ロールごとに最大 256 のルールを設定できます。ルールが適用される順序は、ユーザ指定のルール番号で決まります。ルールは降順で適用されます。たとえば、1つのロールが3つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。

ユーザアカウントおよび RBAC の注意事項と制約事項

ユーザアカウントおよび RBAC には、次の設定ガイドラインと制限事項があります。

- 1 つのユーザ ロールには最大 256 のルールを追加できます。
- デフォルトの機能グループである L3に加えて、最大 64 のユーザ定義機能グループを追加できます。
- 最大 256 人のユーザを設定できます。
- ユーザアカウントには最大 64 個のユーザ ロールを割り当てることができます。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザアカウントが、AAA サーバ上のリモート ユーザアカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザアカウントのユーザ ロールをリモート ユーザに適用します。
- デフォルトの admin と SNMP ユーザアカウントは削除できません。
- デフォルトのユーザ ロールを、デフォルトの admin ユーザアカウントから削除することはできません。
- network-operator ロールでは、**ssh show running-config** および **show startup-config** コマンドを実行できません。
- Cisco Nexus 9000 シリーズスイッチは、VDC 管理者がネットワーク管理者と同じ権限と制限を持つ単一の VDC をサポートします。
- AAA ポリシーに従って、ロールがユーザに最後のロールとして関連付けられている場合、そのロールは、そのユーザから関連付けが解除されるまで削除できません。



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

- Cisco NX-OS Release 10.2(2)F 以降、新しい非同期化 CLI が導入され、SNMP とセキュリティコンポーネントの間のユーザー同期を無効にするオプションを提供します。詳細については、システム管理構成ガイドの **SNMP** の構成の章を参照してください。

リリース 7.0(3)I7(1)から現在のリリースまでのさまざまな機能をサポートする Cisco Nexus 9000 スイッチの詳細については、[Nexus スイッチプラットフォーム サポート マトリックス](#)を参照してください。

- 非同期 CLI が有効になっている場合、リモート ユーザーは SNMP データベースに同期されません。
- DCNM（リリース 12.0.1.a 以降 Nexus Dashboard Fabric Controller と呼ばれる）を使用したセキュリティユーザーには、非同期 CLI が有効でないとき、対応する SNMPv3 プロファイル

イルが存在しません。同期が無効になっている場合、セキュリティコンポーネントで作成されたユーザーはスイッチにログインできますが、コントローラはスイッチを検出しません。コントローラは、セキュリティユーザー用に作成された SNMP 構成を使用してスイッチを検出するためです。さらに、SNMP は、userDB の非同期状態のため、作成されたセキュリティユーザーを認識しないので、スイッチを検出できません。したがって、コントローラによってスイッチが検出されるようにするには、SNMP ユーザーを明示的に作成する必要があります。DCNM 機能とともに非同期 CLI を使用することはお勧めしません。詳細については、Cisco Nexus 9000 NX-OS セキュリティ構成ガイドを参照してください。

- Cisco NX-OS Release 10.3(1)F 以降、タイプ 8 とタイプ 9 パスワードハッシュが Cisco Nexus 9000 シリーズ スイッチでサポートされます。



(注) タイプ 5 は下位互換性をサポートしていますが、タイプ 8 とタイプ 9 をダウングレードすることはできません。

- Cisco NX-OS リリース 10.3(1)F 以降、パスワードの連続文字チェックは Cisco Nexus 9000 シリーズ スイッチでサポートされています。

ユーザアカウントおよび RBAC のデフォルト設定

次の表に、ユーザアカウントおよび RBAC パラメータのデフォルト設定を示します。

Table 13: デフォルトのユーザアカウントおよび RBAC パラメータ

パラメータ	デフォルト
ユーザアカウントパスワード	未定義
ユーザアカウントの有効期限	なし
ユーザアカウント ロール	作成ユーザが network-admin ロールを持つ場合は network-operator
デフォルト ユーザ ロール	network-operator
インターフェイス ポリシー	すべてのインターフェイスにアクセス可能
VLAN ポリシー	すべての VLAN にアクセス可能
VRF ポリシー	すべての VRF にアクセス可能
機能グループ	L3

パスワードの強度確認のイネーブル化

ユーザアカウントに対して弱いパスワードを設定しないように、パスワードの強度確認機能をイネーブルにすることができます。



Note パスワード強度確認をイネーブルにしても、Cisco NX-OS ソフトウェアでは、既存パスワードの強度確認は行われません。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	password strength-check Example: <pre>switch(config)# password strength-check</pre>	パスワードの強度確認をイネーブルにします。デフォルトではイネーブルになっています。 パスワードの強度確認をディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	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 4	(Optional) show password strength-check Example: <pre>switch# show password strength-check</pre>	パスワードの強度確認の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[強力なパスワードの特性](#) (278 ページ)

パスワードの連続文字チェックの有効化

パスワードシーケンスで、キーボード上の並び文字やアルファベットの並び文字は、攻撃に対して脆弱なため、制限が課されます。

パスワードには、次のパスワード文字列シーケンスの長さ制限が課されます。

- 設定可能な値の繰り返しの文字数 (aaaa、bbbb など)
- 連続するアルファベット/数字の文字数 (abcd...、1234...、)
- キーボード上で連続している文字の数 (qwer...、asdf...)

この手順では、パスワードのシーケンスに対する制限の構成方法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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードを入力します。
ステップ 2	[no] userpassphrase sequence alphabet length Value 例 : <pre>switch(config)#userpassphrase sequence alphabet length 4</pre>	連続したアルファベットの長さの制限を設定します。キーボード上で並んだ文字の長さの範囲は 2 ～ 10 です。 例 : userpassphrase sequence alphabet length 4 username user password AbcDe19jd このパスワードの文字は指定数を超えて連続しているため、受け入れられません。 no オプションは、アルファベット順のチェックを無効にします。
ステップ 3	[no] userpassphrase sequence keyboard length Value 例 : <pre>switch(config)# userpassphrase sequence keyboard length 4</pre>	キーボード上で並んだ文字の長さの制限を設定します。キーボード上で並んだ文字の長さの範囲は 2 ～ 10 です。 例 : userpassphrase sequence keyboard length 4 username user password CvBnmwu204

	コマンドまたはアクション	目的
		このパスワードの文字はキーボード上で指定数を超えて連続しているため、受け入れられません no オプションは、キーボード上で並んだ文字のチェックを無効にします。

ユーザアカウントの設定

1 つの Cisco NX-OS デバイスに最大 256 個のユーザアカウントを作成できます。ユーザアカウントは、次の属性を持ちます。

- ユーザー名
- パスワード
- 失効日
- ユーザ ロール

パスワードはクリアテキストか暗号化された形式で入力できます。Cisco NX-OS パスワードは、実行コンフィギュレーションに保存する前にクリアテキストのパスワードを暗号化します。暗号化された形式のパスワードは、これ以上の暗号化を行わずに実行コンフィギュレーションに保存されます。

SHA256 は、パスワードの暗号化に使用されるハッシュアルゴリズムです。暗号化の一環として、64 ビット SALT の 5000 回の反復がパスワードに追加されます。

SHA256 は、パスワードの暗号化に使用されるデフォルトのハッシュアルゴリズムです。タイプ 8 およびタイプ 9 のパスワードのハッシュを生成するには、クリアテキストパスワードとともに PBKDF2/SCRYPT オプションを指定する必要があります。

ユーザアカウントは、最大 64 個のユーザロールを持つことができます。コマンドラインインターフェイス (CLI) の状況依存ヘルプユーティリティを使用して、利用できるコマンドを確認できます。



Note

ユーザアカウントの属性に加えられた変更は、そのユーザがログインして新しいセッションを作成するまで有効になりません。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	(Optional) show role Example: <pre>switch(config)# show role</pre>	使用可能なユーザロールを表示します。必要に応じて、他のユーザ ロールを設定できます。
ステップ 3	username user-id [password [0 5 8 9] password [pbkdf2 scrypt]] [expire date] [role role-name] Example: <pre>switch(config)# username NewUser password 4Ty18Rnt</pre>	ユーザアカウントを設定します。 <i>user-id</i> 引数は、大文字と小文字が区別される英数字で、最大 28 文字です。これはローカルおよびリモート ユーザーの両方に当てはまります。指定できる文字は、A ～ Z の英大文字、a ～ z の英小文字、0 ～ 9 の数字、ハイフン (-)、ピリオド (.)、アンダースコア (_)、プラス符号 (+)、および等号 (=) です。アットマーク (@) はリモート ユーザ名では使用できますが、ローカル ユーザ名では使用できません。 ユーザ名の先頭は英数字で始まる必要があります。 デフォルト パスワードは定義されていません。 • 0 オプションは、パスワードがクリア テキストであることを示しています。 • 5 オプションは、パスワードが SHA-256 ハッシュされていることを示します。 • 8 オプションは、パスワードが PBKDF2 ハッシュされていることを示します。 • 9 オプションは、パスワードが Scrypt ハッシュされていることを示します。

	Command or Action	Purpose
		デフォルト オプションは 0 (クリア テキスト) です。 Note pbkdf2/scrypt キーワードはオプションであり、実行構成に保存されます。 Note パスワードを指定しなかった場合、ユーザは Cisco NX-OS デバイスにログインできません。 Note 暗号化パスワード オプションを使用してユーザ アカウントを作成する場合、対応する SNMP ユーザは作成されません。 Note 非同期 CLI が有効になっている場合、ユーザー アカウントを作成しても、対応する SNMP ユーザーは作成されません。 expire date オプションのフォーマットは YYYY-MM-DD です。デフォルトでは、失効日はありません。 ユーザアカウントは、最大 64 個のユーザ ロールを持つことができます。
ステップ 4	username user-id ssh-cert-dn dn-name {dsa rsa} Example: <pre>switch(config)# username NewUser ssh-cert-dn "/CN = NewUser, OU = Cisco Demo, O = Cisco, C = US" rsa</pre> Example: <pre>switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa</pre>	既存のユーザ アカウント認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。識別名は最大 512 文字で、例に示す形式に従う必要があります。電子メールアドレスと状態がそれぞれ emailAddress と ST に設定されていることを確認します。
ステップ 5	exit Example:	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。

	Command or Action	Purpose
	switch(config)# exit switch#	
ステップ 6	(Optional) show user-account Example: switch# show user-account	ロール設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics[ロールの設定](#) (288 ページ)[ユーザ ロールおよびルールを作成](#) (288 ページ)

ロールの設定

ここでは、ユーザ ロールの設定方法について説明します。

ユーザ ロールおよびルールの作成

最大 64 個のユーザ ロールを設定できます。各ユーザ ロールが、最大 256 個のルールを持つことができます。ユーザ ロールを複数のユーザ アカウントに割り当てることができます。

指定したルール番号は、ルールが適用される順番を決定します。ルールは降順で適用されます。たとえば、1 つのロールが 3 つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。

一致に対して RBACL 処理を実行する場合、部分一致では評価プロセスは停止しません。完全一致が見つかるまで、各ルールの評価が続行されます。完全一致が見つからない場合、リスト内で最も正確なルールが結果として選択されます。また、同じ一致ロジックに対して許可ルールと拒否ルールが存在する場合、（先に評価された）番号の大きいルールが結果として選択されます。



Note ユーザ ロールに設定された読み取り/書き込みルールに関係なく、一部のコマンドは、あらかじめ定義された **network-admin** ロールでのみ実行できます。

Before you begin

ユーザ ロール設定を配布する場合は、設定を配布する対象のすべての Cisco NX-OS デバイスでユーザ ロール設定の配布を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	role name role-name Example: <pre>switch(config)# role name UserA switch(config-role)#</pre>	ユーザ ロールを指定し、ロール コンフィギュレーションモードを開始します。 role-name 引数は、最大 16 文字の長さの英数字のストリングで、大文字小文字が区別されます。
ステップ 3	rule number {deny permit} command command-string Example: <pre>switch(config-role)# rule 1 deny command clear users</pre>	コマンド ルールを設定します。 command-string には、スペースおよび正規表現を含めることができます。たとえば、interface ethernet にはすべてのイーサネットインターフェイスが含まれます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 4	rule number {deny permit} {read read-write} Example: <pre>switch(config-role)# rule 2 deny read-write</pre>	すべての操作の読み取り専用ルールまたは読み取り/書き込みルールを設定します。
ステップ 5	rule number {deny permit} {read read-write} feature feature-name Example: <pre>switch(config-role)# rule 3 permit read feature router-bgp</pre>	機能に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 show role feature コマンドを使用すれば、機能のリストが表示されます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 6	rule number {deny permit} {read read-write} feature-group group-name Example: <pre>switch(config-role)# rule 4 deny read-write feature-group L3</pre>	機能グループに対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 show role feature-group コマンドを使用すれば、機能グループのリストが表示されます。

	Command or Action	Purpose
		必要な規則の数だけこのコマンドを繰り返します。
ステップ 7	rule number {deny permit} {read read-write} oid snmp_oid_name Example: <pre>switch(config-role)# rule 5 deny read-write oid 1.3.6.1.2.1.1.9</pre>	SNMP オブジェクト ID (OID) の読み取り専用または読み書きルールを設定します。OID には最大 32 の要素を入力することができます。このコマンドは、SNMP ベースのパフォーマンス モニタリングツールがデバイスをポーリングするために使用できますが、IP ルーティング テーブル、MAC アドレス テーブル、特定の MIB などのシステムの集中的な拠点へのアクセスは制限されます。 Note 一番深層の OID はスカラ レベルまたはテーブル ルート レベルにすることができます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 8	(Optional) description text Example: <pre>switch(config-role)# description This role does not allow users to use clear commands</pre>	ロールの説明を設定します。説明にはスペースも含めることができます。
ステップ 9	exit Example: <pre>switch(config-role)# exit switch(config)#</pre>	ロー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 10	(Optional) show role Example: <pre>switch(config)# show role</pre>	ユーザロールの設定を表示します。
ステップ 11	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

機能グループの作成

カスタム機能グループを作成して、Cisco NX-OS ソフトウェアが提供するデフォルトの機能リストに追加できます。これらの機能グループは1つまたは複数の機能を含んでいます。最大64個の機能グループを作成できます。



Note デフォルト機能グループ L3 を変更することはできません。

Before you begin

ユーザ ロール設定を配布する場合は、設定を配布する対象のすべての Cisco NX-OS デバイスでユーザ ロール設定の配布を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	role feature-group name group-name Example: switch(config)# role feature-group name GroupA switch(config-role-featuregrp)#	ユーザ ロール機能グループを指定して、ロール機能グループ コンフィギュレーション モードを開始します。 <i>group-name</i> 引数は、最大 32 文字の長さの英数字のストリングで、大文字小文字が区別されます。
ステップ 3	feature feature-name Example: switch(config-role-featuregrp)# feature radius	機能グループの機能を指定します。 必要な機能の数だけこのコマンドを繰り返します。 Note 機能の一覧を表示する場合は、 show role component コマンドを使用します。
ステップ 4	exit Example: switch(config-role-featuregrp)# exit switch(config)#	ロール機能グループ コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show role feature-group Example: switch(config)# show role feature-group	ロール機能グループ設定を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ユーザロールインターフェイスポリシーの変更

ユーザロールインターフェイスポリシーを変更することで、ユーザがアクセスできるインターフェイスを制限できます。デフォルトでは、ユーザロールによってすべてのインターフェイスへのアクセスが許可されます。

Before you begin

1 つまたは複数のユーザロールを作成します。

ユーザロール設定を配布する場合は、設定を配布する対象のすべての Cisco NX-OS デバイスでユーザロール設定の配布をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	role name role-name Example: <pre>switch(config)# role name UserA switch(config-role)#</pre>	ユーザロールを指定し、ロー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 policy deny Example: <pre>switch(config-role)# interface policy deny switch(config-role-interface)#</pre>	ロールインターフェイス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	permit interface interface-list Example: <pre>switch(config-role-interface)# permit interface ethernet 2/1-4</pre>	ロールがアクセスできるインターフェイスのリストを指定します。 必要なインターフェイスの数だけこのコマンドを繰り返します。

	Command or Action	Purpose
ステップ 5	exit Example: switch(config-role-interface)# exit switch(config-role)#	ロール インターフェイス 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	(Optional) show role Example: switch(config-role)# show role	ロール設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch(config-role)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[ユーザ ロールおよびルールの作成](#) (288 ページ)

ユーザ ロール VLAN ポリシーの変更

ユーザ ロール VLAN ポリシーを変更することで、ユーザがアクセスできる VLAN を制限できます。デフォルトでは、ユーザ ロールによってすべての VLAN へのアクセスが許可されます。

Before you begin

1 つまたは複数のユーザ ロールを作成します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	role name role-name Example: switch(config)# role name UserA switch(config-role)#	ユーザ ロールを指定し、ロール 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 policy deny Example: switch(config-role)# vlan policy deny switch(config-role-vlan)#	ロール VLAN ポリシー コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 4	permit vlan vlan-list Example: <pre>switch(config-role-vlan)# permit vlan 1-4</pre>	ロールがアクセスできる VLAN の範囲を指定します。 必要な VLAN の数だけこのコマンドを繰り返します。
ステップ 5	exit Example: <pre>switch(config-role-vlan)# exit switch(config-role)#</pre>	ロール VLAN 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	(Optional) show role Example: <pre>switch(config)# show role</pre>	ロール設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config-role)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[ユーザロールおよびルールの作成](#) (288 ページ)

ユーザロールのVRFポリシーの変更

ユーザロールのVRFポリシーを変更して、ユーザがアクセスできるVRFを制限できます。デフォルトでは、ユーザロールによってすべてのVRFへのアクセスが許可されます。

Before you begin

1 つまたは複数のユーザロールを作成します。

ユーザロール設定を配布する場合は、設定を配布する対象のすべてのCisco NX-OS デバイスでユーザロール設定の配布をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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

	Command or Action	Purpose
ステップ 2	role name <i>role-name</i> Example: <pre>switch(config)# role name UserA switch(config-role)#</pre>	ユーザ ロールを指定し、ロール 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	vrf policy deny Example: <pre>switch(config-role)# vrf policy deny switch(config-role-vrf)#</pre>	ロール VRF 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	permit vrf <i>vrf-name</i> Example: <pre>switch(config-role-vrf)# permit vrf vrf1</pre>	ロールがアクセスできる VRF を指定します。 必要な VRF の数だけこのコマンドを繰り返します。
ステップ 5	exit Example: <pre>switch(config-role-vrf)# exit switch(config-role)#</pre>	ロール VRF 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	(Optional) show role Example: <pre>switch(config-role)# show role</pre>	ロール設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config-role)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[ユーザ ロールおよびルールの作成](#) (288 ページ)

No Service Password-Recovery について

No Service Password-Recovery 機能により、コンソールへのアクセスを持つ誰もがルータおよびルータのネットワークにアクセスする機能を与えられることになります。No Service Password-Recovery 機能を使用すると、[Cisco Nexus 9000 シリーズ NX-OS トラブルシューティング ガイド](#)に記載されている標準的な手順でパスワードを回復できなくなります。

No Service Password-Recovery のイネーブル化

No Service Password-Recovery 機能が有効になっている場合、ネットワーク権限を持つ管理者以外は管理者パスワードを変更できません。

始める前に

no service password-recovery コマンドを開始する場合、シスコでは、デバイスから離れた場所にシステム コンフィギュレーション ファイルのコピーを保存することを推奨しています。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 service password-recovery 例 : <pre>switch(config)# no service password-recovery WARNING: Executing this command will disable the password recovery mechanism. Do not execute this command without another plan for password recovery. Are you sure you want to continue? (y/n) : [y] y switch(config)# copy run start [#####] 100% Copy complete, now saving to disk (please wait)... Copy complete.</pre>	パスワード回復メカニズムを無効にします。
ステップ 3	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 4	Reload 例 : <pre>switch(config)# Reload This command will reboot the system. (y/n)? [n] y 2018 Jun 26 16:23:19 BAR %\$ VDC-1 %\$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line</pre>	

	コマンドまたはアクション	目的
	<pre>Interface CISCO SWITCH Ver 8.34 CISCO SWITCH Ver 8.34 Manual system restart from Command Line Interface writing reset reason 9, ... switch(boot)# config t Enter configuration commands, one per line. End with CNTL/Z. switch(boot) (config)# admin-password Abcd!123\$ ERROR: service password-recovery disabled. Cannot change password! switch(boot) (config)#</pre>	
ステップ 5	exit 例 : <pre>switch(config)# exit switch#</pre>	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 6	(任意) show user-account 例 : <pre>switch# show user-account</pre>	ロール設定を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ アカウントおよび RBAC 設定の確認

ユーザ アカウントおよびRBAC 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show cli syntax roles network-admin	network-admin ロールが使用できるが、コマンドの構文を表示します。
show cli syntax roles network-operator	network-operator ロールで。
show role	ユーザ ロールの設定を表示します。

コマンド	目的
show role feature	機能リストを表示します。
show role feature-group	機能グループの設定を表示します。
show startup-config security	スタートアップ コンフィギュレーションのユーザ アカウント設定を表示します。
show running-config security [all]	実行コンフィギュレーションのユーザ アカウント設定を表示します。 all キーワードを指定すると、ユーザ アカウントのデフォルト値が表示されます。
show user-account	ユーザ アカウント情報を表示します。

ユーザ アカウントおよび RBAC の設定例

次に、ユーザ ロールを設定する例を示します。

```
role name User-role-A
  rule 2 permit read-write feature bgp
  rule 1 deny command clear *
```

次に、BGPを有効にして表示し、EIGRPを表示するようにインターフェイスを設定できるユーザ ロールを作成する例を示します。

```
role name iftest
  rule 1 permit command config t; interface *; bgp *
  rule 2 permit read-write feature bgp
  rule 3 permit read feature eigrp
```

上の例で、ルール 1 はインターフェイス上で BGP を設定することを可能にし、ルール 2 は **config bgp** コマンドを設定して実行レベルの **show** コマンドと **debug** コマンドを BGP に対して有効にすることを有効にし、ルール 3 は実行レベルの **show** コマンドと **debug eigrp** コマンドを有効にすることを可能にしています。

次に、特定のインターフェイスだけを設定できるユーザ ロールを設定する例を示します。

```
role name Int_Eth2-3_only
  rule 1 permit command configure terminal; interface *
  interface policy deny
  permit interface Ethernet2/3
```


次に、ユーザ ロール機能グループを設定する例を示します。

```
role feature-group name Security-features
  feature radius
  feature tacacs
  feature aaa
  feature acl
  feature access-list
```

次に、ユーザ アカウントを設定する例を示します。

```
username user1 password A1s2D4f5 role User-role-A
```

次に、アクセスを OID サブツリーの一部に制限するための OID ルールを追加する例を示します。

```
role name User1
  rule 1 permit read feature snmp
  rule 2 deny read oid 1.3.6.1.2.1.1.9
show role name User1
```

Role: User1

```
Description: new role
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Rule	Perm	Type	Scope	Entity
2	deny	read	oid	1.3.6.1.2.1.1.9
1	permit	read	feature	snmp

次に、指定された OID サブツリーへの書き込み権限を許可する例を示します。

```
role name User1
  rule 3 permit read-write oid 1.3.6.1.2.1.1.5
show role name User1
```

Role: User1

```
Description: new role
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Rule	Perm	Type	Scope	Entity
3	permit	read-write	oid	1.3.6.1.2.1.1.5
2	deny	read	oid	1.3.6.1.2.1.1.9
1	permit	read	feature	snmp

ユーザアカウントおよびRBACに関する追加情報

ここでは、ユーザアカウントおよびRBACの実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	Cisco NX-OS ライセンス ガイド
VRF コンフィギュレーション	『Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング設定ガイド』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
ユーザアカウントおよびRBACに関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 11 章

802.1X の設定

この章では、Cisco NX-OS デバイス上で IEEE 802.1X ポートベースの認証を設定する手順について説明します。

この章は、次の項で構成されています。

- [802.1X について, on page 301](#)
- [音声 VLAN 向け 802.1X について \(309 ページ\)](#)
- [DACL について \(310 ページ\)](#)
- [802.1X の前提条件, on page 310](#)
- [802.1X のガイドラインと制約事項 \(311 ページ\)](#)
- [音声 VLAN に関連した 802.1X のガイドラインと制限事項 \(315 ページ\)](#)
- [802.1X 向け事前ユーザ DACL サポートのガイドラインと制約事項 \(316 ページ\)](#)
- [クリティカル認証のガイドラインと制限事項 \(317 ページ\)](#)
- [802.1X のデフォルト設定, on page 317](#)
- [802.1X の設定, on page 318](#)
- [802.1X 設定の確認, on page 344](#)
- [VXLAN EVPN の 802.1X サポート \(346 ページ\)](#)
- [クリティカル認証の確認 \(351 ページ\)](#)
- [802.1X のモニタリング, on page 351](#)
- [802.1X の設定例, on page 351](#)
- [ユーザ 1 人あたりの DACL の設定例 \(352 ページ\)](#)
- [802.1X に関する追加情報, on page 352](#)

802.1X について

802.1X では、クライアント サーバベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、Cisco NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

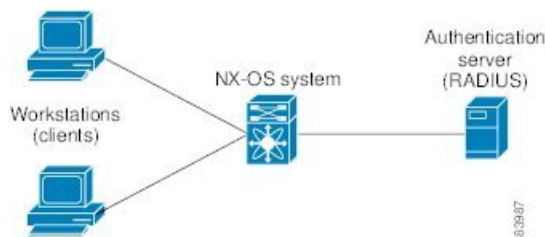
802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN (EAPOL) トラフィック

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。

デバイスのロール

802.1X ポート ベースの認証では、ネットワーク上のデバイスにそれぞれ特定のロールがあります。

Figure 6: 802.1X デバイスのロール



特定のロールは次のとおりです。

サブリカント

LAN および Cisco NX-OS デバイス サービスへのアクセスを要求し、Cisco NX-OS デバイスからの要求に回答するクライアントデバイスです。ワークステーションでは、Microsoft Windows XP が動作するデバイスで提供されるような、802.1X 準拠のクライアントソフトウェアが稼働している必要があります。

認証サーバ

サブリカントの実際の認証を行います。認証サーバはサブリカントの識別情報を確認し、LAN および Cisco NX-OS デバイスのサービスへのアクセスをサブリカントに許可すべきかどうかを Cisco NX-OS デバイスに通知します。Cisco NX-OS デバイスはプロキシとして動作するので、認証サービスはサブリカントに対しては透過的に行われます。認証サーバとして、拡張認証プロトコル (EAP) 拡張機能を備えた Remote Authentication Dial-In User Service (RADIUS) セキュリティ デバイスだけがサポートされています。この認証サーバは、Cisco Secure Access Control Server バージョン 3.0 で使用可能です。RADIUS はサブリカント サーバ モデルを使用し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。

オーセンティケータ

サブリカ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。オーセンティケータは、サブリカ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、サブリカントから識別情報を要求し、得られた識別情報を認証サーバに確認し、サブリカントに回答をリレーします。オーセンティケータには、EAP フレームのカプセル化/カプセル化解除、および認証サーバとの対話を処理する、RADIUS クライアントが含まれています。

オーセンティケータが EAPOL フレームを受信して認証サーバにリレーする際は、イーサネット ヘッダーを取り除き、残りの EAP フレームを RADIUS 形式にカプセル化します。このカプセル化のプロセスでは EAP フレームの変更または確認が行われないため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートする必要があります。オーセンティケータは

認証サーバからフレームを受信すると、サーバのフレーム ヘッダーを削除し、残りの EAP フレームをイーサネット用にカプセル化してサブリカントに送信します。



Note Cisco NX-OS デバイスがなれるのは、802.1X オーセンティケータだけです。

認証の開始およびメッセージ交換

オーセンティケータ（Cisco NX-OS デバイス）とサブリカント（クライアント）のどちらも認証を開始できます。ポート上で認証をイネーブルにした場合、オーセンティケータはポートのリンクステートがダウンからアップに移行した時点で、認証を開始する必要があります。続いて、オーセンティケータは EAP-Request/Identity フレームをサブリカントに送信して識別情報を要求します（通常、オーセンティケータは1つまたは複数の識別情報の要求のあとに、最初の Identity/Request フレームを送信します）。サブリカ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。

サブリカントがブートアップ時にオーセンティケータから EAP-Request/Identity フレームを受信しなかった場合、サブリカントは EAPOL 開始フレームを送信することにより認証を開始することができます。この開始フレームにより、オーセンティケータはサブリカントの識別情報を要求します。



Note ネットワーク アクセス デバイスで 802.1X がイネーブルになっていない場合、またはサポートされていない場合、Cisco NX-OS デバイスはサブリカントからの EAPOL フレームをすべてドロップします。サブリカントが、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、サブリカントはポートが許可ステートにあるものとしてデータを送信します。ポートが許可ステートになっている場合は、サブリカントの認証が成功したことを意味します。

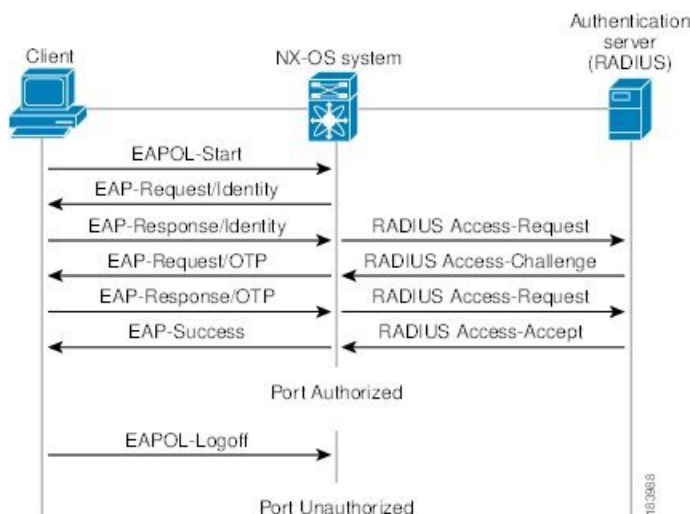
サブリカントが自己の識別情報を提示すると、オーセンティケータは仲介装置としてのロールを開始し、認証が成功または失敗するまで、サブリカントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、オーセンティケータのポートは許可ステートになります。

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。

Figure 7: メッセージ交換

次の図に、サブリカントが RADIUS サーバにワンタイム パスワード（OTP）認証方式を使用して開始するメッセージ交換を示します。OTP 認証デバイスは、シークレット パスフレーズ

を使用して、一連のワンタイム（使い捨て）パスワードを生成します。



ユーザのシークレットパスフレーズは、認証時やパスフレーズの変更時などにネットワークを通過することはありません。

インターフェイスのオーセンティケータ PAE ステータス

インターフェイスで 802.1X をイネーブルにすると、Cisco NX-OS ソフトウェアにより、オーセンティケータ Port Access Entity (PAE) インスタンスが作成されます。オーセンティケータ PAE は、インターフェイスでの認証をサポートするプロトコルエンティティです。インターフェイスで 802.1X をディセーブルにしても、オーセンティケータ PAE インスタンスは自動的にクリアされません。必要に応じ、オーセンティケータ PAE をインターフェイスから明示的に削除し、再度適用することができます。

許可ステートおよび無許可ステートのポート

サブリカントのネットワークへのアクセスが許可されるかどうかは、オーセンティケータのポートステートで決まります。ポートは、無許可ステートで開始します。このステートにあるポートは、802.1X プロトコル パケットを除いたすべての入トラフィックおよび出トラフィックを禁止します。サブリカントの認証に成功すると、ポートは許可ステートに移行し、サブリカントのすべてのトラフィック送受信を通常どおりに許可します。

802.1X 認証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 ポートに接続した場合、オーセンティケータは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 プロトコルの稼働していないポートに接続すると、クライアントは EAPOL 開始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。

ポートには次の許可ステートがあります。

Force authorized

802.1X ポートベースの認証をディセーブルにし、認証情報の交換を必要としないで許可ステートに移行します。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。この許可ステートはデフォルトです。

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。オーセンティケータは、インターフェイスを経由してクライアントに認証サービスを提供することができません。

Auto

802.1X ポートベースの認証をイネーブルにします。ポートは無許可ステートで開始し、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移行したとき、またはサブリカントから EAPOL 開始フレームを受信したときに、認証プロセスが開始します。オーセンティケータは、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。オーセンティケータはサブリカントの 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サブリカントを一意に識別します。

サブリカントの認証に成功すると（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、認証されたサブリカ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、オーセンティケータは要求を再送信できます。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、サブリカントのネットワーク アクセスは認可されません。

サブリカントはログオフするとき、EAPOL ログオフ メッセージを送信します。このメッセージによって、オーセンティケータのポートは無許可ステートに移行します。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL ログオフ フレームを受信した場合、ポートは無許可ステートに戻ります。

MAC 認証バイパス

MAC 認証バイパス機能を使用して、サブリカントの MAC アドレスに基づいてサブリカントを認証するように、Cisco NX-OS デバイスを設定できます。たとえば、プリンタなどのデバイスに接続されている 802.1X 機能を設定したインターフェイスで、この機能をイネーブルにすることができます。

サブリカントからの EAPOL 応答を待機している間に 802.1X 認証がタイムアウトした場合は、MAC 認証バイパスを使用して Cisco NX-OS デバイスはクライアントの許可を試みます。

インターフェイスで MAC 認証バイパス機能をイネーブルにすると、Cisco NX-OS デバイスは MAC アドレスをサブリカント ID として使用します。認証サーバには、ネットワーク アクセスが許可されたサブリカントの MAC アドレスのデータベースがあります。Cisco NX-OS デバイスは、インターフェイスでクライアントを検出した後、クライアントからのイーサネットパケットを待ちます。Cisco NX-OS デバイスは、MAC アドレスに基づいてユーザ名とパスワード

ドを含んだ RADIUS アクセス/要求フレームを認証サーバに送信します。許可に成功した場合、Cisco NX-OS デバイス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。

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で検出される場合、このインターフェイスに接続されているデバイスが 802.1X 対応サブリカントであることを Cisco NX-OS デバイスが判別し、(MAC 認証バイパスではなく) 802.1X 認証を使用してインターフェイスを許可します。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。

Cisco NX-OS デバイスがすでに MAC 認証バイパスを使用してインターフェイスを許可していて、802.1X サブリカントを検出した場合、Cisco NX-OS デバイスはインターフェイスに接続されているクライアントを無許可にしません。再認証を実行する際に、Cisco NX-OS デバイスは 802.1X 認証を優先再認証プロセスとして使用します。

MAC 認証バイパスで許可されたクライアントを再認証することができます。再認証プロセスは、802.1X で認証されたクライアントと同様です。再認証中に、ポートは前に割り当てられた VLAN に残ります。再認証に成功した場合、スイッチはポートを同じ VLAN 内に保持します。

再認証が Session-Timeout RADIUS 属性 (Attribute [27]) と Termination-Action RADIUS 属性 (Attribute [29]) に基づいていて、Termination-Action RADIUS 属性 (Attribute [29]) アクションが初期化の場合、(属性値は DEFAULT)、MAC 認証バイパス セッションが終了して、再認証中に接続が失われます。MAC 認証バイパスがイネーブルで 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許可を開始します。これらの AV ペアの詳細については、RFC 3580「IEEE 802.1X リモート認証ダイヤル イン ユーザ サービス (RADIUS) 使用ガイドライン」を参照してください。

MAC 認証バイパスは、次の機能と相互作用します。

- 802.1X 認証：802.1X 認証がポートでイネーブルの場合にだけ、MAC 認証バイパスをイネーブルにできます。
- ポート セキュリティ：同じレイヤ 2 ポート上で 802.1X 認証とポート セキュリティを構成することはできません。
- Network Admission Control (NAC) レイヤ 2 IP 検証：例外リスト内のホストを含む 802.1X ポートが MAC 認証バイパスで認証されたあとに、この機能が有効になります。

MAC-Based Authentication (MAB) に基づくダイナミック VLAN 割り当て

Cisco Nexus 9000 シリーズ スイッチはダイナミック VLAN 割り当てをサポートします。802.1X 認証または MAB が完了した後。ポートを起動する前に、認証の結果としてピア/ホストを特定の VLAN に配置できるようにすることができます (許可の一部として)。RADIUS サーバは、一般的に Access-Accept 内にトンネル属性を含めることによって目的の VLAN を示します。VLAN をポートにバインドするこの手順は、ダイナミック VLAN 割り当てを構成します。

RADIUS からの VLAN 割り当て

802.1X または MAB によって認証が完了すると、RADIUS サーバからの応答にダイナミック VLAN 情報を含めることができるようになり、これをポートに割り当てることができます。この情報は、トンネル属性の形式の受け入れアクセス メッセージの RADIUS サーバからの応答に存在します。VLAN 割り当てのために、次のトンネル属性が送信されます。

- Tunnel-type=VLAN(13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

アクセス VLAN の設定のために、3 つのパラメータをすべて受け取る必要があります。

シングル ホストおよびマルチ ホストのサポート

802.1X 機能では、1 つのポートのトラフィックを 1 台のエンドポイント装置に限定することも（シングルホストモード）、1 つのポートのトラフィックを複数のエンドポイント装置に許可することも（マルチホストモード）できます。

シングルホストモードでは、802.1X ポートで 1 台のエンドポイント装置のみからのトラフィックが許可されます。エンドポイント装置が認証されると、Cisco NX-OS デバイスはポートを許可ステートにします。エンドポイント装置がログオフすると、Cisco NX-OS デバイスはポートを無許可ステートに戻します。802.1X のセキュリティ違反とは、認証に成功して許可された単一の MAC アドレスとは異なる MAC アドレスをソースとするフレームが検出された場合をいいます。このような場合、このセキュリティ アソシエーション (SA) 違反（他の MAC アドレスからの EAPOL フレーム）が検出されたインターフェイスはディセーブルにされます。シングルホストモードは、ホストツースイッチ型トポロジで 1 台のホストが Cisco NX-OS デバイスのレイヤ 2 ポート（イーサネット アクセス ポート）またはレイヤ 3 ポート（ルーテッド ポート）に接続されている場合にだけ適用できます。

マルチホストモードに設定されている 802.1X ポートで、認証が必要になるのは最初のホストだけです。最初のホストの許可に成功すると、ポートは許可ステートに移行します。ポートが許可ステートになると、後続のホストがネットワークアクセスの許可を受ける必要はありません。再認証に失敗したり、または EAPOL ログオフ メッセージを受信して、ポートが無許可ステートになった場合には、接続しているすべてのクライアントはネットワークアクセスを拒否されます。マルチホストモードでは、SA 違反の発生時にインターフェイスをシャットダウンする機能がディセーブルになります。マルチホストモードは、スイッチツースイッチ型トポロジおよびホストツースイッチ型トポロジの両方に適用できます。

サポートされるトポロジ

802.1X ポートベースの認証は、ポイントツーポイント トポロジをサポートします。

この設定では、802.1X 対応のオーセンティケータ（Cisco NX-OS デバイス）ポートにサブリカント（クライアント）を 1 台だけ接続することができます。オーセンティケータは、ポートのリンクステートがアップステートに移行したときにサブリカントを検出します。サブリカ

トがログオフしたとき、または別のサブリカントに代わったときには、オーセンティケータはポートのリンク ステートをダウンに変更し、ポートは無許可ステータスに戻ります。

ユーザ単位の DACL について

Cisco NX-OS リリース 10.2(1)以降、IEEE 802.1X を使用した認証後のポリシー適用として、Cisco ISE サーバからユーザ単位のダイナミック アクセス コントロール リスト (DACL) をダウンロードできます。

ユーザ単位の DACL を設定して、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。スイッチは、セッションが終了するたびに、または認証が失敗した場合に、ユーザ単位の DACL 設定を削除します。

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 DACL に使用される VSA は、入力方向の `inacl#<n>` であり、その場合、`n` は 1 から 32 です。構文は次のとおりです。

```
ip:inacl#<n>=permit | deny [protocol] [source_subnet] [dest_subnet] [operator] [port]
```

例1: `ip:inacl#1=permit udp any any eq 5555`

例2: `ip:inacl#2=deny udp any any eq 6666`

VSA は入力方向に限りサポートされます。

クリティカル認証

Cisco NX-OS リリース 10.1(1) から、ポートの 802.1X クリティカル認証は、ISP ドメイン内の RADIUS サーバに到達できなかったときに認証に失敗した 802.1X ユーザに対応します。クリティカル認証機能は、802.1X 認証が RADIUS または ISE サーバを介してのみ実行される場合にサポートされます。802.1X ユーザが RADIUS 認証に失敗した場合でも、ネットワークへのアクセスは許可されます。これを行うには、**dot1x authentication event server dead action authorize** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

Cisco NX-OS リリース 10.5 (2) F 以降、802.1x 機能とクリティカル認証機能はマルチドメインポートでサポートされています。

音声 VLAN 向け 802.1X について

音声 VLAN 向け 802.1X の概要

IEEE 802.1X の音声 VLAN 機能は、単一のポートでマルチドメイン 802.1X 認証を可能にし、VoIP 電話とそれらに接続されているデータクライアントの両方の認証をサポートします。この機能を使用すると、1 つの特別なアクセスポートを構成して、2 つの VLAN 識別子に関連付けることができます。1 つは音声トラフィック専用、もう 1 つはデータトラフィック専用です。このセットアップでは、同じポートで 1 つの音声クライアントと 1 つのデータクライアントに対応する、マルチドメインホストモードのサポートが必要です。

ユーザーはこの機能を活用し、単一のアクセスポートを介して接続された音声デバイスとデータデバイスの両方の安全で効率的なネットワークトラフィック管理を保証できます。音声トラフィックとデータトラフィックを別々の VLAN に分離することで、ネットワーク管理者は両方のタイプのデバイスの堅牢なセキュリティと認証を維持しながら、高品質の VoIP 通信を確保できます。

音声 VLAN 用 802.1X の機能

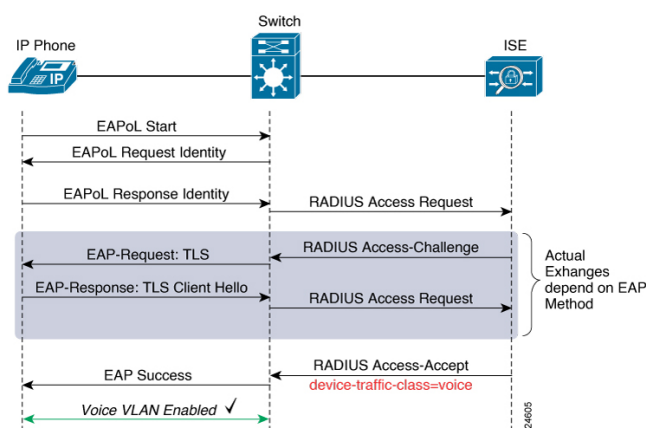
- 単一のポートでのマルチドメイン 802.1X 認証を有効にします。
- 新しいホストモード（マルチドメイン）は、1 つのポートで 1 つの音声デバイス（通常は IP 電話）と 1 つのデータデバイス（通常は PC）をサポートします。
- アイデンティティに基づいてユーザーを区別できるポートで単一のオーセンティケータを実行し、ユーザーを適切なドメイン（データと音声用に異なる VLAN）に配置します。
- 同じポートでデータトラフィックと音声トラフィックの分離を維持します。



音声 VLAN の 802.1X のメッセージ交換

- **VoIP 電話接続**：802.1X が構成されているスイッチに VoIP 電話が接続されています。
- **VoIP 電話認証**：VoIP 電話は、EAP または MAB のいずれかを使用して認証できます。
- **音声デバイスの認識**：VoIP 電話は RADIUS サーバによって音声デバイスとして認識され、802.1X は音声 VLAN 内の電話をセキュア化します。
- **データデバイス接続**：データデバイス（ラップトップなど）は、VoIP 電話を使用してスイッチに接続されます。

- **データデバイス認証**：データデバイスは 802.1X 認証をトリガーし、データ VLAN の RADIUS サーバによって承認されます。



DACL について

ダイナミック ACL (DACL) は、ユーザおよびグループがアクセスできる権限を含む単一の ACL です。dot1x MAB クライアントへのアクセスを制限します。DACL ポリシーが Cisco ISE サーバからプッシュされ、MAC アドレスがブラックリストに登録されます。これにより、ブラックリストに登録された MAC に ACL が適用され、MAB へのアクセスが制限されます。単一の DACL は、すべてのブラックリスト MAB クライアントをサポートします。

Cisco NX-OS Release 9.3(5) では、DACL は Cisco Nexus スイッチで事前設定されています。

802.1X の前提条件

- Cisco Nexus リリース 7.0(3)I7(1) ソフトウェア。

EAP-TLS プロファイルを使用した 802.1X ポートベース認証には、次の前提条件が必要です。

- PKI インフラは、EAP-TLS の証明書管理を提供します。特例を申請する必要があります。
 - RSA キーペアの生成
 - 証明書トラストポイントの作成
 - CA の認証
- 802.1X では、EAP-TLS を提供するために、デバイス上の ISE などのリモート EAP サーバが必要です。ローカル認証サーバはサポートされていません。
- 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。

- AAA サーバーの到達可能性：スイッチが相互に認証するためです。
- スwitchは相互認証を行うため、両方のスイッチに適切な AAA 設定と AAA 接続が必要です。

802.1X のガイドラインと制約事項

802.1X ポートベースの認証には、次の設定に関する注意事項と制約事項があります。

- (中断あり/中断なしの) インサースビス ソフトウェア アップグレード (ISSU) を使用して Cisco Nexus シリーズ スwitchを Cisco NX-OS リリース 9.2(1) にアップグレードする場合は、まず **no feature dot1x** コマンドを使用して 802.1x を無効にします。機能を有効にするには、**feature dot1x** コマンドを使用してマルチ認証を機能させます。
- Cisco NX-OS リリース 9.2(1) 以降では、802.1X ポートでマルチ認証モードが有効になります。ダイナミック VLAN の割り当ては、最初の認証済みホストに対し行われます。ユーザ クレデンシャルに基づいてその後に許可されたデータ ホストは、正しく認証されたと見なされます。ただし、まだ VLAN が割り当てられていないか、ポートで最初に正しく認証されたホストと一致する VLAN 割り当てがなされていることを条件とします。これにより、ポートで正常に認証されたすべてのホストは、確実に同じ VLAN メンバになります。ダイナミック VLAN 割り当ての柔軟性は、最初に認証されたホストだけに当てはまります。
- Cisco NX-OS リリース 9.2(3) 以降、802.1X ポートベース認証は FEX-ST およびホスト インターフェイス (HIF) ポートでサポートされます。IEEE 802.1X ポートベース認証のサポートは、ストレートおよびデュアルホーム FEX の両方に適用されます。
- Cisco Nexus 9000 シリーズ スwitchは、以下のものについては、802.1X をサポートしていません。
 - トランジット トポロジの設定
 - vPC ポート
 - PVLAN ポート
 - L3 (ルーテッド) ポート
 - ポート セキュリティ
 - CTS および MACsec PSK が有効になっているポート。
 - LACP ポートチャネルを使用した 802.1X。



(注) 802.1X は、スタティック ポートチャネルをサポートします。



(注) vPC ポートおよびサポートされていないすべての機能では、802.1X は無効になります。

- Cisco NX-OS ソフトウェアが 802.1X 認証をサポートするのは、物理ポート上だけです。
- ダイナミック VLAN 割り当ては、Cisco Nexus 9300-FX/EX/FX2 プラットフォーム スイッチでのみサポートされます。
- Cisco NX-OS ソフトウェアは、CTS または MACsec PSK 機能については動作しません。グローバルな「mac-learn disable」と 802.1X 機能は相互に排他的であり、同時に設定することはできません。
- 802.1X は IP ソース ガードおよび uRPF 機能とは相互に排他的であり、同時に設定することはできません。Cisco Nexus シリーズ スイッチを Cisco NX-OS リリース 9.2(3) にアップグレードする場合は、これらの機能のいずれかを無効にする必要があります。
- スイッチのリロード中、802.1X は RADIUS アカウンティングの停止を生じさせません。
- Cisco NX-OS ソフトウェアは、次の 802.1X プロトコル拡張機能をサポートしません。
 - 論理 VLAN 名から ID への 1 対多のマッピング
 - Web 許可
 - ダイナミック ドメイン ブリッジ割り当て
 - IP テレフォニー
 - ゲスト VLAN
- 非アクティブなセッションの再認証を防ぐには、authentication timer inactivity コマンドを使用して、非アクティブタイマーを、authentication timer reauthenticate コマンドで設定された再認証間隔よりも短い間隔に設定します。
- インターフェイスで 802.1X が有効になっている異なる VLAN で、同じ MAC が学習されると、セキュリティ違反が発生します。
- DME 対応プラットフォームで 802.1X を有効にした状態で MAC の学習を無効に設定しても、エラー メッセージは表示されません。
- Cisco Nexus リリース 9.2(1) では、VLAN がインターフェイスで設定されていなくても、タグ付き EAPOL フレームは処理され、クライアントのインターフェイスで認証は成功します。
- 孤立ポートで学習されたセキュア MAC は、vPC ピアで同期されません。
- Cisco NX-OS リリース 9.2(1) 以降、MAC 認証バイパスは Cisco Nexus 9300-FX/FX2 TOR スイッチでサポートされます。

- Cisco NX-OS リリース 9.3(5) 以降、802.1X は Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(2) 以降、802.1X は Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(1)F 以降、802.1X は N9K-C9364D-GX2A および N9K-C9332D-GX2B スイッチでサポートされます。
- Cisco NX-OS リリース 10.3(2)F 以降、MAC 認証バイパスとマルチ認証は、N9K-X9788TC-FX および N9K-X97160YC-EX ラインカードを備えた Cisco Nexus 9508 スイッチでサポートされています。
- N9K-X9788TC-FX および N9K-X97160YC-EX ラインカードを備えた Cisco Nexus C9508 スイッチは、802.1Xを使用した次の機能をサポートしていません。
 - dVLAN
 - DACL
 - FEX-AA
 - VXLAN と mac-move
 - CoA
 - 認証方式として MAB のみがサポートされ、EAP はサポートされません
 - サポートは、単一のアクセス VLAN を持つアクセス ポートに対するものです。
- NX-OS リリース 10.3(3)F 以降、IPv6 アンダーレイは、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2 スイッチ、および X97160YC-EX、9700-FX/GX ラインカードを搭載したCisco Nexus 9500 スイッチにおいて、VXLAN EVPN の 802.1X でサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9336C-FX2、93180YC-FX3、93108TC-FX3P スイッチ、および X9716D-GX ラインカードを搭載した Cisco Nexus 9500 スイッチは、MACSec を必要とするアップリンクポートで（証明書を伝送するために）EAP/EAP-TLS を使用する 802.1X ポートベース認証をサポートします。次の制限があります。
 - EAP-TLS でサポートされる TLS バージョンは 1.2 です。
 - スイッチごとに単一の EAP プロファイルをサポートし、複数のインターフェイスで同じ EAP プロファイルを使用できます。
 - サブリカントの MAC 移動プロファイルはサポートされません。
 - オーセンティケータープロファイルは、L3 ポート、トランクポート、vPC で、MACsec EAP-TLS に対してのみ有効になります。



(注) MAB/EAP クライアントの 802.1X オーセンティケーター機能は、L3 またはトランクおよび vPC ポートではサポートされません。

- EAP-TLS は、MACsec が構成されたインターフェイスの EAP でのみサポートされます。
- EAP-TLS は、マルチホスト モードでのみサポートされます。
- 802.1X MACsec 対応インターフェイスでの DACL/クリティカル AUTH/FEX-AA およびその他の 802.1X 機能はサポートされていません。
- EAP-TLS はリモート認証（ISE/RADIUS : ISE 3.0 以降）でのみサポートされ、ローカル認証ではサポートされません。
- EAP-TLS 構成が正しく機能するには、次の順序に従う必要があります。
 - 最初に **macsec eap policy** コマンドを設定してから、**dot1x supplicant eap profile TLS** コマンドを設定する必要があります。
 - EAP profile コマンドの **no** 形式の場合は、まず **dot1x supplicant eap profile TLS** コマンドを削除してから **macsec eap policy** コマンドを削除する必要があります。
 - **no feature** コマンドについては、DME DB の不整合を回避するために、最初に 802.1X 機能を削除してから MACsec 機能を削除することを推奨します。
- スイッチ全体に構成されている単一の EAP プロファイルは、異なるインターフェイスに適用できます。
- **macsec eap policy** がインターフェイスで構成されている場合、通常の 802.1X 認証者機能またはコマンドはサポートされません。
- ピアツーピア MACsec 対応スイッチには、同じ 802.1X または MACsec 設定が必要です。
- コマンドが異なる場合（一方が **should-secure**、もう一方が **must-secure** など）、動作は未定義になり、回復には **shut/no-shut** のトリガーが必要になります。
- トラストポイントを使用して MACsec セキュアセッションが作成され、EAP プロファイルがインターフェイスに追加されると、次のようになります。
 - トラストポイント構成を削除しても、MACsec セッションは削除されません。
 - 802.1X サプリカントコマンドを削除しても、MACsec セッションは削除されません。
 - MACsec セッションは、MACsec インターフェイス固有のコマンドを削除した場合にのみ削除されます。
- MACsec PKI は、中間スイッチまたはホップのないスイッチでサポートされるので、直接接続する必要があります。
- MACsec PKI（802.1X EAP-TLS）モードは、EoR ステートフル スイッチ オーバー（SSO）をサポートしていません。
- EAP-TLS は、次のインターフェイス タイプでのみサポートされます。

- L2/L3 ポート、ポートチャネルメンバーポート、トランクポート、およびブレイクアウトポート
- サポートされていないインターフェイスタイプ：コマンドレベルの制限はありません。
- サポートされる MACsec セッションの数は、物理インターフェイスの規模によって異なります。
- Cisco NX-OS リリース 10.4(3)F 以降、EAP-TLS は Cisco Nexus スイッチで Transport Layer Security バージョン 1.3 および 1.2 をサポートします。



(注) RADIUS サーバーが TLS v1.3 に対応していない場合は、サポートされる最小バージョンである TLS v1.2 が使用されます。

音声 VLAN に関連した 802.1X のガイドラインと制限事項

- Cisco NX-OS リリース 10.5(2)F 以降において、802.1X 音声 VLAN 機能は、次の Cisco Nexus スイッチでサポートされます。
 - N9K-C9348GC-FXP
 - N9K-C93108TC-FX3P
 - N9K-C9348GC-FX3
 - N9K-C9348GC-FX3PH
- 音声 VLAN 構成では、L2 スイッチポートモードアクセスのみがサポートされます。
- 1 つの音声 VLAN と 1 つのデータ VLAN のみがサポートされます。
- ダイナミックアクセス制御リスト (DACL) およびダイナミック VLAN (DVLAN) は、マルチドメイン認証 (MDA) ポートではサポートされません。
- 次のコマンドは、802.1X で構成されたポートの音声 VLAN 構成ではサポートされません。
 - **switchport voice vlan untagged**
 - **switchport voice vlan dot1p**

これらの構成が 802.1X ポートに存在する場合、電話機機能は許可されません。したがって、マルチドメインポートには特定の音声 VLAN ID を構成する必要があります。

- アクセス VLAN と音声 VLAN の両方に同じ値を設定することはサポートされません。同じ値で構成していた場合は、値を変更し、ポートをフラップしてください。

802.1X 向け事前ユーザ DACL サポートのガイドラインと制約事項

- 次のスイッチ プラットフォームは、この機能をサポートしています。
 - Cisco Nexus 9300-FX プラットフォーム スイッチ
 - Cisco Nexus 9300-FX2 プラットフォーム スイッチ
- ユーザー単位の DACL は、IPv4 TCP、UDP、および ICMP ACL ルールをサポートしますが、IPv6 ACL ルールはサポートしません。
- ユーザー単位の DACL は、4 KB 未満の単一の RADIUS 応答に制限され、サポートされる ACE の最大数は 32 です。
- この機能は、スイッチポートの標準 ACL をサポートしていません。
- ポートごとに 1 つの DACL のみがサポートされます。スイッチ全体でサポートされる DACL の最大数は、そのスイッチのポート数と同じです。
- DACL とダイナミック VLAN は、同じポートで同時にサポートされません。
- ISE からの DACL コンテンツの動的な変更はサポートされていません。これを実現するには、**clear dot1x interface** コマンドを使用して以前に適用した DACL をポートからクリアし、ISE からの新しい DACL を適用します。これにより、このポート上のすべてのクライアントで一時的なトラフィックの中断が発生します。
- AA FEX モードの Cisco Nexus 9000 シリーズ スイッチは、ユーザー単位の DACL をサポートしていません。
- ユーザー単位の DACL は、MAB およびマルチ認証ホスト モードのみをサポートします。
- 他のすべての Nexus 9000 802.1x 機能と同様に、ユーザごとの DACL は物理ポート、つまり通常の L2 アクセス ポートでのみサポートされ、トランク、vPC、ポートチャネルとそのメンバー、およびサブインターフェイスではサポートされません。
- スイッチに適用される他のすべての Nexus 9000 ACL と同様に、ユーザごとの DACL の最大制限は 4000 ASCII 文字です。
- ユーザーごとの DACL 機能の MAC 移動プロファイルはサポートされていません。
- Cisco NX-OS リリース 10.2(1) 以降、この機能は Cisco Nexus 9300-FX/FX2/ TOR スイッチでサポートされます。
- Cisco NX-OS リリース 10.5(2)F 以降、DACL 機能は Cisco Nexus 9300-FX3、GX、GX2、H2R、H1 シリーズ スイッチでサポートされています。

クリティカル認証のガイドラインと制限事項

- クリティカル認証は、基本的な MAB クライアントのみをサポートし、FEX-AA や VxLAN などのトポロジではサポートされません。
- 不正なクライアント トラフィックはすべて許可されるため、**authentication event server dead action authorize** コマンドを常に有効にすると、セキュリティ上のリスクが生じます。
- Cisco NX-OS リリース 10.1(2) 以降、クリティカル認証機能は Cisco Nexus 9300-FX/FX2/FX3/GX TOR スイッチでサポートされています。
- Cisco NX-OS リリース 10.2(1)F 以降、クリティカル認証機能は N9K-C9364D-GX2A および N9K-C9332D-GX2B スイッチでサポートされます。
- Cisco NX-OS リリース 10.3(2)F 以降、重要な認証機能は、N9K-X9788TC-FX および N9K-X97160YC-EX ラインカードを備えた Cisco Nexus 9508 スイッチでサポートされています。

802.1X のデフォルト設定

次の表に、802.1X パラメータのデフォルト設定を示します。

Table 14: 802.1X のデフォルトパラメータ

パラメータ	デフォルト
802.1X 機能	ディセーブル
AAA 802.1X 認証方式	設定なし
インターフェイス単位の 802.1x プロトコル イネーブル ステート	ディセーブル (force-authorized) Note ポートはサブリカントとの 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。
定期的な再認証	ディセーブル
再認証の間隔 (秒)	3600 秒
待機タイムアウト時間	60 秒 (Cisco NX-OS デバイスがサブリカ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)
再送信タイムアウト時間	30 秒 (Cisco NX-OS デバイスが EAP-Request/Identity フレームに対するサブリカントからの応答を待ち、要求を再送信するまでの秒数)

パラメータ	デフォルト
最大再送信回数	2 回（Cisco NX-OS デバイスが認証プロセスを再開するまでに、EAP-Request/Identity フレームを送信する回数）
ホスト モード	シングル ホスト
サブリカント タイムアウト時間	30 秒（認証サーバからの要求をサブリカントにリレーするとき、Cisco NX-OS デバイスがサブリカントに要求を再送信するまでに、サブリカントの応答を待つ時間）
認証サーバ タイムアウト時間	30 秒（サブリカントからの応答を認証サーバにリレーするとき、Cisco NX-OS デバイスがサーバに応答を再送信するまでに、サーバからの応答を待つ時間）

802.1X の設定

ここでは、802.1X 機能の設定方法について説明します。

802.1X の設定プロセス

ここでは、802.1X を設定するプロセスについて説明します。

Procedure

-
- ステップ 1** 802.1X 機能をイネーブルにします。
- ステップ 2** リモート RADIUS サーバへの接続を設定します。
- ステップ 3** イーサネット インターフェイスで 802.1X 機能をイネーブルにします。
-

802.1X 機能のイネーブル化

サブリカント デバイスを認証する前に、Cisco NX-OS デバイス上で 802.1X 機能をイネーブルにする必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example:	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

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	feature dot1x Example: switch(config)# feature dot1x	802.1X 機能をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	exit Example: switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show dot1x Example: switch# show dot1x	802.1X 機能のステータスを表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X の AAA 認証方式の設定

802.1X 認証にリモート RADIUS サーバを使用できます。RADIUS サーバおよび RADIUS サーバグループを設定し、デフォルト AAA 認証方式を指定したあとに、Cisco NX-OS デバイスは 802.1X 認証を実行します。

Before you begin

リモート RADIUS サーバグループの名前またはアドレスを取得します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 authentication dot1x default group group-list Example:	802.1X 認証に使用する RADIUS サーバグループを指定します。

	Command or Action	Purpose
	<pre>switch(config)# aaa authentication dot1x default group rad2</pre>	Group-list 引数は、スペースで区切られたグループ名のリストで構成されます。グループ名は、次のように指定します。 • radiusRADIUS サーバのグローバルプールを使用して認証を行います。 • named-group : 認証に RADIUS サーバのグローバルプールを使用します。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。
ステップ 5	(Optional) show radius-server group [group-name] Example: <pre>switch# show radius-server group rad2</pre>	RADIUS サーバ グループの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでの 802.1X 認証の制御

インターフェイス上で実行される 802.1X 認証を制御できます。インターフェイスの 802.1X 認証ステートは、次のとおりです。

自動 (Auto)

インターフェイス上で、802.1X 認証を有効にします。

強制認証

インターフェイス上の 802.1X 認証を無効にし、認証を行わずにインターフェイス上のすべてのトラフィックを許可します。このステートがデフォルトです。

Force-unauthorized

インターフェイス上のすべてのトラフィックを禁止します。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 ethernet slot / port Example: switch(config)# interface ethernet 2/1 switch(config-if)#	設定するインターフェイスを選択し、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 port-control {auto force-authorized forced-unauthorized} Example: switch(config-if)# dot1x port-control auto	インターフェイスの 802.1X 認証ステータスを変更します。デフォルトの設定は force-authorized です。
ステップ 4	exit Example: switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show dot1x all Example: switch# show dot1x all	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	(Optional) show dot1x interface ethernet slot / port Example: switch# show dot1x interface ethernet 2/1	インターフェイスの 802.1X 機能のステータスおよび設定情報を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

音声 VLAN 向け 802.1X の構成

Cisco NX-OS リリース 10.5(2)F 以降では、単一ポートでマルチドメイン 802.1X 認証を有効にできます。

始める前に

Cisco NX-OS デバイスで 802.1X 機能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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 ethernet slot / port 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	設定するインターフェイスを選択し、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 host-mode multi-domain 例 : <pre>switch(config-if)# dot1x host-mode multi-domain</pre>	インターフェイスレベルでマルチドメイン ホストモードを有効化または無効化します。 インターフェイスレベルでマルチドメイン ホストモードを無効化するには、このコマンドの no 形式を使用します。 (注) 音声クライアントは、ホストモード マルチドメインのポートでのみ正常に認証されます。ホストモードがそれ以外の場合、音声クライアントは認証に失敗し、無効になります。
ステップ 4	exit 例 : <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。

EAP-TLS の設定

Cisco NX-OS リリース 10.4(1)F 以降では、802.1X 認証に EAP-TLS プロファイルを使用できます。

始める前に

- Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。
- インターフェイスで、MACsec EAP ポリシーを構成し、**dot1x supplicant eap profile** にアタッチします。MACsec EAP ポリシーの構成については、「[MACsec EAP の構成 \(744 ページ\)](#)」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 例 : <pre>switch# configure terminal switch(config)#</pre>	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] eap profile TLS 例 : <pre>switch(config)# eap profile TLS switch(config-eap-profile)#</pre>	802.1X EAP プロファイル モードを構成します。 コマンドの no フォームは、eap プロファイルを無効にするために使用されます。
ステップ 3	pki-trustpoint trustpoint name 例 : <pre>switch(config-eap-profile)# pki-trustpoint tpl switch(config-eap-profile)#</pre>	使用するトラストポイントを指定します。
ステップ 4	method type 例 : <pre>switch(config-eap-profile)# method TLS switch(config-eap-profile)#</pre>	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。 使用する EAP 方式を指定します。
ステップ 5	interface ethernet slot/port 例 : <pre>switch(config-eap-profile)# interface ethernet 1/30 switch(config-if)#</pre>	設定するインターフェイスを選択し、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	[no] dot1x supplicant eap profile eap profile name 例 : <pre>switch(config-if)# dot1x supplicant eap profile</pre>	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。 802.1X サプリカントを EAP プロファイルに構成します。

インターフェイスでのオーセンティケータ PAE の作成または削除

インターフェイスで 802.1X オーセンティケータ Port Access Entity (PAE) インスタンスを作成または削除できます。



(注) デフォルトでは、インターフェイスで 802.1X をイネーブルにしたときに、Cisco NX-OS ソフトウェアによってインターフェイスでオーセンティケータ PAE インスタンスが作成されます。

始める前に

802.1X 機能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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	(任意) show dot1x interface ethernet slot/port 例 : <pre>switch# show dot1x interface ethernet 2/1</pre>	インターフェイス上の 802.1X の設定を表示します。
ステップ 3	interface ethernet slot/port 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	設定するインターフェイスを選択し、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	[no] dot1x pae authenticator 例 : <pre>switch(config-if)# dot1x pae authenticator</pre>	インターフェイスでオーセンティケータ PAE インスタンスを作成します。インターフェイスから PAE インスタンスを削除するには、 no 形式を使用します。 (注) オーセンティケータ PAE がインターフェイスにすでに存在している場合は、 dot1x pae authentication コマンドを実行してもインターフェイス上の設定は変更されません。

	コマンドまたはアクション	目的
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

クリティカル認証を有効にする

始める前に

- RADIUS のモニタリングを有効にします。
- グループ内のすべてのサーバが RADIUS サーバであ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 例 : <pre>switch# configure terminal switch(config)#</pre>	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 test idle-time minutes 例 : <pre>switch(config)# radius-server test idle-time 1</pre>	グローバルなサーバモニタリング用のパラメータを指定します。デフォルトのユーザ名は test 、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 (注) RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。グループに複数のサーバがある場合は、各サーバのアイドルタイマーを 1 に設定します。
ステップ 3	radius-server deadtime 分 例 : <pre>switch(config)# radius-server deadtime 1</pre>	以前に応答の遅かった RADIUS サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 (注)

	コマンドまたはアクション	目的
		デッドタイムを0より大きい値に設定して、モニタリングを有効にします。
ステップ 4	radius-server host ipv4-address key[0 6 7] key-value 例 : <pre>switch(config)# radius-server host 10.105.222.183 key 7 "fewhg" authentication accounting</pre>	すべての RADIUS サーバ用の RADIUS キーを指定します。key-value がクリアテキスト (0) の形式か、タイプ 6 暗号化 (6) 形式か、タイプ 7 暗号化 (7) 形式かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存する前にクリアテキストのキーを暗号化します。デフォルトの形式はクリアテキストです。最大で 63 文字です。デフォルトでは、RADIUS キーは設定されません。 (注) generate type7_encrypted_secret コマンドを使用して共有秘密をすでに設定している場合、2 番目の例のように引用符で囲んで入力してください。詳細については、RADIUS または TACACS+ の共有秘密の設定 (54 ページ) を参照してください。
ステップ 5	radius-server host ipv4-address test idle-time minutes 例 : <pre>switch(config)# radius-server host 10.105.222.183 test idle-time 1</pre>	サーバモニタリング用のパラメータを個別に指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドルタイマーのデフォルト値は 0 分です。有効な範囲は 0 ~ 1440 分です。 (注) RADIUS サーバの定期的なモニタリングを行うには、アイドルタイマーに 0 より大きな値を設定する必要があります。
ステップ 6	aaa group server radius group-name 例 : <pre>switch(config)# aaa group server radius ISE_2.4 switch(config-radius)#</pre>	RADIUS サーバグループを作成し、そのグループの RADIUS サーバグループコンフィギュレーションサブモードを開始します。group-name 引数は、最大 127 文字の長さの英数字のストリングで、大文字小文字が区別されます。

	コマンドまたはアクション	目的
		RADIUS サーバグループを削除するには、このコマンドの no 形式を使用します。 (注) デフォルトのシステム生成デフォルトグループ (RADIUS) は削除できません。
ステップ 7	server { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } 例 : <pre>switch(config-radius)# server 10.105.222.183</pre>	RADIUS サーバを、RADIUS サーバグループのメンバーとして設定します。指定した RADIUS サーバが見つからなかった場合は、 radius-server host コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 8	use-vrf <i>vrf-name</i> 例 : <pre>switch(config-radius)# use-vrf management</pre>	サーバグループ内のサーバとの接続に使用する VRF を指定します。
ステップ 9	source-interface <i>interface</i> 例 : <pre>switch(config-radius)# source-interface mgmt 0</pre>	このデバイスで設定されているすべての RADIUS サーバグループ用のグローバル発信元インターフェイスを設定します。
ステップ 10	exit 例 : <pre>switch(config-radius)# exit switch(config)#</pre>	RADIUS サーバグループコンフィギュレーションサブモードを終了します。
ステップ 11	authentication event server dead action authorize 例 : <pre>switch(config)# authentication event server dead action authorize</pre>	RADIUS サーバに到達できない場合に、すべてのクライアントを認可します。

インターフェイスの定期再認証のイネーブル化

インターフェイスの 802.1X 定期再認証をイネーブルにし、再認証を実行する頻度を指定します。期間を指定しないで再認証をイネーブルにした場合、再認証を行う間隔はグローバル値にデフォルト設定されます。



Note 再認証プロセス中、すでに認証されているサブリカントのステータスは影響を受けません。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 ethernet slot/port Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	設定するインターフェイスを選択し、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 re-authentication Example: <pre>switch(config-if)# dot1x re-authentication</pre>	インターフェイスに接続されているサブリカントの定期再認証をイネーブルにします。デフォルトでは、定期再認証はディセーブルです。
ステップ 4	(Optional) dot1x timeout re-authperiod seconds Example: <pre>switch(config-if)# dot1x timeout re-authperiod 3300</pre>	再認証の間隔（秒）を設定します。デフォルトは 3600 秒です。値の範囲は 1 ～ 65535 です。 Note インターフェイス上の定期再認証をイネーブルにする場合だけ、このコマンドは Cisco NX-OS デバイスの動作に影響します。
ステップ 5	exit Example: <pre>switch(config-if)# exit switch(config)#</pre>	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	(Optional) show dot1x all Example: <pre>switch(config)# show dot1x all</pre>	802.1X 機能のすべてのステータスおよび設定情報を表示します。

	Command or Action	Purpose
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

手動によるサブリカントの再認証

Cisco NX-OS デバイス全体のサブリカントまたはインターフェイスのサブリカントを手動で再認証できます。



Note 再認証プロセス中、すでに認証されているサブリカントのステータスは影響を受けません。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	dot1x re-authenticate [interface slot/port] Example: <pre>switch# dot1x re-authenticate interface 2/1</pre>	Cisco NX-OS デバイスまたはインターフェイス上のサブリカントを再認証します。

インターフェイスの 802.1X 認証タイマーの変更

Cisco NX-OS デバイスのインターフェイス上で変更できる 802.1X 認証タイマーは、次のとおりです。

待機時間タイマー

Cisco NX-OS デバイスがサブリカントを認証できない場合、スイッチは所定の時間アイドル状態になり、その後再試行します。待機時間タイマーの値でアイドルの時間が決まります。認証が失敗する原因には、サブリカントが無効なパスワードを提供した場合があります。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。デフォルトは、グローバル待機時間タイマーの値です。範囲は 1 ～ 65535 秒です。

レート制限タイマー

レート制限時間中、サブリカントから過剰に送信されている EAPOL-Start パケットを抑制します。オーセンティケータはレート制限時間中、認証に成功したサブリカントからの EAPOL-Start パケットを無視します。デフォルト値は 0 秒で、オーセンティケータはすべての EAPOL-Start パケットを処理します。範囲は 1 ～ 65535 秒です。

レイヤ 4 パケットに対するスイッチと認証サーバ間の再送信タイマー

認証サーバは、レイヤ 4 パケットを受信するたびにスイッチに通知します。スイッチがパケット送信後に通知を受信できない場合、Cisco NX-OS デバイスは所定の時間だけ待機した後、パケットを再送信します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

EAP 応答フレームに対するスイッチとサブリカント間の再送信タイマー

サブリカントは、Cisco NX-OS デバイスの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。Cisco NX-OS デバイス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）だけ待機した後、フレームを再送信します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

EAP 要求フレームに対するスイッチとサブリカント間の再送信タイマー

サブリカントは、EAP 要求フレームを受信したことを Cisco NX-OS デバイスに通知します。オーセンティケータがこの通知を受信できなかった場合、オーセンティケータは所定の時間だけ待機した後、フレームを再送信します。デフォルトは、グローバル再送信時間タイマーの値です。範囲は 1 ～ 65535 秒です。

Inactive period timeout

Cisco NX-OS デバイスが設定された期間にわたって非アクティブのままである場合、timeout inactivity-period 値は、非アクティブ期間を決定します。最小推奨値は 1800 秒です。値が再認証時間の値よりも小さいことを確認する必要があります。



Note このデフォルト値は、リンクの信頼性が低下した場合や、特定のサブリカ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場合にだけ変更してください。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 ethernet slot/port Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)</pre>	設定するインターフェイスを選択し、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	(Optional) dot1x timeout quiet-period seconds Example:	オーセンティケータが EAP-Request/Identity フレームに対するサブリカントからの応答を待ち、要求

	Command or Action	Purpose
	<code>switch(config-if)# dot1x timeout quiet-period 25</code>	を再送信するまでの時間を秒数で設定します。デフォルトはすべてのインターフェイスに設定されるグローバル秒数です。範囲は 1 ～ 65535 秒です。
ステップ 4	(Optional) dot1x timeout ratelimit-period seconds Example: <code>switch(config-if)# dot1x timeout ratelimit-period 10</code>	認証に成功したサブリカントからの EAPOL-Start パケットを無視する時間を秒数で設定します。デフォルト値は 0 秒です。範囲は 1 ～ 65535 秒です。
ステップ 5	(Optional) dot1x timeout server-timeout seconds Example: <code>switch(config-if)# dot1x timeout server-timeout 60</code>	Cisco NX-OS デバイスが認証サーバにパケットを送信する前に待機する時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。
ステップ 6	(Optional) dot1x timeout supp-timeout seconds Example: <code>switch(config-if)# dot1x timeout supp-timeout 20</code>	Cisco NX-OS デバイスが EAP 要求フレームを再送信する前に、サブリカントが EAP 要求フレームに応答してくるのを待機する時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。
ステップ 7	(Optional) dot1x timeout tx-period seconds Example: <code>switch(config-if)# dot1x timeout tx-period 40</code>	サブリカントから EAP 要求フレームを受信した通知が送信されない場合に、EAP 要求フレームを再送信する間隔を秒数で設定します。デフォルトはすべてのインターフェイスに設定されるグローバル秒数です。範囲は 1 ～ 65535 秒です。
ステップ 8	(Optional) dot1x timeout inactivity-period seconds Example: <code>switch(config-if)# dot1x timeout inactivity-period 1800</code>	スイッチが非アクティブ状態を維持できる秒数を設定します。最小推奨値は 1800 秒です。
ステップ 9	exit Example: <code>switch(config)# exit</code> <code>switch#</code>	コンフィギュレーションモードを終了します。
ステップ 10	(Optional) show dot1x all Example: <code>switch# show dot1x all</code>	802.1X の設定を表示します。

	Command or Action	Purpose
ステップ 11	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

MAC 認証バイパスのイネーブル化

サブリカントの接続されていないインターフェイス上で、MAC 認証バイパスをイネーブルにすることができます。

始める前に

Cisco NX-OS デバイスで 802.1X 機能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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 ethernet slot/port 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)</pre>	設定するインターフェイスを選択し、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 mac-auth-bypass [eap] 例 : <pre>switch(config-if)# dot1x mac-auth-bypass</pre>	MAC 認証バイパスをイネーブルにします。デフォルトはバイパスのディセーブルです。 eap キーワードを使用して、許可に EAP を使用するように Cisco NX-OS デバイスを設定します。
ステップ 4	exit 例 : <pre>switch(config-if)# exit switch(config)#</pre>	コンフィギュレーション モードを終了します。
ステップ 5	(任意) show dot1x all 例 : <pre>switch# show dot1x all</pre>	802.1X 機能のすべてのステータスおよび設定情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの 802.1X 認証方法の構成 - MAB

Cisco NX-OS リリース 9.3(5) 以降では、802.1X 対応ポートで受信されるすべてのトラフィックは、MAC 認証バイパス (MAB) によってのみ認証できます。Cisco NX-OS リリース 9.3(5) よりも前では、すべてのトラフィックは最初に EAPOL によって認証され、MAB による認証は EAPOL 認証セッションがタイムアウトした後にのみ行われました。

始める前に

Cisco NX-OS デバイスで MAB 機能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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 ethernet slot/port 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)</pre>	インターフェイスを選択し、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 mac-auth-bypass 例 : <pre>switch(config-if)# dot1x mac-auth-bypass</pre>	MAC 認証バイパスをイネーブルにします。デフォルトはバイパスのディセーブルです。
ステップ 4	[no] dot1x authentication order mab 例 : <pre>switch(config-if)# dot1x authentication order mab</pre>	RADIUS サーバでデータ トラフィックの認証に対して MAB をイネーブルにします。このコマンドの no 形式を使用すると、デフォルトの認証方式を EAPOL に変更します。
ステップ 5	exit 例 :	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
	switch(config-if)# exit switch(config)#	
ステップ 6	(任意) show dot1x all 例 : switch# show dot1x all	802.1X 機能のすべてのステータスおよびコンフィギュレーション情報を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ダイナミック アクセス リストの作成

始める前に

次の状態を確認してください。

- 802.1X MAB クライアントの特定のトラフィック クラスを許可またはブロックするように、すべての ACE で ACL 名 (acl-name) を事前にプログラムします。デバイスに設定されている ACL 名 (acl-name) は、ISE サーバから受信する acl-name と一致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 例 : switch# configure terminal switch(config)#	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	hardware access-list tcam region ing-dacl tcam size 例 : switch(config)# hardware access-list tcam region ing-dacl 256 switch(config)#	TCAM サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。
ステップ 3	ip access-list blacklist 例 : switch(config)# ip access-list creative_blacklist	定義済みのブラックリストを設定し、設定された TCAM サイズに基づいて適用します。

	コマンドまたはアクション	目的
ステップ 4	(任意) show ip access-list 例 : <pre>switch(config)# ip access-list creative_blacklist1</pre>	設定済みの IP アクセス リストを表示します。
ステップ 5	(任意) show ip access-list dynamic 例 : <pre>switch(config)# ip access-list creative_blacklist1_new_Ethernet1/1 statistics per-entry 10 permit udp 0000.1b40.ff13 0000.0000.0000 any range bootps bootpc vlan 100 [match=123] 20 permit udp 0000.1b40.ff13 0000.0000.0000 any eq domain vlan 100 [match=456] 30 deny 0000.1b40.ff13 0000.0000.0000 any [match=789]</pre>	設定済みの IP アクセス リストを表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ単位の DACL 設定

Cisco ISE サーバでユーザごとの DACL を設定できます。その後、さまざまなユーザおよびユーザグループがネットワークにアクセスする方法を制御するために、これを許可ポリシーに実装できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	hardware access-list tcam region ing-dacl 例 : <pre>switch(config)# hardware access-list tcam region ing-dacl</pre>	新しい DACL-TCAM リージョンを作成するようにスイッチで TCAM を設定します。

	コマンドまたはアクション	目的
ステップ 3	exit 例 : <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 4	reload 例 : <pre>switch# reload</pre>	Cisco NX-OS デバイスをリロードします。

次のタスク

ISE のブロックリストされたクライアントの DACL を設定します。



(注) ISE の ACE には、すべての DACL クライアントに対して暗黙的な拒否が内部的に追加されるため、IP の拒否ルールを設定しないでください。

ブロックリストクライアントは 802.1X ポートに接続し、radius access-accept メッセージの一部として ACL AV-Pair をダウンロードします。受信した ACL は、特定のクライアントのポートに適用されます。

DACL の設定方法の詳細については、『Cisco ID サービス エンジン管理者ガイド、リリース 3.0』の「セグメント」の章にある「ダウンロード可能な ACL の権限を設定する」の項を参照してください。

シングル ホスト モードまたはマルチ ホスト モードのイネーブル化

インターフェイス上でシングル ホスト モードまたはマルチ ホスト モードをイネーブルにすることができます。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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。

	Command or Action	Purpose
ステップ 2	interface ethernet slot/port Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)</pre>	設定するインターフェイスを選択し、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 host-mode {multi-host single-host} Example: <pre>switch(config-if)# dot1x host-mode multi-host</pre>	ホスト モードを設定します。デフォルトは、single-host です。 Note 指定したインターフェイスで dot1x port-control インターフェイス設定コマンドが 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	dot1x host-mode multi-auth Example: <pre>switch(config-if)# dot1x host-mode multi-auth</pre>	複数認証モードを設定します。ポートは、EAP または MAB のいずれか、または両方の組み合わせが正常に認証された場合にのみ許可されます。認証に失敗すると、ネットワーク アクセスが制限されます。 EAP または MAB の認証
ステップ 5	exit Example: <pre>switch(config-if)# exit switch(config)#</pre>	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	(Optional) show dot1x all Example: <pre>switch# show dot1x all</pre>	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco NX-OS デバイスでの 802.1X 認証の無効化

Cisco NX-OS デバイス上の 802.1X 認証を無効にできます。デフォルトでは、802.1X 機能を有効にすると、Cisco NX-OS ソフトウェアが 802.1X 認証を有効にします。ただし、802.1X 機能を無効にした場合、設定は Cisco NX-OS デバイスから削除されます。Cisco NX-OS ソフトウェアでは、802.1X の設定を失わずに 802.1X 認証を無効にできます。



Note 802.1X 認証を無効にすると、設定されているポートモードに関係なく、すべてのインターフェイスのポートモードがデフォルトの **force-authorized** になります。802.1X 認証を再び有効にすると、Cisco NX-OS ソフトウェアはインターフェイス上に設定したポートモードを復元します。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 dot1x system-auth-control Example: <pre>switch(config)# no dot1x system-auth-control</pre>	Cisco NX-OS デバイス上の 802.1X 認証を無効にします。デフォルトでは有効になっています。 Note Cisco NX-OS デバイス上の 802.1X 認証を有効にするには、 dot1x system-auth-control コマンドを使用します。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show dot1x Example: <pre>switch# show dot1x</pre>	802.1X 機能のステータスを表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 機能のディセーブル化

Cisco NX-OS デバイス上の 802.1X 機能をディセーブルにできます。

802.1X をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。Cisco NX-OS ソフトウェアは、802.1X を再度イネーブルにして設定を回復する場合に使用できる自動チェックポイントを作成します。詳細については、ご使用のプラットフォームの『Cisco NX-OS システム管理設定ガイド』を参照してください。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 feature dot1x Example: switch(config)# no feature dot1x	802.1X 機能をディセーブルにします。 Caution 802.1X 機能をディセーブルにすると、802.1X のすべての設定が削除されます。
ステップ 3	exit Example: switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X インターフェイス設定のデフォルト値へのリセット

インターフェイスの 802.1X 設定をデフォルト値にリセットすることができます。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 ethernet slot/port Example: switch(config)# interface ethernet 2/1 switch(config-if)	設定するインターフェイスを選択し、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 default Example: switch(config-if)# dot1x default	インターフェイスの 802.1X 設定をデフォルト値に戻します。
ステップ 4	exit Example: switch(config-if)# exit switch(config)#	コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show dot1x all Example: switch(config)# show dot1x all	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでのオーセンティケータとサブリカント間のフレームの最大数の設定

セッションがタイムアウトするまでに、Cisco NX-OS デバイスがインターフェイス上でサブリカントに認証要求を再送信する最大回数を設定できます。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 ethernet slot/port Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	設定するインターフェイスを選択し、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-req count Example: <pre>switch(config-if)# dot1x max-req 3</pre>	最大認証要求リトライ回数を変更します。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。 Note 指定したインターフェイスで dot1x port-control インターフェイス設定コマンドが 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	exit Example: <pre>switch(config)# exit switch#</pre>	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 5	(Optional) show dot1x all Example: <pre>switch# show dot1x all</pre>	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 認証の RADIUS アカウンティングのイネーブル化

802.1X 認証のアクティビティに対する RADIUS アカウンティングをイネーブルにできます。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	dot1x radius-accounting Example: switch(config)# dot1x radius-accounting	802.1X に対する RADIUS アカウンティングをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	exit Example: switch(config)# exit switch#	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show dot1x Example: switch# show dot1x	802.1X の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X の AAA アカウンティング方式の設定

802.1X 機能に対する AAA アカウンティング方式をイネーブルにできます。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
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	aaa accounting dot1x default group group-list	802.1X に対する AAA アカウンティングをイネーブルにします。デフォルトではディセーブルになっています。

	Command or Action	Purpose
		<i>group-list</i> 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • radius : 設定済みのすべての RADIUS サーバ • named-group : 設定済みの任意の RADIUS サーバグループ名
ステップ 3	exit	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) show aaa accounting	AAA アカウンティングの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、802.1X 機能を有効にする例を示します。

```
switch# configure terminal
switch(config)# aaa accounting dot1x default group radius
switch(config)# exit
switch# show aaa accounting
switch# copy running-config startup-config
```

インターフェイスでの再認証最大リトライ回数の設定

セッションがタイムアウトするまでに、Cisco NX-OS デバイスがインターフェイス上でサブリカントに再認証要求を再送信する最大回数を設定できます。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example:	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。

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	interface ethernet slot/port Example: switch(config)# interface ethernet 2/1 switch(config-if)#	設定するインターフェイスを選択し、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 retry-count Example: switch(config-if)# dot1x max-reauth-req 3	最大再認証要求リトライ回数を変更します。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。
ステップ 4	exit Example: switch(config)# exit switch#	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 5	(Optional) show dot1x all Example: switch# show dot1x all	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 設定の確認

802.1X 情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show dot1x	802.1X 機能のステータスを表示します。
show dot1x all [details statistics summary]	802.1X 機能のすべてのステータスおよび設定情報を表示します。
show dot1x interface ethernet slot/port [details statistics summary]	イーサネットインターフェイスの 802.1X 機能のステータスおよび設定情報を表示します。
show running-config dot1x [all]	実行コンフィギュレーション内の 802.1X 機能の設定を表示します。

コマンド	目的
show startup-config dot1x	スタートアップ コンフィギュレーション内の 802.1X 機能の設定を表示します。

これらのコマンドの出力フィールドの詳細については、ご使用のプラットフォームの『Cisco NX-OS セキュリティ コマンド リファレンス』を参照してください。

次に、認証された状態のオーセンティケータとサブリカントの両方としてのポートの EAP-TLS 設定に関する情報を表示する例を示します。

```
switch(config)# show dot1x int eth 5/6 details

Dot1x Info for Ethernet5/6
-----
                PAE = AUTHENTICATOR
                PortControl = AUTO
                HostMode = MULTI HOST
                ReAuthentication = Disabled
                QuietPeriod = 60
                ServerTimeout = 30
                SuppTimeout = 30
                ReAuthPeriod = 3600 (Locally configured)
                ReAuthMax = 2
                MaxReq = 2
                TxPeriod = 30
                RateLimitPeriod = 0
                InactivityPeriod = 0
                Mac-Auth-Bypass = Disabled

Dot1x Info for Ethernet5/6
-----
                PAE = SUPPLICANT
                StartPeriod = 30
                AuthPeriod = 30
                HeldPeriod = 60
                MaxStart = 3

Dot1x Authenticator Client List
-----
                Supplicant = C4:B2:39:2C:EE:50
                Domain = DATA
                Auth SM State = AUTHENTICATED
                Auth BEND SM State = IDLE
                Port Status = AUTHORIZED
                Authentication Method = EAP
                Authenticated By = Remote Server
                Auth-Vlan = 0
                DACL-Applied = False

Dot1x Supplicant Client List
-----
                Authenticator = C4:B2:39:2C:EE:50
                Supp SM State = AUTHENTICATED
                Supp Bend SM State = IDLE
                Port Status = AUTHORIZED
```

VXLAN EVPN の 802.1X サポート

このセクションでは、VXLAN EVPN の 802.1X 機能の構成方法について説明します。

VXLAN EVPN の 802.1X サポートに関する注意事項と制約事項

VXLAN EVPN の 802.1X サポートに関する注意事項と制約事項を次に示します。

- Cisco NX-OS リリース 9.3(7) 以降では、VXLAN EVPN 機能の 802.1X サポートが Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
- ポート チャネル インターフェイス または ポート チャネル のメンバー ポート はサポートされません。
- vPC ポート はサポートされません。
- この機能の現在のサポートでは、802.1X セキュア MAC 更新のために BGP-EVPN コントロール プレーン で定期的および動的な EVPN 更新を使用します。そのため、グローバル ポリシーが「dot1x mac-move deny」であっても、EVPN をまたいで移動することはできません。
- 「dot1x mac-move」ポリシーがファブリック全体で同じに設定されていることを確認します。ノード間で設定の検証は行われないため、設定ポリシーが同期していない場合は予期しない動作が発生する可能性があります。
- 拒否モードと許可モードのローカルからリモートへの MAC 移動動作は許可されます。したがって、拒否モードが有効になっていても、MAC 移動は許可されます。
- 802.1X とポート セキュリティ ポートが異なる VLAN を使用していることを確認します。同じ VLAN を両方のポートに割り当てることはできません。
- 802.1X は VLAN を認識しないため、2 つの異なる VLAN で同じ MAC を使用することはできません。選択された MAC 移動モードに応じて、MAC は新しい VLAN に移動されるか、拒否されます。
- スタティック MAC とセキュア MAC を同時に設定することはできません。
- -R ライン カードを搭載した Cisco Nexus 9504 および Cisco Nexus 9508 プラットフォーム スイッチは、VXLAN でのマルチ認証およびマルチ認証をサポートしていません。
- RADIUS の認可変更は VXLAN EVPN によりサポートされています。
- スケール設定の推奨再認証時間間隔はデフォルト値で、3600 秒です。
- 802.1X はファブリック ピアリングではサポートされていません。

VXLAN EVPN の 802.1X サポートの設定

この手順では、VXLAN EVPN の 802.1X を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal</pre>	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	feature dot1x 例 : <pre>switch(config)# feature dot1x</pre>	802.1X 機能をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	dot1x mac-move {permit deny} 例 : <pre>switch(config)# dot1x mac-move permit</pre>	deny パラメータは MAC 移動を拒否します。 permit パラメータは MAC 移動を許可します。
ステップ 4	(任意) show running-config dot1x all 例 : <pre>switch(config)# show running-config dot1x all</pre> <pre>!Command: show running-config dot1x all !No configuration change since last restart !Time: Thu Sep 20 10:22:58 2018 version 9.2(2) Bios:version 07.64 feature dot1x dot1x system-auth-control dot1x mac-move deny interface Ethernet1/1 dot1x host-mode multi-auth dot1x pae authenticator dot1x port-control auto no dot1x re-authentication dot1x max-req 1 dot1x max-reauth-req 2 dot1x timeout quiet-period 60 dot1x timeout re-authperiod 3600 dot1x timeout tx-period 1 dot1x timeout server-timeout 30 dot1x timeout ratelimit-period 0 dot1x timeout supp-timeout 30 dot1x timeout inactivity-period 0 dot1x mac-auth-bypass interface Ethernet1/33</pre>	802.1X の設定を表示します。

	コマンドまたはアクション	目的
	<pre>dot1x host-mode multi-auth dot1x pae authenticator dot1x port-control auto no dot1x re-authentication dot1x max-req 1 dot1x max-reauth-req 2 dot1x timeout quiet-period 60 dot1x timeout re-authperiod 3600 dot1x timeout tx-period 1 dot1x timeout server-timeout 30 dot1x timeout ratelimit-period 0 dot1x timeout supp-timeout 30 dot1x timeout inactivity-period 0 dot1x mac-auth-bypass</pre>	

VXLAN EVPN の 802.1X サポートの確認

VXLAN EVPN の構成情報での 802.1X サポートを表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show running-config dot1x all	802.1X の実行構成を表示します。
show dot1x all summary	インターフェイスのステータスを表示します。
show dot1x	デフォルト設定を表示します。
show dot1x all	インターフェイスの詳細を表示します。

show running-config dot1x all コマンドの例

```
switch# show running-config dot1x all
!Command: show running-config dot1x all
!No configuration change since last restart
!Time: Thu Sep 20 10:22:58 2018
```

```
version 9.2(2) Bios:version 07.64
feature dot1x
```

```
dot1x system-auth-control
dot1x mac-move deny
```

```
interface Ethernet1/1
  dot1x host-mode multi-auth
  dot1x pae authenticator
  dot1x port-control auto
  no dot1x re-authentication
  dot1x max-req 1
  dot1x max-reauth-req 2
  dot1x timeout quiet-period 60
  dot1x timeout re-authperiod 3600
  dot1x timeout tx-period 1
  dot1x timeout server-timeout 30
  dot1x timeout ratelimit-period 0
```

```

dot1x timeout supp-timeout 30
dot1x timeout inactivity-period 0
dot1x mac-auth-bypass

interface Ethernet1/33
  dot1x host-mode multi-auth
  dot1x pae authenticator
  dot1x port-control auto
  no dot1x re-authentication
  dot1x max-req 1
  dot1x max-reauth-req 2
  dot1x timeout quiet-period 60
  dot1x timeout re-authperiod 3600
  dot1x timeout tx-period 1
  dot1x timeout server-timeout 30
  dot1x timeout ratelimit-period 0
  dot1x timeout supp-timeout 30
  dot1x timeout inactivity-period 0
  dot1x mac-auth-bypass

```

show dot1x all summary コマンドの例

```
switch# show dot1x all summary
```

Interface	PAE	Client	Status
Ethernet1/1	AUTH	none	UNAUTHORIZED
Ethernet1/33	AUTH	00:16:5A:4C:00:07 00:16:5A:4C:00:06 00:16:5A:4C:00:05 00:16:5A:4C:00:04	AUTHORIZED AUTHORIZED AUTHORIZED AUTHORIZED

```
switch#
```

```
switch# show mac address-table vlan 10
```

Legend:

* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen, + - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan

VLAN	MAC Address	Type	age	Secure	NTFY	Ports
* 10	0016.5a4c.0004	secure	-	T	F	Eth1/33
* 10	0016.5a4c.0005	secure	-	T	F	Eth1/33
* 10	0016.5a4c.0006	secure	-	T	F	Eth1/33
* 10	0016.5a4c.0007	secure	-	T	F	Eth1/33

```
switch#
```

```
switch# show mac address-table vlan 10 (VPC-PEER)
```

Legend:

* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen, + - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan

VLAN	MAC Address	Type	age	Secure	NTFY	Ports
* 10	0016.5a4c.0004	secure	-	T	F	vPC Peer-Link
* 10	0016.5a4c.0005	secure	-	T	F	vPC Peer-Link
* 10	0016.5a4c.0006	secure	-	T	F	vPC Peer-Link
* 10	0016.5a4c.0007	secure	-	T	F	vPC Peer-Link

```
switch#
```

```
switch# show mac address-table vlan 10 (RVTEP)
```

Legend:

* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC

```

age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
VLAN      MAC Address      Type      age      Secure NTFY Ports
-----+-----+-----+-----+-----+-----+-----
C   10      0016.5a4c.0004    dynamic    0          F      F      nvel(67.67.67.67)
C   10      0016.5a4c.0005    dynamic    0          F      F      nvel(67.67.67.67)
C   10      0016.5a4c.0006    dynamic    0          F      F      nvel(67.67.67.67)
C   10      0016.5a4c.0007    dynamic    0          F      F      nvel(67.67.67.67)

```

show dot1x コマンドの例

```

switch# show dot1x
          Sysauthcontrol Enabled
          Dot1x Protocol Version 2
          Mac-Move Deny

```

show dot1x all コマンドの例

```

switch# show dot1x all
          Sysauthcontrol Enabled
          Dot1x Protocol Version 2
          Mac-Move Deny

Dot1x Info for Ethernet1/1
-----
          PAE = AUTHENTICATOR
          PortControl = AUTO
          HostMode = MULTI AUTH
          ReAuthentication = Disabled
          QuietPeriod = 60
          ServerTimeout = 30
          SuppTimeout = 30
          ReAuthPeriod = 3600 (Locally configured)
          ReAuthMax = 2
          MaxReq = 1
          TxPeriod = 1
          RateLimitPeriod = 0
          InactivityPeriod = 0
          Mac-Auth-Bypass = Enabled

Dot1x Info for Ethernet1/33
-----
          PAE = AUTHENTICATOR
          PortControl = AUTO
          HostMode = MULTI AUTH
          ReAuthentication = Disabled
          QuietPeriod = 60
          ServerTimeout = 30
          SuppTimeout = 30
          ReAuthPeriod = 3600 (Locally configured)
          ReAuthMax = 2
          MaxReq = 1
          TxPeriod = 1
          RateLimitPeriod = 0
          InactivityPeriod = 0
          Mac-Auth-Bypass = Enabled

```

クリティカル認証の確認

次の例は、クリティカル認証機能が有効になっているかどうかを表示する方法を示しています。

```
switch(config)# show dot1x
                  Sysauthcontrol Enabled
                  Dot1x Protocol Version 2
                  Mac-Move Permit
                  Server-Dead-Action-Authorize Enabled
```

Server-Dead-Action-Authorize パラメータの値が **Enabled** の場合、クリティカル認証機能が有効になります。

802.1X のモニタリング

Cisco NX-OS デバイスが保持している 802.1X のアクティビティに関する統計情報を表示できます。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	show dot1x {all interface ethernet slot/port} statistics Example: switch# show dot1x all statistics	802.1X 統計情報を表示します。

802.1X の設定例

次に、アクセス ポートに 802.1X を設定する例を示します。

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae authenticator
dot1x port-control auto
```

次に、トランク ポートに 802.1X を設定する例を示します。

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae authenticator
```

```
dot1x port-control auto
dot1x host-mode multi-host
```



Note 802.1X 認証が必要なすべてのインターフェイスに対して、**dot1x pae authenticator** コマンドおよび **dot1x port-control auto** コマンドを繰り返してください。

ユーザ 1 人あたりの DACL の設定例

次の例は、ポートの 1 つで設定されたユーザごとの DACL を示しています。DACL が適用されると、ブロックリストトラフィックは除外されます。DACL-Applied パラメータの値が true の場合、クライアントは ISE から ACL を受信したブロックリストクライアントです。

```
switch# show dot1x all summary
Interface    PAE      Client                Status
Ethernet1/1  AUTH    36:12:61:51:21:52    AUTHORIZED
              36:12:61:51:21:53    AUTHORIZED
```

```
switch# show dot1x all details
```

```
-----
Supplicant = 36:12:61:51:21:52
Domain = DATA
Auth SM State = AUTHENTICATED
DACL-Applied = False
-----
```

```
Supplicant = 36:12:61:51:21:53
Domain = DATA
Auth SM State = AUTHENTICATED
DACL-Applied = True
```

次に、ブロックリストされたトラフィックを表示する例を示します。

```
switch# show ip access-list dynamic
IP access list DOT1X_Restricted_base_acl_Ethernet1/1_new statistics per-entry fragments
deny-all
10 permit udp any 3612.6151.2153 0000.0000.0000 any eq 5555 vlan 100 [match=0]
20 permit udp any 3612.6151.2153 0000.0000.0000 any eq 6666 vlan 100 [match=0]
30 deny ip any 3612.6151.2153 0000.0000.0000 any vlan 100 [match=0]
```

802.1X に関する追加情報

ここでは、802.1X の実装に関する追加情報について説明します。

標準

標準	タイトル
IEEE Std 802.1X- 2004 (IEEE Std 802.1X-2001 の改訂版)	『802.1X IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control』

標準	タイトル
RFC 2284	『 <i>PPP Extensible Authentication Protocol (EAP)</i> 』
RFC 3580	『 <i>IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines</i> 』



第 12 章

IP ACL の構成

この章では、Cisco NX-OS デバイスの IP アクセス コントロール リスト (ACL) を設定する方法について説明します。

特に指定がなければ、IP ACL は IPv4 および IPv6 の ACL を意味します。

- [ACL について, on page 355](#)
- [IP ACL の前提条件, on page 376](#)
- [IP ACL の注意事項と制約事項 \(376 ページ\)](#)
- [IP ACL のデフォルト設定, on page 389](#)
- [IP ACL の設定, on page 390](#)
- [IP ACL の設定の確認, on page 431](#)
- [IP ACL の統計情報のモニタリングとクリア \(433 ページ\)](#)
- [IP ACL の設定例, on page 434](#)
- [システム ACL について \(436 ページ\)](#)
- [オブジェクト グループの設定, on page 439](#)
- [オブジェクト グループの設定の確認, on page 444](#)
- [時間範囲の設定, on page 445](#)
- [時間範囲設定の確認, on page 449](#)
- [IP ACL に関する追加情報, on page 450](#)

ACL について

ACL とは、トラフィックのフィルタリングに使用する順序付きのルール セットのことです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。デバイスは、ある ACL がパケットに適用されると判断すると、そのすべてのルールの条件にパケットを照合し、テストします。最初に一致したルールで、そのパケットが許可されるか拒否されるかが決定されます。一致するものがなければ、デバイスは適用可能な暗黙のルールを適用します。デバイスは、許可されたパケットの処理を続行し、拒否されたパケットはドロップします。

ACL を使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。たとえば、ACL を使用して、厳重にセキュリティ保護された

ネットワークからインターネットに HTTP トラフィックが流入するのを禁止できます。また、特定のサイトへの HTTP トラフィックだけを許可することもできます。その場合は、サイトの IP アドレスが、IP ACL に指定されているかどうかによって判定します。

ACL のタイプと適用

セキュリティ トラフィック フィルタリングには次のタイプの ACL を使用できます。

IPv4 ACL

IPv4 トラフィックだけに適用されます。

IPv6 ACL

IPv6 トラフィックだけに適用されます。

MAC ACL

デバイスにより MAC ACL のみが非 IP トラフィックに適用されます。

IP および MAC ACL には以下の種類のアプリケーションがあります。

ポート ACL

レイヤ 2 トラフィックのフィルタリング

UDF ベースの一致による MAC ACL

UDF ベースのマッチングで MAC ACL をフィルタリングします。

ルータ ACL

レイヤ 3 トラフィックのフィルタリング

VLAN ACL

VLAN トラフィックのフィルタリング

VTY ACL

仮想テレタイプ (VTY) トラフィックのフィルタリング

次の表に、セキュリティ ACL の適用例の概要を示します。

Table 15: セキュリティ ACL の適用

適用	サポートするインターフェイス	サポートする ACL のタイプ
ポート ACL	- レイヤ 2 インターフェイス - レイヤ 2 イーサネット ポート チャンネル インターフェイス ポート ACL をトランク ポートに適用すると、その ACL は、当該トランク ポート上のすべての VLAN 上のトラフィックをフィルタリングします。	- IPv4 ACL - の UDF ベースのマッチングで IPv4 ACL をサポートします。 - IPv6 ACL - の UDF ベースのマッチングで IPv6 ACL をサポートします。 - MAC ACL - UDF ベースのマッチングでの MAC ACL

適用	サポートするインターフェイス	サポートする ACL のタイプ
ルータ ACL	• VLAN インターフェイス • 物理層 3 インターフェイス • レイヤ 3 イーサネット サブインターフェイス • レイヤ 3 イーサネット ポート チャンネル インターフェイス • 管理インターフェイス Note VLAN インターフェイスを設定するには、先に VLAN インターフェイスをグローバルにイネーブルにする必要があります。	• IPv4 ACL • IPv6 ACL Note MAC ACL は、MAC パケット分類をイネーブルにする場合だけ、レイヤ 3 インターフェイスでサポートされます。
VLAN ACL	• VLAN	• IPv4 ACL • IPv6 ACL • MAC ACL
VTY ACL	• VTY	• IPv4 ACL • IPv6 ACL

Related Topics

[VLAN ACL について](#) (465 ページ)

[MAC ACL について](#) (451 ページ)

ACL の適用順序

デバイスは、パケットを処理する際に、そのパケットの転送パスを決定します。デバイスがトラフィックに適用する ACL はパスによって決まります。デバイスは、次の順序で ACL を適用します。

1. ポート ACL
2. 入力 VACL
3. 入力ルータ ACL
4. 入力 VTY ACL
5. 出力 VTY ACL
6. 出力ルータ ACL

7. 出力 VACL

パケットが入力 VLAN 内でブリッジされる場合、ルータ ACL は適用されません。

Figure 8: ACL の適用順序

次の図に、デバイスが ACL を適用する順序を示します。

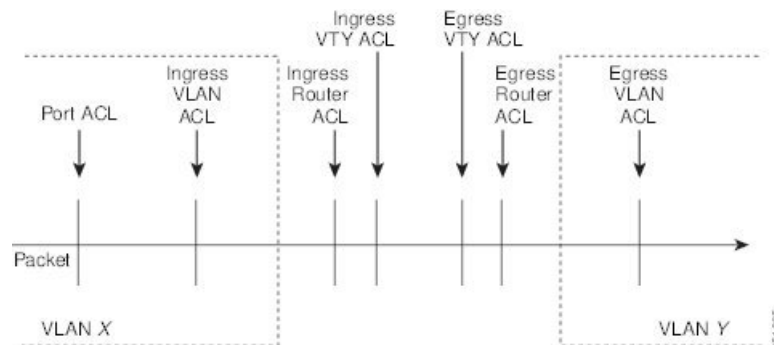
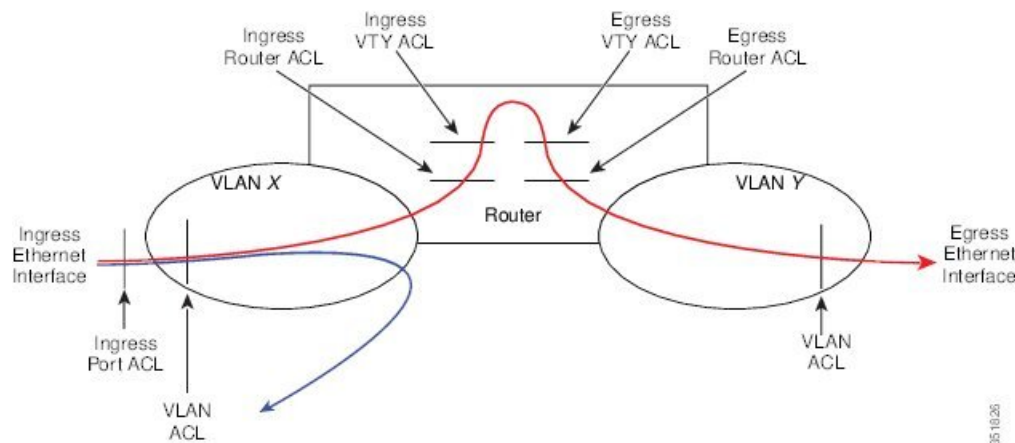


Figure 9: ACL とパケットフロー

次の図に、ACL のタイプに応じた ACL の適用場所を示します。赤いパスは送信元とは異なるインターフェイス上の宛先に送信されるパケットを表しています。青いパスは同じ VLAN 内でブリッジされるパケットを表しています。

デバイスは適用可能な ACL だけを適用します。たとえば、入力ポートがレイヤ 2 ポートの場合、VLAN インターフェイスである VLAN 上のトラフィックには、ポート ACL とルータ ACL が両方とも適用される可能性があります。さらに、その VLAN に VACL が適用される場合、デバイスはその VACL も適用します。



ルールについて

ACL によるネットワーク トラフィックのフィルタリング方法を設定する際に、何を作成、変更、削除するかを決めるのがルールです。ルールは実行コンフィギュレーション内に表示されます。ACL をインターフェイスに適用するか、またはインターフェイスにすでに適用されている ACL 内のルールを変更すると、スーパーバイザ モジュールは実行コンフィギュレーション

内のルールから ACL のエントリを作成し、それらの ACL エントリを適用可能な I/O モジュールに送信します。ACL の設定によっては、ルールよりも ACL エントリの方が数が増えることがあります。特に、ルールを設定するときにオブジェクトグループを使用してポリシーベース ACL を実装する場合などです。

アクセスリストコンフィギュレーションモードでルールを作成するには、**permit** または **deny** コマンドを使用します。デバイスは、許可ルール内の基準と一致するトラフィックを許可し、拒否ルール内の基準と一致するトラフィックをブロックします。ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

ここでは、ルールを設定する際に使用できるオプションをいくつか紹介します。

IP ACL および MAC ACL のプロトコル

IPv4、IPv6、および MAC の ACL では、トラフィックをプロトコルで識別できます。指定の際の手間を省くために、一部のプロトコルは名前で指定できます。たとえば、IPv4 または IPv6 の ACL では、ICMP を名前で指定できます。

プロトコルはすべて番号で指定できます。MAC ACL では、プロトコルをそのプロトコルの EtherType 番号（16 進数）で指定できます。たとえば、MAC ACL ルールの IP トラフィックの指定に 0x0800 を使用できます。

IPv4 および IPv6 ACL では、インターネットプロトコル番号を表す整数でプロトコルを指定できます。

送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。送信元と宛先の指定方法は、IPv4 ACL、IPv6 ACL、MAC ACL のどの ACL を設定するのかによって異なります。

IP ACL および MAC ACL の暗黙ルール

IP ACL および MAC ACL には暗黙ルールがあります。暗黙ルールは、実行コンフィギュレーションには設定されていませんが、ACL 内の他のルールと一致しない場合にデバイスがトラフィックに適用するルールです。ACL のルール単位の統計情報を維持するようにデバイスを設定した場合、暗黙ルールの統計情報はデバイスに維持されません。

すべての IPv4 ACL には、次の暗黙のルールがあります。

```
deny ip any any
```

この暗黙ルールによって、デバイスは不一致 IP トラフィックを確実に拒否します。

すべての IPv6 ACL には、次の暗黙のルールがあります。

```
deny ipv6 any any
```

この暗黙ルールによって、デバイスは不一致 IPv6 トラフィックを確実に拒否します。

**Note**

- IPv6 近隣探索パケット (ルータ要請、およびルータ アドバタイズメント) は、IPv6 ACL の暗黙の **deny ipv6 any any** ルールにより許可されません。
- Cisco Nexus 93180YC-FX、Nexus 93240YC-FX2、Nexus 93360YC-FX2、Nexus 9336C-FX2、Nexus 9336C-FX2-E、Nexus 93180YC-FX3、N9K-C9316D-GX、N9K-C93600CD-GX、Nexus 9364C-GX、N9K-C9332D-GX2B プラットフォーム スイッチ で IPv6 ネイバー探索パケットを許可するには、次のルールを明示的に追加する必要があります。
 - **permit icmp any any router-advertisement**
 - **permit icmp any any router-solicitation**
- ネイバー要請 (NS) メッセージとネイバーアドバタイズメント (NA) メッセージは、暗黙のルールでは一致しません。NS または NA IPv6 トラフィックを照合するには、次のコマンドが必要です。
 - **permit/deny icmp any any nd-na**
 - **permit/deny icmp any any nd-ns**

すべての MAC ACL には、次の暗黙のルールがあります。

```
deny any any protocol
```

この暗黙ルールによって、デバイスは、トラフィックのレイヤ 2 ヘッダーに指定されているプロトコルに関係なく、不一致トラフィックを確実に拒否します。

その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。これらのオプションは、ACL のタイプによって異なります。次のリストには、ほとんどの追加フィルタリングオプションが含まれていますが、すべてを網羅しているわけではありません。

- IPv4 ACL には、次の追加フィルタリング オプションが用意されています。
 - レイヤ 4 プロトコル
 - TCP/UDP ポート
 - ICMP タイプおよびコード
 - IGMP タイプ
 - 優先レベル
 - DiffServ コード ポイント (DSCP) 値
 - ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
 - 確立済み TCP 接続
 - パケット長

- IPv6 ACL では、次のフィルタリング オプションが追加されています。
 - レイヤ 4 プロトコル
 - カプセル化セキュリティ ペイロード
 - ペイロード圧縮プロトコル
 - Stream Control Transmission Protocol (SCTP)
 - SCTP、TCP、および UDP の各ポート
 - ICMP タイプおよびコード
 - DSCP の値
 - ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
 - 確立済み TCP 接続
 - パケット長
- MAC ACL は、次の追加フィルタリング オプションをサポートしています。
 - レイヤ 3 プロトコル (Ethernet)
 - VLAN ID
 - サービス クラス (CoS)
- Cisco NX-OS リリース 9.2(4) 以降、N9K-X96136YC-R、N9K-X9636C-R、および N9K-X9636C-RX ライン カードと N9K-C9504-FM-R を搭載した Cisco Nexus 9500 プラットフォーム スイッチの IPv4 ACL および IPv6 ファブリック モジュールは、次の追加のフィルタリング オプションをサポートしています。
 - ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
 - 確立済み TCP 接続

**Note**

- カーネルでは TCP フラグがサポートされていないため、TCP フラグオプションはカーネル (KStack) ではなく Netstack によって正しく処理されます。さらに、次の syslog メッセージが生成されます。

```
<HOSTNAME> %NPACL-2-IPT_WARNING: npacl [<#>] Warning (注意) : Mgmt  
ACL: <ACL> Seq:<Seq#> には、カーネル スタックでサポートされていない ACL オ  
プション tcp-flags があります。したがって、そのオプションはフィルタ ルールに追  
加されません。
```

- **tcp-flags-mask** オプションはサポートされていません。

シーケンス番号

デバイスはルールของシーケンス番号をサポートしています。入力するすべてのルールにシーケンス番号が割り当てられます（ユーザによる割り当てまたはデバイスによる自動割り当て）。シーケンス番号によって、次の ACL 設定作業が容易になります。

既存のルールの中に新しいルールを追加

シーケンス番号を指定することによって、ACL 内での新規ルールの挿入場所を指定します。たとえば、ルール番号 100 と 110 の間に新しいルールを挿入する必要がある場合は、シーケンス番号 105 を新しいルールに割り当てます。

ルールの削除

シーケンス番号を使用しない場合は、ルールを削除するために、次のようにルール全体を入力する必要があります。

```
switch(config-acl)# no permit tcp 10.0.0.0/8 any
```

このルールに 101 番のシーケンス番号が付いていれば、次コマンドだけでルールを削除できます。

```
switch(config-acl)# no 101
```

ルールの移動

シーケンス番号を使用すれば、同じ ACL 内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号を使用せずにルールを入力すると、デバイスはそのルールを ACL の最後に追加し、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号を割り当てます。たとえば、ACL 内の最後のルールのシーケンス番号が 225 で、シーケンス番号を指定せずにルールを追加した場合、デバイスはその新しいルールにシーケンス番号 235 を割り当てます。

また、Cisco NX-OS では、ACL 内ルールのシーケンス番号を再割り当てできます。シーケンス番号の再割り当ては、ACL 内に、100、101 のように連続するシーケンス番号のルールがある場合、それらのルールの間に 1 つ以上のルールを挿入する必要があるときに便利です。

論理演算子と論理演算ユニット

TCP および UDP トラフィックの IP ACL ルールでは、論理演算子を使用して、ポート番号に基づきトラフィックをフィルタリングできます。Cisco NX-OS では、入力方向でのみ論理演算子をサポートします。

このデバイスは、論理演算ユニット（LOU）というレジスタに、演算子とオペランドの組み合わせを格納します。各タイプの演算子は、次のように LOU を使用します。

eq

LOU には格納されません。

gt

1 LOU を使用します。

- lt**
1 LOU を使用します。
- neq**
1 LOU を使用します。
- range**
1 LOU を使用します。



Note 範囲演算子の場合、LOU しきい値構成を使用して、ACL エントリを構成するときにポート範囲を拡張する方法を制御します。ACL ルールの数が構成されたしきい値を超えたときに LOU 演算子を使用する場合は、**hardware access-list lou resource threshold <x>** コマンドを実行します。ここで <x> は LOU しきい値に達する前に使用される ACL ルールの数を示します。<x> の範囲値は 1 ～ 50 で、LOU しきい値のデフォルト値は 5 です。

ACL ロギング

ACL ロギング機能は、ACL のフローをモニタし、統計情報をログに記録します。

フローは、送信元インターフェイス、プロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート値によって定義されます。フローの統計情報には、転送されたパケット（ACL エントリの許可条件に一致する各フロー）およびドロップされたパケット（ACL エントリの拒否条件に一致する各フロー）の数が含まれます。

Cisco NX-OS リリース 10.4(3)F 以降、Cisco Nexus 9300-FX3/GX/GX2/H2R プラットフォーム スイッチでは、セキュリティ グループ ACL（SGACL）の ACL ロギングが提供されます。

SGACL の場合、フローはセキュリティ グループ タグ（SGT）、宛先グループ タグ（DGT）、送信元 MAC（SMAC）、宛先 MAC（DMAC）、SGACL 許可/拒否情報、パケットが到着した物理インターフェイス、および基本的な 5 つのタプルとは独立した、その特定の SGACL フローのヒットカウントによって定義されます。SGACL ロギングを有効にするには、[ACL ロギングの設定, on page 424](#)を参照してください。

時間範囲

時間範囲を使用して、ACL ルールが有効になる時期を制御できます。たとえば、インターフェイスに着信するトラフィックに特定の ACL を適用するとデバイスが判断し、その ACL のあるルールの時間範囲が有効になっていない場合、デバイスは、トラフィックをそのルールと照合しません。デバイスは、そのデバイスのクロックに基づいて時間範囲を評価します。

時間範囲を使用する ACL を適用すると、デバイスはその ACL で参照される時間範囲の開始時または終了時に影響する I/O モジュールをアップデートします。時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。

IPv4、IPv6、および MAC の各 ACL は時間範囲をサポートしています。デバイスがトラフィックに ACL を適用する場合、有効なルールは次のとおりです。

- 時間範囲が指定されていないすべてのルール
- デバイスはその ACL をトラフィックに適用した時点（秒）が時間範囲に含まれているルール

名前が付けられた時間範囲は再利用できます。多くの ACL ルールを設定する場合は、時間範囲を名前で一度設定すれば済みます。時間範囲の名前は最大 64 の英文字で指定します。

時間範囲には、1 つまたは複数のルールで構成されます。これらのルールは次の 2 種類に分類できます。

絶対

特定の開始日時、終了日時、その両方を持つルール、またはそのどちらも持たないルール。絶対時間範囲のルールがアクティブかどうかは、開始日時または終了日時の有無によって、次のように決まります。

- 開始日時と終了日時が両方指定されている：この時間範囲ルールは、現在の時刻が開始日時よりも後で終了日時よりも前の場合にアクティブになります。
- 開始日時が指定され、終了日時は指定されていない：この時間範囲ルールは、現在の時刻が開始日時よりも後である場合にアクティブになります。
- 開始日時は指定されず、終了日時が指定されている：この時間範囲ルールは、現在の時刻が終了日時よりも前である場合にアクティブになります。
- 開始日時も終了日時も指定されていない：この時間範囲ルールは常にアクティブです。

たとえば、新しいサブネットへのアクセスを許可するようにネットワークを設定する場合、そのサブネットをオンラインにする予定日の真夜中からアクセスを許可するような時間範囲を指定し、この時間範囲をそのサブネットに適用する ACL ルールに使用します。デバイスはこのルールを含む ACL を適用する場合、開始日時が過ぎると、この時間範囲を使用するルールの適用を自動的に開始します。

定期

毎週 1 回以上アクティブになるルール。たとえば、定期時間範囲を使用すると、平日の営業時間中だけ、研究室のサブネットにアクセスできるようにすることができます。デバイスは、そのルールを含む ACL が適用されていて、時間範囲がアクティブな場合にだけ、この時間範囲を使用する ACL ルールを自動的に適用します。



Note デバイスは、時間範囲内のルールの順序に関係なく、時間範囲がアクティブかどうかを判断します。Cisco NX-OS は、時間範囲を編集できるように時間範囲内にシーケンス番号を入れます。

時間範囲には備考を含めることもできます。備考を使用すると、時間範囲にコメントを挿入できます。備考は、最大 100 文字の英数字で指定します。

デバイスは次の方法で時間範囲がアクティブかどうかを判断します。

- 時間範囲に絶対ルールが 1 つまたは複数含まれている：現在の時刻が 1 つまたは複数の絶対ルールの範囲内であれば、その時間範囲はアクティブです。
- 時間範囲に定期ルールが 1 つまたは複数含まれている：現在の時刻が 1 つまたは複数の定期ルールの範囲内であれば、その時間範囲はアクティブです。
- 時間範囲に絶対ルールと定期ルールが両方含まれている：現在の時刻が 1 つまたは複数の絶対ルールと 1 つ以上の定期ルールの範囲内にある場合に、その時間範囲はアクティブです。

時間範囲に絶対ルールと定期ルールが両方含まれている場合、定期ルールがアクティブになるのは、最低 1 つの絶対ルールがアクティブな場合だけです。

ポリシーベース ACL

デバイスはポリシーベース ACL (PBACL) をサポートしています。PBACL を使用すると、オブジェクトグループ全体にアクセスコントロールポリシーを適用できます。オブジェクトグループは、IP アドレスのグループまたは TCP ポートもしくは UDP ポートのグループです。ルール作成時に、IP アドレスやポートを指定するのではなく、オブジェクトグループを指定できます。

IPv4 または IPv6 の ACL の設定にオブジェクトグループを使用すると、ルールの送信元または宛先に対してアドレスまたはポートの追加や削除を行う場合に、ACL を簡単にアップデートできます。たとえば、3 つのルールが同じ IP アドレスグループオブジェクトを参照している場合は、3 つのすべてのルールを変更しなくても、オブジェクトに IP アドレスを追加すれば済みます。

PBACL を使用しても、インターフェイスに ACL を適用する際にその ACL が必要とするリソースは減りません。PBACL の適用時、またはすでに適用されている PBACL のアップデート時には、デバイスはオブジェクトグループを参照する各ルールを展開し、グループ内の各オブジェクトと ACL エントリが 1 対 1 になるようにします。あるルールに、送信元と宛先が両方ともオブジェクトグループとして指定されている場合、この PBACL を適用する際に I/O モジュールに作成される ACL エントリ数は、送信元グループ内のオブジェクト数に宛先グループ内のオブジェクト数をかけた値になります。

ポート、ルータ、Policy-Based Routing (PBR)、VLAN ACL には、次のオブジェクトグループタイプが適用されます。

IPv4 アドレス オブジェクトグループ

IPv4 ACL ルールで送信元または宛先アドレスの指定に使用できます。**permit** コマンドまたは **deny** コマンドを使用してルールを設定する際に、**addrgroup** キーワードを使用すると、送信元または宛先のオブジェクトグループを指定できます。

IPv6 アドレス オブジェクトグループ

IPv6 ACL ルールで送信元または宛先アドレスの指定に使用できます。**permit** コマンドまたは **deny** コマンドを使用してルールを設定する際に、**addrgroup** キーワードを使用すると、送信元または宛先のオブジェクトグループを指定できます。

プロトコル ポート オブジェクト グループ

IPv4 および IPv6 の TCP および UDP ルールで送信元または宛先のポートの指定に使用できます。**permit** または **deny** コマンドを使用してルールを設定する際に、**portgroup** キーワードを使用すると、送信元または宛先のオブジェクト グループを指定できます。



Note ポリシーベースルーティング (PBR) ACLは、ルールを設定するためのdenyアクセスコントロールエントリ (ACE) またはdenyコマンドをサポートしていません。

カーネル スタック ACL

カーネルスタック ACL は、インバンドコンポーネントとアウトバンドコンポーネントを管理するための ACL を構成するための一般的な CLI インフラストラクチャです。

カーネル スタック ACL は、NX-OS ACL CLI を使用して、管理およびフロント パネル ポート上の管理アプリケーションを保護します。単一の ACL を設定することで、NX-OS 上のすべての管理アプリケーションを保護できる必要があります。

カーネル スタック ACL は、ユーザーの手動介入を修正し、ACL が mgmt0 インターフェイスに適用されるときに iptable エントリを自動的にプログラムするコンポーネントです。

以下は、カーネル スタック ACL を構成する例です。

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list kacl1
switch(config-acl)# statistics per-entry
switch(config-acl)# 10 deny tcp any any eq 443
switch(config-acl)# 20 permit ip any any
switch(config-acl)# end
switch#

switch(config-if)# interface mgmt0
switch(config-if)# ip access-group acl1 in
switch(config-if)# ipv6 traffic-filter acl6 in
switch(config-if)#

switch# sh ip access-lists kacl1
IP access list kacl1
statistics per-entry
10 deny tcp any any eq 443 [match=136]
20 permit ip any any [match=44952]
switch(config)#
```

以下は、構成に基づいた iptables エントリのカーネル スタック フィルタリングです。

```
bash-4.4# ip netns exec management iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target prot opt in out source destination
1 9 576 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:443
2 0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0
3 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target prot opt in out source destination
```

```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target prot opt in out source destination
bash-4.4#
```

カーネル スタック ACL サポートの制限は次のとおりです。

- この機能は、**mgmt0** インターフェイスでのみサポートされ、他のインバンドインターフェイスではサポートされません。
- ACL エントリの 5 つのタプル (protocol、source-ip、destination-ip、source-port、および destination-port) は、**iptables** にプログラムされています。ACL エントリで提供される残りのオプションは **iptables** でプログラムされておらず、そのような場合に警告の **syslog** をスローします。

たとえば、「警告: 一部の ACL オプションは **kstack** ではサポートされていません。部分的なルールのみがインストールされます。」
- デバイス ユーザーがホスト **bash** アクセス権を持っている場合、ユーザーは手動で **iptables** を更新できます。この更新により、プログラムされている **iptables** ルールが破損する可能性があります。
- 検証される ACE の最大数は、IPv4 トラフィックの場合は 100、IPv6 トラフィックの場合は加えてさらに 100 です。このスケール以上を適用すると、スループットに影響を与える可能性があります。

統計情報と ACL

このデバイスは IPv4、IPv6、および MAC の ACL に設定した各ルールのグローバル統計を保持できます。1 つの ACL が複数のインターフェイスに適用される場合、ルール統計には、その ACL が適用されるすべてのインターフェイスと一致する (ヒットする) パケットの合計数が維持されます。



Note インターフェイスレベルの ACL 統計はサポートされていません。

設定する ACL ごとに、その ACL の統計情報をデバイスが維持するかどうかを指定できます。これにより、ACL によるトラフィック フィルタリングが必要かどうかに応じて ACL 統計のオン、オフを指定できます。また、ACL 設定のトラブルシューティングにも役立ちます。

デバイスには ACL の暗黙ルールの統計情報は維持されません。たとえば、すべての IPv4 ACL の末尾にある暗黙の **deny ip any any** ルールと一致するパケットのカウントはデバイスに維持されません。暗黙ルールの統計情報を維持する場合は、暗黙ルールと同じルールを指定した ACL を明示的に設定する必要があります。

Related Topics

[IP ACL の統計情報のモニタリングとクリア](#) (433 ページ)

[IP ACL および MAC ACL の暗黙ルール](#) (359 ページ)

Atomic ACL のアップデート

デフォルトでは、Cisco Nexus 9000 シリーズのデバイスのスーパーバイザモジュールで、ACL の変更を I/O モジュールにアップデートする際には、Atomic ACL のアップデートを実行します。Atomic アップデートでは、アップデートされる ACL が適用されるトラフィックを中断させることはありません。しかし、Atomic アップデートでは、ACL のアップデートを受け取る I/O モジュールに、関係する ACL の既存のすべてのエントリに加えて、アップデートされた ACL エントリを保存するのに十分なリソースがあることが必要です。アップデートが行われた後、アップデートに使用されたリソースは開放されます。I/O モジュールに十分なリソースがない場合は、デバイスからエラー メッセージが出力され、この I/O モジュールに対する ACL のアップデートは失敗します。

I/O モジュールに Atomic アップデートに必要なリソースがない場合は、**no hardware access-list update atomic** コマンドを使用して Atomic アップデートをディセーブルにすることができますが、デバイスで既存の ACL を削除して、アップデートされた ACL を適用するには、多少の時間がかかります。ACL が適用されるトラフィックは、デフォルトでドロップされます。

ACL が適用されるすべてのトラフィックを許可し、同時に非 Atomic アップデートを受信するようにするには、**hardware access-list update default-result permit** コマンドを使用してください。

次の例では、ACL に対する Atomic アップデートをディセーブルにする方法を示します。

```
switch# config t
switch(config)# no hardware access-list update atomic
```

次の例では、非 Atomic ACL アップデートの際に、関連するトラフィックを許可する方法を示します。

```
switch# config t
switch(config)# hardware access-list update default-result permit
```

次の例では、Atomic アップデート方式に戻る方法を示します。

```
switch# config t
switch(config)# no hardware access-list update default-result permit
switch(config)# hardware access-list update atomic
```

IP ACL に対する Session Manager のサポート

Session Manager は IP ACL および MAC ACL の設定をサポートしています。この機能を使用すると、ACL の設定を調べて、その設定に必要なとされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。

ACL TCAM リージョン

ハードウェアの ACL Ternary Content Addressable Memory (TCAM) リージョンのサイズを変更できます。

Cisco Nexus 9300 および 9500 シリーズ スイッチでは、出力 TCAM サイズは 1K で、4 つの 256 エントリに分割されます。他の Cisco Nexus 9300 および 9500 シリーズ スイッチでは、入力 TCAM サイズは 4K で、8 つの 256 スライスと 4 つの 512 スライスに分割されます。スライスは割り当ての単位です。1 つのスライスを割り当てることができるのは 1 つのリージョンだけです。たとえば、サイズが 512 のスライスを使用して、サイズがそれぞれ 256 の 2 つの機能を設定することはできません。同様に、256 サイズのスライスを使用して、サイズがそれぞれ 128 の 2 つの機能を設定することはできません。IPv4 TCAM リージョンはシングル幅です。IPv6、QoS、MAC、CoPP、およびシステム TCAM リージョンはダブル幅で、物理 TCAM エントリを 2 倍消費します。たとえば、サイズ 256 の論理リージョンエントリが実際に消費する物理 TCAM エントリは 512 です。

IPv6、ポート ACL、VLAN ACL、およびルータ ACL を作成でき、QoS の IPv6 と MAC アドレスを照合できます。ただし、Cisco NX-OS ではすべてを同時にサポートすることはできません。IPv6、MAC、およびその他希望の TCAM リージョンを有効にするには、既存の TCAM リージョン (TCAM カービング) のサイズを削除または削減する必要があります。すべての TCAM リージョンの設定コマンドでは、新たな変更を TCAM に組み込むことができるかを評価します。できない場合は、エラーを報告し、コマンドは拒否されます。既存の TCAM リージョンのサイズを削除または削減して、新しい要件のためのスペースを確保する必要があります。

N9K-X9636C-RX では、PACL が外部 TCAM リージョンを使用する場合、内部 TCAM は ifacl に 2K を使用する必要があります、入力 RACL-IPv4 は最大 2044 を使用できます。出力 PACL 外部 TCAM リージョンを使用する場合は、追加の 4 つのエントリが必要です。

ACL TCAM リージョン サイズには、次の注意事項と制約事項があります。

- 既存の TCAM リージョンで RACL または PACL をイネーブル化するには、12,288 を超える TCAM リージョンを分割する必要があります。
- VACL リージョンを設定する場合は、入力および出力方向の両方で同じサイズが設定されます。リージョン サイズがいずれかの方向に対応できない設定は拒否されます。
- RACL v6、CoPP、およびマルチキャストの TCAM サイズはデフォルト値です。以下の Cisco Nexus 9504 および Cisco Nexus 9508 ラインカードでは、リロード中にラインカード障害が発生しないように、これらの TCAM サイズをゼロ以外にする必要があります。
 - N9K-X96136YC-R
 - N9K-X9636C-RX
 - N9K-X9636Q-R
 - N9K-X9636C-R
- 出力 RACL が 4K を超える場合、TCAM カービング設定では、入力 RACL (RACL) + 出力 RACL (e-racl) の合計を 20480 にする必要があります。次の TCAM カービングの例を参照してください。

```
hardware access-list tcam region ifacl 0
hardware access-list tcam region ipv6-ifacl 0
hardware access-list tcam region mac-ifacl 0
hardware access-list tcam region racl 0
hardware access-list tcam region ipv6-racl 0
```

```
hardware access-list tcam region span 0
hardware access-list tcam region redirect_v4 0
hardware access-list tcam region redirect_v6 0
hardware access-list tcam region e-racl 20480
```

- IPv6 RACL は IPv6 IFCAL で部分的に使用できます。これは、N9K-X96136YC-R、N9K-X9636C-R、N9K-X9636Q-R、および N9K-X9636C-RX ライン カードを搭載した Cisco Nexus N9K-C9508 および N9K-C9504 に適用されます。
- N9K-X9636C-R および N9K-X9636Q-R ライン カードは、最大 12K の TCAM リージョン サイズをサポートします。より大きな数を設定しても、TCAM リージョンは 12K に設定されます。
- N9K-X96136YC-R および N9K-X9636C-R ライン カードは、2K の出力 RACL をサポートします。
- N9K-X9636C-RX ライン カードは、12K を超える TCAM リージョン サイズをサポートします。RACL IPv4 TCAM リージョンを 100K に設定したときの TCAM リージョンのサイズは、N9K-X9636C-R および N9K-X9636Q-R ライン カードの場合は 12K に、N9K-X9636C-RX ライン カードの場合は 100K に設定されます（他のすべての TCAM リージョンは設定されており、N9K-X9636C-R および N9K-X9636Q-R ライン カード用に 12K に対応するだけのスペースがあることを条件とします）。
- Cisco NX-OS リリース 10.2 (2) F 以降、N9K-X9636C-R および N9K-X9636Q-R ライン カードは、最大 20K の TCAM リージョン サイズをサポートします。より大きな数を構成しても、TCAM リージョンは 20K に再設定されます。
- N9K-X9636C-RX ライン カードでは、内部 TCAM に加えて、128K の外部 TCAM を使用できます。
- リロード前に特定の「ing-racl」リージョンの TCAM 使用率が 50% を超えると、リロードまたはアップグレード後のスイッチ動作に一貫性がなくなる可能性があります。

次の表に、特定の機能を動作させるために設定する必要があるリージョンをまとめます。リージョン サイズは、特定の機能のスケール要件に基づいて選択する必要があります。

表 16: ACL TCAM リージョンごとの機能

機能名	リージョン名
ポート ACL	ifacl : IPv4ポートACL用 ifacl-udf : IPv4 ポート ACL の UDF 用 ing-ifacl : 入力 IPv4、IPv6、および MAC ポート ACL 用 ing-ifacl : 入力 IPv4、IPv6、MAC ポート ACL、および MAC ポート ACL の UDF 用 ipv6-ifacl : IPv6 ポート ACL 用 mac-ifacl : MAC ポート ACL 用
ポート QoS (レイヤ 2 ポートまたはポート チャンネルに適用される QoS 分類ポリシー)	qos、qos-lite、rp-qos、rp-qos-lite、ns-qos、e-qos、または e-qos-lite : IPv4 パケット分類用 ing-l2-qos : 入力レイヤ 2 パケットの分類用 ipv6-qos、rp-ipv6-qos、ns-ipv6-qos、または e-ipv6-qos : IPv6 パケット分類用 mac-qos、rp-mac-qos、ns-mac-qos、または e-mac-qos : 非 IP パケット分類用 (注) Cisco Nexus 9300 シリーズ スイッチの 40G ポートで分類する必要があるトラフィックの場合は、qos リージョンと対応する ns-* qos 領域を分割する必要があります。
VACL	vacl : IPv4 パケット用 ipv6-vacl : IPv6 パケット用 Mac-vacl : 非 IP パケット用

機能名	リージョン名
VLAN QoS (VLAN に適用される QoS 分類ポリシー)	vqos または ns-vqos : IPv4 パケットの分類用 ipv6-vqos または ns-ipv6-vqos : IPv6 パケットの分類用 ing-l3-vlan-qos : 入力レイヤ 3、VLAN、および SVI QoS パケットの分類用 mac-vqos or ns-mac-vqos : 非 IP パケットの分類用 (注) Cisco Nexus 9300 シリーズ スイッチの 40G ポートで分類する必要があるトラフィックの場合は、qos 領域と対応する ns- * qos 領域を分割する必要があります。
RACL	egr-racl : 出力 IPv4 および IPv6 RACL 用 e-racl : 出力 IPv4 RACL 用 e-ipv6-racl : 出力 IPv6 RACL 用 igr-racl : 入力 IPv4 および IPv6 RACL 用 racl : IPv4 RACL の場合 racl-lite : IPv4 RACL 用 racl-udf : IPv4 RACL 上の UDF 用 ipv6-racl : IPv6 RACL の場合
レイヤ 3 QoS (レイヤ 3 ポートまたはポート チャネルに適用される QoS 分類ポリシー)	L3qos、l3qos-lite、または ns-l3qos : IPv4 パケットの分類用 Ipv6-l3qos または ns-ipv6-l3qos : IPv6 パケットの分類用 (注) Cisco Nexus 9300 シリーズ スイッチの 40G ポートで分類する必要があるトラフィックの場合は、qos 領域と対応する ns- * qos 領域を分割する必要があります。

機能名	リージョン名
VLAN 送信元または VLAN フィルタ SPAN (Cisco Nexus 9500 または 9300 シリーズ スイッチ用) 40G ポートの Rx SPAN (Cisco Nexus 9300 シリーズ スイッチのみ)	span
SPAN フィルタ	Ifacl : レイヤ 2 (スイッチ ポート) 送信元インターフェイスでの IPv4 トラフィックのフィルタリング用。 ifacl-udf : IPv4 ポート ACL の UDF 用 Ipv6-ifacl : レイヤ 2 (スイッチ ポート) 送信元インターフェイスでの IPv6 トラフィックのフィルタリング用。 Mac-ifacl : レイヤ 2 (スイッチ ポート) 送信元インターフェイスでの レイヤ 2 トラフィックのフィルタリング用。 racl-udf : IPv4 RACL 上の UDF 用 vacl : VLAN 送信元の IPv4 トラフィックをフィルタリングします。 ipv6-vacl : VLAN 送信元の IPv6 トラフィックをフィルタリングします。 mac-vacl : VLAN 送信元のレイヤ 2 トラフィックをフィルタリングします。 Racl : レイヤ 3 インターフェイスでの IPv4 トラフィックのフィルタリング用。 Ipv6-racl : レイヤ 3 インターフェイスでの IPv6 トラフィックのフィルタリング用。 ing-l2-span-filter : 入力レイヤ 2 SPAN トラフィックのフィルタリング用 ing-l3-span-filter : 入力レイヤ 3 および VLAN SPAN トラフィックのフィルタリング用

機能名	リージョン名
SVI カウンタ (注) この領域は、レイヤ 3 SVI インターフェイスのパケット カウンタを有効にします。	svi
BFD、DHCP リレー、または DHCPv6 リレー	redirect (注) BFD は ing-sup リージョンを使用し、DHCPv4 リレー、DHCPv4 スヌーピング、および DHCPv4 クライアントは ing-redirect リージョンを使用します。
CoPP	copp (注) リージョンサイズを 0 にすることはできません。
システム管理 ACL	system (注) 領域サイズは変更できません。
vPC コンバージェンス (注) この領域は、vPC リンクがダウンし、トラフィックをピアリンクにリダイレクトする必要がある場合にコンバージェンス時間を増加させます。	vPC コンバージェンス (注) この領域サイズを 0 に設定すると、vPC リンク障害のコンバージェンス時間が影響を受ける可能性があります。
ファブリック エクステンダ (FEX)	fex-ifacl、fex-ipv6-ifacl、 fex-ipv6-qos、fex-mac-ifacl、 fex-mac-qos、fex-qos、fex-qos-lite
ダイナミック ARP インスペクション (DAI)	arp-ether
IP ソース ガード (IPSG)	ipsg
マルチキャスト PIM Bidir	mcast_bidir
スタティック MPLS	mpls
ネットワーク アドレス変換 (NAT)	nat
NetFlow	ing-netflow
OpenFlow	OpenFlow

機能名	リージョン名
sFlow	sflow
スーパーバイザ モジュール	egr-sup : 出力スーパーバイザ ing-sup : 入力スーパーバイザ
ポリシーベースルーティング (PBR)	ing-racl : PBR の入力 L3 トラフィックの照合用。
レイヤ 2 Intelligent Traffic Director (ITD)	vacl : VLAN レベルで L2 リダイレクト ACL をプログラムします。
レイヤ 3 Intelligent Traffic Director (ITD)	ing-racl : ITD の L3 リダイレクト ACL をプログラムします。
L2 での拡張ポリシーベース リダイレクト (ePBR)	ing-ifacl : ePBR L2 の L2 リダイレクト ACL をプログラムします。
L3 での拡張ポリシーベース リダイレクト (ePBR)	ing-racl : ePBR L3 の L3 リダイレクト ACL をプログラムします。

関連トピック

[ACL TCAM リージョン サイズの設定](#) (397 ページ)

[TCAM カービングの設定](#) (411 ページ)

[TCAM カービングの設定 : Cisco NX-OS リリース 6.1\(2\)I1\(1\) 用](#)

ACL タイプでサポートされる最大ラベル サイズ

Cisco NX-OS スイッチは、対応する ACL タイプに対して次のラベルサイズをサポートします。

表 17: ACL タイプと最大ラベル サイズ

ACL タイプ	方向 (Direction)	ラベル (Label)	ラベルタイプ
RACL/PBR/VACL/L3-VLAN QoS/L3-VLAN SPAN ACL	受信側	62	BD
PACL/L2 QoS/L2 SPAN ACL	受信側	62 ¹	IF
RACL/VACL/L3-VLAN QoS	送信側	254	BD
L2 QoS	送信側	31	IF
RACL	入力	510	L3

¹ **hardware access-list tcam label ing-ifacl 6** コマンドを入力してスイッチをリロードすると、ラベル サイズを 62 に増やすことができます。

Cisco NX-OS リリース 9.3(6) で、**hardware access-list tcam label ing-ifac1 6** コマンドが導入されました。Cisco Nexus 9300-FX プラットフォーム スイッチにのみ適用されます。

Cisco NX-OS リリース 10.1(2) 以降では、**hardware access-list tcam label ing-ifac1 6** コマンドは、Cisco Nexus 9300-FX2 プラットフォーム スイッチでもサポートされます。

Cisco NX-OS リリース 10.4(3) 以降では、**hardware access-list tcam label ing-ifac1 6** コマンドは、Cisco Nexus 9300-FX3、GX、GX2、H2R、H1 プラットフォーム スイッチでもサポートされます。

IP ACL の前提条件

IP ACL の前提条件は次のとおりです。

- IP ACL を設定するためには、IP アドレッシングおよびプロトコルに関する知識が必要です。
- ACL を設定するインターフェイス タイプについての知識が必要です。

IP ACL の注意事項と制約事項

IP ACL の設定に関する注意事項と制約事項は次のとおりです。



(注) リリース 7.0(3)I7(1)から現在のリリースまでのさまざまな機能をサポートする Cisco Nexus 9000 シリーズ プラットフォーム スイッチの詳細については、[Nexus スイッチ プラットフォーム サポート マトリックス](#)を参照してください。

- Cisco NX-OS リリース 10.2(1)F 以降、入力 PACL は Cisco Nexus 9364D-GX2A および 9332D-GX2B スイッチでサポートされます。
- 出力 PACL と出力 VACL を同じインターフェイスに設定すると、出力 VACL だけが有効になります。
- ACL の設定には Session Manager を使用することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。この機能は、1,000 以上のルールが含まれている ACL に対して特に推奨されます。Session Manager の詳細については、『Cisco Nexus 9000 シリーズ NX-OS システム管理設定ガイド』を参照してください。
- 12K ～ 64K の範囲の IPv4 PACL の設定は、-RX ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチでサポートされます。
- 異なるシーケンス番号を持つ重複した ACL エントリは、設定で許可されます。ただし、これらの重複エントリはハードウェア アクセス リストにプログラムされません。

- 動的に作成されたシステム ACL は、設定目的で明示的に使用しないでください。ダイナミックに作成された ACL を表示するには、**show access-list dynamic** コマンドを使用します。
 - 最大 62 の一意の ACL を設定できます。各 ACL は、1 つのラベルを持ちます。同じ ACL が複数のインターフェイスで設定される場合、同じラベルが共有されます。ただし、各 ACL が一意のエントリを持つ場合、ACL のラベルは共有されず、そのラベルの上限は 62 です。これは、Cisco Nexus 9500 シリーズ スイッチ。
 - 複数のレイヤ 3 インターフェイスに適用される IPv4 および IPv6 RACL および PBR ポリシーは、同じラベルスペースを共有します。まったく同じ ACL と PBR ポリシーのセットが複数のインターフェイスに適用される場合、共有ラベルが使用され、TCAM の使用率が最適化されます。ただし、これらのインターフェイスのいずれかで ACL または PBR を変更すると、そのインターフェイスのラベル共有が切断され、新しいラベルスペースを割り当てるために追加の TCAM リソースが必要になります。これにより、十分なリソースが利用できない場合、TCAM 枯渇エラーが発生する可能性があります。
 - IPv6 拡張ヘッダー ホップバイホップ フィルタは、IPv6 ACL ではサポートされません。
 - 通常、IP パケットに対する ACL 処理は I/O モジュール上で実行されます。これには、ACL 処理を加速化するハードウェアを使用します。場合によっては、スーパーバイザモジュールで処理が実行されることもあります。この場合、特に多数のルールが設定されている ACL を処理する際には、処理速度が遅くなることがあります。管理インターフェイストラフィックは、常にスーパーバイザモジュールで処理されます。次のカテゴリのいずれかに属する IP パケットがレイヤ 3 インターフェイスから出る場合、これらのパケットはスーパーバイザモジュールに送られて処理されます。
 - レイヤ 3 最大伝送単位チェックに失敗し、そのためにフラグメント化を要求しているパケット
 - IP オプションがある IPv4 パケット（他の IP パケットヘッダーのフィールドは、宛先アドレス フィールドの後）
 - 拡張 IPv6 ヘッダー フィールドがある IPv6 パケット
- レート制限を行うことで、リダイレクト パケットによってスーパーバイザモジュールに過剰な負荷がかかるのを回避します。
- 時間範囲を使用する ACL を適用すると、デバイスは、その ACL エントリで参照される時間範囲の開始時または終了時に ACL エントリを更新します。時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。
 - IP ACL を VLAN インターフェイスに適用するためには、VLAN インターフェイスをグローバルにイネーブル化する必要があります。VLAN インターフェイスの詳細については、『Cisco Nexus 9000 シリーズ NX-OS インターフェイス設定ガイド』を参照してください。

- VTY ACL 機能はすべての VTY 回線のすべてのトラフィックを制限します。異なる VTY 回線に異なるトラフィックの制限を指定できません。どのルータの ACL も VTY ACL として設定できます。
- 出力 VTY ACL (アウトバウンド方向の VTY 回線に適用される IP ACL) は、ファイル転送プロトコル (TFTP、FTP、SCP、SFTP など) が出力 VTY ACL 内で明示的に許可されていない限り、スイッチがファイル転送プロトコルによってファイルをコピーするのを禁止します。
- 未定義の ACL をインターフェイスに適用すると、システムは空の ACL と見なし、すべてのトラフィックを許可します。
- IP トンネルは、ACL または QoS ポリシーをサポートしません。
- VXLAN 向け ACL には次の注意事項が適用されます。
 - アクセスからネットワーク方向 (レイヤ 2 からレイヤ 3 のカプセル化パス) のトラフィックに対してレイヤ 2 ポートに適用される入力ポート ACL は、内部ペイロードでサポートされます。
 - アクセス側でポート ACL を使用して、オーバーレイ ネットワークに入るトラフィックをフィルタリングすることを推奨します。
 - ネットワークからアクセス方向 (レイヤ 3 からレイヤ 2 へのカプセル化解除パス) の内部または外部ペイロードで照合されるアップリンク レイヤ 3 インターフェイスに適用される入力ルータ ACL はサポートされません。
 - アクセスからネットワーク方向 (カプセル化パス) の内部または外部ペイロードで照合されるアップリンク レイヤ 3 インターフェイスに適用される出力ルータ ACL はサポートされません。
- Cisco Nexus 9300 および 9500 シリーズ スイッチには、VXLAN トラフィックで使用できる ACL オプションに関する次の制限があります。
 - ネットワークからアクセス方向 (カプセル化解除パス) のトラフィックに対する、レイヤ 2 ポートに適用される出力ポート ACL はサポートされません。
 - アクセスからネットワーク方向 (カプセル化パス) のトラフィックに対する、VLAN に適用される入力 VACL はサポートします。
 - ネットワークからアクセス方向 (カプセル化解除パス) のトラフィックに対する、VLAN に適用される出力 VACL はサポートします。
 - アクセスからネットワーク方向 (カプセル化パス) のトラフィックに対する、SVI に面するテナントまたはサーバに適用される入力 RACL はサポートします。
 - ネットワークのアクセス方向 (カプセル化解除パス) へのトラフィック用に、SVI に面するテナントまたはサーバに適用される出力 RACL はサポートします。
- IPv6 ACL ロギングは、出力 PACL ではサポートされません。
- 出力方向の IPv4 ACL ロギングはサポートされていません。

- VACL の ACL ロギングはサポートされていません。
- ACL ロギングは、**ip port access-group** コマンドで設定されたポート ACL と、**ip access-group** コマンドで設定されたルータ ACL にのみ適用されます。
- DoS 攻撃を防ぐため、IPv4 ACL フローの総数はユーザ定義の最大値に制限されます。この制限に到達すると、新しいログは既存のフローが終了するまで作成されません。
- IPv4 ACL ロギングによって生成される syslog エントリ数は、ACL ロギングプロセスで設定されたログレベルによって制限されています。Syslog エントリの数がこの制限を超えると、ロギング機能が一部のロギングメッセージをドロップする場合があります。したがって、IPv4 ACL ロギングは課金ツールや ACL との一致数を正確に把握するための情報源として使用しないでください。
- 出力ルータ ACL は Cisco Nexus 9300 シリーズ スイッチ アップリンク ポートではサポートされません。
- ネットワーク フォワーディング エンジン (NFE) 対応スイッチの場合、トンネルインターフェイスの外部ヘッダーで照合される入力 RACL はサポートされません。
- 複数のインターフェイスに同じ QoS ポリシーと ACL が適用された場合、ラベルが共有されるのは、QoS ポリシーが **no-stats** オプションで適用されたときだけです。
- スイッチ ハードウェアは、出力 TCAM の範囲チェック (レイヤ 4 動作) をサポートしません。したがって、レイヤ 4 オペレーション ベースの分類をする ACL および QoS ポリシーは、出力 TCAM での複数エントリに拡張する必要があります。

スイッチ ハードウェアは、最大 16 のレイヤ 4 オペランドのみをサポートします。出力 TCAM スペース計画では、この制限を考慮してください。詳細は、[論理演算子と論理演算ユニット \(362 ページ\)](#) のセクションを参照してください。
- Cisco Nexus X96136YC-R、X9636C-RX、X9636C-RX、および X9636Q-R ラインカードの場合、**eg-racl-v6** 構成を EoR スイッチの SVI またはポート オブジェクトに適用する前に、**hardware profile acl-eg-ext module all** コマンドを実行します。
- TCAM リソースは次のシナリオでは共有されま。
 - ルーテッド ACL を複数のスイッチ仮想インターフェイス (SVI) に入力方向で適用する場合。
 - ルーテッド ACL を複数のレイヤ 2 インターフェイスに入力または出力方向で適用する場合。
- TCAM リソースは次のシナリオでは共有されません。
 - VACL (VLAN ACL) が複数の VLAN に適用される場合。
 - ルーテッド ACL を出力方向の複数の SVI に適用する場合。
- HTTP 方式に基づくアクセス リストは、Cisco Nexus 9300-FX、9300-FX2、9300-FXP、9300-GX プラットフォーム スイッチと、X97160YC-EX および X9700-FX ラインカードを

搭載した 9500 スイッチではサポートされません。これらすべてのスイッチでは、UDF ベースの ACL を使用する必要があります。

- HTTP メソッドは FEX ポートではサポートされません。
- 次の注意事項と制約事項は、Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX シリーズ スイッチに適用されます。
 - MAC 圧縮表サイズは 4096 + 512 オーバーフロー TCAM です。
 - MAC アドレスと MAC マスクのオーバーラップは拒否されます。
- -R ライン カードを備えた Cisco Nexus 9504 および Cisco Nexus 9508 スイッチでは、次の TCAM はサポートされません。
 - すべての FEX 関連 TCAM
 - すべての xxx-lite 関連の TCAM リージョン
 - レンジャー関連の TCAM
 - すべての FCoE 関連の TCAM
- ing-netflow リージョンの TCAM カービング設定は、-FX ラインカードでは実行できます。X97160YC-EX ラインカードでは、デフォルトの ing-netflow リージョン TCAM カービングが 1024 であり、それ以外の場合は設定できません。X97160YC-EX および -FX ラインカードのポートの場合、ing-netflow リージョンの推奨最大値は 1024 です。
- Cisco Nexus 9300-GX プラットフォーム スイッチでは、ACL リダイレクトを使用する dot1q VLAN は、1 ～ 509 の VLAN ID のみをサポートします。
 PACL リダイレクトまたは TapAgg が設定されている場合、**switchport access vlan vlan-id** コマンドは 1 ～ 509 の VLAN ID のみをサポートします。
- FHRP VIP 宛てのトラフィックで、トラフィックを許可するように設計された ACL ログが有効な ACE と一致する FHRP スタンバイで入力されるトラフィックの場合、Cisco Nexus 9000 シリーズ スイッチはこのパケットをドロップします。
- Cisco Nexus 9364D-GX2A および 9332D-GX2B スイッチは、出力ルータ ACL で次をサポートしません。
 - ICMP Type Match をサポートする UDF。
 - ACL ログオン出力
 - 追加のフィルタオプション tcp/udp ポートと lt/gt を指定した出力 IPv4 ルータ ACL
 - 追加のフィルタオプション tcp/udp ポートと neq を含む出力 IPv4 ルータ ACL
 - 範囲付きの追加のフィルタオプション tcp/udp ポートを含む出力 IPv4 ルータ ACL
 - フラグ付き出力 IPv4 ルータ ACL
 - 外部 TCAM の出力ルータ ACL

- 出力 PACL のサポート
 - 統計のサポート
 - ラベル共有
- -R および -RX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチには、次の注意事項があります。
 - アトミック ACL 更新は、マルチホップ BFD および CoPP 機能を除くすべての入力 ACL 機能でサポートされます。
 - アトミック ACL 更新は、出力 ACL 機能ではサポートされません。
 - ラベル共有は、同じ ASIC 内の異なるインターフェイス上の同じポリシーでのみサポートされます。
 - Cisco NX-OS リリース 9.2(3) では、次の ACL 統計情報がサポートされています。
 - PACL : IPv4 (内部、外部両方の TCAM を含む)
 - ルータ ACL : IPv4 (入力 RACL-IPv4 と出力 RACL-IPv4 の両方の内部 TCAM)
 - 出力では 2K カウンタのみがサポートされます。
 - 次の ACL 統計情報はサポートされていません。
 - BFD
 - DHCP : IPv4 および IPv6
 - PACL : MAC
 - PACL : IPv6
 - PBR : IPv4 および IPv6
 - RACL : IPv6
 - 外部 TCAM を使用する場合は RACL : IPv4
 - ACL ラベル共有は、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2 プラットフォーム スイッチで機能しますが、次の制限があります。
 - ACL 統計情報はデフォルトで無効になっています。ただし、統計情報は QoS ポリシーに対してだけはデフォルトで有効になっています。
 - ACL ターゲット (ポート/VLAN/SVI など) は、同じスライスおよびポート上にある必要があります。
 - さらに、ラベル スペースは次の機能と共有されます。
 - 入力 RACL、PBR、および入力 L3 QoS
 - 入力 PACL、入力 L2 QoS

- 出力 RACL、出力 QoS



(注) ラベル共有を機能させるには、インターフェイスで同じ機能セットがサポートされていることを確認します。

- `hardware profile acl-stats module xx` コマンドを使用して ACL TCAM エントリのカウンタをイネーブルにすると、`show interface` の `input discard` フィールドは常にゼロになります。この制限は、-R および -RX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチにのみ適用されます。
- -R および -RX ライン カードを備えた Cisco Nexus 9500 プラットフォームスイッチは、以下をサポートしません。
 - 出力のアトミック アップデート
 - 外部 TCAM の出力ルータ ACL
 - UDF を伴う出力 ルータ ACL
 - 出力と入力の両方のルータ ACL v6 カウンタ
 - l4 ops による出力および入力ルータ ACL IPv6
 - サブインターフェイスの出力ルータ ACL
 - IPv6 ICMP タイプおよびコードによる出力および入力ルータ ACL
 - tcp-flag を使用した IPv6 入力ルータ ACL
 - 追加オプション付きの IPv4 ルータ ACL
- Cisco NX-OS リリース 9.3(3) では、出力 IPv4 RACL は、-R および -RX ライン カードを備えた Cisco Nexus 9504 および 9508 スイッチで次をサポートします。
 - TCP フラグ
 - ICMP のタイプとコード
 - ACL ログ
- IPv6 出力 ACL は、-R および -RX ライン カードを備えた Cisco Nexus 9504 および 9508 スイッチで次をサポートします。
 - レイヤ 4 プロトコル
 - TCP フラグ
 - フラグメント
 - IPv4 の ACL ログ

- IPv6 ヘッダーのフィールド

IPv6 出力 ACL には、次の制限が適用されます。

- ポート グループおよびレイヤ 4 操作はサポートされていません。範囲は `eg-racl-ipv6` の複数の ACE エントリに拡張されます。
 - アドレス グループで定義されたホストはサポートされていません。
 - カウンタはサポートされていません。
 - 出力 IPv6 RACL は、サブインターフェイスおよび外部 TCAM ではサポートされません。
 - アトミック更新はサポートされていません。
 - `acl-eg-ext` が有効になっている場合、VXLAN はサポートされません。
- PACL リダイレクトは Cisco Nexus 9300-GX スイッチでサポートされます。次の制限が適用されます。
 - PACL リダイレクトをサポートするには、入力タップインターフェイスで `mode tap-agg` コマンドを実行する必要があります。
 - MPLS ストリップ機能をサポートするには、`mpls strip` および `hardware acl tap-agg` コマンドを設定し、スイッチをリロードする必要があります。
 - ダブルタグ VLAN の場合、2 番目の VLAN の範囲は 2 ～ 510 です。
 - dot1q VLAN を使用した MPLS ストリップはサポートされていません。
 - リダイレクト ポートがアクセス ポートとして設定されている場合でも、着信パケットがタグ付けされている場合、リダイレクト ポートはタグを伝送します。
 - 拒否 ACE では、TapAgg リダイレクトはサポートされていません。
 - Cisco NX-OS リリース 10.1(2) では、Cisco Nexus X9736C-FX、X9788TC-FX、X97160YC-EX ラインカードの混合モードでの PACL リダイレクト機能はサポートされていません。
 - 出力 ACL は、VLAN 間ルーティングフローの 2 番目の VLAN の IP アドレスを宛先とするトラフィックをサポートしません。
 - Cisco Nexus 9300-FX/FX2/FX3/GX プラットフォーム スイッチおよび 93180YC-FX スイッチでは、レイヤ 3 インターフェイスのマルチキャスト MAC 宛先アドレスを持つパケットで RACL を照合できません。ルーティング可能な修飾子を削除するように ACL を設定する場合は、`ignore routable` コマンドを使用します。ただし、`ignore-routable` を RACL に追加して SVI に適用すると、RACL はブリッジされたパケットともマッチします。
 - ワイルドカード ビットが A.B.C.D 形式の場合、Get 操作は不完全なデータを提供したり、シーケンス番号を提供しなかったりします。これは既知の動作です。Open Config モデルには、`srcPrefixMask/dstPrefixMask` がありません。また、連続していないマスクのプレフィッ

クス長にマスクを変換できないため、プレフィックス長に対して意味のある値を返すことはできません。

- **ing-sup** リージョンの最小サイズは512エントリで、**egr-sup** リージョンの最小サイズは256エントリです。これらのリージョンを小さい値に設定することはできません。任意のリージョンサイズを、256の倍数のエントリの値だけで切り分けることができます（ただし、**span** リージョンは512の倍数のエントリで切り分けることができます）。
- Cisco NX-OS リリース 9.3(9) 以降、レイヤ 3 サブインターフェイス送信側ルーター ACL 機能は、Cisco Nexus 9300-FX、および 9300-FX2 プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 10.2(3)F 以降、レイヤ 3 サブインターフェイス送信側ルーター ACL 機能は、Cisco Nexus 9300 シリーズ プラットフォーム スイッチでサポートされています。
- 出力 RACL V6 リージョンの場合、**hw profile mdb-balanced-exem**を設定する必要があります。
- Cisco NX-OS リリース 10.2(2)F 以降、出力 PACL 機能は、Cisco Nexus 9300-GX プラットフォーム スイッチおよび 93108TC-FX3P および 93180YC-FX3 スイッチの出力ルータ ACL でサポートされます。
- Cisco NX-OS リリース 10.2(3)F 以降、サブインターフェイスの出力フィルタリング機能は、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2 プラットフォーム スイッチのレイヤ 3 サブインターフェイス出力ルータ ACL をサポートします。
- Cisco NX-OS リリース 10.2(3)F 以降、ACL LOU しきい値の増加機能は、Cisco Nexus 9500-R プラットフォーム スイッチでの ACL 設定の設定可能な LOU しきい値制限をサポートします。
- Cisco NX-OS リリース 10.3(1)F 以降、ITD NAT VRF 構成は Cisco Nexus 9300-GX プラットフォーム スイッチで提供されます。
- Cisco NX-OS リリース 10.3(1)F 以降、ACL 整合性チェッカーは Cisco Nexus 9808 スイッチでサポートされます。
 - Cisco NX-OS リリース 10.4(1)F 以降、ACL 一貫性チェッカーは、Cisco Nexus 9808 スイッチ（Cisco Nexus X98900CD-A、X9836DM-A ライン カード搭載）サポートされません。
- Cisco NX-OS リリース 10.4(1)F 以降、ACL 一貫性チェッカーは、Cisco Nexus 9804 スイッチ、および Cisco Nexus X98900CD-A および X9836DM-A ライン カードでサポートされません。
- Cisco Nexus 9808/9804 スイッチには、ACL SUP サポートに関する次の制限があります。
 - ACE では、**match COS** および **match VLAN** はサポートされていません。
 - **nd-na** および **nd-ns** パケットが IPv6 ACE と一致することを確認してください。

- TCAM カービングはサポートされません。ただし、個々の機能に現在割り当てられている TCAM を表示できます。現在割り当てられている TCAM を表示するには、**show hardware access-list resource usage** コマンドを使用します。
- 中央 TCAM がサポートされています。ただし、入力 ACL と出力 ACL の両方で共有されます。
- UDF はサポートされていません。
- LOU はサポートされていません。
- IPv6 フラグメントは、出力 RACL で一致しません。
- L2 ACL 機能はサポートされていません。
- ODM マージはサポートされていません。
- IPv6 の次のヘッダー照合は、最も内側の次のヘッダーとの照合を行います。パイプラインは解析できます。
- 一意のバースト値（16 個）のみサポートされています。このため、ユーザーが設定したバースト値は、最も近い 2 電力値（最小 64 から最大 65536）にマッピングされます。
- 各 IPv6 ACL は 1,000 ACE に制限されています。これは、すべての IPv6 ACL（RACL、QoS、または SPAN フィルタ）に適用されます。このような制限は IPv4 ACL には適用されません。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 スイッチでは、統計付きの RACL（Ingress-IPv4/IPv6 および Egress-IPv4/IPv6）がサポートされています。ただし、UDF はサポートされていません。
 - Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9808 スイッチと Cisco Nexus X98900CD-A および X9836DM-A ラインカードで、統計付きの RACL（Ingress-IPv4/IPv6 および Egress-IPv4/IPv6）がサポートされています。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9804 スイッチ、および Cisco Nexus X98900CD-A および X9836DM-A ラインカードの統計付きの RACL（Ingress-IPv4/IPv6 および Egress-IPv4/IPv6）がサポートされています。ただし、UDF はサポートされていません。
- Cisco Nexus 9808/9804 スイッチの ACL 統計を表示するには、**hardware access-list tcam per-entry-stats template racl** コマンドを有効にする必要があります、**hardware access-list tcam per-entry-stats template racl** コマンドを構成した後にスイッチのリロードが必要です。
- Cisco Nexus 9808/9804 スイッチには、CoPP サポートに関する次の制限があります。
 - ステージ 1、ステージ 2、およびステージ 3 の CoPP ポリサー統計は PPS にあります。



(注) CoPP ステージ 3 の統計情報は、システムのスイッチオーバー後にゼロにリセットされます。

- ステージ 2 の出力は LC/モジュール レベルで、ステージ 3 の出力は SUP/CPU レベルです。
- カスタム CoPP では、ポリサー レートと CoS の変更がサポートされています。
- ファブリック/FM はインバンドパスに含まれません。
- CoPP 整合性チェッカーはサポートされていません
- サポートされる CIR の最小値は 125 PPS です。
- CIR 0 がサポートされています。
- CoPP ACL エントリのエントリごとの統計はありません。
- MACsec パケットは BPDU キューにマッピングされます。
- 一意のバースト値 (16 個) のみサポートされています。このため、ユーザーが設定したバースト値は、最も近い 2 電力値 (最小 64 から最大 65536) にマッピングされます。
- Cisco NX-OS リリース 10.4(2)F 以降、Cisco Nexus 9364C-H1 スイッチは CoPP をサポートしますが、次の制限があります。
 - ポリシングのステージは 1 つだけで、ステージ 1 の CoPP ポリサー統計情報は PPS にあります。
 - カスタム CoPP では、ポリサー レートと CoS の変更がサポートされています。
 - ポリサーレートは 572 の倍数です。
 - CoPP 整合性チェッカーはサポートされていません。
- リダイレクト オプションを使用した MAC ACL または PACL (ポート ACL) の拒否 ACE は、Cisco Nexus 9000 シリーズ スイッチではサポートされていません。
- Cisco NX-OS リリース 10.3(2)F 以降、ACL 自動名入力機能は Cisco Nexus 9000 シリーズ プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 10.4(1)F 以降では、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2、および X97160YC-EX, 9700-/FX/GX ライン カードを搭載した Cisco Nexus 9500 で、SUP ルールに対する IP または IPv6 ACL ルールの優先順位を適用するために、新しい ACE キーワード (all) が提供されています。
- Cisco NX-OS リリース 10.4(1)F 以降、セキュリティ ACL は Cisco Nexus 9332D-H2R プラットフォーム スイッチでサポートされています。

- Cisco NX-OS リリース 10.4(2)F 以降、セキュリティ ACL は Cisco Nexus 93400LD-H1 スイッチでサポートされています。
- Cisco Nexus リリース 10.4(3)F 以降、セキュリティ ACL は Cisco Nexus 9364C-H1 スイッチでサポートされます。
- 柔軟な TCAM 設定は、Cisco Nexus 9332D-H2R、9364C-H1、および 93400LD-H1 スイッチでサポートされています。入力および出力リージョンは、このプラットフォームスイッチで 14K の共有 TCAM を使用します。



(注)

- Cisco Nexus 9332D-H2R、9364C-H1、および 93400LD-H1 スイッチでは、Cisco Nexus 9300-FX3、GX2 スイッチのような、共有 TCAM モデルの方向ごとの合計 TCAM サイズの制限はありません。14K の制限は、両方向の TCAM サイズの合計に適用されます。
 - 14K は、それぞれ 512 エントリの 28 ブロックに分割されます。入力または出力方向の TCAM への割り当ては、ブロックサイズの粒度で行われます。設定された入力リージョンサイズの合計が 256 の倍数である場合、ブロックレベルの割り当て粒度にさらに 256 が割り当てられますが、使用はされません。設定されている出力リージョンサイズの合計についても同様です。
-
- Cisco NX-OS リリース 10.4(2)F 以降では、新しい ACE 構成フィルタ `route-tag default-route` がサポートされています。この設定により、トラフィックがデフォルトルートと一致する場合に、QoS 分類のためのトラフィックのフィルタリングが有効になります。この機能強化には、次の注意事項と制限事項が適用されます。
 - **route-tag default-route** コマンドを使用した ACL は、クラスマップ、QoS タイプでのみサポートされます。この機能は次のスイッチでのみサポートされます。
 - Cisco Nexus 9300-FX3
 - Cisco Nexus 9300-GX
 - Cisco Nexus 9300-GX2
 - Cisco Nexus 93400LD-H1
 - Cisco Nexus 9332D-H2R
 - **route-tag default-route** 構成は、IPv4 および IPv6 アクセス リスト ACE でのみサポートされます。
 - スイッチに PBR ACL とデフォルトルートの両方を構成することはできません。両方の構成を共存させることはできません。

- スイッチで **hardware access-list tcam pbr match-default-route** コマンドを構成した場合、PBR ポリシー構成で **route-tag default-route** コマンドを構成することはできません。
- **hardware access-list tcam label ing-ifacl 6** コマンドを使用するように **VXLAN への FabricPath** 機能が構成されていないことを確認します。
- Cisco NX-OS リリース 10.4(3)F 以降では、エンドポイントセキュリティ グループ (ESG) を使用したセキュリティ グループ ACL でクラス E IP アドレスがサポートされています。
- Cisco NX-OS リリース 10.5(1)F 以降では、次の機能に対する、セキュリティ グループ ACL (SGACL) 機能のサポートが提供されています。
 - イーサネットセグメント識別子 (ESI)
 - 仮想拡張可能 LAN トラフィック エンジニアリング (VXLAN-TE)
 - 仮想拡張可能 LAN ポリシーベース ルーティング (VXLAN-PBR)
 - データセンターインターコネクト (DCI) のクラウドセキュリティ (CloudSec)
 - トラフィック ルート管理 (TRM)
- Cisco Nexus NX-OS リリース 10.5(3)F 以降、Cisco Nexus 9364E-SG2-Q と 9364E-SG2-O スイッチでは ACL がサポートされています。
 - レイヤ 4 (TCP/UDP) ポート番号を持つアクセス コントロール リスト (ACL) エントリが一致する場合、「フラグメント」オプションは出力の IPv6 アクセスコントロール エントリ (ACE) に追加されません。
 - ACL ロギング機能はサポートされていません。
 - ACL のハードウェアレートリミッタ値の変更はサポートされていません。
 - PACL はサポートされていません。
- Cisco NX-OS リリース 10.5(3)F 以降、セキュリティ グループ ACL (SGACL) はレイヤ 3 サブインターフェイス、ルーテッドインターフェイス、およびポートチャネル サブインターフェイスをサポートするようになりました。これにより、SGACL ポリシーで使用できるインターフェイスのタイプが広がります。
- Cisco NX-OS リリース 10.5(3)F 以降、Cisco 9364E-SG2-Q スイッチ上で、RACL は、入力と出力方向でサポートされています。
 - サポートされているインターフェイス：L3 物理、L3 ポートチャネル、L3 サブインターフェイス および L3 ポートチャネル サブインターフェイス。
 - サポートされている ACL タイプ：IPv4 および IPv6。
 - 入力 ACL：スライスあたり最大 1,450 の IPv4 エントリまたは 725 の IPv6 エントリ。
 - 出力 ACL：スライスあたり最大 1,022 の IPv4 エントリまたは 511 の IPv6 エントリ。
 - 入力ラベル スケール：機能ごとの TOR ごとに 14 個の固有の ACL。

- 出力ラベル スケール : TOR ごとに 6 個の一意の ACL。
- RACL は、デンス モードの依存関係により、SVI インターフェイスではサポートされていません。

Cisco Nexus 9336C-SE1 スイッチの ACL の注意事項と制限事項

- Cisco NX-OS リリース 10.6 (1) F 以降、Cisco Nexus 9336C-SE1 スイッチは次の ACL 機能をサポートしています。
 - PACL
 - L3 インターフェイス、L3 ポート チャネル インターフェイス、サブインターフェイス、および SVI インターフェイスの RACL
 - PBR ACL
- **mac packet-classify** コマンドは Cisco Nexus 9336C-SE1 スイッチではサポートされていません。
- 各 TCAM スライス は、RACL または PACL の 7136 エントリをサポートします。Cisco Nexus 9336C-SE1 スイッチには 2 つのスライスがあります。

IP ACL のデフォルト設定

次の表に、IP ACL パラメータのデフォルト設定を示します。

Table 18: IP ACL パラメータのデフォルト値

パラメータ	デフォルト
IP ACL	デフォルトでは IP ACL は存在しません。
IP ACL エントリ	1024
ACL ルール	すべての ACL に暗黙のルールが適用されます。
オブジェクト グループ	デフォルトではオブジェクト グループは存在しません。
時間範囲	デフォルトでは時間範囲は存在しません。

Related Topics

[IP ACL および MAC ACL の暗黙ルール](#) (359 ページ)

IP ACL の設定

IP ACL の作成

デバイスに IPv4 ACL または IPv6 ACL を作成し、これにルールを追加できます。

Before you begin

ACL の設定には Session Manager を使用することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • ip access-list name • ipv6 access-list name Example: <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	IP ACL を作成して、IP ACL コンフィギュレーションモードを開始します。 <i>name</i> 引数は 64 文字以内で指定します。 Notice ダイナミック、expanded、および summary という名前は、システム定義のアクセスリスト用に予約済み。構成の表示または確認に競合が生じる可能性があるため、ユーザー定義の ACL にはこれらの名前を使用しないでください。
ステップ 3	(Optional) fragments {permit-all deny-all} Example: <pre>switch(config-acl)# fragments permit-all</pre>	初期状態でないフラグメントのフラグメント処理を最適化します。 fragments コマンドが含まれている ACL がデバイスによってトラフィックに適用される場合、 fragments コマンドは初期状態でないフラグメント（このフラグメントは、ACL 内のどの明示的な permit コマンドまたは deny コマンドとも一致しません）のみと一致します。

	Command or Action	Purpose
ステップ 4	[sequence-number] {permit deny} protocol {source-ip-prefix source-ip-mask} {destination-ip-prefix destination-ip-mask} Example: <pre>switch(config-acl)# permit ip 192.168.2.0/24 any</pre> Example: <pre>switch(config-acl)# 10 permit ipv6 1::1 2::2 3::3 4::4</pre>	IP ACL 内にルールを作成します。多数のルールを作成できます。 sequence-number 引数には、1 ～ 4294967295 の整数を指定します。 permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。 IPv4 および IPv6 アクセス リストの場合、送信元と宛先の IPv4 または IPv6 プレフィックスを指定できます。これは、最初の連続するビットでのみ一致します。または、アドレスのいずれかのビットに一致する送信元と宛先の IPv4 または IPv6 ワイルドカードマスクを指定できます。IPv6 ワイルドカードマスクは、Cisco Nexus 9300-FX/FX2/FXP スイッチでサポートされます。
ステップ 5	(Optional) statistics per-entry Example: <pre>switch(config-acl)# statistics per-entry</pre>	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 Note Cisco NX-OS リリース 9.2(3) 以降では、-R ライン カードを備えた Cisco Nexus 9500 スイッチのサポートが追加されています。Cisco Nexus 9500 プラットフォーム スイッチを使用している場合、これは必須の手順です。
ステップ 6	hardware profile acl-stats module xx Example: <pre>switch(config-acl)# hardware profile acl-stats module 10</pre>	内部 TCAM と外部 TCAM の両方で ACL TCAM エントリのカウンタを有効にします。 Note このコマンドは、-R および -RX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチにのみ適用されます。カウンタを有効にすると、VLAN と SVI の統計情報は失われます。
ステップ 7	reload module xx Example:	スイッチをリロードします。 Note

	Command or Action	Purpose
	<code>switch(config)# reload module 10</code>	Cisco Nexus 9500 プラットフォーム スイッチの場合、このコマンドはオプションであり、 hardware profile ac-stats が適用されているモジュールのみをリロードする必要があります。
ステップ 8	ignore routeable Example: <code>switch(config)# ignore routeable</code>	Cisco Nexus 9300-FX プラットフォーム スイッチでマルチキャストトラフィックのフィルタリングを有効にします。
ステップ 9	(Optional) 次のいずれかのコマンドを入力します。 • show ip access-lists name • show ipv6 access-lists name Example: <code>switch(config-acl)# show ip access-lists acl-01</code>	IP ACL の設定を表示します。
ステップ 10	(Optional) copy running-config startup-config Example: <code>switch(config-acl)# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

IP ACL の変更

既存の IPv4 ACL または IPv6 ACL のルールの追加と削除は実行できますが、既存のルールを変更することはできません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの中に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

Before you begin

ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • ip access-list name • ipv6 access-list name Example: <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	名前で指定した ACL の IP ACL 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	(Optional) [sequence-number] {permit deny} protocol source destination Example: <pre>switch(config-acl)# 100 permit ip 192.168.2.0/24 any</pre>	IP ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。 <i>sequence-number</i> 引数には、1 ～ 4294967295 の整数を指定します。 permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	(Optional) [no] fragments {permit-all deny-all} Example: <pre>switch(config-acl)# fragments permit-all</pre>	初期状態でないフラグメントのフラグメント処理を最適化します。 fragments コマンドが含まれている ACL がデバイスによってトラフィックに適用される場合、 fragments コマンドは初期状態でないフラグメント（このフラグメントは、ACL 内のどの明示的な permit コマンドまたは deny コマンドとも一致しません）のみと一致します。 no オプションを使用すると、フラグメント処理の最適化が削除されます。
ステップ 5	(Optional) no {sequence-number {permit deny} protocol source destination} Example: <pre>switch(config-acl)# no 80</pre>	指定したルールを IP ACL から削除します。 permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。

	Command or Action	Purpose
ステップ 6	(Optional) [no] statistics per-entry Example: <pre>switch(config-acl)# statistics per-entry</pre>	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 no オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 7	(Optional) 次のいずれかのコマンドを入力します。 • show ip access-lists name • show ipv6 access-lists name Example: <pre>switch(config-acl)# show ip access-lists acl-01</pre>	IP ACL の設定を表示します。
ステップ 8	(Optional) copy running-config startup-config Example: <pre>switch(config-acl)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[IP ACL 内のシーケンス番号の変更](#) (396 ページ)

VTY ACL の作成

入力方向または出力方向の全 VTY 回線で、すべての IPv4 または IPv6 トラフィックへのアクセスを制御することにより、VTY ACL を設定できます。

Before you begin

すべての仮想端末回線にユーザが接続できるため、すべての仮想端末回線に同じ制約を設定する必要があります。

ACL の設定には **Session Manager** を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認でき、特に約 1000 以上のルールを含む ACL に役立ちます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 ipv6} access-list name Example: switch(config)# ip access-list vtyacl	ACL を作成し、その ACL の IP 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。 <i>name</i> 引数の最大長は 64 文字です。
ステップ 3	{permit deny} プロトコル 送信元 接続先 [log] [time-range 時間] Example: switch(config-ip-acl)# permit tcp any any	ACL ルールを作成し、指定した送信元とのすべての TCP トラフィックを許可します。
ステップ 4	exit Example: switch(config-ip-acl)# exit switch(config)#	IP アクセス リスト コンフィギュレーション モードを終了します。
ステップ 5	line vty Example: switch(config)# line vty switch(config-line)#	仮想端末を指定し、ラインコンフィギュレーション モードを開始します。
ステップ 6	{ip ipv6} access-class name {in out} Example: switch(config-line)# ip access-class vtyacl out	指定された ACL を使用してすべての VTY 回線に対する着信および発信接続を制限します。 <i>name</i> 引数の最大長は 64 文字です。
ステップ 7	(Optional) show {ip ipv6} access-lists Example: switch# show ip access-lists	任意の VTY ACL を含め、設定された ACL を表示します。
ステップ 8	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。

Before you begin

ACL の設定には **Session Manager** を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	resequence {ip ipv6} access-list name starting-sequence-number increment Example: <pre>switch(config)# resequence access-list ip acl-01 100 10</pre>	ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。 <i>starting-sequence-number</i> 引数と <i>increment</i> 引数は、1 ～ 4294967295 の整数で指定します。
ステップ 3	(Optional) show ip access-lists name Example: <pre>switch(config)# show ip access-lists acl-01</pre>	IP ACL の設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL の削除

IP ACL をデバイスから削除できます。

Before you begin

その ACL がインターフェイスに適用されているかどうかを確認します。削除できるのは、現在適用されている ACL です。ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。デバイスは削除された ACL を空であると見なします。IP ACL が設定されているインターフェイスを探すには、**show ip access-lists** コマンドまたは **show ipv6 access-lists** コマンドと一緒に **summary** キーワードを使用します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • no ip access-list name • no ipv6 access-list name Example: <pre>switch(config)# no ip access-list acl-01</pre>	名前で指定した IP ACL を実行コンフィギュレーションから削除します。
ステップ 3	(Optional) 次のいずれかのコマンドを入力します。 • show ip access-lists name summary • show ipv6 access-lists name summary Example: <pre>switch(config)# show ip access-lists acl-01 summary</pre>	IP ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ACL TCAM リージョン サイズの設定

ハードウェアの ACL Ternary Content Addressable Memory (TCAM) リージョンのサイズを変更できます。TCAM カービング後に、TCAM を認定するには、設定を保存してスイッチをリロードする必要があります。スイッチに障害のあるモジュールがある場合は、設定の保存に時間がかかります。

この手順は、すべての Cisco Nexus 9300、および 9500 シリーズ スイッチで使用できます。ただし、NFE2 対応デバイス（X9432C-S 100G ラインカードや C9508-FM-S ファブリック モジュールなど）は除きます。これらは、TCAM テンプレートを使用して、ACL TCAM リージョン サイズを設定する必要があります。TCAM テンプレートの使用方法の詳細については、「テンプレートを使用した ACL TCAM リージョン サイズの設定」を参照してください。



- (注)
- (を使用して) テンプレートを適用すると、このセクションの `hardware access-list tcam region` コマンドは機能しません。[テンプレートを使用した ACL TCAM リージョン サイズの設定 \(409 ページ\)](#) コマンドを使用するには、テンプレートをコミット解除する必要があります。
 - マルチキャスト PIM Bidir 機能の `hardware access-list tcam region` コマンドは、Broadcom ベースの Cisco Nexus 9000 シリーズ スイッチにのみ適用されます。
 - QoS TCAM カービングの設定については、『*Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*』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 例 : <pre>switch# configure terminal switch(config)#</pre>	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] hardware access-list tcam region region tcam-size 例 : <pre>switch(config)# hardware access-list tcam region mpls 256</pre>	ACL TCAM リージョン サイズを変更します。使用可能なリージョンは次のとおりです。 • n9k-arp-acl : CPU に向かう途中でインターフェイスに入る ARP パケットのレート制限を設定します。arp パケットが設定されたレートに準拠するように、インターフェイスごとにこのレート制限を設定する必要があります。 • arp-ether : ARP / レイヤ 2 Ethertype TCAM リージョンのサイズを設定します。 • copp : CoPP TCAM リージョン サイズを設定します。

	コマンドまたはアクション	目的
		• E-racl : 出力フロー : 出力フローカウンタ TCAM リージョン サイズを設定します。 • copp : CoPP TCAM リージョン サイズを設定します。 • egr-racl : 出力 IPv4 または IPv6 ルータ ACL (RACL) TCAM リージョン サイズを設定します。 • egr-sup : 出力スーパーバイザ TCAM リージョン サイズを設定します。 • e-ipv6-qos : IPv6 出力 QoS TCAM リージョン サイズを設定します。 • e-ipv6-racl : IPv6 出力ルータ ACL (ERACL) TCAM リージョン サイズを設定します。 • e-mac-qos : MAC QoS TCAM リージョン サイズを設定します。 • e-qos : IPv4 出力 QoS TCAM リージョン サイズを設定します。 • e-qos-lite : IPv4 出力 QoS Lite TCAM リージョン サイズを設定します。 • e-racl : IPv4 出力ルータ ACL (ERACL) TCAM リージョン サイズを設定します。 • fex-ifacl : FEX IPv4 ポート ACL TCAM リージョン サイズを設定します。 • fex-ipv6-ifacl : FEX IPv6 ポート ACL TCAM リージョン サイズを設定します。 • fex-ipv6-qos : FEX IPv6 ポート QoS TCAM リージョン サイズを設定します。 • fex-mac-ifacl : FEX MAC ポート ACL TCAM リージョン サイズを設定します。

	コマンドまたはアクション	目的
		• fex-mac-qos : FEX MAC ポート QoS TCAM リージョン サイズを設定します。 • fex-qos : FEX IPv4 ポート QoS TCAM リージョン サイズを設定します。 • fex-qos-lite : FEX IPv4 ポート QoS TCAM リージョン サイズを設定します。 • fhs : fhs TCAM リージョンのサイズを設定します。Cisco Nexus 9300 および 9500 シリーズ スイッチの fhs リージョンに TCAM を設定できます。 • flow : 入力フロー カウンタ TCAM リージョン サイズを設定します。 • ifacl : IPv4 ポート ACL TCAM リージョン サイズを設定します。 • ifacl-udf : IPv4 ポート ACL ユーザ定義フィールド (UDF) TCAM リージョンのサイズを設定します。 • ing-ifacl : 入力 IPv4、IPv6、または MAC ポート ACL TCAM リージョン サイズを設定します。 (注) ユーザ定義フィールド (UDF) を ing-ifacl TCAM リージョンに付加して、UDF ベースの IPv4 または IPv6 ポート ACL を設定できます。UDF ベースの IPv6 ポート ACL。詳細な情報および設定の手順については、「UDF ベース ポート ACL の設定 (417 ページ)」を参照してください。 • ing-l2qos : 入力レイヤ 2 QoS TCAM リージョン サイズを設定します。

	コマンドまたはアクション	目的
		• ing-l2-span-filter : 入力レイヤ 2 SPAN フィルタ TCAM リージョン サイズを設定します。 • ing-l3-span-filter : 入力レイヤ 3 および VLAN SPAN フィルタ TCAM リージョン サイズを設定します。 • ing-l3-vlan-qos : 入力レイヤ 3、VLAN、および SVI QoS TCAM リージョン サイズを設定します。 • ing-netflow : NetFlow TCAM リージョン サイズを設定します。 • ing-racl : IPv4 または IPv6 入力ルータ ACL (RACL) TCAM リージョン サイズを設定します。 • ing-redirect : DHCPv4 リレー、DHCPv4 スヌーピング、および DHCPv4 クライアントのリダイレクト TCAM リージョン サイズを設定します。 • ing-sup : 入力スーパーバイザ TCAM リージョン サイズを設定します。 • ipsg : IP ソース ガード SMAC-IP バインディング TCAM リージョンのサイズを設定します。 • ipv6-ifacl : IPv6 ポート ACL TCAM リージョン サイズを設定します。 • ipv6-l3qos : IPv6 レイヤ 3 QoS TCAM リージョン サイズを設定します。 • ipv6-qos : IPv6 ポート QoS TCAM リージョン サイズを設定します。 • ipv6-racl : IPv6 RACL TCAM リージョン サイズを設定します。 • ipv6-vacl : IPv6 VACL TCAM リージョン サイズを設定します。

	コマンドまたはアクション	目的
		• ipv6-vqos : IPv6 VLAN QoS TCAM リージョン サイズを設定します。 • l3qos : IPv4 レイヤ 3 QoS TCAM リージョン サイズを設定します。 • l3qos-lite : IPv4 レイヤ 3 QoS TCAM リージョン サイズを設定します。 • mac-ifacl : MAC ポート ACL TCAM リージョン サイズを設定します。 • mac-l3qos : MAC レイヤ 3 QoS TCAM リージョン サイズを設定します。 • mac-qos : MAC ポート QoS TCAM リージョン サイズを設定します。 • mac-vacl : MAC VACL TCAM リージョン サイズを設定します。 • mac-vqos—Configures the size of the MAC VLAN QoS TCAM region. • mcast_bidir : マルチキャスト PIM Bidir TCAM リージョンのサイズを設定します。 • mpls : MPLS TCAM リージョン サイズを設定します。 • Nat : ネットワーク : network address translation (NAT) TCAM リージョン サイズを設定します。 • ns-ipv6-l3qos : X9536PQ、X9564PX、および X9564TX ラインカードおよび M12PQ 汎用拡張モジュール (GEM) の IPv6 レイヤ 3 QoS TCAM リージョンのサイズを設定します。 • ns-ipv6-qos : X9536PQ、X9564PX、および X9564TX ラインカードおよび M12PQ 汎用拡張モジュール (GEM) の IPv6 ポート QoS TCAM リージョンのサイズを設定します。

	コマンドまたはアクション	目的
		• ns-ipv6-vqos : X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール (GEM) のIPv6 VLAN QoS TCAM リージョンのサイズを設定します。 • ns-l3qos : X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール (GEM) のIPv4レイヤ3 QoS TCAM リージョンのサイズを設定します。 • ns-mac-l3qos : X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール (GEM) のMACレイヤ3 QoS TCAM リージョンのサイズを設定します。 • ns-mac-qos : X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール (GEM) のMACポートQoS TCAM リージョンのサイズを設定します。 • ns-mac-vqos : X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール (GEM) のMAC VLAN QoS TCAM リージョンのサイズを設定します。 • ns-qos : X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール (GEM) のIPv4ポートQoS TCAM リージョンのサイズを設定します。 • ns-vqos : X9536PQ、X9564PX、およびX9564TXラインカードおよびM12PQ汎用拡張モジュール (GEM) のIPv4 VLAN QoS TCAM リージョンのサイズを設定します。 • openflow : OpenFlow TCAM リージョンのサイズを設定します。

	コマンドまたはアクション	目的
		• qos : IPv4 ポート QoS TCAM リージョン サイズを設定します。 • qos-lite : IPv4 ポート QoS lite TCAM リージョン サイズを設定します。 • racl : IPv4 ルータの ACL (RACL) TCAM リージョン サイズを設定します。 • racl-lite : IPv4 ルータ ACL (RACL) Lite TCAM リージョンのサイズを設定します。 • racl-udf : IPv4 ルータ ACL (RACL) ユーザ定義フィールド (UDF) TCAM リージョンのサイズを設定します。 • redirect : リダイレクト TCAM リージョンのサイズを設定します。 • redirect-tunnel : VXLAN を介した BFD に使用されるリダイレクトトンネル TCAM リージョンのサイズを設定します。 (注) このコマンドは、 TP_SERVICES_PKG ライセンスがインストールされている場合にのみサポートされます。 • rp-ipv6-qos : 100G 9408PCラインカードおよび100G M4PC汎用拡張モジュール (GEM) のIPv6ポート QoS TCAMリージョンのサイズを設定します。 • rp-mac-qos : 100G 9408PCラインカードおよび100G M4PC汎用拡張モジュール (GEM) のMACポートQoS TCAMリージョンのサイズを設定します。 • rp-qos : 100G 9408PCラインカードおよび100GM4PC汎用拡張モジュール

	コマンドまたはアクション	目的
		ル (GEM) のIPv4ポートQoS TCAM リージョンのサイズを設定します。 • rp-qos-lite : 100G 9408PCラインカードおよび100G M4PC汎用拡張モジュール (GEM) のIPv4ポートQoS Lite TCAM リージョンのサイズを設定します。 • sflow : sFlow TCAM リージョン サイズを設定します。 • span : SPAN TCAM リージョン サイズを設定します。 • svi : 入力 SVI カウンタ TCAM リージョン サイズを設定します。 • vacl : IPv4 VACL TCAM リージョン サイズを設定します。 • vpc-convergence : vPCコンバージェンスTCAM リージョンのサイズを設定します。 • vqos : IPv4 VLAN QoS TCAM リージョン サイズを設定します。 • vqos-lite : IPv4 VLAN QoS lite TCAM リージョン サイズを設定します。 • tcam-size : TCAM サイズ。サイズは 256 の倍数です。サイズが 256 より大きい場合は、512 の倍数でなければなりません。FHS の場合、範囲は 0～4096 です。 このコマンドの no 形式を使用して、デフォルトの TCAM リージョン サイズに戻します。 (注) hardware access-list tcam region {racl ifacl vacl} qualify udf udf-names コマンドを使用して IPv4 ユーザー定義フィールド (UDF) を racl、ifacl、および vacl TCAM リージョンにアタッチし、IPv4 UDF ベースの ERSPAN を設定します。 hardware access-list tcam region

	コマンドまたはアクション	目的
		{ ing-ifacl ing-l2-span-filter ing-l3-span-filter } qualify v6udf v6udf-names コマンドを使用して IPv6 UDF を ing-l2-span-filter and ing-l3-span-filter TCAM にアタッチし、IPv6 UDF ベースの ERSpan を設定します。詳細と設定指示については、『Cisco Nexus 9000 シリーズ NX-OS システム管理設定』を参照してください。
ステップ 3	copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 4	(任意) show hardware access-list tcam region 例 : switch(config)# show hardware access-list tcam region	デバイスで次のリロード時に適用される TCAM サイズを表示します。
ステップ 5	hardware access-list tcam label vrf-nat 例 : switch(config)# hardware access-list tcam label vrf-nat	VRF で ITD NAT を設定します。 (注) Cisco NX-OS リリース 10.3(1)F 以降、このコマンドは Cisco Nexus 9300-GX スイッチでサポートされます。
ステップ 6	reload 例 : switch(config)# reload	デバイスがリロードされます。 (注) 新しいサイズの値は、 copy running-config startup-config + reload を入力するか、すべてのラインカードモジュールをリロードした後にのみ有効になります。

例

次に、Cisco Nexus NFE 対応デバイスで n9k-arp-acl TCAM リージョンのサイズを変更する例を示します。

```
switch(config)#hardware access-list tcam region n9k-arp-acl 256switch(config)#copy r s
switch(config)# reload
Configuring storm-control-cpu:
switch (config)# interface ethernet 1/10switch
```

```
switch (config-if)# storm-control-cpu arp rate 150
switch (config)# show access-list storm-control-cpu arp-stats interface ethernet 1/10

slot 1
```

次に、Cisco Nexus 9500 シリーズ スイッチで RACL TCAM リージョンのサイズを変更する例を示します。

```
switch(config)# hardware access-list tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

次に、変更を確認するために、TCAM リージョンのサイズを表示する例を示します。

```
switch(config)# show hardware access-list tcam region
TCAM Region Sizes:

          IPV4 PACL [ifacl] size =    512
          IPV6 PACL [ipv6-ifacl] size =     0
          MAC PACL [mac-ifacl] size =     0
          IPV4 Port QoS [qos] size =    256
          IPV6 Port QoS [ipv6-qos] size =     0
          MAC Port QoS [mac-qos] size =     0
          FEX IPV4 PACL [fex-ifacl] size =     0
          FEX IPV6 PACL [fex-ipv6-ifacl] size =     0
          FEX MAC PACL [fex-mac-ifacl] size =     0
          FEX IPV4 Port QoS [fex-qos] size =     0
          FEX IPV6 Port QoS [fex-ipv6-qos] size =     0
          FEX MAC Port QoS [fex-mac-qos] size =     0
          IPV4 VACL [vacl] size =    512
          IPV6 VACL [ipv6-vacl] size =     0
          MAC VACL [mac-vacl] size =     0
          IPV4 VLAN QoS [vqos] size =     0
          IPV6 VLAN QoS [ipv6-vqos] size =     0
          MAC VLAN QoS [mac-vqos] size =     0
          IPV4 RACL [racl] size =    512
          IPV6 RACL [ipv6-racl] size =     0
          IPV4 Port QoS Lite [qos-lite] size =     0
          FEX IPV4 Port QoS Lite [fex-qos-lite] size =     0
          IPV4 VLAN QoS Lite [vqos-lite] size =     0
          IPV4 L3 QoS Lite [l3qos-lite] size =     0
          Egress IPV4 QoS [e-qos] size =     0
          Egress IPV6 QoS [e-ipv6-qos] size =     0
          Egress MAC QoS [e-mac-qos] size =     0
          Egress IPV4 VACL [vacl] size =    512
          Egress IPV6 VACL [ipv6-vacl] size =     0
          Egress MAC VACL [mac-vacl] size =     0
          Egress IPV4 RACL [e-racl] size =    256
          Egress IPV6 RACL [e-ipv6-racl] size =     0
          Egress IPV4 QoS Lite [e-qos-lite] size =     0
          IPV4 L3 QoS [l3qos] size =     0
          IPV6 L3 QoS [ipv6-l3qos] size =     0
          MAC L3 QoS [mac-l3qos] size =     0
          Ingress System size =    256
          Egress System size =    256
          SPAN [span] size =    256
          Ingress COPP [copp] size =    256
          Ingress Flow Counters [flow] size =     0
          Egress Flow Counters [e-flow] size =     0
```

```

    Ingress SVI Counters [svi] size = 0
    Redirect [redirect] size = 512
    NS IPV4 Port QoS [ns-qos] size = 256
    NS IPV6 Port QoS [ns-ipv6-qos] size = 0
    NS MAC Port QoS [ns-mac-qos] size = 0
    NS IPV4 VLAN QoS [ns-vqos] size = 256
    NS IPV6 VLAN QoS [ns-ipv6-vqos] size = 0
    NS MAC VLAN QoS [ns-mac-vqos] size = 0
    NS IPV4 L3 QoS [ns-l3qos] size = 256
    NS IPV6 L3 QoS [ns-ipv6-l3qos] size = 0
    NS MAC L3 QoS [ns-mac-l3qos] size = 0
    VPC Convergence [vpc-convergence] size = 256
    IPSG SMAC-IP bind table [ipsg] size = 0
    Ingress ARP-Ether ACL [arp-ether] size = 0
    ranger+ IPV4 QoS Lite [rp-qos-lite] size = 0
    ranger+ IPV4 QoS [rp-qos] size = 256
    ranger+ IPV6 QoS [rp-ipv6-qos] size = 256
    ranger+ MAC QoS [rp-mac-qos] size = 256
    NAT ACL[nat] size = 0
    Mpls ACL size = 0
    Ingress IPv4 N3K QoS size = 0
    Ingress IPv6 N3K QoS size = 0
    MOD RSVD size = 0
    sFlow ACL [sflow] size = 0
    mcast bidir ACL size = 0
    Openflow size = 0

```

```

switch(config)# show hardware access-list tcam region
TCAM Region Sizes:

```

```

    IPV4 PACL [ifacl] size = 0
    IPV6 PACL [ipv6-ifacl] size = 0
    MAC PACL [mac-ifacl] size = 0
    IPV4 Port QoS [qos] size = 0
    IPV6 Port QoS [ipv6-qos] size = 0
    MAC Port QoS [mac-qos] size = 0
    FEX IPV4 PACL [fex-ifacl] size = 0
    FEX IPV6 PACL [fex-ipv6-ifacl] size = 0
    FEX MAC PACL [fex-mac-ifacl] size = 0
    FEX IPV4 Port QoS [fex-qos] size = 0
    FEX IPV6 Port QoS [fex-ipv6-qos] size = 0
    FEX MAC Port QoS [fex-mac-qos] size = 0
    IPV4 VACL [vacl] size = 0
    IPV6 VACL [ipv6-vacl] size = 0
    MAC VACL [mac-vacl] size = 0
    IPV4 VLAN QoS [vqos] size = 0
    IPV6 VLAN QoS [ipv6-vqos] size = 0
    MAC VLAN QoS [mac-vqos] size = 0
    IPV4 RACL [racl] size = 1536
    IPV6 RACL [ipv6-racl] size = 0
    IPV4 Port QoS Lite [qos-lite] size = 0
    FEX IPV4 Port QoS Lite [fex-qos-lite] size = 0
    IPV4 VLAN QoS Lite [vqos-lite] size = 0
    IPV4 L3 QoS Lite [l3qos-lite] size = 0
    Egress IPV4 QoS [e-qos] size = 0
    Egress IPV6 QoS [e-ipv6-qos] size = 0
    Egress MAC QoS [e-mac-qos] size = 0
    Egress IPV4 VACL [vacl] size = 0
    Egress IPV6 VACL [ipv6-vacl] size = 0
    Egress MAC VACL [mac-vacl] size = 0
    Egress IPV4 RACL [e-racl] size = 768
    Egress IPV6 RACL [e-ipv6-racl] size = 0
    Egress IPV4 QoS Lite [e-qos-lite] size = 0
    IPV4 L3 QoS [l3qos] size = 256

```

```

IPV6 L3 QoS [ipv6-l3qos] size = 0
MAC L3 QoS [mac-l3qos] size = 0
Ingress System size = 256
Egress System size = 256
SPAN [span] size = 256
Ingress COPP [copp] size = 256
Ingress Flow Counters [flow] size = 0
Egress Flow Counters [e-flow] size = 0
Ingress SVI Counters [svi] size = 0
Redirect [redirect] size = 256
NS IPV4 Port QoS [ns-qos] size = 256
NS IPV6 Port QoS [ns-ipv6-qos] size = 0
NS MAC Port QoS [ns-mac-qos] size = 0
NS IPV4 VLAN QoS [ns-vqos] size = 256
NS IPV6 VLAN QoS [ns-ipv6-vqos] size = 0
NS MAC VLAN QoS [ns-mac-vqos] size = 0
NS IPV4 L3 QoS [ns-l3qos] size = 256
NS IPV6 L3 QoS [ns-ipv6-l3qos] size = 0
NS MAC L3 QoS [ns-mac-l3qos] size = 0
VPC Convergence [vpc-convergence] size = 512
IPSG SMAC-IP bind table [ipsg] size = 0
Ingress ARP-Ether ACL [arp-ether] size = 0

```

次に、デフォルトの RACL TCAM リージョン サイズに戻す例を示します。

```

switch(config)# no hardware profile tcam region racl 512
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y

```

テンプレートを使用した ACL TCAM リージョン サイズの設定

カスタム テンプレートを使用、作成、および適用することで、ACL TCAM リージョン サイズを設定できます。

すべての Cisco Nexus 9300、および 9500 シリーズ スイッチでは、この手順または [ACL TCAM リージョン サイズの構成](#) 手順を使用して ACL TCAM リージョン サイズを構成できます。ただし、NFE2 対応デバイス（X9432C-S 100G ライン カードや C9508-FM-S ファブリック モジュールなど）は、**hardware access-list tcam region** コマンドをサポートしていないため、ACL TCAM リージョン サイズを設定する必要があります。



(注)

- TCAM テンプレートを適用すると、**hardware access-list tcam region** コマンドは機能しません。コマンドを使用するには、テンプレートをコミット解除する必要があります。
- QoS TCAM カービングの設定については、『Cisco Nexus 9000 シリーズ NX-OS サービス品質設定ガイド』を参照してください。
- TCAM プロファイル テンプレートは、C9508-FM-S ファブリック モジュールではサポートされません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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] hardware profile tcam resource template template-name ref-template {nfe nfe2 {I2-I3 I3}} 例 : <pre>switch(config)# hardware profile tcam resource template SR_MPLS_CARVE ref-template nfe2 switch(config-tcam-temp)#</pre>	ACL TCAM リージョン サイズを設定するテンプレートを作成します。 nfe : Network Forwarding Engine (NFE) 対応 Cisco Nexus 9300 および 9500 シリーズ、デフォルト TCAM テンプレート。 nfe2 : NFE2 対応 Cisco Nexus 9500 シリーズ、デバイスのデフォルト TCAM テンプレート。 I2-I3 : レイヤ 2 およびレイヤ 3 設定のデフォルト TCAM テンプレート。 I3 : Cisco Nexus 9200 シリーズ スイッチで。
ステップ 3	(任意) region tcam-size 例 : <pre>switch(config-tcam-temp)# mpls 256</pre>	必要な TCAM リージョンとそのサイズをテンプレートに追加します。テンプレートに追加するリージョンごとにこのコマンドを入力します。使用可能なリージョンのリストについては、 ACL TCAM リージョン サイズの構成 を参照してください。
ステップ 4	exit 例 : <pre>switch(config-tcam-temp)# exit switch(config#)</pre>	TCAM テンプレート コンフィギュレーション モードを終了します。
ステップ 5	[no] hardware profile tcam resource service-template template-name 例 : <pre>switch(config)# hardware profile tcam resource service-template SR_MPLS_CARVE</pre>	すべてのラインカードおよびファブリックモジュールにカスタムテンプレートを適用します。
ステップ 6	(任意) show hardware access-list tcam template {all nfe nfe2 I2-I3 I3 template-name}	すべての TCAM テンプレートまたは特定のテンプレートの設定を表示します。

	コマンドまたはアクション	目的
	例 : <pre>switch(config)# show hardware access-list tcam template SR_MPLS_CARVE</pre>	
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 8	reload 例 : <pre>switch(config)# reload</pre>	デバイスがリロードされます。 (注) この設定は、 copy running-config startup-config + reload を入力した後にのみ有効になります。

TCAM カービングの設定

デフォルトのTCAMリージョン設定はプラットフォームによって異なり、すべてのTCAMリージョンに対応しているわけではありません。希望のリージョンを有効にするには、1つのリージョンのTCAMサイズを減らしてから、希望のリージョンのTCAMサイズを増やします。



(注) QoS TCAM カービングの設定については、『Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide』を参照してください。



(注) Cisco NX-OS リリース 10.3(1)F 以降、次の TCAM の制限が Cisco Nexus 9800 プラットフォームスイッチで適用されます。

- TCAMカービングはサポートされていません。ただし、個々の機能に現在割り当てられている TCAM を表示できます。現在割り当てられている TCAM を表示するには、**show hardware access-list resource usage** コマンドを使用します。
- 中央 TCAM がサポートされています。ただし、入力 ACL と出力 ACL の両方で共有されます。

次の表に、異なるプラットフォームの入出力 TCAM リージョンのデフォルト サイズを示します。

表 19: デフォルト TCAM リージョン設定（入力）：Cisco Nexus 9500 シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1536	1	1536
IPv4 レイヤ 3 QoS	256	2	512
SPAN	256	1	256
CoPP	256	2	512
システム	256	2	512
リダイレクト	256	1	256
vPC コンバージェンス	512	1	512
			4 K

表 20: デフォルト TCAM リージョン設定（出力）：Cisco Nexus 9500 シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	768	1	768
システム	256	1	256
			1 K

表 21: デフォルトの TCAM サイズ：Cisco Nexus 9504 および 9508 プラットフォーム スイッチ

地域	サイズ (Size)
MAC PACL [mac-ifac]	1952
IPv6 ポート QoS [ipv6-qos]	256
IPv6 L3 QoS [ipv6-l3qos]	256
SPAN [span]	96
Ingress CoPP [copp]	128
リダイレクト IPv4	2048
リダイレクト IPv6	2048

表 22: デフォルト TCAM リージョン設定（入力）：Cisco Nexus 9300-FX シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	2304	1	2304
レイヤ 2 QoS	256	1	256

リージョン名	サイズ	幅	合計サイズ
レイヤ 3/VLAN QoS	512	1	512
システム	512	1	512
レイヤ 2 SPAN フィルタ	256	1	256
レイヤ 3 SPAN フィルタ	256	1	256
SPAN	512	1	512
NetFlow/Analytics フィルタ	512	1	512
			5 K

表 23: デフォルト TCAM リージョン設定（出力）：Cisco Nexus 9300-FX シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1792	1	1792
システム	256	1	256
			2 K

表 24: デフォルト TCAM リージョン設定（入力）：Cisco Nexus 9300 シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 ポート ACL	512	1	512
IPv4 ポート QoS	256	2	512
IPv4 VACL	512	1	512
IPv4 RACL	512	1	512
SPAN	256	1	256
CoPP	256	2	512
ACI リーフラインカードの IPv4 ポート QoS	256	1	256
ACI リーフラインカードの IPv4 VLAN QoS	256	1	256
ACI リーフラインカードの IPv4 レイヤ 3 QoS	256	1	256
システム	256	2	512
リダイレクト	512	1	512

リージョン名	サイズ	幅	合計サイズ
vPC コンバージェンス	256	1	256
			4 K

表 25: デフォルト TCAM リージョン設定（出力）：Cisco Nexus 9300 シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 VACL	512	1	512
IPv4 RACL	256	1	256
システム	256	1	256
			1 K

次に、Cisco Nexus 9500 シリーズ スイッチで IPv6 RACL TCAM サイズを 256 に設定する例を示します。サイズが 256 の IPv6 RACL は、IPv6 がダブル幅であるため、512 エントリを使用します。



(注) 別のリージョンの TCAM 設定を変更したり、別のデバイスの TCAM 設定を変更したりするには、同様の手順に従います。

Cisco Nexus 9500 シリーズ スイッチで入力 IPv6 RACL TCAM リージョンのサイズを設定するには、2 つのオプションのいずれか 1 つを実行します。

オプション #1

入力 IPv4 RACL を 1024 エントリ減らし（ $1536 - 1024 = 512$ ）、入力 IPv6 RACL を 512 エントリ増やします。このオプションが優先されます。

```
switch(config)# hardware access-list tcam region racl 512
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

表 26: IPv4 RACL（入力）を減らした後の更新された TCAM リージョン設定

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1024	1	1024
IPv6 RACL	256	2	256 個のエントリ スライスが使用できないため、1024 個の ²
IPv4 レイヤ 3 QoS	256	2	512
SPAN	256	1	256
CoPP	256	2	512

リージョン名	サイズ	幅	合計サイズ
システム	256	2	512
リダイレクト	256	1	256
vPC コンバージェンス	512	1	512
			4 K

² 2 x 512 エントリ スライスが割り当てられます。

オプション #2

IPv4 3 QoS のサイズを 0 に減らして削除し、入力 IPv6 RACL を追加します。このオプションは、IPv4 レイヤ 3 QoS を使用していない場合に使用できます。

```
switch(config)# hardware access-list tcam region l3qos 0
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

表 27: レイヤ 3 QoS（入力）を削除した後の更新された TCAM リージョン設定

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1536	1	1536
IPv6 RACL	256	2	512
IPv4 レイヤ 3 QoS	0	2	0
SPAN	256	1	256
CoPP	256	2	512
システム	256	2	512
リダイレクト	256	1	256
vPC コンバージェンス	512	1	512
			4 K

サイズ 256 の出力 IPv6 RACL をイネーブルにするには、出力 IPv4 RACL を 256 に減らし、出力 IPv6 RACL を追加します。

```
switch(config)# hardware access-list tcam region e-racl 256
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region e-ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

表 28: IPv4 RACL（出力）を減らした後のデフォルト TCAM リージョン設定

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	256	1	256

リージョン名	サイズ	幅	合計サイズ
IPv6 RACL	256	2	512
システム	256	1	256
			1 K

表 29: デフォルトの TCAM サイズ : Cisco Nexus 9800 プラットフォーム スイッチの場合

機能名	サイズ (一次元)
入力 RACLv4	9216
入力 QoSv4	
入力 SPAN フィルタ v4	
出力 RACLv4	
入力 SUP	
入力 RACLv6	4608
入力 QoSv6	
入力 SPAN フィルタ v6	
出力 RACLv6	



- (注) 各 IPv6 ACL は 1,000 ACE に制限されています。これは、すべての IPv6 ACL (RACL、QoS、または SPAN フィルタ) に適用されます。このような制限は IPv4 ACL には適用されません。

TCAM リージョンのサイズを調整した後、**show hardware access-list tcam region** コマンドを入力して、デバイスの次回リロード時に適用可能な TCAM サイズを表示します。



- 注目** すべてのモジュールの同期を維持するには、すべてのラインカードモジュールをリロードするか、**copy running-config startup-config + reload** を入力してデバイスをリロードする必要があります。TCAM リージョン設定が複数であっても、リロードする必要があるのは1回だけです。TCAM リージョン設定がすべて完了するのを待ってから、デバイスをリロードできます。

設定によっては、TCAMサイズを超えたり、スライスが不足したりすることがあります。

TCAM リージョンの設定時に、すべての TCAM リージョンの 4K 入力制限を超えると、次のメッセージが表示されます。

```
ERROR: Aggregate TCAM region configuration exceeded the available Ingress TCAM space.
Please re-configure.
```

スライスの数を超えると、次のメッセージが表示されます。

```
ERROR: Aggregate TCAM region configuration exceeded the available Ingress TCAM slices.
Please re-configure.
```

TCAM リージョンの設定時に、すべての TCAM リージョンの 1K 出力制限を超えると、次のメッセージが表示されます。

```
ERROR: Aggregate TCAM region configuration exceeded the available Egress TCAM space.
Please re-configure.
```

特定の機能の TCAM が設定されていない状態で TCAM カービングを必要とする機能を適用しようとする、次のメッセージが表示されます。

```
ERROR: Module x returned status: TCAM region is not configured. Please configure TCAM
region and retry the command.
```



- (注) 256 というデフォルトのリダイレクト TCAM リージョン サイズは、多数の BFD または DHCP リレー セッションを実行している場合は十分でない可能性があります。より多くの BFD または DHCP リレー セッションに対応するために、TCAM サイズを 512 に増やす必要がある場合があります。



- (注) N9K-C9508 (Fretta) システムに少なくとも 1 つの「N9K-X9624D-R2」ラインカードがある場合、「e-racl」tcam 領域サイズは最大 16K です。

関連トピック

[ACL TCAM リージョン サイズの設定](#) (397 ページ)

UDF ベース ポート ACL の設定

Cisco Nexus 9300 シリーズ スイッチの UDF ベースの MAC アクセス リスト (ACL) を設定できます。この機能により、デバイスはユーザ定義フィールド (UDF) でのマッチングを行い、マッチしたパケットを IPv4 ポート ACL に適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	udf udf-name offset-base offset length 例 :	次のように UDF を定義します。

	コマンドまたはアクション	目的
	<pre>switch(config)# udf pkttoff10 packet-start 10 2</pre> 例 : <pre>switch(config)# udf pkttoff10 header outer 13 20 2</pre>	• udf-name : UDF の名前を指定します。名前には最大 16 文字の英数字を入力できます。 • offset-base : UDF オフセットベースを以下のように指定します。ここで header は、オフセットを考慮したパケット ヘッダーです。 {packet-start header {outer inner {13 14}}}. • オフセット : オフセット ベースからのオフセット バイト数を指定します。オフセット ベース (レイヤ 3/レイヤ 4 ヘッダー) の最初のバイトを照合するには、オフセットを 0 に設定します。 • 長さ : オフセット からバイトの数を指定します。1 または 2 バイトのみがサポートされています。追加のバイトに一致させるためには、複数の UDF を定義する必要があります。 複数の UDF を定義できますが、シスコは必要な UDF のみ定義することを推奨します。
ステップ 3	hardware access-list tcam region ing-ifac1 qualify {udf udf-name v6udf v6udf-name} 例 : <pre>switch(config)# hardware access-list tcam region ing-ifac1 qualify udf pkttoff10</pre>	IPv4 または IPv6 ポート ACL に適用する ing-ifac1 TCAM リージョンに UDF をアタッチします。 TCAM リージョンに接続できる UDF の数は、プラットフォームによって異なります。Cisco Nexus 9200 スイッチの場合は最大 2 つの UDF、Cisco Nexus 9300 スイッチの場合は最大 8 つの UDF、Cisco Nexus 9300-EX スイッチの場合は IPv4 ポート ACL に対して最大 18 の UDF、または IPv6 ポート ACL に対して 7 つの UDF を接続できます。 (注) UDF 修飾子が追加されると、TCAM リージョンはシングル幅から倍幅に拡大します。十分な空きスペースがある

	コマンドまたはアクション	目的
		ことを確認してください。それ以外の場合このコマンドは拒否されます。必要な場合、未使用のリージョンから TCAM スペースが減りますので、このコマンドを再入力します。詳細については、「ACL TCAM リージョンサイズの設定」を参照してください。 (注) このコマンドの no 形式は、UDF を TCAM リージョンから切り離し、リージョンをシングル幅に戻します。
ステップ 4	必須: copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 5	必須: reload 例 : <pre>switch(config)# reload</pre>	デバイスがリロードされます。 (注) UDF 設定は copy running-config startup-config + reload を入力した後のみ有効になります。
ステップ 6	ip access-list udf-acl 例 : <pre>switch(config)# ip access-list udfacl switch(config-acl)#</pre>	IPv4 アクセス コントロール リスト (ACL) を作成して、IP 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 7	次のいずれかのコマンドを入力します。 • permit udf udf-name value mask • permit ip source destination udf udf-name value mask 例 : <pre>switch(config-acl)# permit udf pkttoff10 0x1234 0xffff</pre> 例 : <pre>switch(config-acl)# permit ip any any udf pkttoff10 0x1234 0xffff</pre>	ACLを設定し、UDF (例1) でのみ、または外部パケット フィールドについて現在のアクセス コントロール エントリ (ACE) と併せて UDF で一致させるように設定します (例2) 値とマスクの引数の範囲は 0x0 ~ 0xFFFF です。 シングル ACL は、UDFがある場合とない場合の両方とも、ACE を有することができます。各 ACE には一致する異なる UDF フィールドがあるか、すべての ACE を UDF の同じリストに一致させることができます。

	コマンドまたはアクション	目的
ステップ 8	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ルータ ACL としての IP ACL の適用

IPv4 ACL または IPv6 ACL は、次のタイプのインターフェイスに適用できます。

- 物理層 3 インターフェイスおよびサブインターフェイス
- レイヤ 3 イーサネット ポート チャネル インターフェイス
- VLAN インターフェイス
- 管理インターフェイス

これらのインターフェイス タイプに適用された ACL はルータ ACL と見なされます。



Note 出力ルータ ACL は Cisco Nexus 9300 シリーズ スイッチ アップリンク ポートではサポートされません。

Before you begin

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • interface ethernet <i>slot/port</i> [. <i>number</i>] • interface port-channel <i>channel-number</i> • interface vlan <i>vlan-id</i> • interface mgmt <i>port</i>	指定したインターフェイス タイプのコンフィギュレーション モードを開始します。

	Command or Action	Purpose
	Example: <pre>switch(config)# interface ethernet 2/3 switch(config-if) # switch(config)# interface ethernet 2/3.1 switch(config-if) #</pre>	
ステップ 3	(Optional) encapsulation dot1q 21 Example: <pre>switch(config-if) # encapsulation dot1q 21 switch(config-if) #</pre>	Note このコマンドは、レイヤ3サブインターフェイスにのみ必要です。
ステップ 4	次のいずれかのコマンドを入力します。 • ip access-group access-list {in out} • ipv6 traffic-filter access-list {in out} Example: <pre>switch(config-if) # ip access-group acl1 in</pre>	IPv4 ACL または IPv6 ACL を、指定方向のトラフィックのレイヤ3インターフェイスおよびサブインターフェイスに適用します。各方向にルータ ACL を 1 つ適用できます。
ステップ 5	ip access-list match-local-traffic Example: <pre>switch(config-if) # ip access-list match-local-traffic</pre>	ローカルで生成された一致するトラフィックを一覧表示します。スイッチを通過するトラフィックには影響しません。
ステップ 6	(Optional) show running-config aclmgr Example: <pre>switch(config-if) # show running-config aclmgr</pre>	ACL の設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config-if) # copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[IP ACL の作成](#) (390 ページ)

ポート ACL としての IP ACL の適用

IPv4 ACL または Ipv6 ACL は、レイヤ 2 インターフェイス（物理ポートまたはポート チャネル）に適用できます。これらのインターフェイス タイプに適用された ACL は、ポート ACL と見なされます。



Note インターフェイスを **mac packet-classify** で設定する場合は、**mac packet-classify** コマンドをインターフェイス設定から削除するまで、IP ポート ACL をインターフェイスに適用できません。

Before you begin

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • interface ethernet slot/port • interface port-channel channel-number Example: <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	指定したインターフェイス タイプの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	次のいずれかのコマンドを入力します。 • ip port access-group access-list in • ipv6 port traffic-filter access-list in Example: <pre>switch(config-if)# ip port access-group acl-l2-marketing-group in</pre>	IPv4 または IPv6 ACL をインターフェイスまたはポートチャネルに適用します。ポート ACL では、インバウンドフィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。
ステップ 4	(Optional) show running-config aclmgr Example: <pre>switch(config-if)# show running-config aclmgr</pre>	ACL の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[IP ACL の作成](#) (390 ページ)[MAC パケット分類のイネーブル化または無効化](#) (460 ページ)

IP ACL の VACL としての適用

IP ACL は VACL として適用できます。

Related Topics

[VACL の設定](#) (468 ページ)

SUP ルールに対する IP ACL ルールの優先順位付けの適用

Cisco NX-OS リリース 10.4(1)F 以降では、IP または IPv6 ACL で新しい ACE キーワード (all) がサポートされています。これにより、同じ条件で一致する他の SUP ACL ルールよりも ACL ルールの優先順位が上がり、0 (最高) になります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • ip access-list name • ipv6 access-list name 例 : <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	IP または IPv6 ACL を作成して、ACL コンフィギュレーション モードを開始します。name 引数は 64 文字以内で指定します。
ステップ 3	<pre>[sequence-number] {permit deny} protocol {source-ip-prefix source-ip-mask} {destination-ip-prefix destination-ip-mask} all</pre> 例 : IP の場合 <pre>switch(config-acl)# permit ip 192.168.2.0/24 any all</pre> IPv6 の場合 <pre>switch(config-ipv6-acl)# 10 permit ipv6 1::1 2::2 3::3 4::4 all</pre>	SUP ルールよりも IP または IPv6 ACL ルールを優先する all キーワードを使用して、ACL にルールを作成します。

	コマンドまたはアクション	目的
ステップ 4	次のいずれかのコマンドを入力します。 • interface ethernet slot/port • interface port-channel channel-number 例 : <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	指定したインターフェイス タイプの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	次のいずれかのコマンドを入力します。 • ip port access-group access-list in • ipv6 port traffic-filter access-list in 例 : IP の場合 <pre>switch(config-if)# ip port access-group acl-01 in</pre>	IPv4 または IPv6 ACL をインターフェイスまたはポートチャネルに適用します。ポート ACL では、インバウンドフィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。
ステップ 6	(任意) show running-config aclmgr 例 : <pre>switch(config-if)# show running-config aclmgr</pre>	ACL の設定を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ACL ロギングの設定

ACL ロギング プロセスを設定するには、最初にアクセス リストを作成してから、指定された ACL を使用してインターフェイス上のトラフィックのフィルタリングをイネーブルにし、最後に ACL ロギング プロセス パラメータを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成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	ip access-list name 例 : <pre>switch(config)# ip access-list logging-test switch(config-acl)#</pre>	IPv4 ACL を作成し、IP ACL コンフィギュレーションモードを開始します。 <i>name</i> 引数は 64 文字以内で指定します。
ステップ 3	{permit deny} ip source-address destination-address log 例 : <pre>switch(config-acl)# permit ip any 10.30.30.0/24 log</pre>	条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。システムがルールに一致する各パケットに関する情報ロギングメッセージを生成できるようにするには、 log キーワードを含める必要があります。 <i>Source-address</i> および <i>destination-address</i> 引数には、IP アドレスとネットワークワイルドカード、IP アドレスと可変長サブネットマスク、ホストアドレス、または任意のアドレスを指定する any などがあります。
ステップ 4	exit 例 : <pre>switch(config-acl)# exit switch(config)#</pre>	設定を更新し、IP ACL コンフィギュレーションモードを終了します。
ステップ 5	interface ethernet slot/port 例 : <pre>switch(config)# interface ethernet 1/1 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 6	ip access-group name in 例 : <pre>switch(config-if)# ip access-group logging-test in</pre>	指定された ACL を使用してインターフェイス上の IPv4 トラフィックのフィルタリングをイネーブルにします。着信トラフィックに ACL を適用できます。
ステップ 7	exit 例 : <pre>switch(config-if)# exit switch(config)#</pre>	設定を更新し、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 8	logging ip access-list cache interval interval 例 :	ACL ロギングプロセスのログ更新間隔（秒単位）を設定します。デフォルト

	コマンドまたはアクション	目的
	switch(config)# logging ip access-list cache interval 490	値は 300 秒です。範囲は 5 ～ 86400 秒です。
ステップ 9	logging ip access-list cache entries number-of-flows 例： switch(config)# logging ip access-list cache entries 8001	ACL ロギングプロセスでモニタするフローの最大数を指定します。デフォルト値は 8000 です。サポートされる値の範囲は 0 ～ 1048576 です。
ステップ 10	logging ip access-list cache threshold threshold 例： switch(config)# logging ip access-list cache threshold 490	アラート期限が切れる前に、指定されたパケット数がログ記録された段階で、Syslog メッセージが生成されます。
ステップ 11	logging ip access-list detailed 例： switch(config)# logging ip access-list detailed	show logging ip access-list cache コマンドの出力で表示される次の情報を有効にします。アクセス制御エントリ（ACE）シーケンス番号、ACE アクション、ACL 名、ACL 方向、ACL フィルタタイプ、および ACL 適用インターフェイス。
ステップ 12	hardware rate-limiter access-list-log パケット 例： switch(config)# hardware rate-limiter access-list-log 200	ACL ロギングのためにスーパーバイザモジュールにコピーされるパケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 13	aclog match-log-level severity-level 例： switch(config)# aclog match-log-level 5	ACL の一致を記録する最小シビラティ（重大度）レベルを指定します。デフォルトは 6（情報）です。範囲は 0（緊急）～ 7（デバッグ）です。
ステップ 14	（任意） logging ip access-list include sgt 例： switch(config)# logging ip access-list include sgt	show logging ip access-list cache コマンドの出力に、セキュリティグループタグ（SGT）、宛先グループタグ（DGT）、送信元 MAC（SMAC）、および宛先 MAC（DMAC）の SGACL 情報を表示できるようにします。
ステップ 15	（任意） logging ip access-list include mac 例： switch(config)# logging ip access-list include mac	show logging ip access-list cache コマンドの出力に表示される ACLLOG エントリの一部として MAC アドレスを含めることができるようにします（送信元

	コマンドまたはアクション	目的
		MAC (SMAC) および宛先 MAC (DMAC))。 このコマンドは、detailed オプション (logging ip access-list detailed) とともに設定することも、detailed オプションなしで設定することもできます。
ステップ 16	(任意) show logging ip access-list cache [detail] 例 : <pre>switch(config)# show logging ip access-list cache</pre>	送信元 IP および接続先 IP アドレス、送信元ポートおよび接続先ポート情報、送信元インターフェイスなど、アクティブなログフローに関する情報を表示します。アクティブなフローのその他の情報では、特にサポートされていないすべてのオプションは表示されません。 logging ip access-list detailed コマンドを入力すると、出力には、アクセスコントロールエントリ (ACE) のシーケンス番号、ACE のアクション、ACL の名前、ACL の方向、ACL のフィルタタイプ、および ACL の適用インターフェイスの情報も含まれます。 (注) - 次のコマンドは相互に排他的です : logging ip access-list detailed logging ip access-list include sgt show logging ip access-list cache [detail] コマンドの出力形式は、選択したオプションの構成に基づきます。

要求をリダイレクトするための HTTP メソッドによる ACL の設定

特定の HTTP メソッドを代行受信し、特定のポートに接続されているサーバにリダイレクトするように ACL を設定できます。

次の HTTP メソッドをリダイレクトできます。

- connect

- delete
- get
- head
- post
- put
- トレース

始める前に

hardware access-list tcam region ifacl 512 double-wide コマンドを使用して、IFACL 領域の倍幅 TCAM を有効にします。このコマンドは、グローバル コンフィギュレーションに適用されます。この設定を有効にするには、スイッチをリロードします。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	ip access-list name 例 : <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	IP ACL を作成して、IP ACL コンフィギュレーション モードを開始します。 <i>name</i> 引数は 64 文字以内で指定します。
ステップ 3	[sequence-number] permit protocol source destination http-method method [tcp-option-length length] [redirect interface] 例 : <pre>switch(config-acl)# permit tcp 1.1.1.1/32 any http-method get</pre>	特定の HTTP メソッドをサーバにリダイレクトするように ACL を設定します。 次の HTTP メソッドがサポートされています。 • connect : CONNECT メソッド [0x434f4e4e] で HTTP パケットを照合します。 • delete : DELETE メソッド [0x44454c45] で HTTP パケットを照合します。 • get : GET メソッド [0x47455420] で HTTP パケットを照合します。 • head : HEAD メソッド [0x48454144] で HTTP パケットを照合します。

	コマンドまたはアクション	目的
		• post : POST メソッド [0x504f5354] で HTTP パケットを照合します。 • put : PUT メソッド [0x50555420] で HTTP パケットを照合します。 • trace : TRACE メソッド [0x54524143] で HTTP パケットを照合します。 tcp-option-length オプションは、パケット内の TCP オプションヘッダーの長さを指定します。アクセス コントロール エントリ (ACE) には、最大 4 つの TCP オプション長 (4 バイトの倍数) を設定できます。長さの範囲は 0 ~ 40 です。このオプションを設定しない場合、長さは 0 に指定され、TCP オプションヘッダーのないパケットだけが ACE と一致します。このオプションを使用すると、可変長 TCP オプションヘッダーを持つパケットでも HTTP 方式を照合できます。 リダイレクト オプションは、特定のポートに接続されているサーバに HTTP メソッドをリダイレクトします。HTTP リダイレクト機能は、レイヤ 3 ポートでは機能しません。
ステップ 4	(任意) show ip access-lists name 例 : <pre>switch(config-acl)# show ip access-lists acl-01</pre>	IP ACL の設定を表示します。
ステップ 5	(任意) show run interface interface slot/port 例 : <pre>switch(config-acl)# show run interface ethernet 2/2</pre>	インターフェイスの設定を表示します。

例

次の例では、パケットの TCP オプションヘッダーの長さを指定し、ポート チャネル 4001 に接続されているサーバに post HTTP メソッドをリダイレクトします。

```

switch(config)# ip access-list http-redirect-acl
switch(config-acl)# 10 permit tcp any any http-method get tcp-option-length 4 redirect
port-channel4001
switch(config-acl)# 20 permit tcp any any http-method post redirect port-channel4001
switch(config-acl)# statistics per-entry
switch(config)# interface Ethernet 1/33
switch(config-if)# ip port access-group http-redirect-acl in

```

IPv6 拡張ヘッダーの ACL の設定

この手順は、次のデバイスにのみ適用されます。

- Cisco Nexus 9504 および 9508 モジュラ シャーシ (N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX、および N9K-X96136YC-R)
- Cisco Nexus 3600 プラットフォーム スイッチ (N3K-C36180YC-R および N3K-C3636C-R)

Cisco NX-OS リリース 9.3(7) 以降では、ここにリストされているデバイスで IPv6 ACL を設定する場合、拡張ヘッダーを含む IPv6 パケットの処理に関する新しいルールを含める必要があります。IPv6 拡張ヘッダーの詳細については、『Cisco Nexus 9000 シリーズ NX-OS ユニキャストルーティング設定ガイド』の NX-OS リリース 9.3(x) 以降の「簡素化した IPv6 パケットヘッダー」を参照してください。



(注) この手順で選択した許可ルールまたは拒否ルールは、パケットの他のフィールドに一致する他の ACL ルールに関係なく、少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットに適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	ipv6 access-list name 例 : <pre>switch(config)# ipv6 access-list acl-01 switch(config-acl)#</pre>	MAC ACL を作成して、ACL 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	extension-header {permit-all deny-all} 例 :	一致したパケットに必要なアクションを選択します。

	コマンドまたはアクション	目的
	<pre>switch(config-acl)# extension-header permit-all switch(config-acl)#</pre>	• permit-all : 少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットが許可されます。 • deny-all : 少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットがドロップされます。

IP ACL の設定の確認

IP ACL の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show hardware access-list tcam region	デバイスで次のリロード時に適用される TCAM サイズを表示します。
show hardware access-list tcam template {all nfe nfe2 l2-l3 l3 template-name}	すべての TCAM テンプレートまたは特定のテンプレートの設定を表示します。 nfe : Network Forwarding Engine (NFE) 対応 Cisco Nexus 9300 および 9500 シリーズデバイスのデフォルト TCAM テンプレート。 nfe2 : NFE2 対応 Cisco Nexus 9500 デバイスのデフォルト TCAM テンプレート。 l2-l3 : レイヤ 2 およびレイヤ 3 設定のデフォルト TCAM テンプレート。 l3 : レイヤ 3 構成のデフォルト TCAM テンプレート。
show ip access-lists	IPv4 ACL の設定を表示します。
show ipv6 access-lists	IPv6 ACL の設定を表示します。

コマンド	目的
show logging ip access-list cache [detail]	送信元IPおよび宛先IPアドレス、送信元ポートおよび宛先ポート情報、送信元インターフェイスなど、アクティブなログフローに関する情報を表示します。アクティブなフローのその他の情報では、特にサポートされていないすべてのオプションは表示されません。 logging ip access-list detailed コマンドを入力すると、出力には、アクセスコントロールエントリ（ACE）のシーケンス番号、ACE のアクション、ACL の名前、ACL の方向、ACL のフィルタタイプ、およびACL の適用インターフェイスの情報も含まれます。
show logging ip access-list status	拒否フローの最大数、現在の有効なログ間隔、と現在の有効なしきい値を表示します。
show running-config aclog	ACL のログ実行設定を表示します。
show running-config aclmgr [all]	IP ACL の設定および IP ACL が適用されるインターフェイスを含めて、ACL の実行コンフィギュレーションを表示します。 Note このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。all オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show startup-config aclog	ACL のログスタートアップ設定を表示します。

コマンド	目的
show startup-config aclmgr [all]	ACL のスタートアップ コンフィギュレーションを表示します。 Note このコマンドは、スタートアップコンフィギュレーションのユーザ設定 ACL を表示します。 all オプションを使用すると、スタートアップコンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show hardware access-list interface ethernet X/Y input entries detail	ハードウェア ACL インターフェイスの入力エントリの詳細を表示します。 Note 9500-R 以外のプラットフォームでは、エントリを展開しても範囲が x y のように表示されます。 9500-R の出力例： <pre>permit tcp 100.1.1.0/24 eq 10006 100.1.1.0/24 eq 0x4e24/fffe [0]</pre> 9300-FX3S の出力例： <pre>permit tcp 100.1.1.0/24 eq 10006 100.1.1.0/24 range 20004 20005 routeable 0x1 [0]</pre>

IP ACL の統計情報のモニタリングとクリア

IP ACL の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドのいずれかを使用します。

コマンド	目的
show ip access-lists	IPv4 ACL の設定を表示します。IPv4 ACL に statistics per-entry コマンドが含まれている場合は、 show ip access-lists コマンドの出力に、各ルールと一致したパケットの数が含まれます。

コマンド	目的
show ipv6 access-lists	IPv6 ACL の設定を表示します。IPv6 ACL に statistics per-entry コマンドが含まれている場合は、 show ipv6 access-lists コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear ip access-list counters	すべての IPv4 ACL または特定の IPv4 ACL の統計情報をクリアします。
clear ipv6 access-list counters	すべての IPv6 ACL または特定の IPv6 ACL の統計情報をクリアします。

IP ACL の設定例

acl-01 という名前の IPv4 ACL を作成し、これをポート ACL としてイーサネットインターフェイス 2/1（レイヤ 2 インターフェイス）に適用する例を示します。

```
ip access-list acl-01
  permit ip 192.168.2.0/24 any
interface ethernet 2/1
  ip port access-group acl-01 in
```

acl-120 という名前の IPv6 ACL を作成し、これをルータ ACL としてイーサネットインターフェイス 2/3（レイヤ 3 インターフェイス）に適用する例を示します。

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

次に、single-source という名前の VTY ACL を作成し、それを VTY 回線上的入力 IP トラフィックに対して適用する例を示します。この ACL は、通過するすべての TCP トラフィックを許可し、その他のすべての IP トラフィックをドロップします。

```
ip access-list single-source
  permit tcp 192.168.7.5/24 any
  exit
line vty
  ip access-class single-source in
  show ip access-lists
```

次に、IPv4 ACL ロギングの設定例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list logging-test
switch(config-acl)# permit ip any 2001:DB8:1::1/64 log
switch(config-acl)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ip access-group logging-test in
```



```
switch(config-if)# exit
switch(config)# logging ip access-list cache interval 400
switch(config)# logging ip access-list cache entries 100
switch(config)# logging ip access-list cache threshold 900
switch(config)# hardware rate-limiter access-list-log 200
switch(config)# acllog match-log-level 5
```

以下に、UDF ベース ポート ACL の設定例を示します。

```
switch# configure terminal
switch(config)# hardware access-list tcam region ing-ifacl 256
switch(config)# udf pktofff10 packet-start 10 2
switch(config)# udf pktofff20 packet-start 10 1
switch(config)# hardware access-list tcam region ing-ifacl qualify udf pktofff10 pktofff20

switch# configure terminal
switch(config)# ip access-list udfacl
switch(config-acl)# statistics per-entry
switch(config-acl)# 10 permit ip any any udf pktofff10 0x1234 0xffff

switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# ip port access-group udfacl in
switch(config-if)# switchport
switch(config-if)# no shutdown
```

次に、route-tag default-route の設定例を示します。

```
switch(config)# ip access-list global-acl
switch(config-acl)# 10 permit ip any any route-tag default-route
switch(config-acl)# exit

switch(config)#class-map type qos global
switch(config-cmap-qos)#match access-group name global-acl

switch(config)#class-map type qos domestic
switch(config-cmap-qos)#match access-group name domestic-acl

switch(config)#policy-map type qos pmap
switch(config-pmap)#class global
switch(config-pmap-c)#police cir 100 mbps bc 200 ms conform transmit violate drop
switch(config-pmap)#class domestic
switch(config-pmap-c)#police cir 200 mbps bc 200 ms conform transmit violate drop

switch(config)#interface ethernet1/12
switch(config-if)#service-policy type qos input pmap

switch(config)# show running-config ipqos
!Running configuration last done at: Tue Jun 13 10:08:38 2023
!Time: Tue Jun 13 10:10:05 2023
version 10.4(2) Bios:version 01.08
class-map type qos match-all global
match access-group name global-acl
class-map type qos match-all domestic
match access-group name domestic-acl
policy-map type qos pmap
class global
police cir 100 mbps bc 200 ms conform transmit violate drop
class domestic
police cir 200 mbps bc 200 ms conform transmit violate drop
```

システム ACL について

Cisco Nexus 9500 シリーズ スイッチでは、-R および -RX ライン カードを使用してシステム ACL を設定できます。システム ACL を使用すると、スイッチ内の同じアクセスリストを持つすべてのポートにレイヤ 2 ポート ACL (PACL) を設定できます。システム ACL を設定すると、TCAM の使用率が低下し、ポリシーの適用または変更中に時間とメモリの使用率が低下します。

システム ACL の設定については、次の注意事項と制限事項を参照してください。

- システム PACL は、レイヤ 2 インターフェイスでのみサポートされます。
- -R ライン カードを備えた Cisco Nexus 9500 シリーズ スイッチでスイッチが起動するために、他のすべての基本機能で最大 10K の ACE がサポートされます。-RX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチのハードウェア容量は 64K ACE です。
- N3K-C3636C-R および N3K-C36180YC-R ライン カードを搭載した Cisco Nexus 3600 プラットフォーム スイッチでシステム ACL を設定することもできます。
- IPv4 PACL TCAM リージョン (ifacl) を -R ライン カードの合計物理 TCAM 容量 (12k) よりも多く設定すると、-R ライン カードのみの電源が切断されます。
- ACE 統計情報は、システム ACL ではまだサポートされていません。
- IPv6 は、システム ACL ではまだサポートされていません。
- システム ACL は、ブレイクアウト ポートではサポートされません。
- -R シリーズ ライン カードを搭載した Cisco Nexus シリーズ スイッチでの Quality of Service、ACL、または TCAM カービング設定については、『[Cisco Nexus 3600 NX-OS Quality of Service 設定ガイド、リリース 7.x](#)』を参照してください。
- 非アトミック更新は、すべてのトラフィックをドロップまたは許可します。デフォルトでは、非アトミック更新は ACL 更新が完了するまですべてのトラフィックをドロップします。非アトミック ACL 更新動作は、**hardware access-list update default-result permit** CLI コマンドを使用して制御できます。この CLI は、物理ポートに対してのみ機能します。次の例を参照してください。

```
hardware access-list update default-result permit      => #Allows all the traffic
during ACL updates. There may be < 10secs traffic drop.
no hardware access-list update default-result permit  => #This is the default
behavior. It denies all the traffic during ACL updates.
```

- Cisco NX-OS リリース 9.2(2) 以前のリリースでは、アトミック ACL 更新は Cisco Nexus -R シリーズ ライン カードではサポートされていませんが、非アトミック更新 **hardware access-list update default-result** が Cisco Nexus -R シリーズ ライン カードでサポートされます。

TCAM リージョンの分割

システム ACL を設定する前に、まず TCAM リージョンを分割します。1k 未満の ACL を設定する場合は、TCAM リージョンを分割する必要がないことに注意してください。詳細については、「[ACL TCAM リージョン サイズの設定 \(397 ページ\)](#)」を参照してください。



(注) Cisco NX-OS リリース 7.0(3)F3(4) 以降では、PACL IPv4、RACL IPv4、および RACL IPv6 を 12k を超えて設定できます。

システム ACL の設定

IPv4 ACL を作成したら、システム ACL を設定します。

始める前に

デバイスで IPv4 ACL を作成します。詳細については、「[IP ACL の作成 \(390 ページ\)](#)」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	<code>config t</code>	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	<code>system acl</code>	システム ACL を設定します。
ステップ 3	<code>ip port access-group <pacl name> in</code>	インターフェイスにレイヤ 2 PACL を適用します。ポート ACL では、インバウンドフィルタリングだけがサポートされています。1つのインターフェイスに1つのポート ACL を適用できます。

システム ACL の設定および show コマンドの例

システム ACL の show コマンドについては、次の設定例を参照してください。

1K スケールのシステム PACL の設定（デフォルト TCAM を使用）

1K スケールのシステム PACL の設定については、次の例を参照してください（デフォルト TCAM を使用）。

ステップ 1 : PACL を作成します。

```
config t
ip access-list PACL-DNA
```

```

10 permit ip 1.1.1.1/32 any
20 permit tcp 3.0.0.0/8 255.0.0.0 eq 1500
25 deny udp any any eq 500
26 deny tcp any eq 490 any
... ..
1000 deny any any

```

ステップ 2 : PACL をシステム レベルに適用します。

```

configuration terminal
system acl
  ip port access-group PACL-DNA in

```

スイッチに設定されているシステム ACLを検証するには、**sh run aclmgr | sec system** コマンドを使用します。

```

switch# sh run aclmgr | sec system
system acl
  ip port access-group test in
switch#

```

スイッチに設定されている PACL を検証するには、**sh ip access-lists <name> [summary]** コマンドを使用します。

```

switch# sh ip access-lists test

IP access list test
 10 deny udp any any eq 27
 20 permit ip 1.1.1.1/32 100.100.100.100/32
 30 permit ip 1.2.1.1/32 100.100.100.100/32
 40 permit ip 1.3.1.1/32 100.100.100.100/32
 50 permit ip 1.4.1.1/32 100.100.100.100/32
 60 permit ip 1.5.1.1/32 100.100.100.100/32
 70 permit ip 1.6.1.1/32 100.100.100.100/32
 80 permit ip 1.7.1.1/32 100.100.100.100/32
 90 permit ip 1.8.1.1/32 100.100.100.100/32

switch# sh ip access-lists test summary
IPV4 ACL test
Total ACEs Configured: 12279
Configured on interfaces:
Active on interfaces:
  - ingress
  - ingress

switch#

```

PACL IPv4 (ifacl) TCAMリージョン サイズを検証するには、**show hardware access-list tcam region** コマンドを使用します。

```

switch# show hardware access-list tcam region
*****WARNING*****
*****The output shows NFE tcam region info*****
***Please refer to 'show hardware access-list tcam template' for NFE2***
*****

```

```

        IPV4 PACL [ifacl] size = 12280
        IPV6 PACL [ipv6-ifacl] size = 0
        MAC PACL [mac-ifacl] size = 0
        IPV4 Port QoS [qos] size = 640
        IPV6 Port QoS [ipv6-qos] size = 256
        MAC Port QoS [mac-qos] size = 0
        FEX IPV4 PACL [fex-ifacl] size = 0
        FEX IPV6 PACL [fex-ipv6-ifacl] size = 0
        FEX MAC PACL [fex-mac-ifacl] size = 0
        FEX IPV4 Port QoS [fex-qos] size = 0
        FEX IPV6 Port QoS [fex-ipv6-qos] size = 0
        FEX MAC Port QoS [fex-mac-qos] size = 0
        IPV4 VACL [vacl] size = 0
        IPV6 VACL [ipv6-vacl] size = 0
        MAC VACL [mac-vacl] size = 0
        IPV4 VLAN QoS [vqos] size = 0
        IPV6 VLAN QoS [ipv6-vqos] size = 0
        MAC VLAN QoS [mac-vqos] size = 0
        IPV4 RACL [racl] size = 0
        IPV6 RACL [ipv6-racl] size = 128
        IPV4 Port QoS Lite [qos-lite] size = 0
        FEX IPV4 Port QoS Lite [fex-qos-lite] size = 0
        IPV4 VLAN QoS Lite [vqos-lite] size = 0
        IPV4 L3 QoS Lite [l3qos-lite] size = 0
        Egress IPV4 QoS [e-qos] size = 0
        Egress IPV6 QoS [e-ipv6-qos] size = 0
        Egress MAC QoS [e-mac-qos] size = 0
        Egress IPV4 VACL [vacl] size = 0
        Egress IPV6 VACL [ipv6-vacl] size = 0
        Egress MAC VACL [mac-vacl] size = 0
        Egress IPV4 RACL [e-racl] size = 0
        Egress IPV6 RACL [e-ipv6-racl] size = 0
        Egress IPV4 QoS Lite [e-qos-lite] size = 0
        IPV4 L3 QoS [l3qos] size = 640
        IPV6 L3 QoS [ipv6-l3qos] size = 256
        MAC L3 QoS [mac-l3qos] size = 0
        Ingress System size = 0
        Egress System size = 0
        SPAN [span] size = 96
        Ingress COPP [copp] size = 128
        Ingress Flow Counters [flow] size = 0
switch#

```

ACL 関連のテクニカル サポート情報を表示するには、**show tech-support aclmgr** および **show tech-support aclqos** コマンドを使用します。

```

show tech-support aclmgr
show tech-support aclqos

```

オブジェクト グループの設定

IPv4 ACL および IPv6 ACL のルールに送信元と宛先のアドレスおよびプロトコル ポートを指定する際に、オブジェクト グループを使用できます。

オブジェクト グループに対する Session Manager のサポート

Session Manager はオブジェクト グループの設定をサポートしています。この機能を使用すると、設定セッションを作成し、オブジェクトグループの設定変更を実行コンフィギュレーションにコミットする前に確認できます。Session Manager の詳細については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

IPv4 アドレス オブジェクト グループの作成および変更

IPv4 アドレス グループ オブジェクトの作成および変更を実行できます。



Note Cisco Nexus リリース 7.0(3)I5(2) 以降では、**no host IPv4-address** コマンドはサポートされていません。DME サポートでは、**no sequence** コマンドを使用しない削除はサポートされていません。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	object-group ip address name Example: <pre>switch(config)# object-group ip address ipv4-addr-group-13 switch(config-ipaddr-ogroup)#</pre>	IPv4 アドレス オブジェクト グループを作成し、IPv4 アドレス オブジェクトグループ コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかのコマンドを入力します。 • [sequence-number] host IPv4-address • [sequence-number] IPv4-address/prefix-len • [sequence-number] IPv4-address network-wildcard Example: <pre>switch(config-ipaddr-ogroup)# host 10.99.32.6</pre>	オブジェクト グループのエントリを作成します。作成するエントリごとに、 host コマンドを使用して単一のホストを指定するか、または host コマンドを省略してホストのネットワークを指定します。 IPv4 オブジェクトグループのプレフィックス長を指定できます。これは、最初の連続ビットでのみ一致します。または、アドレスの任意のビットで一致するワイルドカードマスクを指定できます。
ステップ 4	次のいずれかのコマンドを入力します。 • no [sequence-number]	オブジェクト グループのエントリを削除します。オブジェクト グループから

	Command or Action	Purpose
	• no host IPv4-address • no IPv4-address/prefix-len • no IPv4-address network-wildcard Example: <pre>switch(config-ipaddr-ogroup)# no host 10.99.32.6</pre>	削除するエントリごとに、 no 形式の host コマンドを使用します。
ステップ 5	(Optional) show object-group name Example: <pre>switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13</pre>	オブジェクト グループの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config-ipaddr-ogroup)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IPv6 アドレス オブジェクト グループの作成および変更

IPv6 アドレス グループ オブジェクトの作成および変更を実行できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	object-group ipv6 address name Example: <pre>switch(config)# object-group ipv6 address ipv6-addr-group-A7 switch(config-ipv6addr-ogroup)#</pre>	IPv6 アドレス オブジェクト グループを作成し、IPv6 アドレス オブジェクト 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 3	次のいずれかのコマンドを入力します。 • [sequence-number] host IPv6-address • [sequence-number] IPv6-address/prefix-len • [sequence-number] IPv6-address network-wildcard Example:	オブジェクト グループのエントリを作成します。作成するエントリごとに、host コマンドを使用して単一のホストを指定するか、または host コマンドを省略してホストのネットワークを指定します。 IPv6 オブジェクト グループのプレフィックス長を指定できます。これは、最初の

	Command or Action	Purpose
	<pre>switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1</pre> Example: <pre>switch(config-ipv6addr-ogroup)# 10 1::1 2::2</pre>	連続ビットでのみ一致します。の Cisco NX-OS リリース 7.0(3)I7(3)以降でサポートされます。または、アドレスの任意のビットとマッチするワイルドカードを指定できます。IPv6 ワイルドカードマスクは、Cisco Nexus 9300-FX/FX2/FXP スイッチでサポートされます。
ステップ 4	次のいずれかのコマンドを入力します。 • no sequence-number • no host IPv6-address • no IPv6-address/prefix-len • no IPv6-address network-wildcard Example: <pre>switch(config-ipv6addr-ogroup)# no host 2001:db8:0:3ab0::1</pre>	オブジェクト グループからエントリを削除します。オブジェクト グループから削除するエントリごとに、 no 形式の host コマンドを使用します。
ステップ 5	(Optional) show object-group name Example: <pre>switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7</pre>	オブジェクト グループの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config-ipv6addr-ogroup)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

プロトコル ポート オブジェクト グループの作成および変更

プロトコル ポート オブジェクト グループの作成および変更を実行できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	object-group ip port name Example:	プロトコル ポート オブジェクト グループを作成し、ポート オブジェクト グループ コンフィギュレーション モードを開始します。

	Command or Action	Purpose
	switch(config)# object-group ip port NYC-datacenter-ports switch(config-port-ogroup)#	
ステップ 3	[sequence-number] operator port-number [port-number] Example: <pre>switch(config-port-ogroup)# eq 80</pre>	オブジェクト グループのエントリを作成します。作成するエントリごとに、次の演算子コマンドを 1 つ使用します。 • eq : 指定したポート番号に一致します。 • gt : 指定したポート番号より大きい (等しいものは含まない) ポート番号に一致します。 • lt : 指定したポート番号より小さい (等しいものは含まない) ポート番号に一致します。 • neq : 指定したポート番号以外のすべてのポート番号に一致します。 • range : 指定した 2 つのポート番号と、その間の範囲のポート番号に一致します。 Note range コマンドだけは、2 つの <i>port-number</i> 引数を必要とします。
ステップ 4	no {sequence-number operator port-number [port-number]} Example: <pre>switch(config-port-ogroup)# no eq 80</pre>	オブジェクト グループからエントリを削除します。削除するエントリごとに、該当する演算子コマンドを no 形式で使
ステップ 5	(Optional) show object-group name Example: <pre>switch(config-port-ogroup)# show object-group NYC-datacenter-ports</pre>	オブジェクト グループの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config-port-ogroup)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

オブジェクト グループの削除

IPv4 アドレス オブジェクト グループ、IPv6 アドレス オブジェクト グループ、またはプロトコル ポート オブジェクト グループを削除できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 object-group {ip address ipv6 address ip port} name Example: <pre>switch(config)# no object-group ip address ipv4-addr-group-A7</pre>	指定のオブジェクト グループを削除します。
ステップ 3	(Optional) show object-group Example: <pre>switch(config)# show object-group</pre>	すべてのオブジェクト グループを表示します。削除されたオブジェクトグループは表示されません。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

オブジェクト グループの設定の確認

オブジェクト グループの設定情報を表示するには、次のいずれかのコマンドを使用します。

コマンド	目的
show object-group	オブジェクト グループの設定を表示します。
show {ip ipv6} access-lists name [expanded]	ACL設定の拡張統計情報を表示します。
show running-config aclmgr	オブジェクト グループを含めて、ACL の設定を表示します。

時間範囲の設定

時間範囲の Session Manager サポート

Session Manager は時間範囲の設定をサポートしています。この機能を使用すると、設定セッションを作成し、時間範囲の設定変更を実行コンフィギュレーションにコミットする前に確認できます。Session Manager の詳細については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

時間範囲の作成

デバイス上で時間範囲を作成し、これにルールを追加できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル構成モードを開始します。
ステップ 2	time-range name Example: switch(config)# time-range workday-daytime switch(config-time-range)#	時間範囲を作成し、時間範囲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	(Optional) [sequence-number] periodic weekday time to [weekday] time Example: switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59	指定開始日時と終了日時の間（両端を含める）の 1 日以上連続した曜日だけ有効になるような定期ルールを作成します。
ステップ 4	(Optional) [sequence-number] periodic list-of-weekdays time to time Example: switch(config-time-range)# periodic weekdays 06:00:00 to 20:00:00	<i>list-of-weekdays</i> 引数で指定された曜日の、指定開始時刻と終了時刻の間（両端を含む）だけ有効になるような定期ルールを作成します。 <i>list-of-weekdays</i> 引数の値には次のキーワードも使用できます。 • daily : 1 週間のすべての曜日 • weekdays : 月曜日から金曜日まで • weekend : 土曜日から日曜日まで

	Command or Action	Purpose
ステップ 5	(Optional) <i>[sequence-number]</i> absolute start <i>time date</i> [end <i>time date</i>] Example: <pre>switch(config-time-range) # absolute start 1:00 15 march 2013</pre>	start キーワードの後ろに指定した日時から有効になる絶対基準でのルールを作成します。 end キーワードを省略した場合、そのルールは開始日時を過ぎると常に有効になります。
ステップ 6	(Optional) <i>[sequence-number]</i> absolute [start <i>time date</i>] end <i>time date</i> Example: <pre>switch(config-time-range) # absolute end 23:59:59 31 may 2013</pre>	end キーワードの後ろに指定した日時まで有効になる絶対基準でのルールを作成します。 start キーワードを省略すると、そのルールは終了日時を過ぎるまでずっと有効です。
ステップ 7	(Optional) show time-range <i>name</i> Example: <pre>switch(config-time-range) # show time-range workday-daytime</pre>	時間範囲の設定を表示します。
ステップ 8	(Optional) copy running-config startup-config Example: <pre>switch(config-time-range) # copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

時間範囲の変更

既存の時間範囲のルールの追加および削除を実行できます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	time-range <i>name</i> Example: <pre>switch(config)# time-range workday-daytime switch(config-time-range)#</pre>	特定の時間範囲の時間範囲コンフィギュレーションモードを開始します。

	Command or Action	Purpose
ステップ 3	(Optional) [sequence-number] periodic weekday time to [weekday] time Example: <pre>switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59</pre>	指定開始日時と終了日時の間（両端を含める）の 1 日以上連続した曜日だけ有効になるような定期ルールを作成します。
ステップ 4	(Optional) [sequence-number] periodic list-of-weekdays time to time Example: <pre>switch(config-time-range)# 100 periodic weekdays 05:00:00 to 22:00:00</pre>	<i>list-of-weekdays</i> 引数で指定された曜日の、指定開始時刻と終了時刻の間（両端を含む）だけ有効になるような定期ルールを作成します。 <i>list-of-weekdays</i> 引数の値には次のキーワードも使用できます。 • daily : 1 週間のすべての曜日 • weekdays : 月曜日から金曜日まで • weekend : 土曜日から日曜日まで
ステップ 5	(Optional) [sequence-number] absolute start time date [end time date] Example: <pre>switch(config-time-range)# absolute start 1:00 15 march 2013</pre>	start キーワードの後ろに指定した日時から有効になる絶対基準でのルールを作成します。 end キーワードを省略した場合、そのルールは開始日時を過ぎると常に有効になります。
ステップ 6	(Optional) [sequence-number] absolute [start time date] end time date Example: <pre>switch(config-time-range)# absolute end 23:59:59 31 may 2013</pre>	end キーワードの後ろに指定した日時まで有効になる絶対基準でのルールを作成します。 start キーワードを省略すると、そのルールは終了日時を過ぎるまでずっと有効です。
ステップ 7	(Optional) no {sequence-number periodic arguments . . . absolute arguments. . . } Example: <pre>switch(config-time-range)# no 80</pre>	時間範囲から特定のルールを削除します。
ステップ 8	(Optional) show time-range name Example: <pre>switch(config-time-range)# show time-range workday-daytime</pre>	時間範囲の設定を表示します。
ステップ 9	(Optional) copy running-config startup-config Example: <pre>switch(config-time-range)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[時間範囲のシーケンス番号の変更](#) (448 ページ)

時間範囲の削除

デバイスから時間範囲を削除できます。

Before you begin

その時間範囲が ACL ルールのいずれかに使用されているかどうかを確認します。削除できるのは、ACL ルールに使用されている時間範囲です。ACL ルールに使用されている時間範囲を削除しても、その ACL が適用されているインターフェイスの設定には影響しません。デバイスは削除された時間範囲を使用する ACL ルールを空であると見なします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル構成モードを開始します。
ステップ 2	no time-range name Example: switch(config)# no time-range daily-workhours	名前を指定した時間範囲を削除します。
ステップ 3	(Optional) show time-range Example: switch(config-time-range)# show time-range	すべての時間範囲の設定を表示します。 削除された時間範囲は表示されません。
ステップ 4	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲のシーケンス番号の変更

時間範囲のルールに割り当てられているすべてのシーケンス番号を変更できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	resequence time-range name starting-sequence-number increment Example: switch(config)# resequence time-range daily-workhours 100 10 switch(config)#	時間範囲のルールにシーケンス番号を割り当てます。指定した開始シーケンス番号は最初のルールに割り当てられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。
ステップ 3	(Optional) show time-range name Example: switch(config)# show time-range daily-workhours	時間範囲の設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲設定の確認

時間範囲の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show time-range	時間範囲の設定を表示します。
show running-config aclmgr	すべての時間範囲を含めて、ACL の設定を表示します。

IP ACL に関する追加情報

関連資料

関連項目	マニュアル タイトル
TAP アグリゲーション	『Configuring TAP Aggregation and MPLS Stripping』



第 13 章

MAC ACL の設定

この章では、Cisco NX-OS デバイスの MAC アクセス コントロール リスト (ACL) を設定する手順について説明します。

この章は、次の項で構成されています。

- [MAC ACL について, on page 451](#)
- [MAC ACL の注意事項と制約事項 \(452 ページ\)](#)
- [MAC ACL のデフォルト設定, on page 453](#)
- [MAC ACL の設定, on page 453](#)
- [MAC ACL の設定の確認, on page 463](#)
- [MAC ACL の統計情報のモニタリングとクリア, on page 464](#)
- [MAC ACL の設定例, on page 464](#)
- [MAC ACL に関する追加情報, on page 464](#)

MAC ACL について

MAC ACL は、パケットのレイヤ 2 ヘッダーを使用してトラフィックをフィルタリングする ACL です。バーチャライゼーションのサポートなど、MAC ACL の基本的な機能の多くは IP ACL と共通です。

MAC パケット分類

MAC パケット分類により、レイヤ 2 インターフェイス上の MAC ACL を、IP トラフィックなどインターフェイスに入るすべてのトラフィックに適用するか、非 IP トラフィックだけに適用するかを制御できます。

MAC パケット分類の状態	インターフェイスでの効果
イネーブル	• インターフェイス上の MAC ACL は、IP トラフィックなどインターフェイスに入るすべてのトラフィックに適用されます。 • IP ポート ACL をインターフェイスで適用できません。

MAC パケット分類の状態	インターフェイスでの効果
ディセーブル	• インターフェイス上の MAC ACL は、インターフェイスに入る非 IP トラフィックだけに適用されます。 • IP ポート ACL をインターフェイスで適用できます。

MAC ACL の注意事項と制約事項

MAC ACL の設定に関する注意事項と制約事項は次のとおりです。

- MAC ACL は入トラフィックだけに適用されます。
- 適用する ACL エントリが多すぎると、設定が拒否される可能性があります。
- MAC ACL が VACL の一部として適用される場合、MAC パケット分類はサポートされません。
- MAC ACL が Cisco Nexus 9300 シリーズ スイッチ 40G アップリンク ポートの QoS ポリシーの一致基準として使用されている場合、MAC パケット分類はサポートされません。
- **mac address-table limit <16-256> user-defined** コマンドを使用してユーザ定義の MAC 制限を設定すると、FHRP グループ制限が自動的に調整され、ユーザ定義の MAC 制限と FHRP 制限の合計は 490 になります。たとえば、ユーザ定義の MAC 制限を 100 に設定すると、FHRP 制限は 390 に減少します。
- Cisco NX-OS リリース 9.3(2) 以降では、ユーザ定義の MAC アドレス制限を 16 ～ 256 の範囲で設定できます。
- Cisco Nexus 93600CD-GX スイッチは、ポート 1/1-24 でのブレイクアウトをサポートしていません。
- インターフェイスに適用される MAC アクセス リストは、スパニング ツリー プロトコル BPDU などのブリッジ プロトコル データ ユニット (BPDU) トラフィックをブロックしません。
- Cisco NX-OS リリース 10.4(1)F 以降では、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2、および X97160YC-EX, 9700-/FX/GX ライン カードを搭載した Cisco Nexus 9500 で、SUP ルールに対する MAC ACL ルールの優先順位を適用するために、新しい ACE キーワード (all) が提供されています。

MAC ACL のデフォルト設定

次の表に、MAC ACL パラメータのデフォルト設定を示します。

Table 30: MAC ACL のデフォルトパラメータ

パラメータ	デフォルト
MAC ACL	デフォルトでは MAC ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。

MAC ACL の設定

MAC ACL の作成

MAC ACL を作成し、これにルールを追加できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル構成モードを開始します。
ステップ 2	mac access-list name Example: switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#	MAC ACL を作成して、ACL コンフィギュレーション モードを開始します。 Notice ダイナミック、 expanded 、および summary という名前は、システム定義のアクセスリスト用に予約済み。構成の表示または確認に競合が生じる可能性があるため、ユーザー定義の ACL にはこれらの名前を使用しないでください。
ステップ 3	{permit deny} source destination-protocol Example: switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806	MAC ACL 内にルールを作成します。 permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。

	Command or Action	Purpose
ステップ 4	(Optional) statistics per-entry Example: switch(config-mac-acl)# statistics per-entry	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。
ステップ 5	(Optional) show mac access-lists name Example: switch(config-mac-acl)# show mac access-lists acl-mac-01	MAC ACL の設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch(config-mac-acl)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

UDF ベースの MAC ACL の設定

Cisco Nexus9300 シリーズ スイッチの UDF ベースの MAC アクセスリスト (ACL) を設定できます。この機能により、デバイスはユーザ定義フィールド (UDF) で照合し、一致するパケットを MAC ACL に適用できます。

Cisco NX-OS リリース 9.3(3) 以降、Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチで UDF ベース MAC アクセスリスト (ACL) を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	udf udf-name offset-base offset length 例 : switch(config)# udf pkttoff10 packet-start 10 2	次のように UDF を定義します。 • udf-name : UDF の名前を指定します。名前には最大 16 文字の英数字を入力できます。 • offset-base : UDF オフセットベースを {packet-start} のように指定します。

	コマンドまたはアクション	目的
		• オフセット：オフセットベースからバイトオフセットの数を指定します。 • 長さ：オフセットからバイトの数を指定します。1 または 2 バイトのみがサポートされています。追加のバイトに一致させるためには、複数の UDF を定義する必要があります。 複数の UDF を定義できますが、シスコは必要な UDF のみ定義することを推奨します。
ステップ 3	hardware access-list tcam region ing-ifac1 qualify {udf udf-name } 例 : <pre>switch(config)# hardware access-list tcam region ing-ifac1 qualify udf pktoff10</pre>	IPv4 または IPv6 ポート ACL に適用する ing-ifac1 TCAM リージョンに UDF をアタッチします。 最大 18 個の UDF がサポートされます。 (注) UDF 修飾子が追加されると、TCAM リージョンはシングル幅から倍幅に拡大します。十分な空きスペースがあることを確認してください。それ以外の場合このコマンドは拒否されます。必要な場合、未使用のリージョンから TCAM スペースが減りますので、このコマンドを再入力します。詳細については、「ACL TCAM リージョンサイズの設定」を参照してください。 (注) このコマンドの no 形式は、UDF を TCAM リージョンから切り離し、リージョンをシングル幅に戻します。
ステップ 4	必須: copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 5	必須: reload	デバイスがリロードされます。

	コマンドまたはアクション	目的
	例 : <pre>switch(config)# reload</pre>	(注) UDF 設定は copy running-config startup-config+reload を入力した後のみ有効になります。
ステップ 6	mac access-list udf-acl 例 : <pre>switch(config)# mac access-list udfacl switch(config-acl)#</pre>	MAC アクセス コントロール リスト (ACL) を作成して、MAC ACL 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	permit mac source destination udf udf-name value mask 例 : <pre>switch(config-acl)# permit mac any any udf pktofff10 0x1234 0xffff</pre>	MAC ACL を設定して、外部パケットフィールドについて現在のアクセスコントロールエントリ (ACE) と併せて UDF で一致させるように設定します (例 2)。値とマスクの引数の範囲は 0x0~0xFFFF です。 シングル ACL は、UDF がある場合とない場合の両方とも、ACE を有することができます。各 ACE には一致する異なる UDF フィールドがあるか、すべての ACE を UDF の同じリストに一致させることができます。
ステップ 8	interface port-channel channel-number 例 : <pre>switch(config)# interface port-channel 5 switch(config-if)#</pre>	レイヤ 2 のポート チャネル インターフェイスの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 9	mac port access-group udf-access-list 例 : <pre>switch(config-if)# mac port access-group udf-acl-01</pre>	UDF ベース MAC ACL をインターフェイスに適用します。
ステップ 10	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

MAC ACL の変更

MAC ACL をデバイスから削除できます。

Before you begin

MAC ACL が設定されているインターフェイスを探すには、**show mac access-lists** コマンドを、**summary** キーワードを指定して実行します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	mac access-list name Example: <pre>switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#</pre>	名前で指定した ACL の ACL 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	(Optional) [sequence-number] {permit deny} source destination-protocol Example: <pre>switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806</pre>	MAC ACL 内にルールを作成します。 シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。 permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	(Optional) no {sequence-number {permit deny} source destination-protocol} Example: <pre>switch(config-mac-acl)# no 80</pre>	指定したルールを MAC ACL から削除します。 permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 5	(Optional) [no] statistics per-entry Example: <pre>switch(config-mac-acl)# statistics per-entry</pre>	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 no オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 6	(Optional) show mac access-lists name Example: <pre>switch(config-mac-acl)# show mac access-lists acl-mac-01</pre>	MAC ACL の設定を表示します。

	Command or Action	Purpose
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config-mac-acl)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC ACL 内のシーケンス番号の変更

MAC ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。ACL にルールを挿入する必要がある場合で、シーケンス番号が不足しているときは、再割り当てすると便利です。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	resequence mac access-list name starting-sequence-number increment Example: <pre>switch(config)# resequence mac access-list acl-mac-01 100 10</pre>	ACL 内に記述されているルールにシーケンス番号を付けます。starting-sequence number に指定したシーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。
ステップ 3	(Optional) show mac access-lists name Example: <pre>switch(config)# show mac access-lists acl-mac-01</pre>	MAC ACL の設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC ACL の削除

MAC ACL をデバイスから削除できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル構成モードを開始します。
ステップ 2	no mac access-list name Example: switch(config)# no mac access-list acl-mac-01 switch(config)#	名前で指定した MAC ACL を実行コンフィギュレーションから削除します。
ステップ 3	(Optional) show mac access-lists name summary Example: switch(config)# show mac access-lists acl-mac-01 summary	MAC ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ポート ACL としての MAC ACL の適用

MAC ACL をポート ACL として、次のいずれかのインターフェイス タイプに適用できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 ポート チャンネル インターフェイス

Before you begin

適用する ACL が存在し、必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル構成モードを開始します。

	Command or Action	Purpose
ステップ 2	次のいずれかのコマンドを入力します。 • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> Example: <pre>switch(config)# interface port-channel 5 switch(config-if)#</pre>	• レイヤ2またはレイヤ3のインターフェイス コンフィギュレーション モードを開始します。 • レイヤ2またはレイヤ3のポートチャネル インターフェイスの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	mac port access-group <i>access-list</i> Example: <pre>switch(config-if)# mac port access-group acl-01</pre>	MAC ACL をインターフェイスに適用します。
ステップ 4	(Optional) show running-config aclmgr Example: <pre>switch(config-if)# show running-config aclmgr</pre>	ACL の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

MAC ACL の VACL としての適用

MAC ACL を VACL として適用できます。

MAC パケット分類のイネーブル化または無効化

レイヤ2 インターフェイスに対して MAC パケット分類を有効または無効に設定できます。

始める前に

インターフェイスを、レイヤ2 インターフェイスとして設定する必要があります。



- (注) インターフェイスが **ip port access-group** コマンドまたは **ipv6 port traffic-filter** コマンドを使用して設定されている場合は、インターフェイス コンフィギュレーションから **ip port access-group** コマンドおよび **ipv6 port traffic-filter** コマンドを削除しない限り、MAC パケット分類を有効にできません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • interface ethernet slot/port • interface port-channel channel-number 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> 例 : <pre>switch(config)# interface port-channel 5 switch(config-if)#</pre>	• イーサネット インターフェイスに対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。 • ポート チャネル インターフェイスのインターフェイス 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] mac packet-classify 例 : <pre>switch(config-if)# mac packet-classify</pre>	インターフェイスの MAC パケット分類を有効にします。 no オプションを使用すると、インターフェイスの MAC パケット分類が無効になります。
ステップ 4	(任意) 次のいずれかのコマンドを入力します。 • show running-config interface ethernet slot/port • show running-config interface port-channel channel-number 例 : <pre>switch(config-if)# show running-config interface ethernet 2/1</pre> 例 : <pre>switch(config-if)# show running-config interface port-channel 5</pre>	• イーサネット インターフェイスの実行コンフィギュレーションを表示します。 • ポート チャネル インターフェイスの実行コンフィギュレーションを表示します。

	コマンドまたはアクション	目的
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SUP ルールに対する MAC ACL ルールの優先順位付けの適用

Cisco NX-OS リリース 10.4(1)F 以降では、MAC ACL で新しい ACE キーワード (**all**) がサポートされています。これにより、同じ条件で一致する他の SUP ACL ルールよりも ACL ルールの優先順位が上がり、0 (最高) になります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal</pre>	グローバル構成モードを開始します。
ステップ 2	mac access-list name 例 : <pre>switch(config)# mac access-list acl-mac-01 switch(config-acl)#</pre>	MAC ACL を作成して、ACL 構成モードを開始します。 <i>name</i> 引数は 64 文字以内で指定します。
ステップ 3	{permit deny} source destination-protocol all 例 : <pre>switch(config-mac-acl)# 100 permit 00c0.4f00.0000 0000.00ff.ffff any all</pre>	SUP ルールよりも MAC ACL ルールを優先する all キーワードを使用して、MAC ACL にルールを作成します。
ステップ 4	次のいずれかのコマンドを入力します。 interface ethernet slot/port interface port-channel channel-number 例 : <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	指定したインターフェイス タイプの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	mac port access-group access-list in 例 : <pre>switch(config-if)# mac port access-group acl-mac-01 in</pre>	MAC ACL をインターフェイスまたはポート チャネルに適用します。ポート ACL では、インバウンドフィルタリングだけがサポートされています。1つの

	コマンドまたはアクション	目的
		インターフェイスに 1 つのポート ACL を適用できます。
ステップ 6	(任意) show running-config aclmgr 例 : switch(config-if)# show running-config aclmgr	ACL の設定を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : switch(config-if)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC ACL の設定の確認

MAC ACL 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。
show running-config aclmgr [all]	MAC ACL および MAC ACL が適用されるインターフェイスを含めて、ACL の設定を表示します。 Note このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。 all オプションを使用すると、実行コンフィギュレーションのデフォルト (CoPP 設定) とユーザ定義による ACL の両方が表示されます。
show startup-config aclmgr [all]	ACL のスタートアップ コンフィギュレーションを表示します。 Note このコマンドは、スタートアップ コンフィギュレーションのユーザ設定 ACL を表示します。 all オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト (CoPP 設定) とユーザ定義による ACL の両方が表示されます。

MAC ACL の統計情報のモニタリングとクリア

MAC ACL の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドのいずれかを使用します。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。MAC ACL に statistics per-entry コマンドが含まれている場合は、 show mac access-lists コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear mac access-list counters	MAC ACL の統計情報をクリアします。

MAC ACL の設定例

次に、acl-mac-01 という名前の MAC ACL を作成し、これをイーサネット インターフェイス 2/1（レイヤ 2 インターフェイス）に適用する例を示します。

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any 0x0806
interface ethernet 2/1
  mac port access-group acl-mac-01
```

MAC ACL に関する追加情報

関連資料

関連項目	マニュアル タイトル
TAP アグリゲーション	『Configuring TAP Aggregation and MPLS Stripping』



第 14 章

VLAN ACL の設定

この章では、Cisco NX-OS デバイスの VLAN ACL（アクセス リスト）の設定方法を説明します。

この章は、次の項で構成されています。

- [VLAN ACL について, on page 465](#)
- [VACL の前提条件, on page 466](#)
- [VACL の注意事項と制約事項 \(467 ページ\)](#)
- [VACL のデフォルト設定, on page 468](#)
- [VACL の設定, on page 468](#)
- [VACL 設定の確認, on page 471](#)
- [VACL 統計情報のモニタリングとクリア, on page 472](#)
- [VACL の設定例, on page 472](#)
- [VACL に関する追加情報, on page 472](#)

VLAN ACL について

VLAN ACL (VACL) は、MAC ACL または IP ACL の適用例の 1 つです。VACL を設定し、VLAN との間でルーティングされるかまたは VLAN 内でブリッジングされるすべてのパケットに適用できます。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。

VLAN アクセス マップとエントリ

VACL は、アクセス マップを使用して、1 つまたは複数のマップ エントリを順序化したリストを収容します。各マップ エントリは、IP または MAC ACL を処理に関連付けます。各エントリにはシーケンス番号が付き、これに基づいてエントリの優先度を管理できます。

デバイスがパケットに VACL を適用する際、パケットを許可する ACL を含む最初のアクセス マップ エントリで設定されている処理を適用します。

VACL とアクション

アクセス マップ コンフィギュレーション モードでは、**action** コマンドを使用して、次のいずれかのアクションを指定します。

Forward

デバイスの通常の動作によって決定された宛先にトラフィックを送信します。

Redirect

1 つまたは複数の指定インターフェイスにトラフィックをリダイレクトします。

Drop

トラフィックをドロップします。ドロップを処理として指定する場合、ドロップされたパケットのログをデバイスが記録するよう指定することもできます。

VACL の統計情報

VACL の各ルールのグローバル統計が維持されます。VACL を複数の VLAN に適用した場合、保持されるルール統計情報は、その VACL が適用されている各インターフェイス上で一致（ヒット）したパケットの総数になります。



(注) インターフェイスレベルの VACL 統計はサポートされていません。

設定する VLAN アクセス マップごとに、その VACL の統計情報を維持するかどうかを指定できます。この機能を使用すると、VACL によってフィルタリングされたトラフィックのモニタが必要かどうかに応じて、あるいは VLAN アクセスマップの設定のトラブルシューティングが必要かどうかに応じて、VACL 統計をオンまたはオフにできます。

VACL に対する Session Manager のサポート

Session Manager は VACL の設定をサポートしています。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。Session Manager の詳細については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

VACL の前提条件

VACL の前提条件は次のとおりです。

- VACL に使用する IP ACL または MAC ACL が存在し、必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。

VACL の注意事項と制約事項

VACL の設定に関する注意事項は次のとおりです。

- ACLは、セッションマネージャを使用して設定することを推奨します。この機能によって、ACLの設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。Session Managerの詳細については、『[Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#)』を参照してください。
- 適用する ACL エントリが多すぎると、設定が拒否される可能性があります。
- SPAN 宛先ポートへの VACL リダイレクトはサポートされません。
- VACL ロギングはサポートされていません。
- VACL が複数の VLAN に適用されている場合、TCAM リソースは共有されません。
- VACL は、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ライン カードを搭載した Cisco Nexus 9500 Series スイッチではサポートされていません。
- VACL では deny 文はサポートされていません。その代わりに、permit 文と「drop」アクションを組み合わせると、同様の結果を得ることができます。
- VACL を「redirect」オプションを使用して設定する場合、リダイレクトインターフェイスとして定義するインターフェイスは、この VACL の適用先である VLAN のメンバーとして設定する必要があります。リダイレクションを機能させるには、この VLAN がこのインターフェイス上でフォワーディング状態になっている必要があります。これらの条件が満たされない場合、スイッチは VACL とマッチしたパケットをドロップします。
- VACL カウンタをクリアするには、アクティブな VLAN フィルタが設定されていることを確認する必要があります。
- Cisco NX-OS リリース 10.1(2) 以降、VACL は N9K-X9624D-R2 および N9K-C9508-FM-R2 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(1q)F 以降、PTP は N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。

VXLAN の VACL には、次のガイドラインが適用されます。

- アクセスからネットワーク方向（レイヤ 2 からレイヤ 3 のカプセル化パス）においてアクセスで VXLAN VLAN で適用されている VACL は、内部ペイロードでサポートされます。
- アクセス側で VACL を使用して、オーバーレイ ネットワークに入るトラフィックを除外することを推奨します。
- カプセル化解除された VXLAN トラフィックの出力 VACL はサポートされません。

VACL のデフォルト設定

次の表に、VACL パラメータのデフォルト設定値を示します。

Table 31: VACL のデフォルト パラメータ

パラメータ	デフォルト
VACL	デフォルトでは IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。

VACL の設定

VACL の作成または VACL エントリの追加

VACL エントリを新規作成したり、既存の VACL にエントリを追加できます。どちらの場合も、作成した VACL エントリが、1 つまたは複数の ACL を一致トラフィックに適用される処理と関連付ける VLAN アクセス マップ エントリとなります。

Before you begin

VACL に使用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 map-name [sequence-number] Example: <pre>switch(config)# vlan access-map acl-mac-map switch(config-access-map)#</pre>	指定した VLAN アクセス マップの VLAN アクセス マップ コンフィギュレーションモードを開始します。VLAN アクセス マップが存在しない場合は、デバイスによって作成されます。 シーケンス番号を指定しなかった場合、デバイスによって新しいエントリが作成され、このシーケンス番号はアクセス

	Command or Action	Purpose
		マップの最後のシーケンス番号よりも 10 大きい番号となります。
ステップ 3	次のいずれかのコマンドを入力します。 • match {ip ipv6} address ip-access-list • match mac address mac-access-list Example: <pre>switch(config-access-map)# match mac address acl-ip-lab</pre> Example: <pre>switch(config-access-map)# match mac address acl-mac-01</pre>	アクセスマップエントリに ACL を指定します。
ステップ 4	action {drop forward redirect} Example: <pre>switch(config-access-map)# action forward</pre> Example: <pre>switch(config-access-map)# vlan access-map vac11 switch(config-access-map)# action redirect e1/1 switch(config-access-map)# action redirect po100</pre>	ACL に一致したトラフィックにデバイスが適用する処理を指定します。 action コマンドは、drop、forward、および redirect オプションをサポートします。
ステップ 5	(Optional) [no] statistics per-entry Example: <pre>switch(config-access-map)# statistics per-entry</pre>	その VACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 no オプションを使用すると、デバイスはその VACL のグローバル統計の維持を停止します。
ステップ 6	(Optional) show running-config aclmgr Example: <pre>switch(config-access-map)# show running-config aclmgr</pre>	ACL の設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config-access-map)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

VACL または VACL エントリの削除

VACL を削除できます。これにより、VLAN アクセス マップも削除されます。

また、VACL から単一の VLAN アクセス マップ エントリを削除することもできます。

Before you begin

その VACL が VLAN に適用されているかどうかを確認します。削除できるのは、現在適用されている VACL です。VACL を削除しても、その VACL が適用されていた VLAN の設定は影響を受けません。デバイスは削除された VACL を空であると見なします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 vlan access-map map-name [sequence-number] Example: <pre>switch(config)# no vlan access-map acl-mac-map 10</pre>	指定したアクセス マップの VLAN アクセス マップの設定を削除します。 <i>sequence-number</i> 引数を指定して、VACL に複数のエントリが含まれる場合、このコマンドにより指定したエントリだけが削除されます。
ステップ 3	(Optional) show running-config aclmgr Example: <pre>switch(config)# show running-config aclmgr</pre>	ACL の設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL の VLAN への適用

VACL を VLAN に適用できます。

Before you begin

VACL を適用する際には、その VACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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] vlan filter map-name vlan-list list Example: switch(config)# vlan filter acl-mac-map vlan-list 1-20,26-30 switch(config)#	指定したリストによって、VACL を VLAN に適用します。no オプションにより VACL を適用しません。
ステップ 3	(Optional) show running-config aclmgr Example: switch(config)# show running-config aclmgr	ACL の設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL 設定の確認

VACL 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show running-config aclmgr [all]	VACL-related の設定も含めて、ACL の設定を表示します。 Note このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。 all オプションを使用すると、実行コンフィギュレーションのデフォルト (CoPP 設定) とユーザ定義による ACL の両方が表示されます。
show startup-config aclmgr [all]	ACL のスタートアップ コンフィギュレーションを表示します。 Note このコマンドは、スタートアップ コンフィギュレーションのユーザ設定 ACL を表示します。 all オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト (CoPP 設定) とユーザ定義による ACL の両方が表示されます。

コマンド	目的
show vlan filter	VLAN に適用されている VACL の情報を表示します。
show vlan access-map	VLAN アクセス マップに関する情報を表示します。

VACL 統計情報のモニタリングとクリア

VACL の統計情報をモニタまたはクリアを行うには、次の表に示すコマンドのいずれかを使用します。

コマンド	目的
show vlan access-list	VACL の設定を表示します。VLAN アクセス マップに statistics per-entry コマンドが含まれている場合は、 show vlan access-list コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear vlan access-list counters	VACL の統計情報をクリアします。

VACL の設定例

次の例では、**acl-mac-01** という名前の MAC ACL で許可されたトラフィックを転送する VACL を設定し、その VACL を VLAN 50 ～ 82 に適用します。

```
conf t
vlan access-map acl-mac-map
  match mac address acl-mac-01
  action forward
vlan filter acl-mac-map vlan-list 50-82
```

VACL に関する追加情報

関連資料

関連項目	マニュアル タイトル
QoS の設定	『Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide』



第 15 章

ポート セキュリティの設定

この章では、Cisco NX-OS デバイスにポート セキュリティを設定する手順について説明します。

この章は、次の項で構成されています。

- [ポート セキュリティの概要, on page 473](#)
- [ポート セキュリティの前提条件, on page 481](#)
- [ポート セキュリティのデフォルト設定, on page 481](#)
- [ポート セキュリティの注意事項と制約事項, on page 481](#)
- [vPC 上のポート セキュリティの注意事項と制約事項 \(482 ページ\)](#)
- [ポート セキュリティの設定, on page 483](#)
- [ポート セキュリティの設定の確認, on page 494](#)
- [セキュア MAC アドレスの表示, on page 495](#)
- [ポート セキュリティの設定例, on page 495](#)
- [vPC ドメインでのポート セキュリティの設定例 \(495 ページ\)](#)
- [ポート セキュリティに関する追加情報, on page 496](#)
- [VXLAN EVPN のポート セキュリティ サポート \(497 ページ\)](#)

ポート セキュリティの概要

ポート セキュリティを使用すると、限定された MAC アドレス セットからの入力トラフィックだけを許可するようなレイヤ 2 物理インターフェイスおよびレイヤ 2 ポート チャネル インターフェイスを設定できます。この制限されたセット内の MAC アドレスは、セキュア MAC アドレスと呼ばれます。さらに、デバイスは、これらの MAC アドレスからのトラフィックでも、同じ VLAN 内の別のインターフェイスからの場合は許可しません。セキュア MAC アドレスの数は、インターフェイス単位で設定します。



Note

特に指定がなければ、インターフェイスは物理インターフェイスとポートチャネル インターフェイスの両方を意味します。同様に、レイヤ 2 インターフェイスはレイヤ 2 物理インターフェイスとレイヤ 2 ポート チャネル インターフェイスの両方を意味します。

セキュア MAC アドレスの学習

MAC アドレスは学習というプロセスによってセキュア アドレスになります。MAC アドレスは、1 つのインターフェイスだけでセキュア MAC アドレスになることができます。デバイスは、ポートセキュリティが有効に設定されたインターフェイスごとに、スタティックまたはダイナミック方式で、限られた数の MAC アドレスを学習できます。デバイスがセキュア MAC アドレスを格納する方法は、デバイスがセキュア MAC アドレスを学習した方法によって異なります。

スタティック方式

スタティック学習方式では、ユーザが手動でインターフェイスの実行コンフィギュレーションにセキュア MAC アドレスを追加したり、設定から削除したりできます。実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーすると、デバイスを再起動してもスタティック セキュア MAC アドレスには影響がありません。

スタティック セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- ユーザが明示的に設定からアドレスを削除した場合。
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合。

スタティック方式では、ダイナミック方式のアドレス学習がイネーブルになっているかどうかに関係なく、セキュア アドレスを追加できます。

ダイナミック方式

デフォルトでは、インターフェイスのポートセキュリティをイネーブルにすると、ダイナミック学習方式がイネーブルになります。この方式では、デバイスは、入力トラフィックがインターフェイスを通過するときに MAC アドレスをセキュア アドレスにします。アドレスがまだ保護されていず、デバイスが該当する最大値に達していない場合、デバイスはそのアドレスを保護し、トラフィックを許可します。

デバイスは、ダイナミック セキュア MAC アドレスをメモリに保存します。ダイナミック セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- デバイスが再起動した場合
- インターフェイスが再起動した場合
- アドレスが、ユーザによって設定されたインターフェイスのエージング期限に達した場合
- ユーザがアドレスを明示的に削除した場合
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合

スティッキ方式

スティッキ方式をイネーブルにすると、デバイスは、ダイナミックアドレス学習と同じ方法で MAC アドレスをセキュアアドレスにしますが、この方法で学習されたアドレスは NVRAM に保存されます。そのため、スティッキ方式で学習されたアドレスは、デバイスの再起動後も維持されます。スティッキセキュア MAC アドレスは、インターフェイスの実行コンフィギュレーション内にはありません。

ダイナミックとスティッキのアドレス学習は両方同時にイネーブルにできません。あるインターフェイスのスティッキ学習をイネーブルにした場合、デバイスはダイナミック学習を停止して、代わりにスティッキ学習を実行します。スティッキ学習をディセーブルにすると、デバイスはダイナミック学習を再開します。

スティッキセキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- ユーザがアドレスを明示的に削除した場合
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合

ダイナミック アドレスのエージング

デバイスは、ダイナミック方式で学習された MAC アドレスのエージングを行い、エージングの期限に達すると、アドレスをドロップします。エージングの期限は、インターフェイスごとに設定できます。有効な範囲は 0 ～ 1440 分です。0 を設定すると、エージングはディセーブルになります。

MAC アドレスのエージングを判断するためにデバイスが使用する方法も設定できます。アドレス エージングの判断には、次に示す 2 つの方法が使用されます。

Inactivity

適用可能なインターフェイス上のアドレスからデバイスが最後にパケットを受信して以降の経過時間。

絶対値 (Absolute)

デバイスがアドレスを学習して以降の経過時間。これがデフォルトのエージング方法ですが、デフォルトのエージング時間は 0 分（エージングはディセーブル）です。



Note

絶対エージングタイムを設定すると、送信元 MAC からのトラフィックが流れていても、MAC エージングが発生します。ただし、MAC エージングおよび再学習中に、一時的なトラフィック ドロップが発生する可能性があります。

セキュア MAC アドレスの最大数

デフォルトでは、各インターフェイスのセキュア MAC アドレスは 1 つだけです。各インターフェイス、またはインターフェイス上の各 VLAN に許容可能な最大 MAC アドレス数を設定できます。最大数は、スタティックまたはダイナミックに学習された MAC アドレスにも適用されます。



Tip アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、そのデバイスにはポートの全帯域幅が保証されます。

各インターフェイスに許容されるセキュア MAC アドレスの数は、次の 3 つの制限によって決定されます。

デバイスの最大数

デバイスが許容できるセキュア MAC アドレスの最大数は 8192 です。この値は変更できません。新しいアドレスを学習するとデバイスの最大数を超過してしまう場合、たとえインターフェイスや VLAN の最大数に達していなくても、デバイスは新しいアドレスの学習を許可しません。

インターフェイスの最大数

ポートセキュリティで保護されるインターフェイスごとに、セキュア MAC アドレスの最大数 1025 を設定できます。デフォルトでは、インターフェイスの最大アドレス数は 1 です。インターフェイスの最大数を、デバイスの最大数より大きくすることはできません。

VLAN の最大数

ポートセキュリティで保護される各インターフェイスについて、VLAN あたりのセキュア MAC アドレスの最大数を設定できます。VLAN の最大数は、インターフェイスに設定されている最大数より大きくできません。VLAN 最大数の設定が適しているのは、トランクポートの場合だけです。VLAN の最大数には、デフォルト値はありません。

インターフェイスあたりの、VLAN とインターフェイスの最大数は必要に応じて設定できます。ただし、新しい制限値が、適用可能なセキュアアドレス数よりも少ない場合は、まず、セキュア MAC アドレスの数を減らす必要があります。

セキュリティ違反と処理

次の 2 つのイベントのいずれかが発生すると、ポートセキュリティ機能によってセキュリティ違反がトリガーされます。

MAC 数違反

あるインターフェイスにセキュア MAC アドレス以外のアドレスから入力トラフィックが着信し、そのアドレスを学習するとセキュア MAC アドレスの適用可能な最大数を超過してしまう場合

あるインターフェイスに VLAN とインターフェイスの両方の最大数が設定されている場合は、どちらかの最大数を超えると、違反が発生します。たとえば、ポートセキュリティが設定されている単一のインターフェイスについて、次のように想定します。

- VLAN 1 の最大アドレス数は 5 です。
- このインターフェイスの最大アドレス数は 10 です。

デバイスは、次のいずれかが発生すると違反を検出します。

- デバイスが VLAN 1 のアドレスをすでに 5 つ学習していて、6 つめのアドレスからのインバウンドトラフィックが VLAN 1 のインターフェイスに着信した場合。
- このインターフェイス上のアドレスをすでに 10 個学習していて、11 番目のアドレスからのインバウンドトラフィックがこのインターフェイスに着信した場合。

デバイスが実行できる処理は次のとおりです。

シャットダウン

違反をトリガーしたパケットの受信インターフェイスをシャットダウンします。このインターフェイスはエラーディセーブル状態になります。これがデフォルトの処理です。インターフェイスの再起動後も、セキュア MAC アドレスを含めて、ポートセキュリティの設定は維持されます。

シャットダウン後にデバイスが自動的にインターフェイスを再起動するように設定するには、**errdisable** 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。あるいは、**shutdown** および **no shut down** のインターフェイス コンフィギュレーション コマンドを入力することにより、手動でインターフェイスを再起動することもできます。

制限

セキュア MAC アドレス以外のアドレスからの入力トラフィックをドロップします。

デバイスはドロップされたパケット数を保持しますが、これをセキュリティ違反回数と呼びます。インターフェイスで発生するセキュリティ違反が最大数に到達するまでアドレス学習を継続します。最初のセキュリティ違反のあとに学習されたアドレスからのトラフィックはドロップされます。

MAC 移動違反

あるインターフェイスのセキュア MAC アドレスになっているアドレスからの入力トラフィックが、そのインターフェイスと同じ VLAN 内の別のインターフェイスに着信した場合

レイヤ 2 転送モジュール (L2FM) のロギング レベルが 4 または 5 に増加した場合にのみ、MAC 移動通知が表示されます。

MAC 移動違反が発生すると、デバイスはインターフェイスのセキュリティ違反カウンタを増分し、設定された違反モードに関係なく、インターフェイスはエラーディセーブルになります。違反モードが[制限 (Restrict)]または[保護 (Protect)]に設定されている場合、違反はシステム ログに記録されます。

MAC移動違反は、設定された違反モードに関係なく、インターフェイスがエラーディセーブルになるため、**errdisable** コマンドを使用して自動 **errdisable** リカバリをイネーブルにすることを推奨します。

ポートセキュリティとポートタイプ

ポートセキュリティを設定できるのは、レイヤ2インターフェイスだけです。各種のインターフェイスまたはポートとポートセキュリティについて次に詳しく説明します。

アクセスポート

レイヤ2アクセスポートとして設定したインターフェイスにポートセキュリティを設定できます。アクセスポートでポートセキュリティが適用されるのは、アクセスVLANだけです。アクセスポートには、VLAN最大数を設定しても効果はありません。

トランクポート

レイヤ2トランクポートとして設定したインターフェイスにポートセキュリティを設定できます。デバイスがVLAN最大数を適用するのは、トランクポートに関連付けられたVLANだけです。

SPANポート

SPAN送信元ポートにはポートセキュリティを設定できますが、SPAN宛先ポートには設定できません。

イーサネットポートチャネル

レイヤ2イーサネットポートチャネルインターフェイスのポートセキュリティはアクセスモードまたはトランクモードで設定できます。



Note ポートセキュリティは、Cisco Nexus 9300-FX/FX2/FX3 シリーズスイッチ上の非 vPC 展開でのみ FEX インターフェイスに対してサポートされます。Cisco NX-OS リリース 9.3(5) 以降、Cisco Nexus 9300-FX3 シリーズスイッチがサポートされます。

ポートセキュリティとポートチャネルインターフェイス

ポートセキュリティは、レイヤ2ポートチャネルインターフェイスでサポートされます。ポートチャネルインターフェイス上で動作するポートセキュリティは、ここで説明する内容以外は、物理インターフェイスの場合と同じです。

一般的なガイドライン

ポートチャネルインターフェイスのポートセキュリティは、アクセスモードまたはトランクモードのいずれかで動作します。トランクモードでは、ポートセキュリティで適用されるMACアドレスの制限が、VLAN単位ですべてのメンバーポートに適用されます。

ポートチャネルインターフェイスのポートセキュリティを有効にしても、ポートチャネルのロードバランシングには影響しません。

ポートセキュリティは、ポート チャンネル インターフェイスを通過するポート チャンネル制御トラフィックには適用されません。ポートセキュリティを使用すると、セキュリティ違反にならないようにして、ポート チャンネル制御パケットを通過させることができます。ポート チャンネル制御トラフィックには、次のプロトコルが含まれます。

- ポート集約プロトコル (PAgP)
- リンク集約制御プロトコル (LACP)
- Inter-Switch Link (ISL)
- IEEE 802.1Q

セキュア メンバ ポートの設定

ポート チャンネル インターフェイスのポートセキュリティ設定は、メンバ ポートのポートセキュリティ設定には影響しません。

メンバ ポートの追加

セキュア インターフェイスをポート チャンネル インターフェイスのメンバ ポートとして追加した場合、デバイスはメンバ ポートで学習されたダイナミック セキュア アドレスをすべて廃棄しますが、メンバ ポートのその他のポートセキュリティ設定はすべて実行コンフィギュレーションに保持します。セキュア メンバ ポートで学習されたスティック方式とスタティック方式のセキュア MAC アドレスも、NVRAM ではなく実行コンフィギュレーションに保存されます。

ポートセキュリティがメンバ ポートでは有効になっていて、ポート チャンネル インターフェイスでは有効になっていない場合、メンバ ポートをポート チャンネル インターフェイスに追加しようとするすると警告されます。セキュア メンバ ポートをセキュア ポート チャンネル インターフェイス以外のインターフェイスに強制的に追加するには、**force** キーワードを指定して **channel-group** コマンドを使用します。

ポートがポート チャンネル インターフェイスのメンバである間は、メンバ ポートのポートセキュリティを設定できません。これを行うには、まずメンバ ポートをポート チャンネル インターフェイスから削除する必要があります。

メンバ ポートの削除

メンバ ポートをポート チャンネル インターフェイスから削除すると、メンバ ポートのポートセキュリティ設定が復元されます。ポート チャンネル インターフェイスに追加する前にそのポートで学習されたスタティック方式のセキュア MAC アドレスは、NVRAM に復元され、実行コンフィギュレーションからは削除されます。



(注) ポート チャンネル インターフェイスを削除したあとで、すべてのポートのセキュリティを必要に応じて確保するためには、すべてのメンバ ポートのポートセキュリティ設定を詳細に検査することを推奨します。

ポート チャネル インターフェイスの削除

セキュア ポート チャネル インターフェイスを削除すると、次の処理が行われます。

- ポート チャネル インターフェイスの学習されたセキュア MAC アドレスがすべて廃棄されます。これには、ポート チャネル インターフェイスで学習されたスタティック方式のセキュア MAC アドレスが含まれます。
- 各メンバ ポートのポート セキュリティ設定が復元されます。ポート チャネル インターフェイスに追加する前にそれらのメンバポートで学習されたスタティック方式のセキュア MAC アドレスは、NVRAM に復元され、実行コンフィギュレーションからは削除されます。ポート チャネル インターフェイスへの参加前にメンバポートでポート セキュリティが有効になっていなかった場合、そのメンバポートでは、ポート チャネル インターフェイスの削除後もポート セキュリティが有効になりません。



(注) ポート チャネル インターフェイスを削除したあとで、すべてのポートのセキュリティを必要に応じて確保するためには、すべてのメンバ ポートのポート セキュリティ設定を詳細に検査することを推奨します。

ポート セキュリティの無効化

いずれかのメンバポートでポート セキュリティが有効になっている場合、ポート チャネル インターフェイスのポート セキュリティを無効にできません。これを行うには、まずすべてのセキュア メンバポートをポート チャネル インターフェイスから削除します。メンバポートのポート セキュリティを無効にしたあと、必要に応じて、ポート チャネル インターフェイスに再度追加できます。

ポート タイプの変更

レイヤ2 インターフェイスにポート セキュリティを設定し、そのインターフェイスのポート タイプを変更した場合、デバイスは次のように動作します。

ポートからトランク ポートへのアクセス

レイヤ2 インターフェイスをアクセス ポートからトランク ポートに変更すると、デバイスはダイナミック方式で学習されたすべてのセキュアアドレスをドロップします。デバイスは、スタティック方式で学習したアドレスをネイティブ トランク VLAN に移行します。

スイッチ ポートからルート ポート

インターフェイスをレイヤ2 インターフェイスからレイヤ3 インターフェイスに変更すると、デバイスはそのインターフェイスのポート セキュリティをディセーブルにし、そのインターフェイスのすべてのポート セキュリティ設定を廃棄します。デバイスは、学習方式に関係なく、そのインターフェイスのセキュア MAC アドレスもすべて廃棄します。

ルートポートからスイッチポート

インターフェイスをレイヤ3インターフェイスからレイヤ2インターフェイスに変更すると、デバイス上のそのインターフェイスのポートセキュリティ設定はなくなります。

ポートセキュリティの前提条件

ポートセキュリティの前提条件は次のとおりです。

- ポートセキュリティで保護するデバイスのポートセキュリティをグローバルにイネーブル化すること。

ポートセキュリティのデフォルト設定

次の表に、ポートセキュリティパラメータのデフォルト設定を示します。

パラメータ	デフォルト
ポートセキュリティがグローバルにイネーブルかどうか	ディセーブル
インターフェイス単位でポートセキュリティがイネーブルかどうか	ディセーブル
MAC アドレス ラーニング方式	Dynamic
セキュア MAC アドレスのインターフェイス最大数	1
セキュリティ違反時の処理	シャットダウン

ポートセキュリティの注意事項と制約事項

ポート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。

- ポートセキュリティは、スイッチドポートアナライザ（SPAN）の宛先ポートをサポートしません。
- ポートセキュリティは他の機能に依存しません。
- Cisco NX-OS リリース 10.2(1)F 以降、USB ポートの無効化は Cisco NX-OS スイッチでサポートされています。USB ポートを無効または有効にするには、**[no] port usb disable** コマンドを使用します。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションの設定後、このアソシエーションを削除すると、プライマリ VLAN 上に作成されたすべてのスタティック MAC アドレスは、プライマリ VLAN 上に限り存続します。

**Note**

一部の状況では、エラーメッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

プライマリ VLAN とセカンダリ VLAN 間の関連付けを設定した後、次の手順を実行します。

- セカンダリ VLAN のスタティック MAC アドレスは作成できません。
- セカンダリ VLAN を学習したダイナミック MAC アドレスは期限切れになります。

vPC 上のポートセキュリティの注意事項と制約事項

ポートセキュリティに関する注意事項および制限事項とは別に、vPC のポートセキュリティに関する次の注意事項および制限事項を満たしていることを確認します。

- ポートセキュリティは、vPC 展開の FEX インターフェイスではサポートされません。
- vPC ドメイン内の両方の vPC ピアで、ポートセキュリティをグローバルに有効にする必要があります。
- 両方の vPC ピアの vPC インターフェイス上でポートセキュリティを有効にする必要があります。
- プライマリ vPC ピアでスタティックセキュア MAC アドレスを設定する必要があります。スタティック MAC アドレスは、セカンダリ vPC ピアと同期されます。セカンダリピアでスタティックセキュア MAC アドレスも設定できます。第二スタティック MAC アドレスはセカンダリ vPC 設定に表示されますが、有効にはなりません。
- プライマリ vPC ポートとセカンダリ vPC ポートの両方で、最大 MAC カウント値が同じであることを確認する必要があります。
- セカンダリ vPC ポートでは、スタティック MAC の制限チェックは行われません。シスコは、最大 MAC カウントで定義されているように、セカンダリ vPC ポートで同じ数のスタティック MAC を設定することを推奨します。
- 学習したすべての MAC アドレスは vPC ピア間で同期されます。
- 両方の vPC ピアは、ダイナミックまたはスタティック MAC アドレスの学習方式で設定できます。シスコは、同じ方法を使用して両方の vPC ピアを設定することを推奨します。これは、vPC ロールの変更など、特定の場合にポートのシャットダウン（errDisabled 状態）を防ぐのに役立ちます。
- ダイナミック MAC アドレスは、両方の vPC ピアでエージング期限に達した後にのみドロップされます。
- セキュア MAC アドレスの最大数は、プライマリ vPC スイッチ上で設定します。プライマリ vPC スイッチは数の検証を行い、セカンダリ スイッチで最大数設定を無視します。

- 違反時の処理は、プライマリ vPC 上で設定します。セキュリティ違反がトリガーされると、プライマリ vPC スイッチに定義されたセキュリティ処理が常に実行されます。
- 両方の vPC ピアで設定が正しいことを確認するには、**show vpc consistency-parameters id** コマンドを使用できます。
- スイッチでインサースerviceソフトウェアアップグレード（ISSU）が実行されている間、ポートセキュリティの動作はそのピア スイッチ上で停止されます。ピア スイッチはどの新しい MAC アドレスも学習せず、この動作中に発生した MAC の移動は無視されます。ISSU が完了すると、ピア スイッチに通知され、通常のポートセキュリティ機能が再開します。
- 上位バージョンへの ISSU がサポートされていますが、下位バージョンへの ISSU はサポートされていません。

ポート セキュリティの設定

ポートセキュリティのグローバルなイネーブル化またはディセーブル化

デバイスに対してポートセキュリティ機能のグローバルなイネーブル化またはディセーブル化が可能です。デフォルトで、ポートセキュリティはグローバルにディセーブルになっています。

ポートセキュリティをディセーブルにすると、インターフェイスのすべてのポートセキュリティ設定が無効になります。ポートセキュリティをグローバルにディセーブル化すると、すべてのポートセキュリティ設定が失われます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] feature port-security Example: switch(config)# feature port-security	ポートセキュリティをグローバルにイネーブル化します。 no オプションを使用するとポートセキュリティはグローバルに無効化されます。
ステップ 3	(Optional) show port-security Example: switch(config)# show port-security	ポートセキュリティのステータスを表示します。

	Command or Action	Purpose
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ2インターフェイスに対するポートセキュリティのイネーブル化またはディセーブル化

レイヤ2インターフェイスに対してポートセキュリティ機能のイネーブル化またはディセーブル化が可能です。デフォルトでは、ポートセキュリティはすべてのインターフェイスでディセーブルです。

インターフェイスのポートセキュリティをディセーブルにすると、そのインターフェイスのすべてのスイッチポートのポートセキュリティ設定が失われます。

Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

レイヤ2イーサネットインターフェイスがポートチャネルインターフェイスのメンバである場合、レイヤ2イーサネットインターフェイスに対するポートセキュリティはイネーブルまたはディセーブルにできません。

セキュアレイヤ2ポートチャネルインターフェイスのメンバのいずれかのポートセキュリティがイネーブルになっている場合、先にポートチャネルインターフェイスからセキュアメンバポートをすべて削除しない限り、そのポートチャネルインターフェイスのポートセキュリティをディセーブルにできません。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 interface ethernet slot/port interface port-channel channel-number Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	ポートセキュリティを設定するイーサネットインターフェイスまたはポートチャネルインターフェイスの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。

	Command or Action	Purpose
ステップ 3	switchport Example: switch(config-if) # switchport	そのインターフェイスを、レイヤ2インターフェイスとして設定します。
ステップ 4	[no] switchport port-security Example: switch(config-if) # switchport port-security	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。 no オプションを使用すると、そのインターフェイスのポートセキュリティがディセーブルになります。
ステップ 5	(Optional) show running-config port-security Example: switch(config-if) # show running-config port-security	ポートセキュリティの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch(config-if) # copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

スティック MAC アドレス ラーニングのイネーブル化またはディセーブル化

インターフェイスのスティック MAC アドレス ラーニングをディセーブルまたはイネーブルに設定できます。スティック学習をディセーブルにすると、そのインターフェイスはダイナミック MAC アドレス ラーニング（デフォルトの学習方式）に戻ります。

デフォルトでは、スティック MAC アドレス ラーニングはディセーブルです。

Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config) #	グローバル構成モードを開始します。

	Command or Action	Purpose
ステップ 2	次のいずれかのコマンドを入力します。 • interface ethernet slot/port • interface port-channel channel-number Example: switch(config)# interface ethernet 2/1 switch(config-if)#	スティック MAC アドレス ラーニングを設定するインターフェイスのインターフェイス 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 Example: switch(config-if)# switchport	そのインターフェイスを、レイヤ 2 インターフェイスとして設定します。
ステップ 4	[no] switchport port-security mac-address sticky Example: switch(config-if)# switchport port-security mac-address sticky	そのインターフェイスのスティック MAC アドレス ラーニングをイネーブルにします。 no オプションを使用するとスティック MAC アドレス ラーニングが無効になります。
ステップ 5	(Optional) show running-config port-security Example: switch(config-if)# show running-config port-security	ポート セキュリティの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch(config-if)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスのスタティック セキュア MAC アドレスの追加

レイヤ 2 インターフェイスにスタティック セキュア MAC アドレスを追加できます。



Note MAC アドレスが任意のインターフェイスでセキュア MAC アドレスである場合、その MAC アドレスがすでにセキュア MAC アドレスとなっているインターフェイスからその MAC アドレスを削除するまで、その MAC アドレスをスタティック セキュア MAC アドレスとして別のインターフェイスに追加することはできません。

デフォルトでは、インターフェイスにスタティック セキュア MAC アドレスは設定されません。

Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

インターフェイスのセキュア MAC アドレス最大数に達していないことを確認します。必要に応じて、セキュア MAC アドレスを削除するか、インターフェイスの最大アドレス数を変更できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 interface ethernet slot/port interface port-channel channel-number Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	指定したインターフェイスのインターフェイス 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] switchport port-security mac-address address [vlan vlan-ID] Example: <pre>switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE</pre>	現在のインターフェイスのポートセキュリティにスタティック MAC アドレスを設定します。そのアドレスからのトラフィックを許可する VLAN を指定する場合は、 vlan キーワードを使用します。
ステップ 4	(Optional) show running-config port-security Example: <pre>switch(config-if)# show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスのスタティック セキュア MAC アドレスの削除

レイヤ 2 インターフェイスのスタティック セキュア MAC アドレスを削除できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • interface ethernet slot/port • interface port-channel channel-number Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	スタティックセキュア MAC アドレスを削除するインターフェイスのインターフェイス 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 switchport port-security mac-address address Example: <pre>switch(config-if)# no switchport port-security mac-address 0019.D2D0.00AE</pre>	現在のインターフェイスのポートセキュリティからスタティックセキュア MAC アドレスを削除します。
ステップ 4	(Optional) show running-config port-security Example: <pre>switch(config-if)# show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

スティッキ セキュア MAC アドレスの削除

スティッキセキュア MAC アドレスを削除できます。この際、削除するアドレスが設定されているインターフェイスで、スティッキ方式のアドレス学習を一時的にディセーブルにする必要があります。

始める前に

ポートセキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • interface ethernet slot/port • interface port-channel channel-number 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	スティッキセキュア MAC アドレスを削除するインターフェイスのインターフェイス 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 switchport port-security mac-address sticky 例 : <pre>switch(config-if)# no switchport port-security mac-address sticky</pre>	インターフェイスのスティッキ MAC アドレス ラーニングをディセーブルにします。これにより、インターフェイスのスティッキセキュア MAC アドレスが、ダイナミックセキュア MAC アドレスに変換されます。
ステップ 4	clear port-security dynamic address address 例 : <pre>switch(config-if)# clear port-security dynamic address 0019.D2D0.02GD</pre>	指定したダイナミックセキュア MAC アドレスを削除します。
ステップ 5	(任意) show port-security address interface {ethernet slot/port port-channel channel-number} 例 : <pre>switch(config)# show port-security address interface ethernet 2/1</pre>	セキュア MAC アドレスを表示します。削除したアドレスは表示されません。
ステップ 6	(任意) switchport port-security mac-address sticky 例 : <pre>switch(config-if)# switchport port-security mac-address sticky</pre>	そのインターフェイスのスティッキ MAC アドレス ラーニングを再度イネーブルにします。

ダイナミック セキュア MAC アドレスの削除

ダイナミックに学習されたセキュア MAC アドレスを削除できます。

Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	clear port-security dynamic {interface ethernet slot/port address address} [vlan vlan-ID] Example: <pre>switch(config)# clear port-security dynamic interface ethernet 2/1</pre>	ダイナミックに学習されたセキュア MAC アドレスを削除します。次の方法で指定できます。 interface キーワードを使用すると、指定したインターフェイスでダイナミックに学習されたアドレスがすべて削除されます。 address キーワードを使用すると、指定した単一のダイナミック学習アドレスが削除されます。 特定の VLAN のアドレスを削除するようにコマンドに制限を加えるには、vlan キーワードを使用します。
ステップ 3	(Optional) show port-security address Example: <pre>switch(config)# show port-security address</pre>	セキュア MAC アドレスを表示します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC アドレスの最大数の設定

レイヤ2インターフェイスで学習可能なMACアドレスまたはスタティックに設定可能なMACアドレスの最大数を設定できます。レイヤ2インターフェイス上のVLAN単位でもMACアドレスの最大数を設定できます。インターフェイスに設定できる最大アドレス数は1025です。システムの最大アドレス数は8192です。

デフォルトでは、各インターフェイスのセキュアMACアドレスの最大数は1です。VLANには、セキュアMACアドレス数のデフォルトの最大値はありません。

**Note**

インターフェイスですでに学習されているアドレス数またはインターフェイスにスタティックに設定されたアドレス数よりも小さい数を最大数に指定すると、デバイスはこのコマンドを拒否します。ダイナミック方式で学習されたアドレスをすべて削除するには、**shutdown** および **no shutdown** のコマンドを使用して、インターフェイスを再起動します。

Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • interface ethernet slot/port • interface port-channel channel-number Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。 <i>slot</i> は、MACアドレスの最大数を設定するインターフェイスです。
ステップ 3	[no] switchport port-security maximum number [vlan vlan-ID] Example: <pre>switch(config-if)# switchport port-security maximum 425</pre>	現在のインターフェイスで学習可能なMACアドレスまたはスタティックに設定可能なMACアドレスの最大数を設定します。有効な <i>number</i> の最高値は1025です。 no オプションを使用すると、MACアドレスの最大数がデフォルト値（1）にリセットされます。 最大数を適用するVLANを指定する場合は、 vlan キーワードを使用します。

■ アドレス エージング タイプおよび時間を設定する

	Command or Action	Purpose
ステップ 4	(Optional) show running-config port-security Example: <pre>switch(config-if)# show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

アドレス エージング タイプおよび時間を設定する

MAC アドレス エージングのタイプと期間を設定できます。デバイスは、ダイナミック方式で学習された MAC アドレスがエージング期限に到達する時期を判断するためにこれらの設定を使用します。

デフォルトのエージング タイプは絶対エージングです。

デフォルトのエージング タイムは 0 分（エージングは無効）です。

Before you begin

ポートセキュリティがグローバルに有効にされている必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 interface ethernet slot/port interface port-channel channel-number Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	MAC エージングのタイプと期間を設定するインターフェイスのインターフェイス 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] switchport port-security aging type {absolute inactivity} Example:	ダイナミックに学習された MAC アドレスにデバイスが適用するエージング タイプを設定します。no オプションを使

	Command or Action	Purpose
	<code>switch(config-if)# switchport port-security aging type inactivity</code>	用すると、エージング タイプがデフォルト値（絶対エージング）にリセットされます。
ステップ 4	[no] switchport port-security aging time minutes Example: <code>switch(config-if)# switchport port-security aging time 120</code>	ダイナミックに学習された MAC アドレスがドロップされるまでのエージング タイムを分単位で設定します。 <i>minutes</i> の最大値は 1440 です。 no オプションを使用すると、エージング タイムがデフォルト値である 0（エージングは無効）にリセットされます。
ステップ 5	(Optional) show running-config port-security Example: <code>switch(config-if)# show running-config port-security</code>	ポートセキュリティの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <code>switch(config-if)# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

セキュリティ違反時の処理の設定

セキュリティ違反が発生した場合にデバイスが実行する処理を設定できます。違反時の処理は、ポートセキュリティをイネーブルにしたインターフェイスごとに設定できます。

デフォルトのセキュリティ処理では、セキュリティ違反が発生したポートがシャットダウンされます。

Before you begin

ポートセキュリティがグローバルにイネーブル化されている必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル構成モードを開始します。

	Command or Action	Purpose
ステップ 2	次のいずれかのコマンドを入力します。 • interface ethernet slot/port • interface port-channel channel-number Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	セキュリティ違反時の処理を設定するインターフェイスのインターフェイス 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] switchport port-security violation {protect restrict shutdown} Example: <pre>switch(config-if)# switchport port-security violation restrict</pre>	現在のインターフェイスのポートセキュリティにセキュリティ違反時の処理を設定します。 no オプションを使用すると、違反時の処理がデフォルト値（インターフェイスのシャットダウン）にリセットされます。
ステップ 4	(Optional) show running-config port-security Example: <pre>switch(config-if)# show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ポートセキュリティの設定の確認

ポートセキュリティの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config port-security	ポートセキュリティの設定を表示します。
show port-security	デバイスのポートセキュリティのステータスを表示します。
show port-security interface	特定のインターフェイスのポートセキュリティのステータスを表示します。
show port-security address	セキュア MAC アドレスを表示します。
show vpc consistency-parameters vpc id	両方の vPC ピアの設定を確認します。

セキュア MAC アドレスの表示

セキュア MAC アドレスを表示するには、**show port-security address** コマンドを使用します。

ポート セキュリティの設定例

次に示す例は、VLAN とインターフェイスのセキュア アドレス最大数が指定されているイーサネット 2/1 インターフェイスのポートセキュリティ設定です。この例のインターフェイスはトランク ポートです。違反時の処理は Restrict（制限）に設定されています。

```
feature port-security
interface Ethernet 2/1
  switchport
  switchport port-security
  switchport port-security maximum 10
  switchport port-security maximum 7 vlan 10
  switchport port-security maximum 3 vlan 20
  switchport port-security violation restrict
```

vPC ドメインでのポート セキュリティの設定例

次に、vPC ドメインで vPC ピア上のポート セキュリティをイネーブルにして設定する例を示します。最初のスイッチがプライマリ vPC ピアであり、2 番目のスイッチがセカンダリ vPC ピアです。スイッチでポートセキュリティを設定する前に、vPC ドメインを作成し、vPC ピアリンク 隣接関係が確立されていることを確認します。

例：孤立ポートでのポート セキュリティの設定

```
primary_switch(config)# feature port-security
primary_switch(config-if)# int e1/1
primary_switch(config-if)# switchport port-security
primary_switch(config-if)# switchport port-security max 1025
primary_switch(config-if)# switchport port-security violation restrict
primary_switch(config-if)# switchport port-security aging time 4
primary_switch(config-if)# switchport port-security aging type absolute
primary_switch(config-if)# switchport port-security mac sticky
primary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
primary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# feature port-security
secondary_switch(config)# int e3/1
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# switchport port-security max 1025
secondary_switch(config-if)# switchport port-security violation restrict
secondary_switch(config-if)# switchport port-security aging time 4
secondary_switch(config-if)# switchport port-security aging type absolute
secondary_switch(config-if)# switchport port-security mac sticky
secondary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
```

例：vPC レッグ上のポートセキュリティの設定

```
secondary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
secondary_switch(config-if)# copy running-config startup-config
```

例：vPC レッグ上のポートセキュリティの設定

```
primary_switch(config)# feature port-security
primary_switch(config-if)# int po10
primary_switch(config-if)# switchport port-security
primary_switch(config-if)# switchport port-security max 1025
primary_switch(config-if)# switchport port-security violation restrict
primary_switch(config-if)# switchport port-security aging time 4
primary_switch(config-if)# switchport port-security aging type absolute
primary_switch(config-if)# switchport port-security mac sticky
primary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
primary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
primary_switch(config-if)# vpc 10
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# feature port-security
secondary_switch(config)# int po10
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# switchport port-security max 1025
secondary_switch(config-if)# switchport port-security violation restrict
secondary_switch(config-if)# switchport port-security aging time 4
secondary_switch(config-if)# switchport port-security aging type absolute
secondary_switch(config-if)# switchport port-security mac sticky
secondary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
secondary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
secondary_switch(config-if)# vpc 10
secondary_switch(config-if)# copy running-config startup-config
```

ポートセキュリティに関する追加情報

関連資料

関連項目	マニュアルタイトル
レイヤ2スイッチング	『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』

MIB

Cisco NX-OS はポートセキュリティに関して読み取り専用の SNMP をサポートしています。

MIB	MIB のリンク
CISCO-PORT-SECURITY-MIB Note トラップは、セキュア MAC アドレスの違反の通知についてサポートされています。	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2

VXLAN EVPN のポートセキュリティ サポート

このセクションでは、VXLAN EVPN のポートセキュリティ機能の構成方法について説明します。

VXLAN EVPN のポートセキュリティ サポートに関する注意事項と制約事項

VXLAN EVPN のポートセキュリティ サポートに関する注意事項と制約事項を次に示します。

- Cisco NX-OS リリース 10.3(3)F 以降、L2 ポートセキュリティ機能は、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2、9408 の VXLAN BGP EVPN（シングル VTEP）および X97160YC-EX、9700-FX/GX ライン カードを搭載した Cisco Nexus 9500 スイッチでサポートされますが、次の制限があります。
 - 単一の VTEP ソリューションのみがサポートされます。ただし、セキュア MAC モビリティは VXLAN 環境ではサポートされません。
- Cisco NX-OS リリース 10.3(3)F 以降、IPv6 アンダーレイは、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2 スイッチおよび X97160YC-EX、9700-FX/GX ラインカードを搭載した Cisco Nexus 9500 スイッチにおいて、VXLAN EVPN のポートセキュリティ（単一 VTEP）でサポートされます。
- ポートセキュリティは、ファブリック ピアリングではサポートされていません。
- L2 ポートセキュリティ機能が有効になっている場合、次の動作が観察されます。
 - セキュア MAC は静的 MAC として送信され、リモート VTEP では静的 MAC として認識されます。したがって、リモート VTEP 上のセキュア MAC をダイナミック MAC として学習しようとする試みがある場合（同じ MAC を持つ悪意のあるホストが原因で）、それは阻止されます。
 - 違反した MAC に **restrict** オプションが設定されている場合、これらの違反した MAC は **static drop** セットを使用して送信されます。リモート VTEP では、MAC は静的ドロップで構成されるため、リモート VTEP からこれらのホストにトラフィックを送信しようすると、リモート VTEP 自体でドロップされます。
 - ローカルの静的 MAC とセキュア MAC の両方がスティッキー ビットを使用してファブリックにアドバタイズされるため、リモート VTEP については、リモート静的 MAC がセキュア MAC または静的 MAC のどちらの VTEP からのものであっても違いはありません。
 - ローカル スタティックがすでに存在する場合は、リモート スタティック（セキュア またはスタティック）よりも優先されます。
 - MAC に対してローカルで行われたセキュリティの決定に基づいて、ローカル VTEP からファブリックへのセキュア ポートで学習された MAC に複数の更新が存在する可

能性がありますが、MAC の最終的なセキュリティ動作はローカルおよびリモート VTEP で一貫しています。

- セキュア MAC の **inactivity** 値を指定できます。アクティビティがない場合、セキュア MAC は削除され、セキュア MAC ホストは別のポートに移動することがあります。

VXLAN EVPN のポートセキュリティ サポートの確認

VXLAN EVPN の構成情報のポートセキュリティ サポートを表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show running-config interface <interface-name>	インターフェイスの実行中の構成を表示します。
show port-security	ポートセキュリティ 構成情報を表示します。

show running-config interface コマンドの例

```
switch(config-if)# show run inter e1/48
!Command: show running-config interface Ethernet1/48
!Running configuration last done at: Thu Feb 16 08:39:43 2023
!Time: Fri Feb 17 06:07:33 2023

version 10.3(3) Bios:version 01.08

interface Ethernet1/48
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 200
  spanning-tree port type edge trunk
  switchport port-security maximum 1025
  switchport port-security
  no shutdown

LVTEP:
-----
switch(config-if)# show mac address-table inter e1/48
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen, + - primary entry using vPC Peer-Link,
    (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan,
    (NA) - Not Applicable
```

VLAN	MAC Address	Type	age	Secure	NTFY	Ports
* 101	0012.0100.0001	secure	-	T	F	Eth1/48
* 101	0012.0100.0002	secure	-	T	F	Eth1/48
* 101	0012.0100.0003	secure	-	T	F	Eth1/48
* 101	0012.0100.0004	secure	-	T	F	Eth1/48

show port-security コマンドの例

```
switch(config-if)# show port-security
Total Secured Mac Addresses in System (excluding one mac per port)      : 1024
Max Addresses limit in System (excluding one mac per port) : 7168
```



```

-----
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)          (Count)          (Count)
-----
Ethernet1/48      1025           1025           0                  Shutdown

```

```
switch(config-if)# show port-security address interface e1/48
```

```

-----
                        Secure Mac Address Table
-----
Vlan      Mac Address      Type      Remaining  Remotely  Remotely  Ports
          (Count)          age      learnt    aged      out
          (mins)
-----
101      0012.0100.0001    DYNAMIC   0          No        No        Ethernet1/48
101      0012.0100.0002    DYNAMIC   0          No        No        Ethernet1/48
101      0012.0100.0003    DYNAMIC   0          No        No        Ethernet1/48
101      0012.0100.0004    DYNAMIC   0          No        No        Ethernet1/48

```

```
RVTEP:
```

```

-----
Standalone_VTEP_EX# show mac address-table
C 101      0012.0100.0001    static    -          F          F          nve1(20:20:20::20)
C 101      0012.0100.0002    static    -          F          F          nve1(20:20:20::20)
C 101      0012.0100.0003    static    -          F          F          nve1(20:20:20::20)
C 101      0012.0100.0004    static    -          F          F          nve1(20:20:20::20)

```




第 16 章

DHCP の設定

この章では、Cisco NX-OS デバイスで Dynamic Host Configuration Protocol (DHCP) を設定する手順について説明します。

この章は、次の項で構成されています。

- [DHCP スヌーピングについて, on page 502](#)
- [DHCP リレー エージェントについて \(508 ページ\)](#)
- [DHCPv6 リレー エージェントについて \(511 ページ\)](#)
- [DHCPv6 スマート リレー エージェント \(512 ページ\)](#)
- [DHCPv6 スマート リレーの注意事項と制約事項 \(513 ページ\)](#)
- [DHCP クライアントについて \(513 ページ\)](#)
- [DHCP の前提条件, on page 513](#)
- [DHCP のガイドラインと制約事項 \(513 ページ\)](#)
- [DHCP のデフォルト設定, on page 516](#)
- [DHCP の設定, on page 517](#)
- [DHCPv6 の設定 \(540 ページ\)](#)
- [ローカル ゲスト シェル/Docker でのサーバーへの DHCP リレー \(549 ページ\)](#)
- [DHCP クライアントの有効化 \(553 ページ\)](#)
- [UDP リレーの設定 \(554 ページ\)](#)
- [DHCP 設定の確認, on page 558](#)
- [IPv6 RA ガードの統計情報の表示 \(561 ページ\)](#)
- [DHCP スヌーピング バインディングの表示, on page 561](#)
- [DHCP スヌーピング バインディング データベースのクリア \(562 ページ\)](#)
- [DHCP のモニタリング \(562 ページ\)](#)
- [DHCP スヌーピング統計情報のクリア \(562 ページ\)](#)
- [DHCP リレー統計情報のクリア \(563 ページ\)](#)
- [DHCPv6 リレー統計情報のクリア \(563 ページ\)](#)
- [DHCPv6-PD バインドのクリア \(563 ページ\)](#)
- [DHCP の設定例, on page 564](#)
- [DHCP クライアントの設定例 \(564 ページ\)](#)
- [DHCP に関する追加情報, on page 565](#)

DHCP スヌーピングについて

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバとの間でファイアウォールのような機能を果たします。DHCP スヌーピングでは次のアクティビティを実行します。

- 信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外します。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

DHCP スヌーピングは、グローバルおよび VLAN 単位でイネーブルにできます。デフォルトでは、この機能はグローバルおよびすべての VLAN でディセーブルです。この機能は、1 つの VLAN または特定の VLAN 範囲でイネーブルにできます。

信頼できる送信元と信頼できない送信元

DHCP スヌーピングがトラフィックの送信元を信頼するかどうかを設定できます。信頼できない送信元の場合、トラフィック攻撃やその他の敵対的アクションが開始される可能性があります。こうした攻撃を防ぐため、DHCP スヌーピングは信頼できない送信元からのメッセージをフィルタリングします。

企業ネットワークでは、信頼できる送信元はその企業の管理制御下にあるデバイスです。これらのデバイスには、ネットワーク内のスイッチ、ルータ、およびサーバが含まれます。ファイアウォールを越えるデバイスやネットワーク外のデバイスは信頼できない送信元です。一般的に、ホスト ポートは信頼できない送信元として扱われます。

サービス プロバイダーの環境では、サービス プロバイダー ネットワークにないデバイスは、信頼できない送信元です（カスタマー スイッチなど）。ホスト ポートは、信頼できない送信元です。

Cisco NX-OS デバイスでは、接続インターフェイスの信頼状態を設定することにより、送信元を信頼できるものとして扱うことができます。

すべてのインターフェイスのデフォルトの信頼状態は、信頼できない状態になります。DHCP サーバインターフェイスは、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。ユーザのネットワーク内でデバイス（スイッチまたはルータ）に接続されている場合、他のインターフェイスも信頼できるインターフェイスとして設定できます。ホスト ポート インターフェイスは、通常、信頼できるインターフェイスとしては設定しません。



Note DHCP スヌーピングを適切に機能させるためには、すべての DHCP サーバが信頼できるインターフェイスを介してデバイスと接続される必要があります。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングは、代行受信した DHCP メッセージから抽出した情報を使用し、ダイナミックにデータベースを構築し維持します。DHCP スヌーピングがイネーブルにされた VLAN に、ホストが関連付けられている場合、データベースには、リース IP アドレスがある信頼できない各ホストのエントリが保存されています。データベースには、信頼できるインターフェイスを介して接続するホストに関するエントリは保存されません。



Note DHCP スヌーピング バインディング データベースは DHCP スヌーピング バインディング テーブルとも呼ばれます。

デバイスが特定の DHCP メッセージを受信すると、DHCP スヌーピングはデータベースをアップデートします。たとえば、デバイスが DHCPACK メッセージをサーバから受信すると、この機能によってデータベースにエントリが追加されます。IP アドレスのリース期限が過ぎたり、デバイスがホストから DHCPRELEASE メッセージを受信すると、この機能によってデータベース内のエントリが削除されます。

DHCP スヌーピング バインディング データベースの各エントリには、ホストの MAC アドレス、リース IP アドレス、リース期間、バインディング タイプ、VLAN 番号、およびホストに関連するインターフェイス情報が保存されます。

ダイナミック ARP インスペクション (DAI) および IP ソース ガードも、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た情報を使用します。

`clear ip dhcp snooping binding` コマンドを使用すると、バインディング データベースからエントリ削除できます。

vPC 環境での DHCP スヌーピング

仮想ポート チャネル (vPC) では、2 台の Cisco NX-OS スイッチを 3 番目のデバイスに 1 つの論理ポート チャネルとして認識させることができます。第 3 のデバイスは、スイッチ、サーバ、ポート チャネルをサポートするその他の任意のネットワーク デバイスのいずれでもかまいません。

標準的な vPC 環境では、DHCP 要求は一方の vPC ピア スイッチに到達でき、応答は他方の vPC ピア スイッチに到達できるため、一方のスイッチには部分的な DHCP (IP-MAC) バインディング エントリが生成され、他方のスイッチにはバインディング エントリが生成されません。その結果、DHCP スヌーピング、およびダイナミック ARP インスペクション (DAI) や IP ソース ガードなどのそれに関連する機能は中断されます。この問題は Cisco Fabric Service over Ethernet (CFS over Ethernet) 分散を使用して、すべての DHCP パケット (要求および応答) が両方のスイッチに確実に認識されるようにすることで対処されます。これにより、vPC リンクの背後に存在するすべてのクライアントについて、両方のスイッチで同じバインディング エントリが作成および管理されるようになります。

CFS over Ethernet 分散ではまた、vPC リンク上の DHCP 要求および応答を 1 台のスイッチのみが転送するようにもできます。vPC 以外の環境では、両方のスイッチが DHCP パケットを転送します。

DHCP スヌーピング バインディング エントリの同期

ダイナミック DHCP バインディング エントリは、次のシナリオで同期される必要があります。

- リモート vPC がオンラインになったとき、その vPC リンクのすべてのバインディング エントリがピアと同期する必要があります。
- DHCP スヌーピングがピア スイッチでイネーブルになっている場合、すべての vPC リンクのダイナミック バインディング エントリがピアと同期する必要があります。

パケット検証

デバイスは、DHCP スヌーピングがイネーブルの VLAN にある信頼できないインターフェイスで受信された DHCP パケットを検証します。デバイスは、次のいずれかの条件が発生しないかぎり、DHCP パケットを転送します（これらの条件が発生した場合、パケットはドロップされます）。

- 信頼できないインターフェイスで DHCP 応答パケット（DHCPACK、DHCPNAK、または DHCP OFFER などのパケット）を受信した場合。
- 信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合。このチェックは、DHCP スヌーピングの MAC アドレス検証オプションがオンの場合だけ、実行されます。
- DHCP スヌーピング バインディング テーブル内にエントリを持つ信頼できないホストから DHCPRELEASE または DHCPDECLINE メッセージを受信したが、バインディング テーブル内のインターフェイス情報が、このメッセージを受信したインターフェイスと一致しない場合。

さらに、DHCP パケットの厳密な検証をイネーブルにすることもできます。これにより、DHCP パケットのオプション フィールドが確認されます。これには、オプション フィールドの最初の 4 バイト内の「マジック クッキー」値も含まれます。デフォルトでは、厳密な検証はディセーブルになっています。有効にすると、**ip dhcp packet strict-validation** コマンドを使用してイネーブルにすると、DHCP スヌーピングで無効なオプション フィールドを含むパケットを処理した場合に、パケットがドロップされます。

DHCP スヌーピングの Option 82 データ挿入

DHCP では、多数の加入者に対する IP アドレスの割り当てを一元管理できます。Option 82 をイネーブルにすると、デバイスはネットワークに接続する加入者デバイス（およびその MAC アドレス）を識別します。加入者 LAN 上のマルチ ホストをアクセス デバイスの同一ポートに接続でき、これらは一意に識別されます。

Cisco NX-OS デバイスで Option 82 をイネーブルにすると、次のイベントが順番に発生します。

1. 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。

2. Cisco NX-OS デバイスはこの DHCP 要求を受信すると、パケット内に Option 82 情報を追加します。Option 82 情報には、デバイスの MAC アドレス（リモート ID サブオプション）と、ポート ID の vlan-ifindex（非 vPC の場合）または vlan-vpcid（vPC の場合）が含まれ、これらは受信されたパケットの発信元です（回線 ID サブオプション）。



Note vPC ピア スイッチの場合、リモート ID サブオプションには vPC スイッチの MAC アドレスが入ります。これは両方のスイッチにおいて一意です。この MAC アドレスは vPC ドメイン ID とともに計算されます。Option 82 情報は、DHCP 要求が他の vPC ピア スイッチに転送される前に最初に受信したスイッチで挿入されます。

3. デバイスは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
4. 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、このリモート ID、回線 ID、またはその両方を使用して、IP アドレスの割り当てやポリシーの適用を行うことができます。たとえば、単一のリモート ID または回線 ID に割り当てることのできる IP アドレスの数を制限するポリシーなどです。DHCP サーバは、DHCP 応答内に Option 82 フィールドをエコーします。
5. DHCP サーバは Cisco NX-OS デバイスに応答を送信します。Cisco NX-OS デバイスは、リモート ID フィールド、および場合によっては回線 ID フィールドを検査することで、最初に Option 82 データを挿入したのがこのデバイス自身であることを確認します。Cisco NX-OS デバイスは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントと接続しているインターフェイスにパケットを転送します。

上記の一連のイベントが発生した場合、次の値は変更されません。

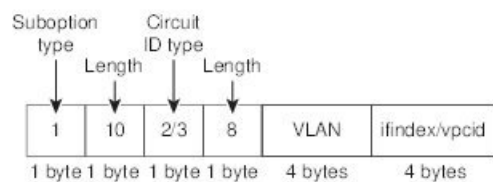
- 回線 ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - 回線 ID タイプ
 - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
 - サブオプション タイプ
 - サブオプション タイプの長さ
 - リモート ID タイプ
 - 回線 ID タイプの長さ

次の図は、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。Cisco NX-OS デバイスがこのパケット形式を使用するのは、DHCP スヌーピングがグローバルにイネーブル化され、Option 82 データの挿入と削除がイネーブルに設定された場合

です。回線 ID サブオプションの場合、モジュール フィールドはモジュールのスロット番号となります。

Figure 10: サブオプションのパケット形式

Circuit ID Suboption Frame Format



Remote ID Suboption Frame Format

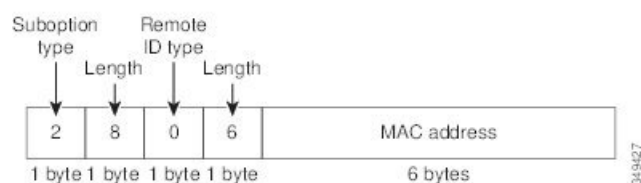


Figure 11: サブオプションのパケット形式（非 TLV 形式）

DHCP リレー エージェントについて

DHCP リレー エージェント

DHCP リレーエージェントを実行するようにデバイスを設定できます。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 パケットを転送します。これは、クライアントとサーバが同じ物理サブネット上にない場合に便利な機能です。リレー エージェントは DHCP メッセージを受信すると、新規の DHCP メッセージを生成して別のインターフェイスに送信します。リレーエージェントはゲートウェイアドレスを設定し（DHCP パケットの `giaddr` フィールド）、パケットにリレー エージェント情報のオプション（Option 82）を追加して（設定されている場合）、DHCP サーバに転送します。サーバからの応答は、Option 82 を削除してからクライアントに転送されます。

Option 82 をイネーブルにすると、デバイスはデフォルトでバイナリの `ifindex` 形式を使用します。必要に応じて Option 82 設定を変更して、代わりに符号化ストリング形式を使用できます。



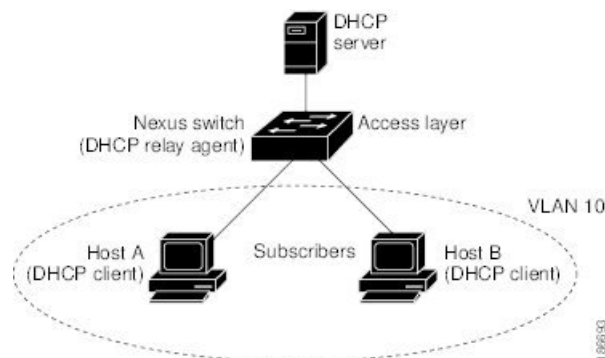
Note デバイスは、Option 82 情報がすでに含まれている DHCP 要求を中継するときには、Option 82 情報を変更せずに元のままの状態ですべての要求と一緒に転送します。

DHCP リレー エージェントの Option 82

リレー エージェントによって転送された DHCP パケットに関する Option 82 情報のデバイスでの挿入および削除をイネーブルにすることができます。

Figure 12: 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

次の図のメトロポリタンイーサネットネットワークでは、アクセスレイヤのデバイスに接続されている加入者に、DHCP サーバが IP アドレスを一元的に割り当てます。各 DHCP クライアントと、これらに関連付けられた DHCP サーバは、同一の IP ネットワークまたはサブネット内に存在しません。したがって、DHCP リレー エージェントをヘルパー アドレスによって設定することで、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。



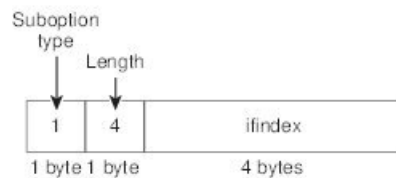
Cisco NX-OS デバイス上で DHCP リレー エージェントの Option 82 をイネーブルにすると、次の一連のイベントが発生します。

1. 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。
2. Cisco NX-OS デバイスはこの DHCP 要求を受信すると、パケット内に Option 82 情報を追加します。Option 82 情報には、デバイスの MAC アドレス (リモート ID サブオプション) と、ポート ID の ifindex (非 VXLAN VLAN の場合) または vn-segment-id-mod-port (VXLAN VLAN の場合) が含まれ、これらは受信されたパケットの発信元です (回線 ID サブオプション)。DHCP リレーでは、回線 ID には、DHCP リレーが設定されている SVI または レイヤ 3 インターフェイスの ifindex が入力されます。
3. デバイスは、DHCP パケットにリレー エージェントの IP アドレスを追加します。
4. デバイスは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
5. 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、このリモート ID、回線 ID、またはその両方を使用して、IP アドレスの割り当てやポリシーの適用を行うことができます。たとえば、単一のリモート 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ポリシーなどです。DHCP サーバは、DHCP 応答内に Option 82 フィールドをエコーします。
6. Cisco NX-OS デバイスがサーバへの要求を中継した場合、DHCP サーバはその NX-OS デバイスに応答をユニキャストします。Cisco NX-OS デバイスは、リモート ID フィールド、および場合によっては回線 ID フィールドを検査することで、最初に Option 82 データを挿入したのがこのデバイス自身であることを確認します。Cisco NX-OS デバイスは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントと接続しているインターフェイスにパケットを転送します。

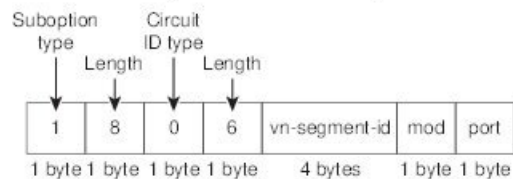
次の図は、回線 ID サブオプションおよびリモート ID サブオプションのパケット形式を示しています。

Figure 13: サブオプションの packets 形式

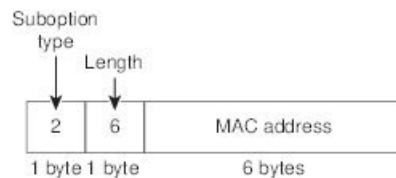
Circuit ID Suboption Frame Format (for non-VXLAN VLANs)



Circuit ID Suboption Frame Format (for VXLAN VLANs)



Remote ID Suboption Frame Format



349 (28)

DHCP リレー エージェントに対する VRF サポート

DHCP ブロードキャスト メッセージを Virtual Routing and Forwarding (VRF; 仮想ルーティング/転送) インスタンスのクライアントから別の VRF の DHCP サーバに転送するように、DHCP リレー エージェントを設定できます。単一の DHCP サーバを使用して複数の VRF のクライアントの DHCP をサポートできるため、IP アドレス プールを VRF ごとではなく 1 つにまとめることにより、IP アドレスを節約できます。VRF の一般的な情報については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

DHCP リレー エージェントに対する VRF サポートをイネーブルにするには、DHCP リレー エージェントに対する Option 82 をイネーブルにする必要があります。

DHCP リレー アドレスと VRF 情報を設定したインターフェイスに DHCP 要求が着信した場合、DHCP サーバのアドレスが、別の VRF のメンバであるインターフェイスのネットワークに属するものであれば、デバイスは要求に Option 82 情報を挿入し、サーバの VRF の DHCP サーバに転送されます。Option 82 情報は次のとおりです。

VPN 識別子

DHCP 要求を受信するインターフェイスが属する VRF の名前。

リンクの選択

DHCP 要求を受信するインターフェイスのサブネット アドレス。DHCP スマート リレーがイネーブルの場合、リンクの選択にはアクティブな `giaddr` のサブネットが指定されます。

サーバ識別子オーバーライド

DHCP 要求を受信するインターフェイスの IP アドレス。DHCP スマート リレーがイネーブルの場合、サーバの識別子にはアクティブな `giaddr` が指定されます。



- (注) DHCPサーバは、VPN識別子、リンクの選択、サーバ識別子オーバーライドの各オプションをサポートする必要があります。

デバイスは DHCP 応答メッセージを受信すると、Option 82 情報を取り除き、クライアントの VRF の DHCP クライアントに応答を転送します。

DHCP スマート リレー エージェント

DHCP リレー エージェントは、ホストからブロードキャスト DHCP 要求パケットを受信すると、インバウンドインターフェイスのプライマリ アドレスに `giaddr` を設定し、それらのパケットをサーバに転送します。サーバは、プールが使い果たされるまで `giaddr` サブネット プールから IP アドレスを割り当て、それ以降の要求を無視します。

最初のサブネットプールが使い果たされるか、またはサーバがそれ以降の要求を無視した場合は、セカンダリ IP アドレス サブネット プールから IP アドレスを割り当てるように DHCP スマート リレー エージェントを設定できます。この機能拡張は、ホストの数がプール内の IP アドレスの数を超えている場合や、セカンダリ アドレスを使用してインターフェイス上に複数のサブネットが設定されている場合に有効です。

DHCPv6 リレー エージェントについて

DHCPv6 リレー エージェント

DHCPv6 リレー エージェントを実行するようにデバイスを設定できます。DHCPv6 リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送します。これは、クライアントとサーバが同じ物理サブネット上にない場合に便利な機能です。リレー エージェントは DHCPv6 メッセージを受信すると、新規の DHCPv6 メッセージを生成して別のインターフェイスに送信します。リレー エージェントはゲートウェイ アドレス (DHCPv6 パケットの `giaddr` フィールド) をセットし、DHCPv6 サーバに転送します。

DHCPv6 リレー エージェントに対する VRF サポート

DHCPv6 ブロードキャスト メッセージを仮想ルーティング/転送 (VRF) インスタンスのクライアントから別の VRF の DHCPv6 サーバに転送するように、DHCPv6 リレー エージェントを設定できます。単一の DHCPv6 サーバを使用して複数の VRF のクライアントの DHCP をサポートできるため、IP アドレス プールを VRF ごとではなく 1 つにまとめることにより、IP アドレスを節約できます。VRF の一般的な情報については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

v6 リレー エージェントを介した委任プレフィックスの IPv6 可用性

DHCPv6 プレフィックス委任 (DHCPv6-PD) 機能は、完全なサブネットおよびその他のネットワークおよびインターフェイス パラメータを DHCPv6-PD サーバから DHCPv6-PD クライアントに割り当てることを目的としています。これは、RFC3633 で定義されている DHCPv6 リレー エージェントの拡張です。



- (注)
- プレフィックス委任は、First Hop Security (FHS) とインターワーキングしません。
 - DHCPv6 は、リレー チェーンによるプレフィックス委任をサポートしていません。

リレーエージェントは、IANA オプションを使用して、勧誘パケットで受信したネットワークアドレス要求を DHCPv6 サーバに転送します。クライアントがプレフィックスアドレスも必要とする場合、要求に IAPD オプションを追加します。DHCPv6 サーバは、プールで使用方法可能な場合、要求されたプレフィックスを委任します。

CLI が有効になっている場合、DHCPv6-PD は、プレフィックスがスイッチからルーティングできるように、委任されたプレフィックスのスイッチに静的ルートを追加します。DHCPv6-PD バインドは、委任されたプレフィックス用に作成された IPv6 ルートとともに、クライアントごとに作成されます。

追加された静的ルートは、OSPFv3 ルーティング プロトコルを介してネイバーに配布されます。



- (注)
- 現在、DHCPv6-PD ルート配布は、IS-IS、BGP などの他の回送プロトコルではサポートされていません。詳細については、『Cisco Nexus 9000 Series NX-OS ユニキャスト ルーティング構成ガイド』の「再配布の構成」のセクションを参照してください。

DHCPv6 スマート リレー エージェント

DHCPv6 スマート リレー エージェントは、ホストから請求パケットを受信すると、インバウンドインターフェイスのアドレスにリンク アドレスを設定し、それらのパケットをサーバに

転送します。サーバは、プールが使い果たされるまでリンク アドレス サブネット プールから IP アドレスを割り当て、それ以降の要求を無視します。

最初のサブネットプールが使い果たされるか、またはサーバがそれ以降の要求を無視した場合は、セカンダリ IP アドレス サブネット プールから IP アドレスを割り当てるように DHCPv6 スマート リレー エージェントを設定できます。この機能拡張は、ホストの数がプール内の IP アドレスの数を超えている場合や、セカンダリアドレスを使用してインターフェイス上に複数のサブネットが設定されている場合に有効です。任意のアドレスサブネットプールから IP アドレスを割り当てることができます。

DHCPv6 スマート リレーの注意事項と制約事項

DHCPv6 スマート リレーの注意事項および制約事項は、次のとおりです。

- vPC環境では、インターフェイスのIPv6アドレスのサブネットが両方のスイッチで同じであることが推奨されます。
- インスタンスでDHCPv6スマートリレーを使用するホストの数は10000に制限されています。
- クラウドベースのプラットフォームでサポートされます。

DHCP クライアントについて

DHCP クライアント機能によって、インターフェイスに IPv4 または IPv6 アドレスを設定できます。インターフェイスには、ルーテッドポート、管理ポート、スイッチ仮想インターフェイス (SVI) が含まれます。

DHCP の前提条件

DHCP の前提条件は、次のとおりです。

- DHCP スヌーピングまたは DHCP リレー エージェントを設定するためには、DHCP についての知識が必要です。

DHCP のガイドラインと制約事項

DHCP 設定時の注意事項と制約事項は次のとおりです。

- POAP の安全性を確保するために、DHCP スヌーピングが有効であることを確認し、ファイアウォール ルールを設定して意図しない、または悪意のある DHCP サーバをブロックしてください。

- Cisco Nexus 9000 シリーズ スイッチは、bootp パケットのリレーをサポートしていません。ただし、スイッチはレイヤ 2 スイッチの bootp パケットをサポートします。
- DHCP サブネット ブロードキャストはサポートされていません。
- 最高の DHCP スヌーピングスケールをサポートするには、DHCP パケットの Option 82 情報の挿入を有効にする必要があります。
- デバイス上でグローバルに DHCP スヌーピングを有効化するには、DHCP サーバおよび DHCP リレーエージェントとして機能するデバイスを、事前に設定し有効にしておく必要があります。
- ネットワークで DHCP スヌーピングの後に DHCP リレーが続くことはできません (DHCP スヌーピングは、同じ Cisco Nexus デバイスで DHCP リレーが設定されている場合、機能しません)。
- DHCP スヌーピング、DAI と FHS は、-R/-RX/-R2 ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチではサポートされていません。
- DHCP スヌーピングは VXLAN VLAN ではサポートされません。
- DHCP スヌーピングは、同じ MAC アドレスと VLAN をスタティック バインディング エントリに持つ複数の IP アドレスをサポートします。
- DHCP サーバがデフォルト VRF を介して到達可能な場合、VXLAN は DHCP リレーをサポートします。
- DHCP スヌーピングを使用して設定を行っている VLAN で VLAN ACL (VACL) が設定されている場合、その VACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。VLAN およびその VLAN の SVI 上で DHCP スヌーピングと DHCP リレーの両方が有効になっていると、DHCP リレーが優先されます。
- DHCP サーバアドレスを使用して設定を行っているレイヤ 3 インターフェイスで入力ルータ ACL が設定されている場合、そのルータ ACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。
- DHCP クライアントおよびサーバが異なる VRF に存在する状態で DHCP リレーを使用する場合、VRF 内で 1 つの DHCP サーバだけを使用します。
- DHCP スヌーピング機能が有効のときには、アクセス コントロール リスト (ACL) の統計情報はサポートされません。
- vPC リンク内のスイッチ間で DHCP 設定が同期されていることを確認します。同期されていないと、ランタイム エラーが発生し、パケットがドロップされる場合があります。
- DHCP スマートリレーは、有効であるインターフェイスの IP アドレスのうち、最初の 100 個に制限されます。
- DHCP スマートリレーを使用するには、インターフェイスでヘルパーアドレスを設定する必要があります。

- vPC 環境で DHCP スマートリレーが有効になっている場合、プライマリ インターフェイスの IP アドレスはピア間でサブネットを共有する必要があります。セカンダリ インターフェイスの IP アドレスも、ピア間でサブネットを共有する必要があります。
- インターフェイスで DHCPv6 サーバアドレスを設定する場合は、宛先インターフェイスをグローバル IPv6 アドレスで使用することはできません。
- DHCPv6 クライアントが再バインドを開始すると、DHCPv6-PD ルートは生成されません。クライアントの既存の IAPD エントリは更新されますが、作成されません。IAPD ルートを作成するには、DHCPv6 リレーエージェントが完全な送信要求、アドバタイズ、要求、応答を確認する必要があります。
- 番号が付けられないインターフェイスで DHCP リレーを使用する場合は、オプション 82 を挿入するようにスイッチを設定する必要があります。
- オプション 14 **Rapid Commit** が存在する場合、DHCPv6 プレフィックス委任ルートは生成されません。IAPD ルートを生成するには、送信要求、アドバタイズ、要求、応答の完全なシーケンスが必要です。
- DHCP クライアント機能には、次のガイドラインと制限事項が適用されます。
 - 複数のSVIを設定できますが、各インターフェイスVLANは異なるサブネットにある必要があります。DHCPクライアント機能では、同じデバイス上の異なるインターフェイスVLANに同じサブネットを持つ異なるIPアドレスを設定することはできません。
 - DHCPクライアントとDHCPリレーは、同じスイッチではサポートされません。
 - DHCPクライアントは、レイヤ3サブインターフェイスではサポートされません。
 - Cisco Nexus 9300 シリーズ スイッチおよび Cisco Nexus 9500 シリーズ スイッチでは、DHCP クライアントがサポートされています。
 - DHCP クライアントは、N9K-X9636C-R、N9K-X9636C-RX、N9K-X9636Q-R、および N9K-X96136YC-R ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチではサポートされません。
- Cisco NX-OS リリース 9.3(3) 以降、DHCP スヌーピングおよび DHCP リレーは Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチでサポートされています。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 スイッチの Cisco Nexus X9836DM-A ライン カードで DHCP リレーがサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9808 スイッチの Cisco Nexus X98900CD-A ライン カードで DHCP リレーがサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、DHCP リレーは Cisco Nexus 9804 スイッチ、Cisco Nexus X98900CD-A および X9836DM-A ライン カードでサポートされます。
- Cisco NX-OS リリース 10.5(3)F 以降、Cisco Nexus 93C64E-SG2-Q スイッチでは DHCP リレーがサポートされています。



(注) DHCP 設定制限については、『Cisco Nexus 9000 シリーズ NX-OS 検証スケーラビリティ ガイド』を参照してください。

Cisco Nexus 9336C-SE1 スイッチ上の CoPP のガイドラインと制限事項

- Cisco NX-OS リリース 10.6(1)F 以降、DHCP リレーは Cisco Nexus 9336C-SE1 スイッチでサポートされます。
- DHCP リレーがスイッチで設定され、RACL も適用される場合、RACL はユニキャスト DHCP リレー トラフィックをドロップします。これは、RACL およびその他のセキュリティ ポリシーの処理順序が、DHCP リレーなどのコントロールプレーン トラフィックよりも高い優先順位を持つために発生します。

DHCP のデフォルト設定

次の表に、DHCP パラメータのデフォルト設定を示します。

Table 32: デフォルトの DHCP パラメータ

パラメータ	デフォルト
DHCP 機能	ディセーブル
DHCP スヌーピング	ディセーブル
VLAN 上で DHCP スヌーピング	無効
DHCP スヌーピングの MAC アドレス検証	有効
DHCP スヌーピングの Option 82 サポート	ディセーブル
DHCP スヌーピング信頼状態	信頼できない
DHCP リレー エージェント	イネーブル
DHCPv6 リレー エージェント	イネーブル
DHCP リレー エージェントに対する VRF サポート	ディセーブル

パラメータ	デフォルト
DHCPv6 リレー エージェントに対する VRF サポート	ディセーブル
リレー エージェントの DHCP Option 82	ディセーブル
DHCP スマート リレー エージェント	ディセーブル
DHCP サーバの IP アドレス	なし

DHCP の設定

DHCP の最小設定

Procedure

ステップ 1 DHCP 機能をイネーブルにします。

DHCP 機能がディセーブルになっていると、DHCP スヌーピングを設定できません。

ステップ 2 DHCP スヌーピングをグローバルにイネーブルにします。

ステップ 3 少なくとも 1 つの VLAN で、DHCP スヌーピングをイネーブルにします。

デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。

ステップ 4 DHCP サーバとデバイスが、信頼できるインターフェイスを使用して接続されていることを確認します。

ステップ 5 (Optional) DHCP リレー エージェントをイネーブルにします。

ステップ 6 (Optional) DHCP サーバとクライアントが異なる VRF に存在する場合は、次の手順に従います。

- DHCP リレー エージェントの Option 82 をイネーブルにします。
- DHCP リレー エージェントに対して VRF サポートをイネーブルにします。

ステップ 7 (Optional) インターフェイスに DHCP サーバの IP アドレスを設定します。

DHCP 機能のイネーブル化またはディセーブル化

デバイスの DHCP 機能をイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP はディセーブルです。

DHCP 機能がディセーブルの場合、DHCP リレー エージェント、DHCP スヌーピング、および DHCP に依存するすべての機能は設定できません。また、すべての DHCP 設定がデバイスから削除されます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] feature dhcp Example: switch(config)# feature dhcp	DHCP 機能をイネーブルにします。 no オプションを使用すると、DHCP 機能がディセーブルになり、DHCP 設定が消去されます。
ステップ 3	(Optional) show running-config dhcp Example: switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP スヌーピングの設定

DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化

デバイスに対して DHCP スヌーピング機能のグローバルなイネーブル化またはディセーブル化が可能です。

Before you begin

DHCP 機能がイネーブルになっていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] ip dhcp snooping Example: switch(config)# ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブル化します。このコマンドの no 形式を使用すると、DHCP スヌーピングがディセーブルになります。
ステップ 3	(Optional) show running-config dhcp Example: switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化

1 つまたは複数の VLAN に対して DHCP スヌーピングをイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。

Before you begin

DHCP 機能がイネーブルにされていることを確認します。



Note

DHCP スヌーピングを使用して設定を行っている VLAN で VACL が設定されている場合、その VACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example:	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。

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	[no] ip dhcp snooping vlan <i>vlan-list</i> Example: switch(config)# ip dhcp snooping vlan 100,200,250-252	<i>vlan-list</i> で指定する VLAN の DHCP スヌーピングをイネーブルにします。このコマンドの no 形式を使用すると、指定した VLAN の DHCP スヌーピングがディセーブルになります。
ステップ 3	(Optional) show running-config dhcp Example: switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP スヌーピングの MAC アドレス検証のイネーブル化またはディセーブル化

DHCP スヌーピングの MAC アドレス検証をイネーブルまたはディセーブルにします。信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合、アドレス検証によってデバイスはパケットをドロップします。MAC アドレス検証はデフォルトでイネーブルになります。

Before you begin

DHCP 機能がイネーブルにされていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# config t switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] ip dhcp snooping verify mac-address Example: switch(config)# ip dhcp snooping verify mac-address	DHCP スヌーピングの MAC アドレス検証をイネーブルにします。このコマンドの no 形式を使用すると、MAC アドレス検証がディセーブルになります。
ステップ 3	(Optional) show running-config dhcp Example:	DHCP 設定を表示します。

	Command or Action	Purpose
	<code>switch(config)# show running-config dhcp</code>	
ステップ 4	(Optional) copy running-config startup-config Example: <code>switch(config)# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Option 82 データの挿入および削除の有効化または無効化

DHCP リレー エージェントを使用せずに転送された DHCP パケットへの Option 82 情報の挿入および削除を有効または無効にできます。デフォルトでは、デバイスは DHCP パケットに Option 82 情報を挿入しません。



Note Option 82 に対する DHCP リレー エージェントのサポートは、個別に設定されます。



Note より大きい DHCP pps の規模をサポートするには、DHCP パケットへの Option 82 情報の挿入を有効にします。



Note Option82 はコマンド コンフィギュレーションのフォーマット文字列で指定されているように追加する必要があります。

- Option82 文字列の長さは、フォーマット文字列の長さに応じて長くなります。
- 回線 ID には、フォーマット文字列の ASCII 値を含める必要があります。

Before you begin

DHCP 機能が有効にされていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル設定モードを開始します。

	Command or Action	Purpose
ステップ 2	[no] ip dhcp snooping information option Example: <pre>switch(config)# ip dhcp snooping information option</pre>	DHCP パケットの Option 82 情報の挿入および削除を有効にします。このコマンドの no 形式を使用すると、Option 82 情報の挿入および削除が無効になります。
ステップ 3	(Optional) [no] ip dhcp option82 sub-option circuit-id format_type string format Example: <pre>switch(config)# ip dhcp snooping sub-option circuit-id format-type string format</pre> Example: <pre>switch(config)# ip dhcp snooping sub-option circuit-id format-type string format? WORD Format string (Max Size 64)</pre>	Option 82 を次のように設定します。 • <i>format-type</i> を指定しない場合には、<i>circuit-id</i> には入力ポートが表示されます。たとえば <i>ethernet1/1</i> のようになります。 • フォーマットで <i><word></i> を指定すると、<i>circuit-id</i> には指定した単語が表示されます。 • <i>%h</i> を (<i><word></i> の代わりに) 指定すると、<i>circuit-id</i> にはホスト名が表示されます。 • <i>%p</i> を (<i><word></i> の代わりに) 指定すると、<i>circuit-id</i> にはポート名が表示されます。 • <i>%h:%p</i> を (<i><word></i> の代わりに) 指定すると、<i>circuit-id</i> にはホストとポート両方の名前が表示されます。 Note <i>no</i> オプションを使用すると、この動作が無効になります。
ステップ 4	(Optional) [no] ip dhcp snooping sub-option format non-tlv Example: <pre>switch(config)# ip dhcp snooping sub-option format non-tlv</pre>	オプション 82 情報の回路 ID およびリモート ID サブオプションからサブタイプとその長さを削除します。
ステップ 5	interface interface slot/port Example: <pre>switch(config)# interface ethernet 2/2 switch(config-if)#</pre>	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。slot port は、スヌーピングを有効または無効にするインターフェイスです。

	Command or Action	Purpose
ステップ 6	(Optional) ip dhcp option82 sub-option circuit-id Example: <pre>switch(config-if)# ip dhcp option82 sub-option circuit-id? WORD Format string (Max Size 64)</pre> Example: <pre>switch(config-if)# ip dhcp option82 sub-option circuit-id test switch(config-if)#</pre>	インターフェイスでオプション 82 を設定します。 Note このコマンドは、SVI およびサブインターフェイスではサポートされていません。 Note <i>no</i> オプションを使用すると、この動作が無効になります。
ステップ 7	exit Example: <pre>switch(config-if)# exit switch(config)#</pre>	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 8	(Optional) show ip dhcp option82 info interface intf_name	DHCP 設定を表示します。そのインターフェイスで option82 が有効か無効か、および option82 が有効になっているインターフェイスの送信パケットが表示されます。
ステップ 9	(Optional) show running-config dhcp Example: <pre>switch(config)# show running-config dhcp</pre>	DHCP 設定を表示します。
ステップ 10	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

DHCP パケットの厳密な検証のイネーブル化またはディセーブル化

DHCP パケットの厳密な検証をイネーブルまたはディセーブルにできます。デフォルトでは、DHCP パケットの厳密な検証はディセーブルになっています。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example:	グローバル設定モードを開始します。

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	[no] ip dhcp packet strict-validation Example: switch(config)# ip dhcp packet strict-validation	DHCP パケットの厳密な検証をイネーブルにします。このコマンドの no 形式を使用すると、DHCP パケットの厳密な検証がディセーブルになります。
ステップ 3	(Optional) show running-config dhcp Example: switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの信頼状態の設定

各インターフェイスが DHCP メッセージの送信元として信頼できるかどうかを設定できます。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。DHCP の信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 ポート チャネル インターフェイス

Before you begin

DHCP 機能がイネーブルにされていることを確認します。

ユーザがそのインターフェイスをレイヤ 2 インターフェイスとして設定していることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	次のいずれかのオプションを使用します。 • interface ethernet slot/port	• 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。 <i>slot/port</i> は、DHCP スヌーピングで

	Command or Action	Purpose
	interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	trusted または untrusted に設定するレイヤ 2 イーサネット インターフェイスです。 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。 <i>slot/port</i> は、DHCP スヌーピングで trusted または untrusted に設定するレイヤ 2 ポートチャネル インターフェイスです。
ステップ 3	[no] ip dhcp snooping trust Example: <pre>switch(config-if)# ip dhcp snooping trust</pre>	DHCP スヌーピングに関して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します。このコマンドの no 形式を使用すると、ポートは信頼できないインターフェイスとして設定されます。
ステップ 4	(Optional) show running-config dhcp Example: <pre>switch(config-if)# show running-config dhcp</pre>	DHCP 設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー信頼ポート機能のイネーブル化またはディセーブル化

DHCP リレー信頼ポート機能をイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP パケット内のゲートウェイアドレスがすべてゼロに設定され、リレー情報オプションがすでにパケット内に存在する場合、DHCP リレー エージェントはパケットを廃棄しません。**ip dhcp relay information option trust** コマンドをグローバルに設定すると、ゲートウェイアドレスがすべてゼロに設定された場合、DHCP リレー エージェントはパケットを廃棄します。

始める前に

DHCP 機能がイネーブルにされていることを確認します。

インターフェイスを DHCP リレーの信頼済みまたは信頼できないポートとして設定する

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] ip dhcp relay information option trust 例： switch(config)# ip dhcp relay information option trust	DHCP リレー信頼ポートの機能を有効にします。このコマンドの no 形式を使用すると、この機能がディセーブルになります。
ステップ 3	(任意) show ip dhcp relay 例： switch(config)# show ip dhcp relay	DHCP リレーの設定を表示します。
ステップ 4	(任意) show ip dhcp relay information trusted-sources 例： switch(config)# show ip dhcp relay information trusted-sources	DHCP リレー信頼ポート設定を表示します。
ステップ 5	(任意) show running-config dhcp 例： switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 6	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

インターフェイスを DHCP リレーの信頼済みまたは信頼できないポートとして設定する

レイヤ3 インターフェイスは、DHCP リレー信頼または非信頼インターフェイスとして設定できます。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。DHCP リレーの信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ3 イーサネット インターフェイスおよびサブインターフェイス
- レイヤ3 ポート チャネル インターフェイス

始める前に

DHCP 機能がイネーブルにされ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 例 : <pre>switch# configure terminal switch(config)#</pre>	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 [ethernet slot/port[.number] port-channel channel-number] 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。ここで、 slot/port は、信頼または非信頼として設定するレイヤ 3 イーサネット インターフェイスです。 channel-number は、信頼または非信頼として設定するレイヤ 3 ポートチャネルインターフェイスです。
ステップ 3	[no] ip dhcp relay information trusted 例 : <pre>switch(config-if)# ip dhcp relay information trusted</pre>	インターフェイスを DHCP リレーエージェント情報の信頼できるインターフェイスとして設定します。このコマンドの no 形式を使用すると、ポートは信頼できないインターフェイスとして設定されます。 (注) 任意のレイヤ 3 インターフェイスで、インターフェイスが global コマンドまたはインターフェイス レベル コマンドのいずれかによって信頼できるように設定されている場合、そのインターフェイスは信頼できるインターフェイスと見なされます。したがって、信頼済みポート コマンドがグローバル レベルで有効になっている場合、レイヤ 3 インターフェイスはインターフェイス レベル設定では信頼できない中断としてみなされます。
ステップ 4	(任意) show ip dhcp relay information trusted-sources 例 : <pre>switch(config-if)# show ip dhcp relay information trusted-sources</pre>	DHCP リレー信頼ポート設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	(任意) show running-config dhcp 例 : switch(config-if)# show running-config dhcp	DHCP 設定を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : switch(config-if)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

すべてのインターフェイスの信頼状態の設定

すべてのレイヤ 3 インターフェイスは、DHCP リレー信頼または非信頼インターフェイスとして設定できます。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。DHCP リレーの信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 3 イーサネット インターフェイスおよびサブインターフェイス
- レイヤ 3 ポート チャネル インターフェイス

ip dhcp relay information trust-all コマンドをイネーブルにすると、インターフェイス レベルの設定に関係なく、どのレイヤ 3 インターフェイスも非信頼とは見なされなくなります。

始める前に

DHCP 機能がイネーブルにされ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 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] ip dhcp relay information trust-all 例 : switch(config)# ip dhcp relay information trust-all	インターフェイスを DHCP メッセージの信頼できる送信元として設定します。このコマンドの no 形式を使用すると、ポートは信頼できないインターフェイスとして設定されます。
ステップ 3	(任意) show ip dhcp relay information trusted-sources 例 :	DHCP リレー信頼ポート設定を表示します。

	コマンドまたはアクション	目的
	<code>switch(config)# show ip dhcp relay information trusted-sources</code>	
ステップ 4	(任意) show running-config dhcp 例 : <code>switch(config)# show running-config dhcp</code>	DHCP 設定を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <code>switch(config)# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー エージェントのイネーブル化またはディセーブル化

DHCP リレー エージェントをイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP リレー エージェントはイネーブルです。

Before you begin

DHCP 機能がイネーブルになっていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル設定モードを開始します。
ステップ 2	[no] ip dhcp relay Example: <code>switch(config)# ip dhcp relay</code>	DHCP リレー エージェントをイネーブルにします。 no オプションを使用すると、DHCP リレー エージェントがディセーブルになります。
ステップ 3	(Optional) show ip dhcp relay Example: <code>switch(config)# show ip dhcp relay</code>	DHCP リレーの設定を表示します。
ステップ 4	(Optional) show running-config dhcp Example: <code>switch(config)# show running-config dhcp</code>	DHCP 設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー エージェントに対する Option 82 の有効化または無効化

デバイスに対し、リレー エージェントによって転送された DHCP パケットへの Option 82 情報の挿入と削除を有効または無効にできます。

デフォルトでは、DHCP リレー エージェントは DHCP パケットに Option 82 情報を挿入しません。

Before you begin

DHCP 機能が有効になっていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	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	switch(config)# [no] ip dhcp relay information option	DHCP リレー エージェントによって転送されるパケットに対する Option 82 情報の挿入および削除を有効にします。Option 82 情報は、デフォルトでバイナリ ifIndex 形式です。 no オプションを使用すると、この動作が無効になります。
ステップ 3	(Optional) switch(config)# [no] ip dhcp relay sub-option circuit-id customized	VLAN+スロット+ポート形式で Option 82 をプログラムします。このコマンドは、SVIにのみ適用されます。 no オプションを使用すると、この動作が無効になります。
ステップ 4	(Optional) [no] ip dhcp relay sub-option format non-tlv Example: <pre>switch(config)# ip dhcp relay sub-option format non-tlv</pre>	オプション 82 情報の回路 ID およびリモート ID サブオプションからサブタイプとその長さを削除します。

	Command or Action	Purpose
ステップ 5	(Optional) switch(config)# [no] ip dhcp relay sub-option circuit-id format-type string	デフォルトの ifIndex バイナリ形式の代わりに符号化されたストリング形式を使用するように、オプション 82 を設定します。no オプションを使用すると、この動作が無効になります。 VLAN および SVI の場合： - このコマンドと ip dhcp relay sub-option circuit-id カスタマイズ コマンドの両方を設定すると、ip dhcp relay sub-option circuit-id format-type string コマンドがプログラムされます。 ip dhcp relay sub-option circuit-id format-type string コマンドを削除すると、ip dhcp relay sub-option circuit-id カスタマイズ コマンドがプログラムされます。 - 両方のコマンドが削除されると、ifindex がプログラムされます。 他のインターフェイスでは、ip dhcp relay sub-option circuit-id format-type string コマンドが設定されている場合は、それが使用されます。それ以外の場合は、デフォルトの ifindex がプログラムされます。
ステップ 6	(Optional) switch(config)# show ip dhcp relay	DHCP リレーの設定を表示します。
ステップ 7	(Optional) switch(config)# show running-config dhcp	DHCP 設定を表示します。 Note このコマンドの出力では、二重引用符の有無の設定にかかわらず、circuit-id パラメータ値が二重引用符で囲まれて表示されます。
ステップ 8	(Optional) switch(config)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

DHCP リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化

ある VRF のインターフェイスで受信した DHCP 要求を、別の VRF の DHCP サーバにリレーする機能をサポートするように、デバイスを設定できます。

始める前に

DHCP リレー エージェントの Option 82 をイネーブルに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 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] ip dhcp relay information option vpn 例 : switch(config)# ip dhcp relay information option vpn	DHCP リレーエージェントに対して VRF サポートをイネーブルにします。 no オプションを使用すると、この動作がディセーブルになります。
ステップ 3	[no] ip dhcp relay sub-option type cisco 例 : switch(config)# ip dhcp relay sub-option type cisco	リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID リレー エージェント Option 82 サブオプションを設定する場合は、DHCP をイネーブルにして、シスコ独自の番号である 150、152、および 151 を使用します。 no オプションを使用すると、DHCP では、リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID サブオプションに対して、RFC 番号 5、11、151 が使用されるようになります。
ステップ 4	(任意) show ip dhcp relay 例 : switch(config)# show ip dhcp relay	DHCP リレーの設定を表示します。
ステップ 5	(任意) show running-config dhcp 例 : switch(config)# show running-config dhcp	DHCP 設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP Server Identifier オーバーライド サブオプション

Cisco NX-OS リリース 9.3(3) 以降では、サーバ ID オーバーライド オプションを無効にできます。このオプションは、DHCP リレー VPN 設定または送信元インターフェイス設定の DHCP オプション 82 パケットにはデフォルトで追加されます。

始める前に

DHCP リレー エージェントの Option 82 をイネーブルに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 例 : <pre>switch# configure terminal</pre>	グローバル設定モードを開始します。
ステップ 2	[no] ip dhcp relay information option server-id-override-disable 例 : <pre>switch(config)# ip dhcp relay information option server-id-override-disable</pre>	DHCP オプション 82 パケットのサーバ ID オーバーライド オプションを無効にします。 (注) このコマンドの no 形式を使用すれば、サーバ ID オーバーライド オプションを再度有効にできます。

インターフェイスへの DHCP サーバアドレスの設定

1 つのインターフェイスに複数の DHCP サーバ IP アドレスを設定できます。インバウンド DHCP BOOTREQUEST パケットがインターフェイスに着信すると、リレー エージェントはそのパケットを指定されたすべての DHCP サーバ IP アドレスに転送します。リレー エージェントは、すべての DHCP サーバからの応答を、要求を送信したホストへ転送します。

Before you begin

DHCP 機能が有効になっていることを確認します。

DHCP サーバが正しく設定されていることを確認します。

インターフェイスに設定する、各 DHCP サーバの IP アドレスを決定します。

DHCP サーバがインターフェイスとは異なる VRF に含まれている場合、VRF サポートがイネーブルになっていることを確認します。



Note DHCP サーバアドレスを設定しているインターフェイスで入力ルータ ACL が設定されている場合、そのルータ ACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	次のいずれかのオプションを使用します。 • interface ethernet <i>slot/port</i>[<i>.number</i>] • interface vlan <i>vlan-id</i> • interface port-channel <i>channel-id</i>[<i>.subchannel-id</i>] Example: <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	• 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。 <i>slot/port</i> は、DHCP サーバ IP アドレスを設定する物理イーサネット インターフェイスです。サブインターフェイスを設定する場合は、<i>number</i> 引数を使用してサブインターフェイス番号を指定します。 Note ポートチャネル サブインターフェイスは、Cisco NX-OS リリース 6.1(2)I3(3) および 6.1(2)I3(3a) のみサポートされます。Cisco NX-OS リリース 9.2(1) ではサポートされていません。 • 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。<i>vlan-id</i> は、DHCP サーバ IP アドレスを設定する VLAN の ID です。 • 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。 <i>channel-id</i> は、DHCP サーバ IP アドレスを設定するポート チャネル

	Command or Action	Purpose
		の ID です。サブチャネルを設定する場合は、 <i>subchannel-id</i> 引数を使用してサブチャネル ID を指定します。
ステップ 3	ip dhcp relay address <i>IP-address</i> [<i>use-vrf</i> <i>vrf-name</i>] Example: <pre>switch(config-if)# ip dhcp relay address 10.132.7.120 use-vrf red</pre>	リレーエージェントがこのインターフェイスで受信した BOOTREQUEST パケットを転送する DHCP サーバの IP アドレスを設定します。 複数の IP アドレスを設定するには、アドレスごとに ip dhcp relay address コマンドを使用します。
ステップ 4	(Optional) show ip dhcp relay address Example: <pre>switch(config-if)# show ip dhcp relay address</pre>	設定済みのすべての DHCP サーバアドレスを表示します。
ステップ 5	(Optional) show running-config dhcp Example: <pre>switch(config-if)# show running-config dhcp</pre>	DHCP 設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー送信元インターフェイスの設定

DHCP リレーエージェントの送信元インターフェイスを設定できます。デフォルトでは、DHCP リレー エージェントは発信パケットの送信元アドレスとしてリレー エージェント アドレスを使用します。送信元インターフェイスを設定すると、リレーされたメッセージの送信元アドレスとして、より安定したアドレス（ループバック インターフェイス アドレスなど）を使用することができます。DHCP リレーの送信元インターフェイスが設定されている場合、送信元インターフェイスの VRF が DHCP サーバの VRF と同じである場合、デバイスは設定された送信元インターフェイスの IP アドレスを **giaddr** として DHCP パケットに追加します。それ以外の場合、サーバーに到達可能なインターフェイスの IP アドレスが **giaddr** として使用されます。

始める前に

DHCP 機能がイネーブルになっていることを確認します。

DHCP リレー エージェントがイネーブルであることを確認します。

CLI dhcp リレー情報オプションと ip dhcp リレー情報オプション vpn が有効になっ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 例 : <pre>switch# configure terminal switch(config)#</pre>	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] ip dhcp relay source-interface interface 例 : <pre>switch(config)# ip dhcp relay source-interface loopback 2</pre>	DHCP リレー エージェントの送信元 インターフェイスを設定します。 (注) - DHCP リレー送信元インターフェイスは、グローバルに、インターフェイスごとに、またはその両方に設定できます。グローバルおよびインターフェイス レベルの両方が設定されている場合は、インターフェイス レベルの設定がグローバル設定を上書きします。 - 送信元インターフェイス設定を持つインターフェイスで DHCP リレーを設定する場合は、サーバーとクライアントが同じ VRF にあるか、異なる VRF にあるかには関係なく、Option 82 または VPN 設定が有効になっていることを確認してください。
ステップ 3	(任意) show ip dhcp relay [interface interface] 例 : <pre>switch(config)# show ip dhcp relay</pre>	DHCP リレーの設定を表示します。
ステップ 4	(任意) show running-config dhcp 例 : <pre>switch(config)# show running-config dhcp</pre>	DHCP 設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP スマート リレーのグローバルなイネーブル化またはディセーブル化

デバイスの DHCP スマート リレーをグローバルにイネーブルまたはディセーブルに設定できます。

Before you begin

DHCP 機能がイネーブルになっていることを確認します。

DHCP リレー エージェントがイネーブルであることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	[no] ip dhcp smart-relay global Example: <pre>switch(config)# ip dhcp smart-relay global</pre>	DHCP スマート リレーをグローバルにイネーブルにします。このコマンドの no 形式を使用すると、DHCP スマート リレーがディセーブルになります。
ステップ 3	(Optional) show ip dhcp relay Example: <pre>switch(config)# show ip dhcp relay</pre>	DHCP スマート リレー設定を表示します。
ステップ 4	(Optional) show running-config dhcp Example: <pre>switch(config)# show running-config dhcp</pre>	DHCP 設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ 3 インターフェイスでの DHCP スマート リレーの有効化または無効化

レイヤ 3 インターフェイスで DHCP スマート リレーを有効または無効に設定できます。

Before you begin

DHCP 機能がイネーブルになっていることを確認します。

DHCP リレー エージェントがイネーブルであることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	interface interface slot/port Example: <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	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。 <i>slot/port</i> は、DHCP スマート リレーを有効または無効にするインターフェイスです。
ステップ 3	[no] ip dhcp smart-relay Example: <pre>switch(config-if)# ip dhcp smart-relay</pre>	インターフェイスで DHCP スマート リレーを有効にします。このコマンドの no 形式を使用すると、DHCP スマート リレーが無効になります。
ステップ 4	exit Example: <pre>switch(config-if)# exit switch(config)#</pre>	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 5	exit Example: <pre>switch(config)# exit switch#</pre>	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。

	Command or Action	Purpose
ステップ 6	(Optional) show ip dhcp relay Example: switch# show ip dhcp relay	DHCP スマート リレー設定を表示します。
ステップ 7	(Optional) show running-config dhcp Example: switch# show running-config dhcp	DHCP 設定を表示します。
ステップ 8	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー サブネット選択の設定

インターフェイスにプライマリ IP アドレスとセカンダリ IP アドレスの両方が含まれている場合、デフォルトでは、DHCP リレーはプライマリサブネットに基づいてサーバに IP アドレスの割り当てを要求します。DHCP リレーでセカンダリ IP アドレスを使用する場合は、DHCP スマート リレーを有効にする必要があります。スマート リレーを有効にすると、DHCP リレーは最初にプライマリ サブネットの IP アドレスを要求します。プライマリ サブネットの IP アドレスを取得できない場合、セカンダリ サブネットの IP アドレスを要求します。セカンダリ サブネットの IP アドレスは、デフォルトでは選択されません。

DHCP リレーサブネット選択機能の導入により、要件に基づいてプライマリまたはセカンダリサブネットの IP アドレスを選択するオプションを利用できるようになりました。DHCP リレーサブネット選択を設定すると、DHCP リレー パケットには、送信元およびリレー エージェントのサブネット選択で使用するサブネットの情報が含まれるようになります。VPN または送信元インターフェイス オプションがある場合、オプション 82 のリンク選択は、設定されたサブネットに基づいて更新されます。

DHCP スマート リレーとサブネット選択の設定は、インターフェイス レベルでは相互に排他的です。DHCP スマート リレーがグローバルに有効になっており、サブネット選択がインターフェイス レベルで設定されている場合は、インターフェイス設定が優先されます。

DHCP VPN または送信元インターフェイス オプションでは、DHCP サーバはオプション 82 のリンク選択を使用して IP アドレスを割り当てる必要があります。

始める前に

DHCP 機能がイネーブルになっ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 例 : switch# configure terminal switch(config)#	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 vlan <i>vlan-id</i> 例 : switch(config)#interface vlan 3 switch(config-if)#	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	ip dhcp relay subnet-selection <i>ip address</i> 例 : switch(config-if)#ip dhcp relay subnet-selection 20.20.21.1	指定された IP アドレスの DHCP リレー サブネット選択を設定します。

DHCPv6 の設定

DHCPv6 リレー エージェントのイネーブル化またはディセーブル化

DHCPv6 リレー エージェントをイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCPv6 リレー エージェントはイネーブルです。

始める前に

DHCP 機能がイネーブルになっ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 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] ipv6 dhcp relay 例 : switch(config)# ipv6 dhcp relay	DHCPv6 リレー エージェントをイネーブルにします。 no オプションを使用すると、リレー エージェントがディセーブルになります。

	コマンドまたはアクション	目的
ステップ 3	(任意) show ipv6 dhcp relay [interface interface] 例 : switch(config)# show ipv6 dhcp relay	DHCPv6 リレーの設定を表示します。
ステップ 4	[no] ipv6 dhcp relay prefix-delegation route 例 : switch(config)# ipv6 dhcp relay prefix-delegation route	IPv6 プレフィックス ルートの追加を有効にします。 no オプションは、プレフィックス ルートの追加を無効にします。
ステップ 5	(任意) show ipv6 dhcp relay prefix-delegation 例 : switch(config)# show ipv6 dhcp relay prefix-delegation	DHCPv6 IAPD エントリ (クライアント IP、インターフェイス、リース タイマー、および委任されたプレフィックス) を表示します。
ステップ 6	(任意) show running-config dhcp 例 : switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCPv6 リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化

ある VRF のインターフェイスで受信した DHCPv6 要求を、別の VRF の DHCPv6 サーバにリレーする機能をサポートするように、デバイスを設定できます。

始める前に

DHCP 機能がイネーブルになっていることを確認します。

DHCPv6 リレー エージェントが有効であ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 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	[no] ipv6 dhcp relay option vpn 例 : <pre>switch(config)# ipv6 dhcp relay option vpn</pre>	DHCPv6 リレー エージェントに対して VRF サポートをイネーブルにします。 no オプションを使用すると、この動作がディセーブルになります。
ステップ 3	[no] ipv6 dhcp relay option type cisco 例 : <pre>switch(config)# ipv6 dhcp relay option type cisco</pre>	これにより、DHCPv6 リレー エージェントが、ベンダー固有オプションの一部として仮想サブネット選択 (VSS) の詳細情報を挿入します。 no オプションを使用すると、DHCPv6 リレー エージェントが VSS 詳細情報を、VSS オプションの一部として (68) 挿入します。これは、RFC-6607 で定義された動作です。このコマンドは、RFC-6607 に対応していないものの、クライアント VRF 名に基づいた IPv6 アドレスを割り当てる DHCPv6 サーバを使用する場合に役立ちます。
ステップ 4	(任意) show ipv6 dhcp relay [interface interface] 例 : <pre>switch(config)# show ipv6 dhcp relay</pre>	DHCPv6 リレーの設定を表示します。
ステップ 5	(任意) show running-config dhcp 例 : <pre>switch(config)# show running-config dhcp</pre>	DHCP 設定を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

DHCPv6 スマート リレーのグローバルな有効化または無効化

デバイスの DHCPv6 スマート リレーをグローバルに有効または無効に設定できます。

始める前に

DHCP 機能がイネーブルになっていることを確認します。

DHCPv6 リレー エージェントが有効であ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 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] ipv6 dhcp smart-relay global 例 : switch(config)# ipv6 dhcp smart-relay global	DHCPv6 スマート リレーをグローバルに有効にします。このコマンドの no 形式を使用すると、DHCPv6 スマート リレーが無効になります。
ステップ 3	(任意) show ipv6 dhcp relay 例 : switch(config)# show ipv6 dhcp relay	DHCPv6 スマート リレー設定を表示します。
ステップ 4	(任意) show running-config dhcp 例 : switch(config)# show running-config dhcp	DHCPv6 の設定を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

レイヤ 3 インターフェイスでの DHCPv6 スマート リレーの有効化または無効化

レイヤ 3 インターフェイスで DHCP スマート リレーを有効または無効に設定できます。

始める前に

DHCP 機能がイネーブルになっていることを確認します。

DHCPv6 リレー エージェントが有効であ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 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interface interface slot/port 例 : switch(config)# interface ethernet 2/3 switch(config-if)#	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。 <i>slot/port</i> は、DHCPv6 スマート リレーを有効または無効にするインターフェイスです。
ステップ 3	[no] ipv6 dhcp smart-relay 例 : switch(config-if)# ipv6 dhcp smart-relay	インターフェイスで DHCPv6 スマート リレーを有効にします。このコマンドの no 形式を使用すると、DHCPv6 スマート リレーが無効になります。
ステップ 4	exit 例 : switch(config-if)# exit switch(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ます。
ステップ 5	exit 例 : switch(config)# exit switch#	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 6	(任意) show ipv6 dhcp relay 例 : switch# show ipv6 dhcp relay	DHCPv6 スマート リレー設定を表示します。
ステップ 7	(任意) show running-config dhcp 例 : switch# show running-config dhcp	DHCPv6 の設定を表示します。
ステップ 8	(任意) copy running-config startup-config 例 : switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスへの DHCPv6 サーバアドレスの設定

1 つのインターフェイスに複数の DHCPv6 サーバ IP アドレスを設定できます。インバウンド DHCPv6 BOOTREQUEST パケットがインターフェイスに着信すると、リレー エージェントはそのパケットを指定されたすべての DHCP サーバ IP アドレスに転送します。リレー エージェントは、すべての DHCPv6 サーバからの応答を、要求を送信したホストへ転送します。

始める前に

DHCP 機能が有効になっていることを確認します。

DHCPv6 サーバが正しく設定されていることを確認します。

インターフェイスに設定する、各 DHCPv6 サーバの IP アドレスを決定します。

DHCPv6 サーバがインターフェイスとは異なる VRF に含まれている場合、VRF サポートがイネーブルになっていることを確認します。



- (注) DHCPv6 サーバアドレスを設定しているインターフェイスで入力ルータ ACL が設定されている場合、そのルータ ACL で DHCP サーバと DHCPv6 ホストの間の DHCP トラフィックが許可され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 例 : <pre>switch# configure terminal switch(config)#</pre>	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	次のいずれかのオプションを使用します。 • interface ethernet slot/port • interface port-channel channel-id 例 : <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	• 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。 <i>slot/port</i> は、DHCPv6 サーバ IP アドレスを設定する物理イーサネット インターフェイスです。 • 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。 <i>channel-id</i> は、DHCPv6 サーバ IP アドレスを設定するポート チャネルの ID です。
ステップ 3	[no] ipv6 dhcp relay address IPv6-address [use-vrf vrf-name] [interface interface] 例 :	リレー エージェントがこのインターフェイスで受信した BOOTREQUEST パケッ

	コマンドまたはアクション	目的
	<pre>switch(config-if)# ipv6 dhcp relay address FF02:1::FF0E:8C6C use-vrf red</pre>	トを転送する DHCPv6 サーバの IP アドレスを設定します。 サーバが異なる VRF 上にあり、もう 1 つの interface 引数を使用して宛先の出力インターフェイスを指定する場合は、use-vrf オプションを使用してサーバの VRF 名を指定します。 サーバアドレスには、リンクスコープのユニキャストまたはマルチキャストアドレス、またはグローバルまたはサイトローカルのユニキャストまたはマルチキャストアドレスを使用できます。リンクスコープのサーバアドレスおよびマルチキャストアドレスを指定する場合、interface オプションは必須です。グローバルまたはサイトスコープのサーバアドレスには許可されていません。 複数の IP アドレスを設定するには、アドレスごとに ipv6 dhcp relay address コマンドを使用します。
ステップ 4	(任意) show running-config dhcp 例 : <pre>switch(config-if)# show running-config dhcp</pre>	DHCPv6 の設定を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCPv6 オプション 79 のイネーブル化

Cisco NX-OS Release 9.3(3) 以降では、オプション 79 を使用して、DHCPv6 クライアントのリンク層アドレスの使用をイネーブル化できます。この機能をイネーブルにすると、スイッチはリレー転送パケットにオプション 79 を追加し、IPv6 クライアントのリンク層アドレスが、DHCPv6 パケットのオプション フィールドに挿入されます。

この機能は、通常の DHCPv6 と VXLAN を使用する DHCPv6 の両方でサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : 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	ipv6 dhcp relay option79 例 : switch(config)# ipv6 dhcp relay option79	DHCPv6 ホストのリンク層アドレスを送送するために、リレーサーバから DHCP サーバに送信される DHCP リレー転送 パケットをイネーブルにします。 このコマンドは、送信されるリレー転送 パケットにのみ影響します。

DHCPv6 リレー送信元インターフェイスの設定

DHCPv6 リレー エージェントの送信元インターフェイスを設定できます。デフォルトでは、DHCPv6 リレー エージェントは発信パケットの送信元アドレスとしてリレー エージェント アドレスを使用します。送信元インターフェイスを設定すると、リレーされたメッセージの送信元アドレスとして、より安定したアドレス（ループバック インターフェイス アドレスなど）を使用することができます。

始める前に

DHCP 機能がイネーブルになっていることを確認します。

DHCPv6 リレー エージェントが有効であ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 例 : switch# configure terminal switch(config)#	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 relay source-interface interface 例 : switch(config)# ipv6 dhcp relay source-interface loopback 2	DHCPv6 リレー エージェントの送信元 インターフェイスを設定します。 (注) DHCPv6 リレー送信元インターフェイスは、グローバルに、インターフェイスごとに、またはその両方に設定できます。グローバルおよびインターフェ

	コマンドまたはアクション	目的
		イス レベルの両方が設定されている場合は、インターフェイス レベルの設定がグローバル設定を上書きします。
ステップ 3	(任意) show ipv6 dhcp relay [interface interface] 例 : switch(config)# show ipv6 dhcp relay	DHCPv6 リレーの設定を表示します。
ステップ 4	(任意) show running-config dhcp show running-config dhcp 例 : switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IPv6 RA ガードの設定

Cisco Nexus 9300 シリーズ スイッチで IPv6 ルータ アドバタイズメント (RA) ガード機能を設定できます。この機能は、レイヤ 2 インターフェイス上のすべての着信 IPv6 RA パケットをドロップするために使用されます。

始める前に

DHCP を有効にする必要があります (**feature dhcp** コマンドを使用)。

インターフェイスで DHCP リレーを有効にするには、DHCP (ダイナミック IP アドレッシング) を使用して IPv4 または IPv6 アドレスが割り当てられているインターフェイスで DHCP を無効にする必要があります。

PTP (機能 **ptp**) と NV オーバーレイ (機能 **nv オーバーレイ**) の両方が設定されていないことを確認します。これらの機能が設定されると、ダイナミック ifacl ラベルが予約されます。ただし、使用可能なダイナミック ifacl ラベル ビットは 2 つだけです。これらの機能の両方がすでに設定されている場合、IPv6 RA ガードにダイナミック ifacl ラベルを使用できず、機能を有効にできません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interface interface slot/port 例 : switch(config)# interface ethernet 2/2 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	[no] ipv6 nd raguard 例 : switch(config-if)# ipv6 nd raguard	指定したインターフェイスに IPv6 RA ガード機能を適用します。
ステップ 4	(任意) copy running-config startup-config 例 : switch(config-if)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ローカル ゲスト シェル/Docker でのサーバーへの DHCP リレー

Cisco NX-OS リリース 10.6(2) 以降、Cisco Nexus 9000 スイッチは、ゲスト シェルまたは Docker コンテナとして、スイッチ内でローカルに実行されているサーバーへの DHCP 要求のリレーをサポートしています。この機能により、スイッチはインターフェイスで受信した DHCP クライアント要求をローカルにホストされている DHCP サーバーに転送できるため、ネットワーク環境内で一元化された柔軟な IP アドレス割り当てが可能になります。

ローカル ゲストへの DHCP リレーの利点

この機能は、複数の利点を提供します：

- ローカル DHCP サーバーのデプロイメントが可能：管理者はスイッチ上で DHCP サーバーを直接実行できるため、外部 DHCP サーバーの必要性がなくなります。
- 統合リレー エージェント機能：スイッチは、インターフェイスで受信した DHCP クライアント要求をローカル サーバーに転送し、クライアントと DHCP サーバー間のシームレス コミュニケーションを確保します。

- 高度な DHCP オプションのサポート：Option 82 がサポートされ、インターフェイス ベースの識別とより詳細な IP アドレス割り当てポリシーが可能です。
- 自動化と柔軟性の向上：コンテナまたはリモート対応マシンを利用する環境で、IP アドレス割り当ての効率的な管理を促進します。

ローカル ゲスト シェル/Docker へのDHCPリレーの仕組み

構成すると、スイッチは、クライアントデバイスと、ゲスト シェル内でまたはスイッチ上の Docker コンテナとしてローカルに実行されている DHCP サーバーとの間で DHCP パケットをリレーします。

process_summary

スイッチは、DHCP 要求と応答をリレーすることにより、DHCP クライアントとローカルでホストされている DHCP サーバーとの通信を容易にします。

process_workflow

次のワークフローは、この操作をまとめたものです。

1. スwitchに接続されている DHCP クライアントは、DHCP 要求を送信します。
2. スwitchはこれらの要求を受信し、ループバック インターフェイスを使用して、ゲスト シェルまたは Docker でローカルに実行されている DHCP サーバーに中継します。
3. Option 82 (circuit-id) 情報は、クライアント インターフェイスを識別するためにスイッチによって挿入できます。
4. ローカル DHCP サーバーは要求を処理し、スイッチに応答を返します。
5. スwitchは、その応答を適切なクライアントに転送します。

注意事項と制約事項

この機能には、次の注意事項および制約事項が適用されます：

- この機能は、FX、FX2、FX3、GX、GX2 および HX シリーズの Cisco Nexus 9000 Cloudscale ToR プラットフォームでのみサポートされています。
- DHCPv4 のみがサポートされています。DHCPv6 はサポートされていません。
- 設定は、レイヤ 3 インターフェイスおよび SVI で許可されます。インターフェイスがレイヤ 3 からレイヤ 2 に変更されると、ローカルホスト設定は自動的に削除されます。
- 単一の VRF では、スイッチごとに設定できるローカル DHCP サーバー インスタンスは 1 つだけです。別の VRF でローカル リレーを設定しようとする、CLI にエラーが表示されます。ただし、複数の VRF のクライアントを、この 1 つのローカル サーバにリレーできます。

- この機能は、非ホストモードで構成された Docker コンテナで実行されている DHCP サーバーをサポートしていません。
- インターフェイス ベースの識別では、Option 82 (circuit-id) の挿入がサポートされていません。
- NX-OS 10.6(2)F にアップグレードする際、設定に `ip dhcp relay address 127.0.0.1` が含まれている場合は、アップグレード後にこの設定を削除します。次に、**localhost** キーワードを使用して機能を再設定します。

この手順を完了しないと、実行コンフィギュレーションに設定が含まれていても、機能が動作しません。

ローカルホストを使用した機能の再設定は、Cisco Nexus 9300 シリーズ スイッチでのみサポートされています。

ローカル ゲスト シェル/Docker への DHCPリレーの構成

Before you begin

- インターフェイスがレイヤ3モード（スイッチポートなし）になっていることを確認します。
- この機能は、IPv4 でのみサポートされています。
- DHCP サーバーは、スイッチ上でゲスト シェルまたは Docker（ホスト モード）で実行されている必要があります。

手順

ステップ 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。

例：

```
configure terminal interface Ethernet1/10
```

ステップ 2 インターフェイスがレイヤ3モードであることを確認します。

例：

```
no switchport
```

ステップ 3 （任意） VRF へのインターフェイスを割り当てます。

例：

```
vrf member asdf
```

ステップ 4 ローカル サーバーへの DHCPリレーを有効にします。

例：

```
ip dhcp relay address localhost
```

VRF を指定します（必要な場合）：

```
ip dhcp relay address localhost use-vrf asdf
```

ステップ 5 設定を保存します。

例：

```
copy running-config startup-config
```

ステップ 6 （任意）構成を削除します。

例：

```
no ip dhcp relay address localhost
```

ローカル ゲスト シェル/Docker への DHCP リレーの確認

手順

ステップ 1 構成済みのリレー アドレスの表示

例：

```
show ip dhcp relay address Interface Relay Address VRF Name -----
----- Ethernet1/10 localhost asdf Ethernet1/12 localhost asdf
```

- ローカル DHCP リレーが有効になっているインターフェイスと、リレー アドレスおよび VRFを表示します。
- REST メソッドを使用してこの機能を構成する場合は、address プロパティで IP アドレスを 127.0.0.1 として指定します。

管理対象オブジェクト（MO）パスを使用します：

```
sys/dhcp/inst/relayif-[<interface-name>]/addr-[<vrf-name>]-[<v4address>]
```

例：

```
sys/dhcp/inst/relayif-[eth1/34]/addr-[asdf]-[127.0.0.1] "dhcpRelayAddr": {
"attributes": { "address": "127.0.0.1", "counter": "1", "vrf": "asdf" } }
```

ステップ 2 DHCP リレー統計の表示

例：

```
show ip dhcp relay statistics Message Type Rx Tx Drops Discover 45 5 129 Offer 7 7 0
Request 222 5 225 Ack 5 5 0 Release 11 0 11 Decline 0 0 0 Inform 0 0 0 Nack 0 0 0 Total
290 22 365
```

- インターフェイスおよびリレーアドレスごとに受信、送信、およびドロップされた DHCP メッセージの数を表示します。

ステップ 3 詳細なインターフェイス設定のチェック

例：

```
show system internal dhcp database interface layer3 config 1) fe80:33::4:8 interface
Ethernet1/12 ... Number of DHCPv4 Relay Addresses: 0 v4 Relay address localhost configured:
Yes ... Interface: Ethernet1/13, iod: 22, vrf: asdf Number of DHCPv4 Relay Addresses:
0 v4 Relay address localhost configured: Yes ...
```

- ローカルホストリレー設定のステータスを含む、レイヤ3インターフェイスの詳細な設定情報を提供します。

DHCP クライアントの有効化

DHCP クライアント機能によって、インターフェイスに IPv4 または IPv6 アドレスを設定できます。インターフェイスには、ルーテッドポート、管理ポート、スイッチ仮想インターフェイス（SVI）が含まれます。レイヤ 3 サブインターフェイスはサポートされません。



- (注) DHCPクライアントはDHCPリレーおよびDHCPスヌーピングプロセスに依存しないため、`feature dhcp` コマンドを有効にする必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	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	次のいずれかのオプションを使用します。 interface ethernet slot/port interface mgmt 0 interface vlan vlan-id 例： <pre>switch(config)# interface vlan 3 switch(config-if)#</pre>	- 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。 <i>slot/port</i> は、DHCP スマートリレーを有効または無効にするインターフェイスです。 - 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、DHCPクライアント機能を有効にするインターフェイスとして管理インターフェイスを指定します。 - インターフェイスコンフィギュレーションモードを開始します。<i>vlan-id</i> は、DHCPクライアント機能を有効にするVLANのIDです。

	コマンドまたはアクション	目的
ステップ 3	ipv6 address use-link-local-only 例 : <pre>switch(config-if)# ipv6 address use-link-local-only</pre>	次の手順でインターフェイスにIPv6アドレスを割り当てる前に、このコマンドを入力する必要があります。インターフェイスにIPv4アドレスを割り当てる場合、このコマンドは必要ありません。
ステップ 4	[no] {ip ipv6} address dhcp 例 : <pre>switch(config-if)# ip address dhcp</pre>	インターフェイスの IPv4 または IPv6 アドレスを割り当てます。 IP を削除するには、このコマンドの no 形式を使用します。
ステップ 5	（任意） 次のいずれかのオプションを使用します。 • show running-config interface ethernet slot/port • show running-config interface mgmt 0 • show running-config interface vlan vlan-id 例 : <pre>switch(config-if)# show running-config interface vlan 3</pre>	実行コンフィギュレーションのインターフェイスに割り当てられたIPv4またはIPv6アドレスを表示します。
ステップ 6	（任意） copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 {ip ipv6} address dhcp コマンドだけが保存されます。割り当てられたIPアドレスは、実行コンフィギュレーションに表示されても保存されません。

UDP リレーの設定

UDP リレーについて

デフォルトではルータはブロードキャストパケットを転送しません。ブロードキャストパケットを転送するには、ルータの設定が必要です。UDP リレー機能を使用して、DHCPv4 ポート 67 および 68 を除く UDP ポート宛てのブロードキャストをリレーできます。UDP リレー機能は、IP ヘルパー機能とも呼ばれます。

UDP リレー機能を有効にするには、**ip forward-protocol udp** コマンドを使用します。デフォルトでは、UDP リレー機能は無効です。

パケットを転送するには、転送先IPアドレスまたはネットワーク アドレスで IP アドレス オブジェクト グループを設定し、IP アドレス オブジェクト グループを L3 インターフェイスに関連付けます。

UDP リレー機能は、次のタイプのレイヤ 3 インターフェイスでサポートされます。

- 物理ポート
- インターフェイス VLAN (SVI)
- L3 ポート チャンネル
- L3 サブインターフェイス

UDP リレーの注意事項と制約事項

UDP リレーには、次の注意事項と制約事項があります。

- Cisco NX-OS リリース 9.3(5) 以降、UDP リレーは Cisco Nexus 9300-FX/FX2/FXP、と X97160YC-EX、9700-FX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチでサポートされています。
- UDP リレーは、Cisco Nexus 9300-FX3/GX/GX2/H2R/H1 シリーズスイッチおよび -R/-RX ラインカードを搭載した Cisco Nexus 9500 プラットフォームスイッチではサポートされていません。
- UDP ポートは 1 ～ 65565 の範囲である必要があります。
- 任意の L3 または SVI インターフェイスを最大 1 つのオブジェクトグループに関連付けることができます。したがって、任意のインターフェイスを最大 300 の UDP リレー IP アドレスに関連付けることができます。
- UDP リレー機能は、7 つの UDP ポートをサポートします。
- おおじえく とグループ名には最大 64 文字までの英数字を指定できます。
- DHCP と UDP リレーは共存できません。
- サブネット ブロードキャストはサポートされていません。
- Cisco NX-OS リリース 10.6(1)F 以降では、`ip forward-protocol udp <port>` を構成する前に、`ip forward-protocol udp` をグローバルで有効にする必要があります。グローバル構成を有効にしないと、警告メッセージが表示されます。

UDP リレーの設定

始める前に

DHCP 機能が有効になっていることを確認します。

手順

ステップ 1 **configure terminal**

例 :

```
switch# configure terminal
switch(config)#
```

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] ip forward-protocol udp**

例 :

```
switch(config)# ip forward-protocol udp
```

UDP リレー機能を有効にします。デフォルトでは、UDP リレー機能は無効です。ただし、UDP ポートの定義済みセットでは有効になっています。

ステップ 3 (任意) **[no] ip forward-protocol udp udp-port-number**

例 :

```
switch(config)# ip forward-protocol udp 1
```

デフォルト以外の UDP ポートで UDP リレー機能を有効にします。

(注)

DHCPポートを除く1〜65565の範囲のUDPポートに対してUDP転送を有効または無効にできません。

ステップ 4 **[no] object-group udp relay ip address object-group-name**

例 :

```
switch(config)# object-group udp relay ip address relay1
switch(config-udp-ogroup)#
```

パケットの転送先となる宛先 IP アドレスで構成されるオブジェクト グループを設定します。

ステップ 5 **[no] {host host-addr| network-addr network-mask| network-addr/mask-length}**

例 :

```
switch(config-udp-ogroup)# host 192.0.2.1
192.0.2.254 255.255.255.0
10.1.1.1/24
```

パケットの転送先となる宛先 IP アドレスを設定します。

(注)

作成するエントリごとに、**host** コマンドを使用して単一のホストを指定するか、または **host** コマンドを省略してホストのネットワークを指定します。

ステップ 6 **exit**

例：

```
switch(config-udp-ogroup)# exit
```

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 **interface ethernet slot/port**

例：

```
switch(config)# interface ethernet 1/1  
switch(config-if)#
```

オブジェクト **froup** をレイヤ 3 インターフェイスに対応付けます。

(注)

L3 インターフェイスは、物理ポート、インターフェイス VLAN (SVI)、L3 ポートチャネル、または L3 サブインターフェイスです。

ステップ 8 **ip udp relay addrgroup object-group-name**

例：

```
switch(config-if)# ip udp relay addrgroup group1
```

オブジェクト **group** をインターフェイスに関連付けます。

ステップ 9 **exit**

例：

```
switch(config-if)# exit  
switch(config)#
```

インターフェイス コンフィギュレーション モードを終了します。

UDP リレーの設定例

この例では、実行中の設定を表示し、UDP リレーを設定します。

UDP リレーの設定

この例では、UDP リレー機能を設定するための実行中のコンフィギュレーションを示します。

```
configure terminal  
feature dhcp  
ip forward-protocol udp  
object-group udp relay ip address <udprelay1>  
  host <20.1.2.2>  
  <30.1.1.1> <255.255.255.0>
```

```
<10.1.1.1/24>
exit
interface ethernet <e1/1>
ip udp relay addrgroup <udprelay1>
exit
```

UDP リレーの設定の確認

UDP リレーの設定情報を表示するには、次のいずれかの操作を行います。

コマンド	目的
show ip udp relay	UDP リプレイ 設定を表示します。
show ip udp relay interface [{ <i>interface-type</i> <i>interface-range</i> }]	インターフェイス レベル属性を表示します。
show ip udp relay object-group	設定済みのすべての UDP リレー オブジェクト グループ、および関連する IP アドレスを表示します。
show ip udp relay object-group <i>object-group-name</i>	オブジェクトグループ、および関連する IP アドレスを表示します。

DHCP 設定の確認

DHCP 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show ip dhcp relay	DHCP リレーの設定を表示します。
show ipv6 dhcp relay [<i>interface interface</i>]	DHCPv6 リレーのグローバル設定またはインターフェイスレベルの設定を表示します。

コマンド	目的
show ipv6 dhcp relay prefix-delegation	リレー エージェントの DHCPv6 IAPD エントリを次のオプションとともに表示します。 • client : クライアントのプレフィックスバインディングを表示します。 detail : 詳細情報を表示します。 interface : インターフェイスのプレフィックスバインディングを表示します。 prefix : 特定のプレフィックスバインディングを表示します。

コマンド	目的
show ipv6 route dhcpv6	次のオプションを使用して、dhcpv6 が所有する接続されたルートを表示します。 • all : バックアップネクストホップのプロトコルのルートも表示します。 bind-label : このバインドラベルのみを持つルートを表示します。 detail : ルートを詳細に表示します interface : この出力インターフェースのみを持つルートを表示します next-hop : このネクストホップのみを持つルートを表示します。 summary : ルートカウントを表示します。 updated : 最終更新時刻でフィルタリングされたルートを表示します。 vrf : VRF ごとの情報を表示します。 Note DHCPv6-PD 機能が有効になっていることを確認します。
show ip dhcp relay address	デバイスに設定されているすべての DHCP サーバアドレスを表示します。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。

コマンド	目的
show running-config dhcp [all]	実行コンフィギュレーションの DHCP 設定を表示します。 Note show running-config dhcp コマンドは、 ip dhcp relay コマンドと ipv6 dhcp relay コマンドを表示しますが、これらはデフォルトで設定されています。
show running-config interface {ethernet slot/port mgmt 0 vlan vlan-id}	DHCPクライアントが有効な場合に、インターフェイスに割り当てられたIPv4またはIPv6アドレスを表示します。
show startup-config dhcp [all]	スタートアップ コンフィギュレーション内の DHCP 設定を表示します。

IPv6 RA ガードの統計情報の表示

IPv6 RA ガード統計情報を表示または消去するには、次のいずれかの作業を実行します。

コマンド	目的
show ipv6 raguard statistics	IPv6 関連 RA ガードの統計情報を表示します。

次に、サンプルの統計情報例を示します。

```
switch# show ipv6 raguard statistics
-----
Interface      Rx          Drops
-----
Ethernet1/53   4561102     4561102
```

DHCP スヌーピング バインディングの表示

Use the **show ip dhcp snooping binding [ip-address | mac-address | dynamic | static | vlan vlan-id | interface interface-type interface-number]** DHCP スヌーピング バインディング データベースのすべてのエントリを表示します。

```
MacAddress      IpAddress LeaseSec Type   VLAN Interface
-----
0f:00:60:b3:23:33 10.3.2.2  infinite static  13   Ethernet2/46
0f:00:60:b3:23:35 10.2.2.2  infinite static  100  Ethernet2/10
```

DHCP スヌーピング バインディング データベースのクリア

clear ip dhcp snooping binding コマンドを使用して、DHCP スヌーピング バインディング データベースからすべてのエントリをクリアします。

DHCP スヌーピング バインディング データベースから、特定のイーサネット インターフェイスに関連付けられたエントリをクリアするには、**clear ip dhcp snooping binding interface ethernet slot/port** コマンドを使用して、DHCP スヌーピング バインディング データベースから、特定のイーサネット インターフェイスに関連するエントリをクリアします。

DHCP スヌーピング バインディング データベースから、特定のポートチャネル インターフェイスに関連付けられたエントリをクリアするには、**clear ip dhcp snooping binding interface port-channel channel-number** コマンドを使用して、DHCP スヌーピング バインディング データベースから、特定のポート チャネル インターフェイスに関連するエントリをクリアします。

DHCP スヌーピング バインディング データベースから、特定の VLAN エントリに関連付けられたエントリを 1 つだけクリアするには、**clear ip dhcp snooping binding vlan vlan-id [mac mac-address ip ip-address interface {ethernet slot /port | port-channel channel-number}]** コマンドを使用して、DHCP スヌーピング バインディング データベースから特定の VLAN エントリをクリアします。

DHCP のモニタリング

DHCP スヌーピングをモニタするには、**show ip dhcp snooping statistics** コマンドを使用します。

DHCP リレーの統計情報をグローバルまたはインターフェイス レベルでモニタするには、**show ip dhcp relay statistics [interface interface]** グローバルまたはインターフェイス レベルで DHCP リレー統計情報をモニタするコマンド。

DHCPv6 リレーの統計情報をグローバルまたはインターフェイス レベルでモニタするには、**show ipv6 dhcp relay statistics [interface interface]** グローバルまたはインターフェイス レベルで DHCPv6 リレー統計情報をモニタするコマンド。

DHCP スヌーピング統計情報のクリア

clear ip dhcp snooping statistics [vlan vlan-id] コマンドを使用して、DHCP スヌーピング統計情報をクリアします。

DHCP リレー統計情報のクリア

グローバル DHCP リレーの統計情報をクリアするには、**clear ip dhcp relay statistics** コマンドを使用します。

特定のインターフェイスに関する DHCPv6 リレーの統計情報をクリアするには、**clear ip dhcp relay statistics interface interface** コマンドを使用して、特定のインターフェイスの DHCP リレー統計情報をクリアします。

clear ip dhcp global statistics コマンドを使用し、DHCP 統計情報をグローバルにクリアします。

DHCPv6 リレー統計情報のクリア

グローバル DHCPv6 リレーの統計情報をクリアするには、**clear ipv6 dhcp relay statistics** コマンドを使用します。

特定のインターフェイスに関する DHCPv6 リレーの統計情報をクリアするには、**clear ipv6 dhcp relay statistics interface interface** コマンドを使用して、特定のインターフェイスの DHCPv6 リレー統計情報をクリアします。

DHCPv6-PD バインドのクリア

次のクリア コマンドは、バインディング、および対応する IPv6 ルートもクリアします。

一般的な vPC 環境では、vPC ピア スイッチで DHCPv6-PD バインドをクリアすると、他の vPC ピア スイッチで対応する IPv6 ルートとともにバインドがクリアされます。

DHCPv6-PD バインドのすべてのエントリをクリアするには、**clear ipv6 dhcp relay prefix-delegation all** コマンドを使用します。

DHCPv6-PD バインドのクライアントの IPv6 アドレス エントリをクリアするには、**clear ipv6 dhcp relay prefix-delegation client** コマンドを使用します。

DHCPv6-PD バインドの特定のインターフェイスに関連付けられたエントリをクリアするには、**clear ipv6 dhcp relay prefix-delegation interface** コマンドを使用します。



(注) CLI を介した有効な PD エントリのクリア後、更新/再バインド パケットによる PD エントリとルート学習は残りません。

DHCP の設定例

次の例では、2 つの VLAN で DHCP スヌーピングをイネーブルにし、Option 82 のサポートをイネーブルにして、イーサネットインターフェイス 2/5 を **trusted** に設定して、DHCP サーバがこのインターフェイスに接続できるようにします。

```
feature dhcp
ip dhcp snooping
ip dhcp snooping information option

interface ethernet 2/5
  ip dhcp snooping trust
ip dhcp snooping vlan 1
ip dhcp snooping vlan 50
```

次の例では、DHCP リレー エージェントをイネーブルにして、イーサネットインターフェイス 2/3 に DHCP サーバ IP アドレス (10.132.7.120) を設定します。DHCP サーバは **red** という名前の VRF インスタンス内にあります。

```
feature dhcp
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn

interface ethernet 2/3
  ip dhcp relay address 10.132.7.120 use-vrf red
```

次に、DHCP スマート リレー エージェントをイネーブルにして使用する例を示します。この例では、デバイスはイーサネットインターフェイス 2/2 上で受信された DHCP ブロードキャストパケットを DHCP サーバ (10.55.11.3) に転送し、giaddr フィールド内に 192.168.100.1 を挿入します。DHCP サーバに 192.168.100.0/24 ネットワークのためのプールが設定されている場合、その DHCP サーバは応答します。サーバが応答しない場合、デバイスは giaddr フィールド内の 192.168.100.1 を使用して、さらに 2 つの要求を送信します。それでもデバイスが応答を受信しない場合は、代わりに giaddr フィールド内で 172.16.31.254 を使用し始めます。

```
feature dhcp
ip dhcp relay
ip dhcp smart-relay global

interface ethernet 2/2
  ip address 192.168.100.1/24
  ip address 172.16.31.254/24 secondary
ip dhcp relay address 10.55.11.3
```

DHCP クライアントの設定例

次に、DHCP クライアント機能を使用して VLAN インターフェイスに IPv4 アドレスを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface vlan 7
switch(config-if)# no shutdown
```

```
switch(config-if)# ip address dhcp
switch(config-if)# show running-config interface vlan 7
interface Vlan7
no shutdown
ip address dhcp
```

DHCP に関する追加情報

関連資料

関連項目	マニュアル タイトル
ダイナミック ARP インスペクション (DAI)	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
IP ソース ガード	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
vPC	『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』
VRF およびレイヤ 3 のバーチャライゼーション	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』

標準

標準	タイトル
RFC 2131	ダイナミック ホスト構成プロトコル (https://datatracker.ietf.org/doc/html/rfc2131)
RFC 3046	DHCP リレー エージェント情報オプション (https://datatracker.ietf.org/doc/html/rfc3046)
RFC 3633	ダイナミック ホスト構成プロトコル (DHCP) バージョン 6 (RFC) の IPv6 プレフィックス オプション (https://tools.ietf.org/html/rfc3633)
RFC 6607	DHCPv4 および DHCPv6 の仮想サブネット選択オプション (https://datatracker.ietf.org/doc/html/rfc6607)
RFC 6939	DHCPv6 のクライアント リンク層アドレス オプション (https://datatracker.ietf.org/doc/html/rfc6939)



第 17 章

IPv6 ファースト ホップ セキュリティの 設定

この章では、Cisco NX-OS デバイスで First Hop Security (FHS) 機能を設定する方法を説明します。

この章は、次の項で構成されています。

- [ファーストホップセキュリティについて \(567 ページ\)](#)
- [ファーストホップセキュリティの注意事項と制約事項 \(569 ページ\)](#)
- [vPC ファーストホップセキュリティ設定について, on page 569](#)
- [RA ガード \(573 ページ\)](#)
- [DHCPv6 ガード \(574 ページ\)](#)
- [IPv6 スヌーピング \(575 ページ\)](#)
- [IPv6 FHS の設定方法 \(576 ページ\)](#)
- [設定例 \(585 ページ\)](#)
- [IPv6 ファーストホップセキュリティに関する追加情報, on page 587](#)

ファーストホップセキュリティについて

レイヤ2 およびレイヤ3 スイッチは、サーバ仮想化、オーバーレイトランスポート仮想化 (OTV)、レイヤ2 モビリティなどのテクノロジーを使用して、レイヤ2 ドメインで動作します。これらのデバイスは、特にエンドノードに面している場合に、「ファーストホップ」と呼ばれることがあります。ファーストホップセキュリティ機能は、エンドノードを保護し、IPv6 またはデュアルスタック ネットワークでのリンク操作を最適化します。

ファーストホップセキュリティ (FHS) は、IPv6 リンクの動作を最適化し、大規模な L2 ドメインの拡張に役立つ一連の機能です。これらの機能は、さまざまな不正ユーザや設定ミスのユーザから保護します。拡張 FHS 機能は、さまざまな展開シナリオまたは攻撃ベクトルに使用できます。

次の FHS 機能がサポートされています。

- IPv6 RA ガード

- DHCPv6 ガード
- IPv6 スヌーピング



(注) この機能のイネーブル化の詳細については、[ファーストホップセキュリティの注意事項と制約事項 \(569 ページ\)](#) を参照してください。



(注) FHS 機能をイネーブルにするには、**feature dhcp** コマンドを使用します。

IPv6 グローバル ポリシー

IPv6 グローバル ポリシーは、ストレージおよびアクセス ポリシー データベースのサービスを提供します。IPv6 スヌーピング、DHCPv6 ガード、および IPv6 RA ガードは、IPv6 グローバル ポリシーの機能です。IPv6 スヌーピング、DHCPv6 ガード、または RA ガードをグローバルに設定するたびに、ポリシーの属性が、ソフトウェア ポリシー データベースに保存されます。その後ポリシーはインターフェイスに適用され、ポリシーが適用されたこのインターフェイスを含めるためにソフトウェア ポリシー データベース エントリが更新されます。

FHS を設定するには、**hardware access-list tcam region ing-redirect tcam_size** コマンドを使用します。**ing-racl** リージョンのサイズを変更して、**ing-redirect** リージョンにスペースを割り当てることができます。

- Cisco Nexus 9300-FX/FX2 プラットフォームスイッチでは、FHS パケットはソフトウェア処理のために **copp-s-dhcpreq** キューを使用します。
- Cisco Nexus 9300、9500 プラットフォーム スイッチは、クラスデフォルトを使用します。



(注) In-Service Software Upgrades (ISSU) を使用して Cisco Nexus シリーズスイッチを Cisco NX-OS Release 7.0(3)I7(1) にアップグレードする場合は、ポート レベルの FHS ポリシーを設定する前に Cisco NX-OS ボックスをリロードする必要があります。

IPv6 ファーストホップ セキュリティ バインディング テーブル

デバイスに接続されている IPv6 ネイバーのデータベース テーブルは、IPv6 スヌーピングなどの情報源から作成されます。このデータベース (またはバインディング) テーブルは、スプーフィングやリダイレクト攻撃を防止するために、リンク層アドレス (LLA)、IPv6 アドレス、および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 ガード機能によって使用されます。

ファーストホップセキュリティの注意事項と制約事項

ファーストホップセキュリティの一般的な注意事項と制限事項は次のとおりです。

- インターフェイスまたはVLANでFHSを有効にする前に、**hardware access-list tcam region ing-redirect tcam_size** コマンドを使用して **ing-redirect** TCAM カービングが実行されていることを確認してください。**ing-racl** リージョンのサイズを変更して、**ing-redirect** リージョンにスペースを割り当てることができます。

ファーストホップセキュリティでサポートされるプラットフォームとリリース

サポートされるリリース	サポートされるプラットフォーム
7.0(3)I7(1) 以降	Cisco Nexus 9300-FX/FX2 シリーズ スイッチ
9.3(5) 以降	Cisco Nexus 9300-GX シリーズ スイッチおよび N9K-C93180YC-FX3S スイッチ
10.1(1) 以降	Cisco Nexus 9300-FX3 シリーズ スイッチ
10.2(3)F 以降	Cisco Nexus 9300-GX2 シリーズ スイッチ
10.4(1)F 以降	Cisco Nexus 9332D-H2R シリーズスイッチ
10.4(2)F 以降	Cisco Nexus 93400LD-H1 シリーズスイッチ
10.4(3)F 以降	CiscoNexus 9364C-H1 シリーズスイッチ

vPC ファーストホップセキュリティ設定について

IPv6 ファーストホップセキュリティ vPC はさまざまな方法で導入できます。次のベストプラクティス展開シナリオを推奨します。

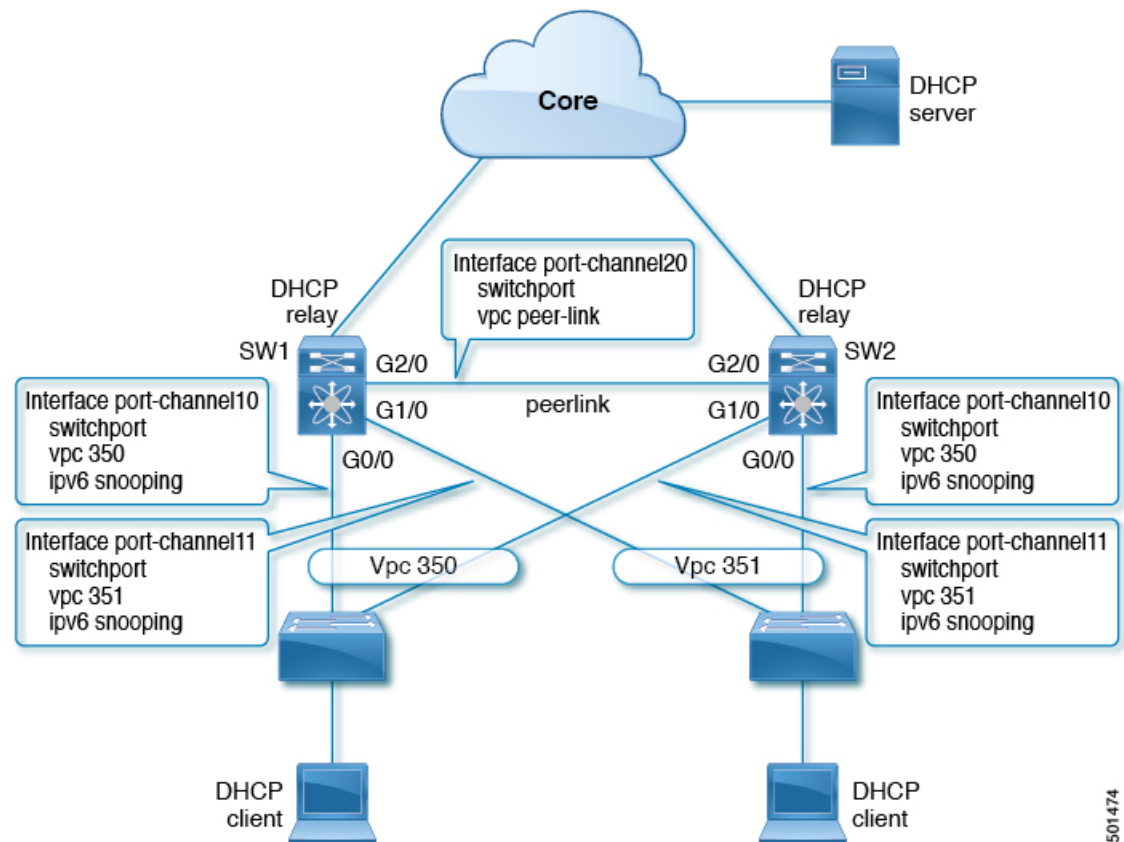
- DHCP リレー オンスタック
- vPC レッグの DHCP リレー
- 孤立ポートの DHCP クライアントとリレー

DHCP リレー オンスタック

この導入シナリオでは、vPC リンクの背後にあるクライアント、またはNexusスイッチで実行されているDHCPリレーを使用する中間スイッチの背後にあるクライアントを、直接接続できます。Nexusスイッチで実行されているDHCPリレーを使用する中間スイッチの背後にあるクライアントに接続することは、理想的な手段です。VLANレベルではなく、vPCインターフェイスリンク上のIPv6スヌーピング機能を直接設定できるからです。インターフェイスレベルでの設定は、次の理由で効率的です。

- 制御トラフィック（DHCP/ND）は、ピアリンクを経由する場合、CPU にリダイレクトされて両方の vPC ピアで処理されることはありません。
- ピアリンク経由でスイッチングされたパケットに、2 回目の処理は行われません。

Figure 14: DHCP リレー オンスタックでの FHS



図では、スヌーピング ポリシーは両方の vPC リンクで有効になっています。このシナリオでは、2 つの vPC ピアが vPC リンクの背後にあるすべてのホスト IP/MAC バインディングを学習し、それらを相互に同期します。2 つの vPC ピアは、IPv6 ND と IPv6 DHCP 制御プロトコルの両方を使用してバインディングを学習します。

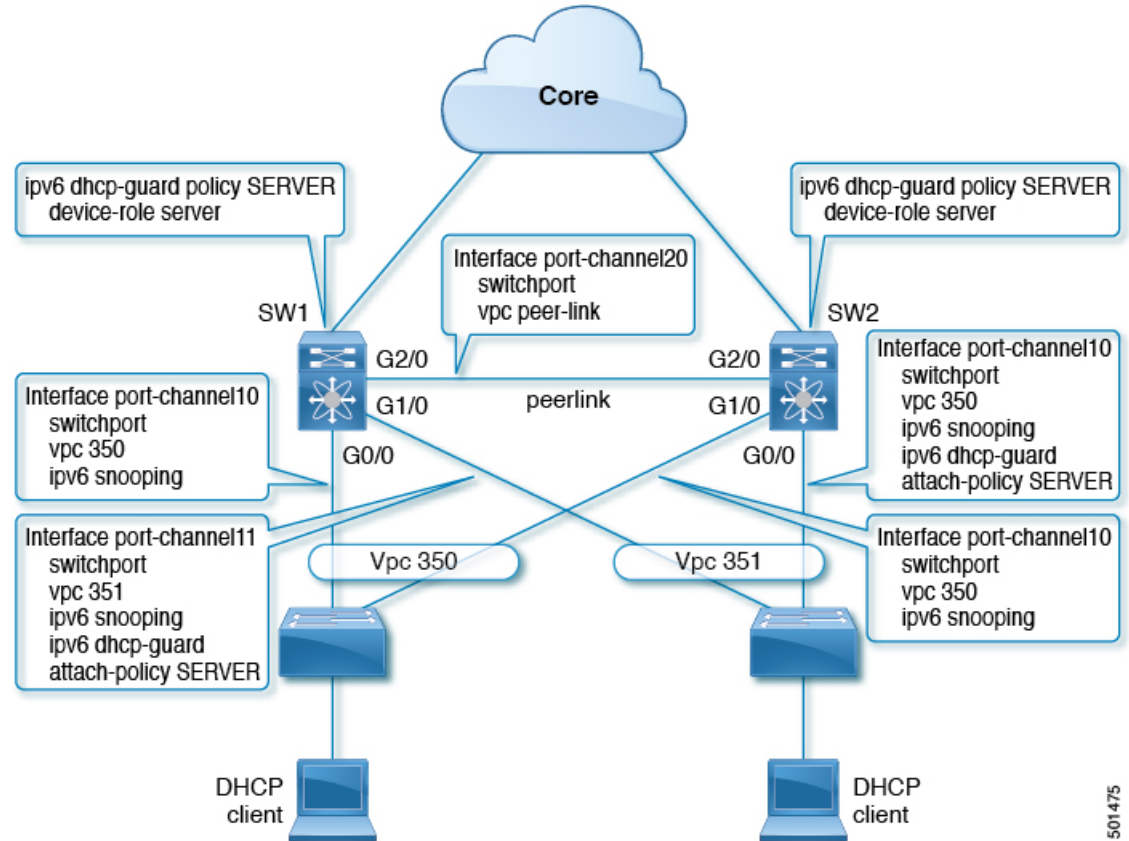
VPC レッグでの DHCP リレー

この設定では、リレー エージェントは vPC ピアで実行されません。代わりに、DHCP リレー エージェント（または DHCP サーバ）が vPC リンクの背後で実行されます（アクセスできる場所に置くことも、さらにはコアのどこかに配置することもできます）。このような導入シナリオでは、IPv6 スヌーピング機能は DHCP サーバメッセージを暗黙的に信頼せず、デフォルトで DHCP サーバメッセージをドロップします。IPv6 ポリシーをカスタマイズして、次を実装できます。

- セキュリティレベルに関する補足情報。

- デバイスロール サーバを使用した IPv6 DHCP ガード ポリシー。この設定では、IPv6 スヌーピングは vPC リンクに接続された DHCP サーバ メッセージを信頼します。

Figure 15: 外部 DHCP リレーを使用した FHS 設定



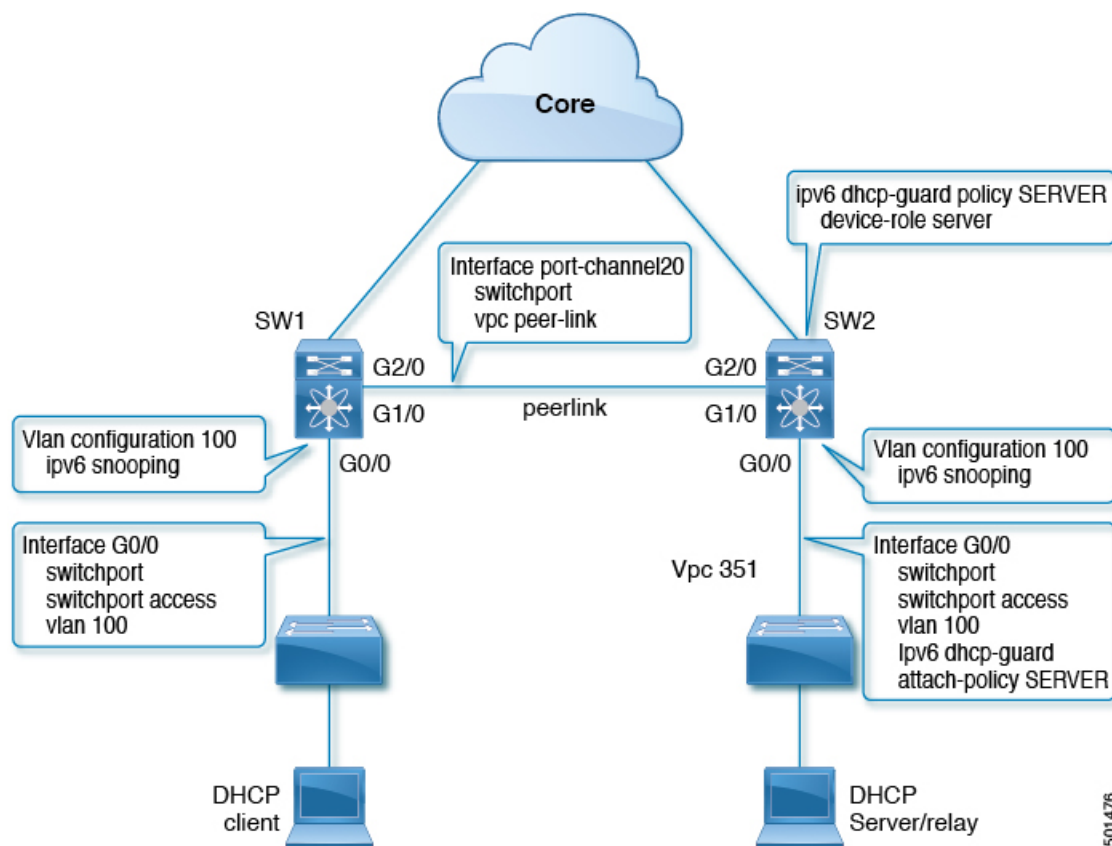
図では、クライアントはデフォルトの IPv6 スヌーピング ポリシーを持つ vPC リンクの背後に配置されています。DHCP サーバトラフィックが到達するリンクに、ipv6 スヌーピングと、ipv6 dhcp-guard attach-policy SERVER ポリシーの両方をアタッチできます。DHCP 制御トラフィックを介してクライアントバインディングエントリを作成するには、サーバまたはリレー側とクライアント側の両方の IPv6 スヌーピング ポリシーが必要です。これは、IPv6 スヌーピングがバインディングを作成するためにはクライアントとサーバの両方のパケットを確認する必要があるためです。また、IPv6 DHCP ガード ポリシーを設定して、IPv6 スヌーピング ポリシーによる DHCP サーバトラフィックを許可する必要があります。vPC ピアは vPC ポートで学習されたすべての新しく学習されたクライアントエントリを同期するため、両方のピアに同じ設定が必要です。

孤立ポートでの DHCP クライアント リレー

この設定では、孤立ポートを介してクライアントを接続できます。IPv6 スヌーピング機能は、vPC ポートのクライアントバインディングのみを同期します。孤立ポートは両方の vPC ピアに直接接続されていないため、同期されません。このような設定では、IPv6 スヌーピング機能は両方のスイッチで独立して実行されます。この図は、次のことを示しています。

- 最初のスイッチで、クライアント側インターフェイスに IPv6 スヌーピング ポリシーをアタッチする必要があります。ただし、vPC ピアの背後にある孤立ポート上のサーバからの DHCP サーバパケットに対応するには、VLAN レベルでポリシーを付加する必要があります。このような場合、VLAN に適用されるポリシーは、クライアント トラフィック インターフェイスと DHCP サーバ トラフィックの両方を検査します。インターフェイスごとに個別の IPv6 スヌーピング ポリシーは必要ありません。vPC ピア経由で着信する DHCP トラフィックも暗黙的に信頼され、ポリシーが必要な場合は、vPC ピアによって自動的にドロップされます。
- また、2 番目のスイッチで VLAN レベルで IPv6 を設定する必要があります。また、孤立ポートに面するサーバで「デバイス ロール サーバ」を使用して IPv6 DHCP ガード ポリシーを設定する必要があります。これにより、IPv6 スヌーピング機能による DHCP サーバパケットのドロップが防止されます。両方のスイッチはクライアント バインディング エントリを個別に学習し、クライアントが vPC リンク上にないため、それらを同期しません。

Figure 16: 孤立ポート上のクライアントおよび DHCP リレーによる FHS 設定



501476

RA ガード

IPv6 RA ガードの概要

IPv6 RA ガード機能は、ネットワーク デバイス 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、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。RA は、リンクで自身をアナウンスするためにデバイスによって使用されます。IPv6 RA ガード機能は、それらの RA を分析して、承認されていないデバイスから送信された RA を除外します。ホスト モードでは、ポート上の RA 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 (L2) 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。L2 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 RA ルータ アドバタイズメントとフラグ

ルータ アドバタイズメントは、リンク上で通信するためのグローバル ユニキャスト アドレスおよびその他のアドレス指定情報を作成または取得する方法をデバイスに提案します。RA メッセージは 4 つのフラグを使用して、これがどのように行われるかをデバイスに通知します。

1. アドレス自動構成フラグ (A フラグ) : A フラグはデフォルトで有効になっています。このフラグは、指定したプレフィックスが IPv6 自動構成に使用できることをローカル リンク上のホストに知らせます。
2. その他の構成フラグ (O フラグ) : O フラグはデフォルトで無効になっています。このフラグは、ステートレス DHCPv6 サーバーからグローバル ユニキャスト アドレス以外のアドレス指定情報を取得するようにホストに指示します。この情報には、DNS サーバーのアドレスとドメイン名が含まれる場合があります。
3. 管理対象アドレス構成フラグ (M フラグ) : M フラグはデフォルトで無効になっています。このフラグは、グローバル ユニキャスト アドレスおよびその他すべてのアドレス指定情報にステートフル DHCPv6 サーバーを使用するようにホストに指示します。ステートフル DHCPv6 が必要な場合は、**ipv6 managed-config-flag** コマンドを使用して M フラグを有効にします。



(注) M フラグが有効な場合、A フラグは通常無効にする必要があります。M フラグを手動で有効にしても、A フラグは自動的に無効になりません。A フラグを無効にするには、**ipv6 nd prefix ipv6-prefix/prefix-length no-autoconfig** コマンドを使用します。

4. オンリンク フラグ (L フラグ) : L フラグもデフォルトで有効になっています。L フラグは、特定のプレフィックスがこのリンクまたはサブネット上にあることを識別します。IPv6

は、接続先 IP アドレスがリンクに対してローカルであるかどうかを判断するために、IPv4 のように論理 AND ハッシュを実行しません。L フラグが無効になっている場合、すべてのパケットはデフォルトゲートウェイに送信されます。A フラグと L フラグは、デフォルトで ICMPv6 ルーター アドバタイズメント (RA) を介してアドバタイズされます。

IPv6 RA ガードの注意事項と制約事項

IPv6 RA ガードの注意事項と制約事項は次のとおりです。

- IPv6 RA ガード機能は、IPv6 トラフィックがトンネリングされる環境では保護を行いません。
- Cisco NX-OS リリース 10.1(1) から、Cisco Nexus 9300-GX プラットフォーム スイッチで IPV6 RA ガードはサポートされます。
- この機能は、TCAM (Ternary Content Addressable Memory) がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスで設定できます。
- この機能は、ホスト モードとルータ モードをサポートしています。
- この機能は、入力方向だけでサポートされます。出力方向ではサポートされません。
- この機能は、補助 VLAN およびプライベート VLAN (PVLAN) でサポートされています。PVLAN の場合、プライマリ VLAN の機能が継承され、ポート機能とマージされます。
- IPv6 RA ガード機能によってドロップされたパケットはスパニングできます。

DHCPv6 ガード

DHCP の概要 : DHCPv6 ガード

DHCPv6 ガード機能は、サーバからクライアントに DHCP パケットを転送する、承認されていない DHCP サーバとリレー エージェントから発信される DHCP 応答やアドバタイズメントメッセージをブロックします。クライアントメッセージまたはリレーエージェントによってクライアントからサーバに送信されるメッセージはブロックされません。フィルタリングの決定は、受信側スイッチポート、トランク、または VLAN に割り当てられたデバイスロールによって決定されます。この機能は、トラフィックリダイレクションまたはサービス妨害 (DoS) を防止するのに役立ちます。

パケットは、3つのDHCPタイプメッセージのいずれかに分類されます。すべてのクライアントメッセージは、デバイスロールに関係なく常にスイッチングされます。DHCPサーバメッセージは、デバイスロールがserverに設定されている場合にのみ、さらに処理されます。DHCPサーバアドバタイズメントの追加処理は、サーバプリファレンス チェックのために行われます。

デバイスがDHCPサーバとして設定されている場合は、デバイスロールの設定に関係なく、すべてのメッセージを切り替える必要があります。

DHCPv6 ガードの制限事項

DHCPv6 ガードの注意事項と制約事項は次のとおりです。

- DHCPサーバから到着するパケットがリレー転送またはリレー応答である場合、デバイスロールのみがチェックされます。さらに、IPv6DHCPガードは、スイッチで実行されているローカルリレーエージェントによって送信されたパケットにポリシーを適用しません。

IPv6 スヌーピング

IGMP スヌーピングの概要

IPv6 の「スヌーピング」機能は、レイヤ 2 IPv6 のファーストホップ機能をいくつか組み合わせたもので、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。この機能によって、Duplicate Address Detection (DAD)、アドレス解決、デバイス検出やネイバーキャッシュに対する攻撃といった、ネイバー探索メカニズムに固有のいくつかの脆弱性が軽減されます。

IPv6 スヌーピングは、レイヤ 2 ネイバー テーブル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て保護し、信頼できるバインディングテーブルを構築するためにスヌーピングメッセージを分析します。有効なバインディングのない IPv6 スヌーピング メッセージはドロップされます。IPv6 スヌーピング メッセージは、その IPv6 から 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。

ターゲット（プラットフォームのターゲット サポートによって異なり、デバイス ポート、スイッチ ポート、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、および VLAN が含まれることがある）に IPv6 スヌーピングが設定されている場合、IPv6 トラフィックのスヌーピングプロトコルと Dynamic Host Configuration Protocol (DHCP) をルーティングデバイスのスイッチ統合セキュリティ機能 (SISF) インフラストラクチャにリダイレクトするためのキャプチャ命令がハードウェアにダウンロードされます。スヌーピング トラフィックの場合、Neighbor Discovery Protocol (NDP) メッセージは SISF に送信されます。DHCPv6 の場合、dhcpv6_client および dhcpv6_server ポートから送信された UDP メッセージがリダイレクトされます。

IPv6 スヌーピングはその「キャプチャ ルール」を分類子に登録します。分類子では、特定のターゲットにあるすべての機能のルールがすべて集約され、対応する ACL がプラットフォーム依存モジュールにインストールされます。分類子は、リダイレクトされたトラフィックを受信すると、（トラフィックを受信しているターゲットに対して）登録されているすべての機能からすべてのエントリ ポイント（IPv6 スヌーピング エントリ ポイントを含む）を呼び出します。IPv6 スヌーピングのエントリ ポイントは最後に呼び出されるため、他の機能によって行われた決定が IPv6 スヌーピングの決定よりも優先されます。

IPv6 スヌーピングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

加えて、IPv6 スヌーピングは、正確なバインディング テーブルに依存するその他多くの IPv6 の機能の基盤です。この機能は、アドレス収集のためにリンク上のスヌーピングおよびDHCP メッセージを検査した後に、それらのアドレスをバインディング テーブルに入力します。また、この機能は、アドレスの所有権を強制し、特定のノードが要求可能なアドレスの数を制限します。

IPv6 スヌーピングに関する注意事項と制限事項

IPv6スヌーピングの注意事項と制限事項は次のとおりです。

- 両方の vPC ピアで同じ設定を実行する必要があります。IPv6 スヌーピングの自動整合性チェッカはサポートされていません。
- IPv6 スヌーピング機能は、TCAM (Ternary Content Addressable Memory) がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスまたは VLAN のみで設定できます。
- IPv6 スヌーピングが DHCP バインディングを学習するには、サーバとクライアントの両方の応答を確認する必要があります。IPv6 スヌーピング ポリシーは、インターフェイス (またはVLAN) に面したクライアントと、インターフェイス (またはVLAN) に面した DHCP サーバの両方にアタッチする必要があります。DHCP リレーの場合、サーバの応答を確認するために、IPv6 スヌーピングポリシーを VLAN レベルでアタッチする必要があります。

IPv6 FHS の設定方法

デバイスでの IPv6 RA ガード ポリシーの設定



- (注) **ipv6 nd raguard** コマンドがポートで設定されている場合、ルータ送信要求メッセージはこれらのポートに複製されません。ルータ要請メッセージを複製するには、ルータ側のすべてのポートをルータ ロールに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 例 : <pre>Device# configure terminal</pre>	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 nd rguard policy policy-name 例 : <pre>Device(config)# ipv6 nd rguard policy policy1</pre>	RA ガード ポリシー名を定義して、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	device-role {host router monitor switch} 例 : <pre>Device(config-rguard-policy)# device-role router</pre>	ポートに接続されているデバイスの役割を指定します。 • device-role host : 通常のノードまたはホストを接続するインターフェイスまたは VLAN。これは、IPv6 RA ガード ポリシーを適用します。 device-role ホストは、着信 RS パケットを許可し、着信 RA または RR パケットをブロックします。別のインターフェイスで受信された RS パケットは、デバイスロールホストにリダイレクトされません。RA および RR パケット（許可されている）のみがデバイスロールホストにリダイレクトされます。 • device-role switch : device-role スイッチは device-role ホストと同様に動作します。たとえば、トランク ポートのラベルとして使用できます。 • device-role monitor : このデバイスはネットワーク トラフィックをモニタします。これは、RS パケットもこのインターフェイスに送信されることを除き、device-role ホストと同様に動作します。これは、トラフィックのキャプチャに役立ちます。 • device-role router : ルータに接続するインターフェイス。このインター

	コマンドまたはアクション	目的
		フェイスは、着信 RS、RA、または RR パケットを許可します。
ステップ 4	hop-limit {maximum minimum limit} 例 : Device(config-raguard-policy)# hop-limit minimum 3	(任意) アドバタイズされたホップ カウント制限の検証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。
ステップ 5	managed-config-flag {on off} 例 : Device(config-raguard-policy)# managed-config-flag on	(任意) アドバタイズされた管理アドレスの設定フラグが on であることの検証をイネーブルにします。 (注) M フラグを有効にする場合は、A フラグを無効にすることをお勧めします。 • 設定されていない場合、このチェックは回避されます。
ステップ 6	other-config-flag {on off} 例 : Device(config-raguard-policy)# other-config-flag on	(任意) アドバタイズされた [Other] 設定パラメータの検証をイネーブルにします。
ステップ 7	router-preference maximum {high low medium} 例 : Device(config-raguard-policy)# router-preference maximum high	(任意) アドバタイズされたデフォルトルータの設定パラメータの値が指定された制限値以下であることの検証をイネーブルにします。
ステップ 8	trusted-port 例 : Device(config-raguard-policy)# trusted-port	(任意) このポリシーが信頼できるポートに適用されることを指定します。 • すべての RA ガード ポリシングが無効になります。
ステップ 9	exit 例 : Device(config-raguard-policy)# exit	RA ガード ポリシー コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。

インターフェイスの IPv6 RA ガードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>Device# configure terminal</pre>	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 type number 例 : <pre>Device(config)# interface ethernet 1/1</pre> 例 : <pre>Device(config)# vlan configuration 10</pre>	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス モードにするか、VLAN 設定モードにします。
ステップ 3	ipv6 nd raguard attach-policy [policy-name] 例 : <pre>Device(config-if)# ipv6 nd raguard attach-policy</pre>	指定したインターフェイスに IPv6 RA ガード機能を適用します。
ステップ 4	exit 例 : <pre>Device(config-if)# exit</pre>	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 5	show ipv6 nd raguard policy [policy-name] 例 : <pre>switch# show ipv6 nd raguard policy host</pre> <pre>Policy host configuration:</pre> <pre> device-role host</pre> <pre>Policy applied on the following interfaces:</pre> <pre>Et0/0 vlan all</pre> <pre>Et1/0 vlan all</pre>	RA ガードを使用して設定されているすべてのインターフェイスで RA ガードポリシーを表示します。
ステップ 6	debug ipv6 snooping raguard [filter interface vlanid] 例 : <pre>Device# debug ipv6 snooping raguard</pre>	IPv6 RA ガード スヌーピング情報のデバッグを有効にします。

DHCP の設定 : DHCPv6 ガード

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>Device# configure terminal</pre>	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 dhcp guard policy policy-name 例 : <pre>Device(config)# ipv6 dhcp guard policy poll</pre>	DHCPv6 ガード ポリシー名を定義して、DHCP ガード 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 {client server} 例 : <pre>Device(config-dhcpv6-policy)# device-role server</pre>	ターゲット（インターフェイスまたは VLAN）に接続されているデバイスのデバイス ロールを指定します。 • device-role client : 通常の DHCPv6 クライアントが接続されているインターフェイス。着信サーバ パケットをブロックします。 • device-role server : 通常の DHCPv6 サーバが接続されているインターフェイス。このインターフェイスから発信されるすべての DHCPv6 パケットを許可します。
ステップ 4	preference min 制限 例 : <pre>Device(config-dhcpv6-policy)# preference min 0</pre>	（オプション）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有効にします。設定されていない場合、このチェックは回避されます。
ステップ 5	preference max 制限 例 : <pre>Device(config-dhcpv6-policy)# preference max 255</pre>	（オプション）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有効にします。設定されていない場合、このチェックは回避されます。

	コマンドまたはアクション	目的
ステップ 6	trusted-port 例 : <pre>Device(config-dhcpv6-policy)# trusted-port</pre>	(任意) このポリシーが信頼できるポートに適用されることを指定します。すべての DHCP ガードポリシーが無効になります。
ステップ 7	exit 例 : <pre>Device(config-dhcpv6-policy)# exit</pre>	DHCP ガード 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。
ステップ 8	interface type number 例 : <pre>Device(config)# interface Ethernet 1/1</pre>	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 9	switchport 例 : <pre>Device(config-if)# switchport</pre>	レイヤ 3 モードになっているインターフェイスを、レイヤ 2 設定用にレイヤ 2 モードにします。
ステップ 10	ipv6 dhcp guard [attach-policy policy-name] 例 : <pre>Device(config-if)# ipv6 dhcp guard attach-policy poll</pre>	DHCPv6 ガードポリシーをインターフェイスに適用します。
ステップ 11	exit 例 : <pre>Device(config-if)# exit</pre>	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、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 12	vlan configuration vlan-id 例 : <pre>Device(config)# vlan configuration 1</pre>	VLAN を指定し、VLAN 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	ipv6 dhcp guard [attach-policy policy-name] 例 : <pre>Device(config-vlan-config)# ipv6 dhcp guard attach-policy poll</pre>	DHCPv6 ガードポリシーを VLAN に適用します。

	コマンドまたはアクション	目的
ステップ 14	exit 例 : Device(config-vlan-config)# exit	VLAN 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。
ステップ 15	exit 例 : Device(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、特権 EXEC モードに戻ります。
ステップ 16	show ipv6 dhcp guard policy [policy-name] 例 : Device# show ipv6 dhcp policy guard poll	(オプション) ポリシー設定と、そのポリシーが適用されるインターフェイスを表示します。

IPv6 スヌーピングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : 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	ipv6 snooping policy <i>policy-name</i> 例 : Device(config)# ipv6 snooping policy policy1	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング 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	device-role { node switch } 例 : Device(config-snoop-policy)# device-node switch	ターゲット（インターフェイスまたは VLAN）に接続されているデバイスのロールを指定します。 • node - がデフォルトです。バインディングが作成され、エントリがプローブされます。 • スイッチ : エントリはプローブされず、信頼できるポートが有効になっている場合、バインディングは作成されません。

	コマンドまたはアクション	目的
ステップ 4	[no] limit address-count 例 : <pre>Device(config-snoop-policy)# limit address-count 500</pre>	バインディング エントリの数を制限します。no limit address-count は制限なしを意味します。
ステップ 5	[no] protocol dhcp ndp 例 : <pre>Device(config-snoop-policy)# protocol dhcp</pre> <pre>Device(config-snoop-policy)# protocol ndp</pre>	DHCP または NDP グリーニングのいずれかをオンまたはオフにします。
ステップ 6	trusted-port 例 : <pre>Device(config-snoop-policy)# trusted-port</pre>	ポリシーを信頼できるポートに適用することを指定します。エントリが信頼できるポートである場合、そのトラフィックはブロックまたはドロップされません。
ステップ 7	security-level glean guard inspect 例 : <pre>Device(config-snoop-policy)# security-level guard</pre>	ポリシーに適用するセキュリティのタイプ（グリーニング、ガード、または検査）を指定します。各セキュリティレベルの意味は次のとおりです。 • glean : バインディングを学習しますが、パケットはドロップしません。 • inspect : アドレス盗難などの問題を検出した場合に、バインディングを学習し、パケットをドロップします。 • guard : inspect と同様に機能しますが、さらに脅威の場合に IPv6、ND、RA、および IPv6 DHCP サーバパケットをドロップします。
ステップ 8	tracking 例 : <pre>Device(config-snoop-policy)# tracking enable</pre>	トラッキングをイネーブルにします。
ステップ 9	exit 例 : <pre>Device(config-snoop-policy)# exit</pre>	IPv6 スヌーピング 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
ステップ 10	interface type-number 例 : Device(config-if)# interface ethernet 1/25	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 11	[no] switchport 例 : Device(config-if)# switchport	レイヤ 2 モードとレイヤ 3 モードを切り替えます。
ステップ 12	ipv6 snooping attach-policy policy-name 例 : Device(config-if)# ipv6 snooping attach-policy policy1	インターフェイスに IPv6 スヌーピング ポリシーを適用します。
ステップ 13	exit 例 : Device(config-if)# exit	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、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	vlan configuration vlan-id 例 : Device(config)# vlan configuration 333	VLAN を指定し、VLAN コンフィギュレーションモードを開始します。
ステップ 15	ipv6 snooping attach-policy policy-name 例 : Device(config-vlan-config)# ipv6 snooping attach-policy policy1	IPv6 スヌーピング ポリシーを VLAN に適用します。
ステップ 16	exit 例 : Device(config-vlan-config)# exit	VLAN 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。
ステップ 17	exit 例 : Device(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、特権 EXEC モードに戻ります。
ステップ 18	show ipv6 snooping policy policy-name 例 : Device(config)# show ipv6 snooping policy policy1	ポリシー設定と、そのポリシーが適用されるインターフェイスを表示します。

IPv6 スヌーピングの確認とトラブルシューティング

手順

	コマンドまたはアクション	目的
ステップ 1	show ipv6 snooping capture-policy [interface type number] 例 : <pre>Device# show ipv6 snooping capture-policy interface ethernet 0/0</pre>	スヌーピング ND メッセージキャプチャポリシーを表示します。
ステップ 2	show ipv6 snooping counter [interface type number] 例 : <pre>Device# show ipv6 snooping counter interface Ethernet 1/1</pre>	インターフェイス カウンタによってカウントされたパケットに関する情報を表示します。
ステップ 3	show ipv6 snooping features 例 : <pre>Device# show ipv6 snooping features</pre>	デバイスに設定されているスヌーピング機能に関する情報を表示します。
ステップ 4	show ipv6 snooping policies [interface type number] 例 : <pre>Device# show ipv6 snooping policies</pre>	設定されているポリシーと、ポリシーが接続されているインターフェイスに関する情報を表示します。
ステップ 5	debug ipv6 snooping 例 : <pre>Device# debug ipv6 snooping</pre>	IPv6 でスヌーピング情報のデバッグをイネーブルにします。

設定例

例 : IPv6 RA ガードの設定

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

```
Device(config-if)# ipv6 nd raguard attach-policy
```

例 : DHCP—DHCPv6 ガードの設定

```
Device# show running-config interface ethernet 1/1

Building configuration...
Current configuration : 129 bytes
!
interface ethernet1/1
 switchport
 switchport access vlan 222
 switchport mode access
 access-group mode prefer port
 ipv6 nd raguard
end
```

例 : DHCP—DHCPv6 ガードの設定

次の例は、DHCPv6 ガードの設定例を示しています。

```
configure terminal
ipv6 dhcp guard policy poll
 device-role server
 preference min 0
 preference max 255
 trusted-port
interface Ethernet 1/1
 switchport
 ipv6 dhcp guard attach-policy poll
 vlan configuration 1
   ipv6 dhcp guard attach-policy poll
show ipv6 dhcp guard policy poll
```

例 : IPv6 ファーストホップセキュリティ バインディング テーブルの設定

```
config terminal
 ipv6 neighbor binding vlan 100 2001:db8::1 interface ethernet3/0
 ipv6 neighbor binding max-entries 100
 ipv6 neighbor binding logging
 ipv6 neighbor binding retry-interval 8
 exit
show ipv6 neighbor binding
```

例 : IPv6 スヌーピングの設定

```
switch (config)# ipv6 snooping policy policy1
switch(config-ipv6-snooping)# ipv6 snooping attach-policy policy1
switch(config-ipv6-snooping)# exit
.
.
.
Device# show ipv6 snooping policies policy1
Policy policy1 configuration:
```



```
trusted-port
device-role node
Policy applied on the following interfaces:
  Et0/0      vlan all
  Et1/0      vlan all
Policy applied on the following vlans:
  vlan 1-100,200,300-400
```

IPv6 ファーストホップ セキュリティに関する追加情報

ここでは、IPv6 ファーストホップ セキュリティに関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『Cisco NX-OS ライセンス ガイド』
コマンド リファレンス	『Cisco Nexus 7000 Series NX-OS Security Command Reference』



第 18 章

ダイナミック ARP インспекションの設定

この章では、Cisco NX-OS デバイスでダイナミック アドレス解決プロトコル (ARP) インспекション (DAI) を設定する方法について説明します。

この章は、次の項で構成されています。

- [DAI について, on page 589](#)
- [DAI の前提条件, on page 594](#)
- [DAI の注意事項と制約事項 \(594 ページ\)](#)
- [DAI の DHCP リレーの注意事項と制約事項 \(595 ページ\)](#)
- [DAI のデフォルト設定, on page 595](#)
- [DAI の設定, on page 596](#)
- [DAI の設定の確認, on page 602](#)
- [DAI の統計情報のモニタリングとクリア, on page 602](#)
- [DAI の設定例, on page 602](#)
- [DHCP リレーの DAI の例, on page 607](#)
- [DAI に関する追加情報, on page 608](#)

DAI について

ARP

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 がホスト A に情報を送信しようとして、ホスト B の ARP キャッシュにホスト A の MAC アドレスがないという場合、ARP の用語では、ホスト B が送信者、ホスト A はターゲットになります。

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。

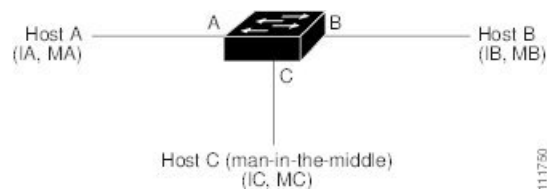
ARP スプーフィング攻撃

ARP では、たとえ ARP 要求を受信していなくても、ホストからの応答が可能なので、ARP スプーフィング攻撃と ARP キャッシュ ポイズニングが発生する可能性があります。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。

ARP スプーフィング攻撃は、サブネットに接続されているデバイスの ARP キャッシュに偽りの情報を送信することにより、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、ルータに影響を及ぼす可能性があります。ARP キャッシュに偽りの情報を送信することを ARP キャッシュ ポイズニングといいます。スプーフ攻撃では、サブネット上の他のホストに対するトラフィックの代行受信も可能です。

Figure 17: ARP キャッシュ ポイズニング

次の図に、ARP キャッシュ ポイズニングの例を示します。



ホスト A、B、C は、それぞれインターフェイス A、B、C を介してデバイスに接続されています。これらのインターフェイスは同一サブネットに属します。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 がホスト B に IP データを送信する必要がある場合、ホスト A は IP アドレス IB に関連付けられた MAC アドレスを求める ARP 要求をブロードキャストします。ホスト B が ARP 要求を受信すると、ホスト B の ARP キャッシュに IP アドレス IA と MAC アドレス MA を持つホストの ARP バインディングが設定されます。たとえば、IP アドレス IA は MAC アドレス MA にバインドされます。ホスト B が応答し、応答がホスト A に到達すると、ホスト A の ARP キャッシュに、IP アドレス IB と MAC アドレス MB を持つホストの ARP バインディングが設定されます。要求と応答の両方がローカル IP アドレスを宛先としていないため、その間のデバイスは ARP キャッシュに入力されません。

ホスト C は、バインディングを伴う 2 つの偽造 ARP 応答をブロードキャストすることにより、ホスト A、ホスト B の ARP キャッシュをポイズニングできます。偽造 ARP 応答の 1 つは、IP アドレス IA と MAC アドレス MC を持つホストの応答、もう 1 つは IP アドレス IB と MAC アドレス MC を持つホストの応答です。これにより、ホスト B は、IA を宛先とするトラフィックの宛先 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。同様にホスト A は、IB に送られるはずのトラフィックの宛先 MAC アドレスとして MC を使用します。

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。このトポロジでは、ホスト C は、ホスト A からホスト B へのトラフィック ストリーム内に自身を割り込ませています。これは、*man-in-the-middle* 攻撃の典型的な例です。

DAI および ARP スプーフィング攻撃

DAI を使用することで、有効な ARP 要求および応答だけがリレーされるようになります。DAI がイネーブルになり適切に設定されている場合、Cisco Nexus デバイスは次のアクティビティを実行します。

- 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。

DAI は DHCP スヌーピング バインディング データベースに保存された有効な IP アドレスと MAC アドレスのバインディングに基づいて、ARP パケットの有効性を判断します。また、このデータベースにはユーザが作成するスタティック エントリも保存できます。ARP パケットを信頼できるインターフェイス上で受信した場合は、デバイスはこのパケットを検査せずに転送します。信頼できないインターフェイス上では、デバイスは有効性を確認できたパケットだけを転送します。

DAI では、パケット内の IP アドレスが無効な場合に ARP パケットをドロップするのか、または ARP パケット本体の MAC アドレスがイーサネット ヘッダーに指定されたアドレスと一致しない場合に ARP パケットをドロップするのかを設定できます。

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

DAI は、デバイス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上で受信されたパケットは、DAI のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、DAI の有効性検査が行われます。

一般的なネットワーク構成では、次のガイドラインに従ってインターフェイスの信頼状態を設定します。

Untrusted

ホストに接続されているインターフェイス

Trusted

デバイスに接続されているインターフェイス

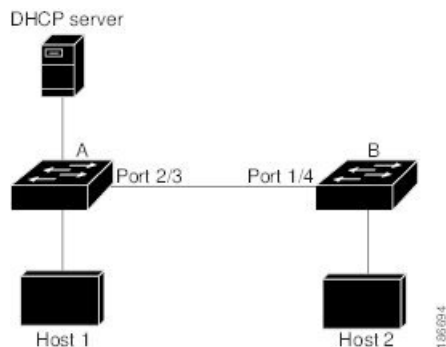
この設定では、デバイスからネットワークに送信される ARP パケットはすべて、セキュリティ検査をバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。

**Caution**

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。

Figure 18: DAI をイネーブルにした VLAN での ARP パケット検証

次の図では、デバイス A およびデバイス B の両方が、ホスト 1 およびホスト 2 を収容する VLAN 上で DAI を実行していると仮定します。ホスト 1 およびホスト 2 が、デバイス A に接続されている DHCP サーバから IP アドレスを取得すると、デバイス A だけがホスト 1 の IP/MAC アドレスをバインドします。デバイス A とデバイス 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 パケットはデバイス 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。



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、ネットワークにセキュリティホールが生じる可能性があります。デバイス A が DAI を実行していなければ、ホスト 1 はデバイス B の ARP キャッシュを簡単にポイズニングできます（デバイス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 も同様）。この状況は、デバイス B が DAI を実行している場合でも起こりえます。

DAI は、DAI が稼働するデバイスに接続されているホスト（信頼できないインターフェイス上）がネットワーク内の他のホストの ARP キャッシュをポイズニングしないように保証します。ただし、DAI が稼働するデバイスに接続されているホストのキャッシュがネットワークの他の部分のホストによってポイズニングされるのを防ぐことはできません。

VLAN 内の一部のデバイスで DAI が稼働し、他のデバイスでは稼働していない場合は、DAI が稼働しているデバイス上のインターフェイスの信頼状態を次のガイドラインに従って設定します。

信頼できない

ホスト、または DAI を実行していないデバイスに接続されているインターフェイス

信頼できる

DAI を実行しているデバイスに接続されているインターフェイス

DAI が稼働していないデバイスからのパケットのバインディングの有効性を判断できない場合は、DAI が稼働しているデバイスを DAI が稼働していないデバイスからレイヤ 3 で隔離します。



Note ネットワークの設定によっては、VLAN 内の一部のデバイスで ARP パケットを検証できない場合もあります。

DAI パケットのロギング

Cisco NX-OS は処理された DAI パケットについてのログ エントリのバッファを維持しています。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。

ログに記録するパケットのタイプを指定することもできます。デフォルトでは、Cisco Nexus デバイスは DAI がドロップしたパケットだけをログに記録します。

ログ バッファがあふれると、デバイスは最も古い DAI ログ エントリを新しいエントリで上書きします。バッファ内の最大エントリ数を設定できます。



Note Cisco NX-OS は、ログに記録される DAI パケットに関するシステム メッセージを生成しません。

ダイナミック ARP インспекションを使用した DHCP リレー

DAI は、DHCP スヌーピング クライアント バインディング データベースを使用して ARP パケットを検証します。Cisco NX-OS リリース 10.1(1) よりも前のリリースでは、このデータベースはスイッチで実行される DHCP スヌーピング プロセスによって構築されていました。スイッチが DHCP リレーとして動作する場合、バインディング データベースは構築されません。スヌーピング、DHCP リレー、および DAI を同時にイネーブルにすると、着信 DHCP パケットを処理するために、リレー プロセスがスヌーピングよりも優先されます。したがって、スヌーピングはバインディング データベースを構築しません。DAI はバインディング データベースに依存しているため、DHCP リレーでは動作できません。ただし、Cisco NX-OS リリース 10.1(1) 以降では、DHCP リレー DAI を使用してバインディング データベースを構築できます。

スイッチが DHCP 要求を受信すると、クライアントの MAC アドレス、VLAN、および着信 インターフェイスで構成される一時バインディング エントリが作成されます。サーバから DHCPACK を受信すると、バインディング エントリが修飾されます。提供された IP アドレスが限定一時エントリに追加され、バインディング エントリ タイプが `dhcp-relay` として更新されます。

Cisco NX-OS リリース 10.1(1) 以降のリリースにアップグレードし、この機能を有効にすると、ISSU はエラーなしで処理されます。Cisco NX-OS リリース 10.1(1) から以前のリリースにダウングレードする前に、この機能を無効にしてください。

DAI の前提条件

- DHCP を設定するには、その前に DAI 機能をイネーブルにする必要があります。「[DHCP の設定, on page 501](#)」を参照してください。
- DAI を有効にする VLAN を設定する必要があります。『Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド』を参照してください。
- **hardware access-list tcam region ipsg** コマンドを使用して、DAI の ACL TCAM リージョンサイズを設定する必要があります。arp-ether リージョンが有効でない限り、DAI 設定は受け入れられません。「[ACL TCAM リージョンサイズの設定, on page 397](#)」を参照してください。

DAI の注意事項と制約事項

DAI に関する注意事項と制約事項は次のとおりです。

- DAI は入力セキュリティ機能であり、出力検査は行いません。
- DAI は、DAI をサポートしないデバイス、またはこの機能が無効にされていないデバイスに接続されているホストに対しては、効果がありません。man-in-the-middle 攻撃は 1 つのレイヤ 2 ブロードキャスト ドメインに限定されるため、DAI が有効なドメインを、DAI が実行されないドメインから切り離す必要があります。これにより、DAI が有効なドメイン内のホストの ARP キャッシュをセキュリティ保護できます。
- **feature dhcp** コマンドを使用して DHCP 機能を無効にすると、I/O モジュールが DHCP を受信する前、または DAI の設定前に約 30 秒の遅延が発生します。この遅延は、DHCP 機能が無効になった設定から、DHCP 機能が無効になった設定に変更するために使用する方式には関係なく発生します。たとえば、ロールバック機能を使用して、DHCP 機能を無効にする設定に戻した場合、ロールバックを完了してから約 30 秒後に I/O モジュールが DHCP と DAI 設定を受信します。
- DAI は、アクセス ポート、トランク ポート、ポートチャネル ポートでサポートされます。
- ポート チャネルに対する DAI の信頼設定によって、そのポート チャネルに割り当てたすべての物理ポートの信頼状態が決まります。たとえば、ある物理ポートを信頼できるインターフェイスとして設定し、信頼できないインターフェイスであるポートチャネルにその物理ポートを追加した場合、その物理ポートは信頼できない状態になります。
- ポートチャネルから物理ポートを削除した場合、その物理ポートはポートチャネルの DAI 信頼状態の設定を保持しません。
- ポートチャネルの信頼状態を変更すると、デバイスはそのチャネルを構成するすべての物理ポートに対し、新しい信頼状態を設定します。

- ARP パケットが有効かどうかを判定するために DAI でスタティック IP-MAC アドレス バインディングを使用するように設定する場合は、スタティック IP-MAC アドレス バインディングを設定していることを確認します。
- ARP パケットが有効かどうかを判定するために DAI でダイナミック IP-MAC アドレス バインディングを使用するように設定する場合は、DHCP スヌーピングが無効になっていることを確認します。
- ARP ACL はサポートされていません。
- Cisco NX-OS リリース 9.3(3) 以降、DAI は Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチでサポートされています。

DAI の DHCP リレーの注意事項と制約事項

- 次の Cisco Nexus プラットフォーム スイッチは、この機能をサポートしています。
 - Cisco Nexus 9300-FX プラットフォーム スイッチ
- バインディング データベース エントリはハードウェアに保存されません。
- バインディング データベースは、すべての VRF に共通です。複数の VRF がある場合は、各 VRF を一意の VLAN にマッピングします。
- IP ソース ガード (IPSG) はこの機能をサポートしていません。
- IPv4 エントリだけがバインディング データベースに保存されます。IPv6 はサポートされていません。
- この機能は vPC をサポートしていません。

DAI のデフォルト設定

次の表に、DAI パラメータのデフォルト設定を示します。

Table 33: デフォルトの DAI パラメータ

パラメータ	デフォルト
DAI	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。
有効性検査	検査は実行されません。

パラメータ	デフォルト
ログ バッファ	DAI をイネーブルにした場合は、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。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 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。

DAI の設定

VLAN での DAI の有効化と無効化

VLAN に対して DAI を有効または無効にすることができます。デフォルトでは、DAI はすべての VLAN で無効です。

始める前に

DHCP 機能が有効にされていることを確認します。

DAI を有効にする VLAN が設定されている。

DAI (arp-ether) の ACL TCAM リージョン サイズが設定され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 例 : switch# configure terminal switch(config)#	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] ip arp inspection vlan vlan-list 例 : switch(config)# ip arp inspection vlan 13	VLAN の特定のリストに対して DAI を有効にします。 no オプションを使用すると、指定した VLAN の DAI が無効になります。
ステップ 3	(任意) show ip arp inspection vlan vlan-id 例 : switch(config)# show ip arp inspection vlan 13	特定の VLAN の DAI 設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ2 インターフェイスの DAI 信頼状態の設定

レイヤ2 インターフェイスの DAI インターフェイス信頼状態を設定できます。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。

デバイスは、信頼できるレイヤ2 インターフェイス上で受信した ARP パケットを転送しますが、検査は行いません。

信頼できないインターフェイス上では、デバイスはすべての ARP 要求および ARP 応答を代行受信します。デバイスは、ローカルキャッシュをアップデートして、代行受信したパケットを適切な宛先に転送する前に、そのパケットの IP-MAC アドレスバインディングが有効かどうかを検証します。そのパケットのバインディングが無効であると判断すると、デバイスはそのパケットをドロップし、ロギングの設定に従ってログに記録します。

Before you begin

DAI を有効にする場合は、DHCP 機能が有効であることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 type port/slot Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	[no] ip arp inspection trust Example: <pre>switch(config-if)# ip arp inspection trust</pre>	インターフェイスを、信頼できる ARP インターフェイスとして設定します。 no オプションを使用すると、そのインターフェイスは信頼できない ARP インターフェイスとして設定されます。

	Command or Action	Purpose
ステップ 4	(Optional) show ip arp inspection interface <i>type port/slot</i> Example: <pre>switch(config-if)# show ip arp inspection interface ethernet 2/1</pre>	特定のインターフェイスの信頼状態および ARP パケット レートを表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

追加検証の有効化または無効化

ARP パケットの追加検証を有効または無効にできます。デフォルトでは、ARP パケットの追加検証は有効になりません。追加検証が設定されていない場合、送信元 MAC アドレス、ARP パケットの IP/MAC バインドエントリと照合する送信元 IP アドレスのチェックは、ARP 送信元 MAC アドレスと ARP 送信者 IP アドレスを使用して実行されます。

DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、記録、および廃棄します。宛先 MAC アドレス、送信元および宛先 IP アドレス、送信元 MAC アドレスに対し、追加検証を有効にすることができます。

追加検証を実装するには、**ip arp inspection validate** コマンドで次のキーワードを使用します。

dst-mac

ARP 応答のイーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較して検査します。有効にすると、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。

ip

ARP 本文をチェックして、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 アドレスは ARP 応答内だけで検査されます。

src-mac

ARP 要求と応答のイーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信者 MAC アドレスと比較して検査します。有効にすると、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。

追加検証を有効にする場合は、次の点に注意してください。

- 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。指定するキーワードは、1 つでも、2 つでも、3 つすべてでもかまいません。

- 各 **ip arp inspection validate** コマンドにより、それまでに指定したコマンドの設定が置き換えられます。**ip arp inspection validate** コマンドによって **src-mac** および **dst-mac** 検証を有効にし、2 つめの **ip arp inspection validate** コマンドで IP 検証を有効にした場合は、2 つめのコマンドを入力した時点で **src-mac** と **dst-mac** の検証が無効になります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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] ip arp inspection validate {[src-mac] [dst-mac] [ip]} Example: <pre>switch(config)# ip arp inspection validate src-mac dst-mac ip</pre>	追加の DAI 検証を有効にします。このコマンドの no 形式を使用すると、DAI の厳密な検証が無効になります。
ステップ 3	(Optional) show running-config dhcp Example: <pre>switch(config)# show running-config dhcp</pre>	DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI のログ バッファ サイズの設定

DAI のログ バッファ サイズを設定できます。デフォルトのバッファ サイズは 32 メッセージです。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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

	Command or Action	Purpose
ステップ 2	[no] ip arp inspection log-buffer entries number Example: <pre>switch(config)# ip arp inspection log-buffer entries 64</pre>	DAI のログ バッファ サイズを設定します。 no オプションを使用すると、デフォルトのバッファ サイズ (32 メッセージ) に戻ります。設定できるバッファ サイズは、1 ~ 1024 メッセージです。
ステップ 3	(Optional) show running-config dhcp Example: <pre>switch(config)# show running-config dhcp</pre>	DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI のログ フィルタリングの設定

DAI パケットを記録するかどうかをデバイスが判断する方法を設定できます。デフォルトでは、デバイスはドロップされる DAI パケットをログに記録します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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] ip arp inspection vlan vlan-list logging dhcp-bindings {all none permit} Example: <pre>switch(config)# ip arp inspection vlan 100 dhcp-bindings permit</pre>	次のようにして、DAI ログ フィルタリングを設定します。このコマンドの no 形式を使用すると、DAI ログ フィルタリングが削除されます。 • all : DHCP バインディングと一致するすべてのパケットをロギングします。 • none : DHCP バインディングに一致するパケットを記録しません。 • permit : DHCP バインディングによって許可されるパケットを記録します。

	Command or Action	Purpose
ステップ 3	(Optional) show running-config dhcp Example: <pre>switch(config)# show running-config dhcp</pre>	DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI を使用した DHCP リレーの有効化

DHCP リレーと DAI が有効になっている場合は、バインディング データベースを作成できます。この機能は、デフォルトで無効にされています。

Before you begin

DAI および DHCP リレーを有効にします。DHCP スヌーピングをグローバルおよび VLAN で有効にします。詳細については、「*DHCP の設定*」の章を参照してください。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 dhcp relay dai Example: <pre>switch(config)# ip dhcp relay dai</pre>	リレーでのバインディング データベースの作成を有効にします。
ステップ 3	(Optional) show ip dhcp snooping binding relay Example: <pre>switch(config)# show ip dhcp snooping binding relay</pre>	dhcp-relay タイプのバインディング エントリを表示します。
ステップ 4	(Optional) show system internal dhcp database global config Example: <pre>switch(config)# show system internal dhcp database global config</pre>	リレー DAI 機能が有効かどうかを表示します。

DAI の設定の確認

DAI の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip arp inspection	DAI のステータスを表示します。
show ip arp inspection interfaces [ethernet slot/port port-channel number]	特定のインターフェイスまたはポートチャネルの信頼状態および ARP パケット レートを表示します。
show ip arp inspection log	DAI のログ設定を表示します。
show ip arp inspection vlan vlan-id	特定の VLAN の DAI 設定を表示します。
show running-config dhcp [all]	DAI の設定を表示します。

DAI の統計情報のモニタリングとクリア

DAI の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドを使用します。

コマンド	目的
show ip arp inspection statistics [vlan vlan-id]	DAI の統計情報を表示します。
clear ip arp inspection statistics vlan vlan-id	DAI 統計情報をクリアします。
clear ip arp inspection log	DAI ログをクリアします。

DAI の設定例

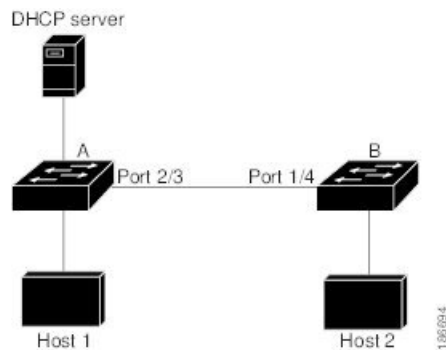
DAI をサポートする 2 つのデバイス

2 つのデバイスが DAI をサポートする場合の DAI の設定手順を次に示します。

Figure 19: DAI をサポートする 2 つのデバイス

次の図に、この例のネットワーク構成を示します。ホスト 1 はデバイス A に、ホスト 2 はデバイス B にそれぞれ接続されています。デバイスは両方とも、ホストが配置されている VLAN 1 で DAI を実行しています。DHCP サーバはデバイス 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。デバイス A はホスト 1 およびホスト 2 の

バインディングを持ち、デバイス B はホスト 2 のバインディングを持ちます。デバイス A のイーサネットインターフェイス 2/3 は、デバイス B のイーサネットインターフェイス 1/4 に接続されています。



DAI では、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスとのバインディングを、DHCP スヌーピングバインディングデータベース内のエントリに基づいて検証します。IP アドレスを動的に割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。

- この構成は、DHCP サーバがデバイス A から別の場所に移動されると機能しません。
- この構成によってセキュリティが損なわれないようにするには、デバイス A のイーサネットインターフェイス 2/3、およびデバイス B のイーサネットインターフェイス 1/4 を、信頼できるインターフェイスとして設定します。

デバイス A の設定

デバイス A で DAI をイネーブルにし、イーサネットインターフェイス 2/3 を信頼できるインターフェイスとして設定するには、次の作業を行います。

Procedure

ステップ 1 デバイス A にログインして、デバイス A とデバイス B の間の接続を確認します。

```

switchA# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID         Local Intrfce   Hldtme   Capability   Platform         Port ID
switchB           Ethernet2/3     177      R S I        WS-C2960-24TC    Ethernet1/4
switchA#
  
```

ステップ 2 VLAN 1 で DAI をイネーブルにし、設定を確認します。

```

switchA# configure terminal
switchA(config)# ip arp inspection vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
  
```

```

IP Address Validation      : Disabled
Vlan : 1
-----
Configuration      : Enabled
Operation State : Active
switchA(config)#

```

ステップ3 イーサネット インターフェイス 2/3 を、信頼できるインターフェイスとして設定します。

```

switchA(config)# interface ethernet 2/3
switchA(config-if)# ip arp inspection trust
switchA(config-if)# exit
switchA(config)# exit
switchA# show ip arp inspection interface ethernet 2/3

```

Interface	Trust State	Rate (pps)	Burst Interval
Ethernet2/3	Trusted	15	5

ステップ4 バインディングを確認します。

```

switchA# show ip dhcp snooping binding

```

MacAddress	IpAddress	LeaseSec	Type	VLAN	Interface
00:60:0b:00:12:89	10.0.0.1	0	dhcp-snooping	1	Ethernet2/3

```

switchA#

```

ステップ5 DAI がパケットを処理する前、およびあとの統計情報を調べます。

```

switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#

```

ホスト 1 が IP アドレス 10.0.0.1 および MAC アドレス 0002.0002.0002 を持つ 2 つの ARP 要求を送信すると、両方の要求が許可されます。これは、次の統計情報で確認できます。

```

switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0

```

```
IP Fails-ARP Res    = 0
```

ホスト 1 が、IP アドレス 10.0.0.3 を持つ ARP 要求を送信しようとする、このパケットはドロップされ、エラー メッセージがログに記録されます。

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Ethernet2/3, vlan
1. ([0002.0002.0002/10.0.0.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Fri Jan 23 2015])
```

この場合に表示される統計情報は次のようになります。

```
switchA# show ip arp inspection statistics vlan 1
switchA#
Vlan : 1
-----
ARP Req Forwarded   = 2
ARP Res Forwarded   = 0
ARP Req Dropped     = 2
ARP Res Dropped     = 0
DHCP Drops          = 2
DHCP Permits        = 2
SMAC Fails-ARP Req  = 0
SMAC Fails-ARP Res  = 0
DMAC Fails-ARP Res  = 0
IP Fails-ARP Req    = 0
IP Fails-ARP Res    = 0
switchA#
```

デバイス B の設定

デバイス B で DAI をイネーブルにし、イーサネット インターフェイス 1/4 を信頼できるインターフェイスとして設定するには、次の作業を行います。

Procedure

ステップ 1 デバイス B にログインして、デバイス B とデバイス A の間の接続を確認します。

```
switchB# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID         Local Intrfce   Hldtme   Capability   Platform         Port ID
switchA           Ethernet1/4     120      R S I        WS-C2960-24TC    Ethernet2/3
switchB#
```

ステップ 2 VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
switchB# configure terminal
switchB(config)# ip arp inspection vlan 1
switchB(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

```
Vlan : 1
-----
Configuration : Enabled
Operation State : Active
switchB(config)#
```

ステップ3 イーサネット インターフェイス 1/4 を、信頼できるインターフェイスとして設定します。

```
switchB(config)# interface ethernet 1/4
switchB(config-if)# ip arp inspection trust
switchB(config-if)# exit
switchB(config)# exit
switchB# show ip arp inspection interface ethernet 1/4
Interface      Trust State    Rate (pps)     Burst Interval
-----
Ethernet1/4    Trusted        15             5
switchB#
```

ステップ4 DHCP スヌーピング バインディングのリストを確認します。

```
switchB# show ip dhcp snooping binding
-----
MacAddress      IpAddress      LeaseSec      Type           VLAN  Interface
-----
00:01:00:01:00:01  10.0.0.2      4995          dhcp-snooping  1     Ethernet1/4
switchB#
```

ステップ5 DAI がパケットを処理する前、およびあとの統計情報を調べます。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 0
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

ホスト 2 が、IP アドレス 10.0.0.2 および MAC アドレス 0001.0001.0001 を持つ ARP 要求を送信すると、このパケットは転送され、統計情報が更新されます。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded = 1
ARP Res Forwarded = 0
ARP Req Dropped   = 0
ARP Res Dropped   = 0
DHCP Drops        = 0
DHCP Permits      = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
```

```
IP Fails-ARP Res    = 0
switchB#
```

ホスト 2 が IP アドレス 10.0.0.1 を持つ ARP 要求を送信しようとする、この要求はドロップされ、システム メッセージがログに記録されます。

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Ethernet1/4, vlan
1. ([0001.0001.0001/10.0.0.1/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri Jan 23 2015])
```

この場合に表示される統計情報は次のようになります。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----
ARP Req Forwarded   = 1
ARP Res Forwarded   = 0
ARP Req Dropped     = 1
ARP Res Dropped     = 0
DHCP Drops          = 1
DHCP Permits        = 1
SMAC Fails-ARP Req  = 0
SMAC Fails-ARP Res  = 0
DMAC Fails-ARP Res  = 0
IP Fails-ARP Req    = 0
IP Fails-ARP Res    = 0
switchB#
```

DHCP リレーの DAI の例

次の例では、DHCP リレー DAI 機能がイネーブルかどうかを示します。この機能が有効でない場合、データベースの **DHCP Relay DAI enabled** エントリの値は **No** になっています。

```
switch(config)# show system internal dhcp database global config

Snooping enabled: Yes
Snoop option-82 enabled: No
Relay enabled: Yes
.
.
DHCP Relay DAI enabled : No
Validate source mac: No
Validate destination mac: No
```

DAI に関する追加情報

関連資料

関連項目	マニュアル タイトル
ACL TCAM リージョン	IP ACL の構成（355 ページ）
『DHCP and DHCP snooping』	DHCP の設定（501 ページ）

標準

標準	タイトル
RFC-826	イーサネット アドレス解決プロトコル (https://datatracker.ietf.org/doc/html/rfc826)



第 19 章

IP ソース ガードの設定

この章では、Cisco NX-OS デバイスで IP ソース ガードを設定する手順について説明します。

この章は、次の項で構成されています。

- [IP ソース ガードについて, on page 609](#)
- [IP ソース ガードの前提条件, on page 610](#)
- [IP ソース ガードの注意事項と制約事項 \(610 ページ\)](#)
- [IP ソース ガードのデフォルト設定, on page 611](#)
- [IP ソース ガードの設定, on page 611](#)
- [IP ソース ガード バインディングの表示, on page 614](#)
- [IP ソース ガードの統計情報のクリア \(614 ページ\)](#)
- [IP ソース ガードの設定例, on page 615](#)
- [その他の参考資料, on page 615](#)

IP ソース ガードについて

IP ソース ガードは、インターフェイス単位のトラフィック フィルタです。各パケットの IP アドレスと MAC アドレスが、IP と MAC のアドレス バインディングのうち、次に示す 2 つの送信元のどちらかと一致する場合だけ、IP トラフィックを許可します。

- Dynamic Host Configuration Protocol (DHCP) スヌーピング バインディング テーブル内のエントリ
- 設定したスタティック IP ソース エントリ

信頼できる IP および MAC のアドレス バインディングのフィルタリングは、スプーフィング攻撃（有効なホストの IP アドレスを使用して不正なネットワークアクセス権を取得する攻撃）の防止に役立ちます。IP ソース ガードを妨ぐためには、攻撃者は有効なホストの IP アドレスと MAC アドレスを両方スプーフィングする必要があります。

DHCP スヌーピングで信頼状態になっていないレイヤ 2 インターフェイスの IP ソース ガードをイネーブルにできます。IP ソース ガードは、アクセス モードとトランク モードで動作するように設定されているインターフェイスをサポートしています。IP ソース ガードを最初にイ

ネーブルにすると、次のトラフィックを除いて、そのインターフェイス上のインバウンド IP トラフィックがすべてブロックされます。

- DHCP パケット。DHCP パケットは、DHCP スヌーピングによって検査が実行され、その結果に応じて転送またはドロップされます。
- Cisco NX-OS デバイスに設定したスタティック IP ソース エントリからの IP トラフィック。

デバイスが IP トラフィックを許可するのは、DHCP スヌーピングによって IP パケットの IP アドレスと MAC アドレスのバインディング テーブル エントリが追加された場合、またはユーザがスタティック IP ソース エントリを設定した場合です。

パケットの IP アドレスと MAC アドレスがバインディング テーブル エントリにも、スタティック IP ソース エントリにもない場合、その IP パケットはドロップされます。たとえば、**show ip dhcp snooping binding** コマンドによって表示されたバインディング テーブル エントリが次のとおりであるとしています。

MacAddress	IpAddress	LeaseSec	Type	VLAN	Interface
00:02:B3:3F:3B:99	10.5.5.2	6943	dhcp-snooping	10	Ethernet2/3

IP アドレスが 10.5.5.2 の IP パケットをデバイスが受信した場合、IP ソース ガードによってこのパケットが転送されるのは、このパケットの MAC アドレスが 00:02:B3:3F:3B:99 のときだけです。

IP ソース ガードの前提条件

IP ソース ガードの前提条件は次のとおりです。

- IP ソース ガードを設定するには、その前に DHCP 機能および DHCP スヌーピングをイネーブルにする必要があります。[DHCP の設定, on page 501](#)を参照してください。
- **hardware access-list tcam region ipsg** コマンドを使用して、IP ソース ガード用の ACL TCAM のリージョン サイズを設定する必要があります。[ACL TCAM リージョン サイズの設定, on page 397](#)を参照してください。



Note

デフォルトでは、ipsg のリージョン サイズはゼロです。SMAC-IP バインディングの保存と適用をするには、このリージョンに十分なエントリを割り当てる必要があります。

IP ソース ガイドの注意事項と制約事項

IP ソース ガードに関する注意事項と制約事項は次のとおりです。

- IP ソース ガードは、インターフェイス上の IP トラフィックを、IP-MAC アドレス バインディング テーブル エントリ または スタティック IP ソース エントリ に送信元が含まれているトラフィックだけに制限します。インターフェイス上の IP ソース ガードを初めてイネーブルにする際には、そのインターフェイス上のホストが DHCP サーバから新しい IP アドレスを受信するまで、IP トラフィックが中断されることがあります。
- IP ソース ガードの機能は、DHCP スヌーピング (IP-MAC アドレス バインディング テーブルの構築および維持に関して)、またはスタティック IP ソース エントリの手動での維持に依存しています。
- IP ソース ガードは、ファブリックエクステンダ (FEX) ポートまたは汎用拡張モジュール (GEM) ポートではサポートされていません。
- IP ソース ガードは、EoR ではサポートされません。
- Cisco NX-OS リリース 9.3(5) 以降、IP Source Guard は Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチでサポートされています。
- IP ソース ガードは、Cisco Nexus 9300-X クラウド スケール スイッチで TCAM カービングを必要としません。
- IPSG が有効になっている場合、インターフェイスでポート セキュリティを有効にすることはできません。

IP ソース ガードのデフォルト設定

次の表に、IP ソース ガードのパラメータのデフォルト設定を示します。

Table 34: IP ソース ガードのパラメータのデフォルト値

パラメータ	デフォルト
IP ソース ガード	各インターフェイスでディセーブル
IP ソース エントリ	なし。デフォルトではスタティック IP ソース エントリはありません。デフォルトの IP ソース エントリもありません。

IP ソース ガードの設定

レイヤ2インターフェイスに対する IP ソース ガードの有効化または無効化

レイヤ2インターフェイスに対して IP ソース ガードをイネーブルまたは無効に設定できます。デフォルトでは、すべてのインターフェイスに対して IP ソース ガードは無効です。

Before you begin

DHCP 機能と DHCP スヌーピングが有効になっていることを確認します。

IPSG (ipsg) の ACL TCAM リージョンサイズが設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interface ethernet slot/port Example: switch(config)# interface ethernet 2/3 switch(config-if)#	指定したインターフェイスに対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 3	[no] ip verify source dhcp-snooping-vlan Example: switch(config-if)# ip verify source dhcp-snooping vlan	インターフェイスの IP ソース ガードを有効にします。このコマンドの no 形式を使用すると、そのインターフェイスの IP ソース ガードが無効になります。
ステップ 4	(Optional) show running-config dhcp Example: switch(config-if)# show running-config dhcp	IP ソース ガードの設定も含めて、DHCP スヌーピングの実行コンフィギュレーションを表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch(config-if)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

スタティック IP ソース エントリの追加または削除

デバイス上のスタティック IP ソース エントリの追加または削除を実行できます。デフォルトでは、固定 IP ソース エントリは作成されません。

**Note**

Cisco NX-OS 10.6(1) 以降では、無効な MAC アドレスや非 L2 インターフェイスを使用するなど、無効な IP ソース バインディング設定を入力すると、候補セッションまたは REST で設定している場合でも、即座にエラーメッセージが表示されます。これは、CLI を介して直接設定したときにすでに見られる動作と一致します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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] ip source binding ip-address mac-address vlan vlan-id interface interface-type slot/port Example: <pre>switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3</pre>	現在のインターフェイスのスタティック IP ソース エントリを作成します。スタティック IP ソース エントリを削除するには、このコマンドの no 形式を使用します。
ステップ 3	(Optional) show ip dhcp snooping binding [interface interface-type slot/port] Example: <pre>switch(config)# show ip dhcp snooping binding interface ethernet 2/3</pre>	スタティック IP ソース エントリを含めて、指定したインターフェイスの IP-MAC アドレスバインディングを表示します。スタティックエントリは、Type カラムの表示で示されます。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

トランク ポート用 IP ソース ガードの設定

IPソースガードがポートに設定されている場合、そのポートに着信するトラフィックは、TCAMで許可するDHCPスヌーピングエントリがない限りドロップされます。ただし、トランクポートでIPソースガードが設定されており、特定のVLANで着信するトラフィックにこのチェックを行わせない場合（DHCPスヌーピングが有効になっていない場合でも）、除外するVLANのリストを指定できます。

始める前に

DHCP 機能と DHCP スヌーピングが有効になっ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 例： switch# configure terminal switch(config)#	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] ip dhcp snooping ipsg-excluded vlan vlan-list 例： switch(config)# ip dhcp snooping ipsg-excluded vlan 1001-1256,3097	トランクポート上のIPソースガードの DHCPスヌーピングチェックから除外するVLANのリストを指定します。
ステップ 3	(任意) show ip ver source [ethernet slot/port port-channel channel-number] 例： switch(config)# show ip ver source	除外されるVLANを表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ソース ガード バインディングの表示

show ip ver source [ethernet slot/port | port-channel channel-number] を使用します コマンドを使用して、IP-MAC アドレスのバインディングを表示します。

IP ソース ガードの統計情報のクリア

IP ソース ガード統計情報をクリアするには、次の表に示すコマンドを使用します。

コマンド	目的
clear access-list ipsg stats [instance number module number]	IPソースガード統計情報をクリアします。

IP ソース ガードの設定例

スタティック IP ソース エントリを作成し、インターフェイスの IP ソース ガードをイネーブルにする例を示します。

```
ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3
interface ethernet 2/3
  no shutdown
  ip verify source dhcp-snooping-vlan
  show ip ver source
```

```
IP source guard excluded vlans:
```

```
-----
None
```

```
-----
IP source guard is enabled on the following interfaces:
```

```
-----
ethernet2/3
```

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
ACL TCAM リージョン	IP ACL の構成 (355 ページ)
『DHCP and DHCP snooping』	DHCP の設定 (501 ページ)



第 20 章

パスワード暗号化の設定

この章では、Cisco NX-OS デバイスにパスワード暗号化を設定する手順について説明します。
この章は、次の項で構成されています。

- [AES パスワード暗号化およびプライマリ暗号キーについて \(617 ページ\)](#)
- [パスワード暗号化の注意事項と制約事項 \(618 ページ\)](#)
- [パスワード暗号化のデフォルト設定 \(620 ページ\)](#)
- [パスワード暗号化の設定 \(620 ページ\)](#)
- [パスワード暗号化の設定の確認 \(624 ページ\)](#)
- [パスワード暗号化の設定例 \(625 ページ\)](#)

AES パスワード暗号化およびプライマリ暗号キーについて

強力で、反転可能な 128 ビットの高度暗号化規格 (AES) パスワード暗号化を有効にすることができます。タイプ 6 暗号化とも言います。タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能を有効にし、パスワード暗号化および復号化に使用されるプライマリ暗号キーを構成する必要があります。

AES パスワード暗号化を有効にしてプライマリ キーを構成すると、タイプ 6 パスワード暗号化を無効にしない限り、サポートされているアプリケーション (現在は RADIUS と TACACS+) の既存および新規作成されたクリア テキスト パスワードがすべて、タイプ 6 暗号化の形式で保存されます。また、既存の弱いすべての暗号化パスワードをタイプ 6 暗号化パスワードに変換するように Cisco NX-OS を構成することもできます。

関連トピック

- [プライマリ キーの設定および AES パスワード暗号化機能の有効化 \(620 ページ\)](#)
- [グローバル RADIUS キーの設定 \(73 ページ\)](#)
- [特定の RADIUS サーバ用のキーの設定 \(74 ページ\)](#)
- [グローバル TACACS+ キーの設定 \(111 ページ\)](#)
- [特定の TACACS+ サーバ用のキーの設定 \(112 ページ\)](#)

[プライマリ キーの設定および AES パスワード暗号化機能の有効化](#) (620 ページ)

パスワード暗号化の注意事項と制約事項

パスワード暗号化設定時の注意事項と制約事項は次のとおりです。

- AES パスワード暗号化機能、関連付けられた暗号化と復号化のコマンド、およびプライマリ キーを設定できるのは、管理者権限 (`network-admin`) を持つユーザだけです。
- Cisco NX-OS リリース 10.3(3)F 以降、RPM キーチェーン インフラストラクチャは、Cisco Nexus 9000 シリーズ プラットフォーム スイッチの RPM レガシー キーチェーンの AES パスワード暗号化をサポートします。
- タイプ 6 暗号化パスワードを含む構成は、ロールバックに準拠していません。
- プライマリ キーがなくても AES パスワード暗号化機能を有効にできますが、プライマリ キーがシステムに存在する場合だけ暗号化が開始されます。
- TACACS+ および RPM レガシー キーチェーンの場合、AES パスワード暗号化機能をイネーブルにし、プライマリ キーを設定した後、**encryption re-encrypt obfuscated** コマンドを実行して、パスワードをタイプ 6 暗号化パスワードに変換する必要があります。
- プライマリ キーを削除するとタイプ 6 暗号化が停止され、同じプライマリ キーが再構成されない限り、既存のすべてのタイプ 6 暗号化パスワードが使用できなくなります。
- デバイス設定を別のデバイスに移行するには、他のデバイスに移植する前に設定を復号化するか、または設定が適用されるデバイス上に同じプライマリ キーを設定します。
- タイプ 6 暗号化は、MACsec キーチェーンおよび RPM レガシー キーチェーンでのみサポートされます。cloudsec キーではサポートされていません。
- Cisco NX-OS リリース 9.3(6) 以降、タイプ 6 暗号化パスワードを元の状態に戻すことは、MACsec キーチェーンではサポートされていません。
- Cisco NX-OS リリース 10.3(3)F 以降、タイプ 6 暗号化パスワードを元の状態に戻すことは、RPM 汎用キーチェーンではサポートされていません。
- タイプ 6 暗号化は、AES パスワード暗号化機能が有効で、プライマリ キーが設定されている場合にのみ設定できます。
- プライマリ キーが構成され、AES パスワード暗号化機能がスイッチで有効になっている場合、キーチェーン `infra` の下の各 MACsec キー ストリング構成は、タイプ 6 暗号化で自動的に暗号化されます。
- プライマリ キーの設定は、スイッチに対してローカルです。あるスイッチからタイプ 6 に構成された実行データを取得し、別のプライマリ キーが設定されている別のスイッチに適用すると、新しいスイッチでの復号化は失敗します。

- タイプ6暗号化の後にスタートアップ構成を消去し、構成の置換機能を使用すると、プライマリキーがPSSに保存されないため、構成の置換は失敗します。したがって、MACsecタイプ6暗号化キー文字列の構成が失われます。
- タイプ6のキーを構成すると、SKSDが提供する復号コマンドを適用しないと、既存のタイプ6の暗号化キー文字列をタイプ7の暗号化キー文字列に変更できません。
- タイプ6暗号化がサポートされていない古いイメージでコールドリブートによってシステムをダウングレードする場合は、コールドリブートを続行する前に設定を取り出す必要があります。これを行わないと、設定が失われます。
- システムをダウングレードすると、タイプ6の構成は失われます。
- ISSDによってシステムをダウングレードすると、機能確認チェックが呼び出され、ダウングレードに進む前に設定を削除するように通知されます。**encryption decrypt** コマンドを使用して、タイプ6暗号化キーをタイプ7暗号化キーに変換してから、ダウングレードを続行できます。
- ISSUのアップグレード中に、タイプ7暗号化キーを含む古いイメージからタイプ6暗号化をサポートする新しいイメージに移行する場合、再暗号化が強制されるまで、rpmは既存のキーをタイプ6暗号化キーに変換しません。再暗号化を適用するには、**encryption re-encrypt obfuscated** コマンドを使用します。
- タイプ7暗号化キーを含む古いイメージからタイプ6暗号化をサポートする新しいイメージへのISSUアップグレード後、古いイメージに保存されている構成ファイル、またはアップグレード後にタイプ6に対してパスワードを再暗号化せずに保存された構成ファイルを使用して構成の置換が行われた場合（**encryption re-encrypt obfuscated** コマンドを使用して）、構成の置換は失敗します。
- タイプ6暗号化の後にプライマリキーを変更すると、既存のタイプ6暗号化キー文字列に対する復号コマンドは失敗します。既存のタイプ6キースtringを削除し、新しいキースtringを設定する必要があります。
- RPM レガシー キーチェーンの場合、タイプ6キースtringは、AESパスワード暗号化機能を有効にしてプライマリキーを設定しなくても構成できますが、これらのタイプ6キースtringは、AESパスワード暗号化機能が有効になり、タイプ6キースtringが生成されたプライマリキーが設定されるまでは使用できません。
- Cisco NX-OS リリース 10.3(2)F 以降、DME ペイロードおよび非インタラクティブ モードを使用して、プライマリキーを構成できます。
- アップグレード中、デバイスのリロード中に、バイナリを復元せずにASCII再生がトリガーされると、プライマリキーが失われます。プライマリキーは、デバイスのリロード後に再構成する必要があります。**key config-key ascii** コマンドを使用して、プライマリキーを再構成し、暗号化の問題を回避します。ただし、バイナリ復元を使用したアップグレードでは、再起動後にプライマリキーが保持されます。
- 送信元イメージとターゲットイメージの両方がタイプ6暗号化をサポートするダウングレード中、デバイスのリロード中にバイナリを復元せずにASCII再生がトリガーされると、プライマリキーが失われます。プライマリキーは、デバイスのリロード後に再構成

する必要があります。**key config-key ascii** コマンドを使用して、プライマリ キーを再設定し、暗号化の問題を回避します。ただし、送信元イメージとターゲットイメージの両方がタイプ6暗号化をサポートしている場合、バイナリ復元を使用したダウングレードでは、再起動後のプライマリ キーが保持されます。

タイプ6暗号化をサポートするイメージからタイプ6暗号化をサポートしないイメージにシステムをダウングレードすると、互換性チェックは失敗します。

パスワード暗号化のデフォルト設定

次の表に、パスワード暗号化パラメータのデフォルト設定を示します。

表 35: パスワード暗号化パラメータのデフォルト設定

パラメータ	デフォルト
AES パスワード暗号化機能	無効
プライマリ 鍵	未設定

パスワード暗号化の設定

ここでは、Cisco NX-OS デバイスでパスワード暗号化を設定する手順について説明します。

プライマリ キーの設定および AES パスワード暗号化機能の有効化

タイプ6暗号化用のプライマリ キーを構成し、高度暗号化規格（AES）パスワード暗号化機能を有効にすることができます。

Cisco NX-OS リリース 10.3(3)F 以降では、RPM レガシー キーチェーンでタイプ6暗号化がサポートされています。

Procedure

	Command or Action	Purpose
ステップ 1	[no] key config-key ascii [<new_key> old <old_master_key>] Example: <pre>switch# key config-key ascii New Master Key: Retype Master Key:</pre>	プライマリ キー（マスター キー）を、AES パスワード暗号化機能で使用するよう設定します。プライマリ キーは、16 ～ 32 文字の英数字を使用できます。このコマンドの no 形式を使用すると、いつでもプライマリ キーを削除できます。

	Command or Action	Purpose
		プライマリ キーを設定する前に AES パスワード暗号化機能を有効にすると、プライマリ キーが設定されていない限りパスワード暗号化が実行されないことを示すメッセージが表示されます。プライマリ キーがすでに設定されている場合は、新しいプライマリ キーを入力する前に現在のプライマリ キーを入力するように求められます。 Note Cisco NX-OS リリース 10.3(2)F 以降、DME ペイロードおよび非インタラクティブ モードを使用して、プライマリ キーを構成できます。
ステップ 2	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 3	[no] feature password encryption aes tam Example: <pre>switch(config)# feature password encryption aes tam</pre>	AES パスワード暗号化機能を有効化または無効化します。
ステップ 4	encryption re-encrypt obfuscated Example: <pre>switch(config)# encryption re-encrypt obfuscated</pre>	既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換します。
ステップ 5	(Optional) show encryption service stat Example: <pre>switch(config)# show encryption service stat</pre>	AES パスワード暗号化機能とプライマリ キーの設定ステータスを表示します。
ステップ 6	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 Note このコマンドは、実行コンフィギュレーションとスタートアップ コンフィギュレーションのプライマリ キーを同期するために必要です。

Related Topics

- [AES パスワード暗号化およびプライマリ暗号キーについて](#) (617 ページ)
- [AES パスワード暗号化およびプライマリ暗号キーについて](#) (617 ページ)
- [キーのテキストの設定](#) (636 ページ)
- [キーの受け入れライフタイムおよび送信ライフタイムの設定](#) (639 ページ)

既存のパスワードのタイプ 6 暗号化パスワードへの変換

既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換できます。

Before you begin

AES パスワード暗号化機能を有効にし、プライマリ キーを設定したことを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	encryption re-encrypt obfuscated Example: <pre>switch# encryption re-encrypt obfuscated</pre>	既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換します。

タイプ 6 暗号化パスワードの元の状態への変換

タイプ 6 暗号化パスワードを元の状態に変換できます。この機能は、macsec キーチェーンではサポートされていません。

Before you begin

プライマリ キーを設定したことを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	encryption decrypt type6 Example: <pre>switch# encryption decrypt type6 Please enter current Master Key:</pre>	タイプ 6 暗号化パスワードを元の状態に変換します。

MACsec キーでのタイプ 6 暗号化の有効化

Advanced Encryption Standard (AES) パスワード暗号化機能とも呼ばれるタイプ 6 暗号化機能を使用すると、タイプ 6 暗号化形式で MACsec キーを安全に保存できます。

Cisco NX-OS リリース 9.3(5) 以降では、MACsec 機能をサポートするすべての Cisco Nexus 9000 シリーズ スイッチに、タイプ 6 暗号化形式で MACsec キーを保存できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] key config-key ascii 例 : switch(config)# key config-key ascii switch(config)# New Master Key: Switch(config)# Retype Master Key:	プライマリ キー（マスター キー）を構成します。
ステップ 3	[no] feature password encryption aes 例 : switch(config)# feature password encryption aes	AES パスワード暗号化機能を有効化または無効化します。
ステップ 4	key chain name macsec 例 : switch(config)# key chain 1 macsec switch(config-macseckeychain)#	MACSec キーチェーンを作成して MACSec キーのセットを保持し、MACSec キーチェーン設定モードを開始します。
ステップ 5	key key-id 例 : switch(config-macseckeychain)# key 1000 switch(config-macseckeychain-macseckey)#	MAC sec キーを作成し、MACsec キー設定モードを開始します。範囲は 1 ～ 32 オクテットで、最大サイズは 64 です。AES_128 は 32 ビットで使用され、AES_256 は 64 ビットで使用されます。
ステップ 6	key-octet-string <i>octet-string</i> cryptographic-algorithm {AES_128_CMAC AES_256_CMAC} 例 : switch(config-macseckeychain-macseckey)# key-octet-string abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm AES_256_CMAC	そのキーの octet スtring を設定します。 <i>octet-string</i> 引数には、最大 64 文字の 16 進数文字を含めることができます。オクテット キーは内部でエンコードされるため、 show running-config macsec コマンドの出力にクリア テキストのキーが現れることはありません。 キーオクテット文字列には、次のものが含まれます。 • 0 暗号化タイプ - 暗号化なし（デフォルト）

	コマンドまたはアクション	目的
		• 6 Encryption Type-Proprietary (Type-6 encrypted) • 7 暗号化タイプ - 最大 64 文字の、独自仕様 WORD キー オクテット 文 列

タイプ 6 暗号化パスワードの削除

Cisco NX-OS デバイスからすべてのタイプ 6 暗号化パスワードを削除できます。

Procedure

	Command or Action	Purpose
ステップ 1	encryption delete type6 Example: switch# encryption delete type6	すべてのタイプ 6 暗号化パスワードを削除します。

パスワード暗号化の設定の確認

パスワード暗号化の設定情報を表示するには、次の作業を行います。

コマンド	目的
show encryption service status	AES パスワード暗号化機能とプライマリ キーの設定ステータスを表示します。
show encryption mkey info [all hash-prefix last-updated length protection-type]	プライマリキーの詳細を表示します。 • all : タイプ 6 プライマリ キーのすべての詳細を表示します。 • hash-prefix : 保存されているタイプ 6 プライマリ キーのハッシュの最初の 16 文字を表示します。 • last-updated : タイプ 6 プライマリ キーが最後に変更された時刻を YYYY-MM-DD HH:MM:SS.SSS 形式で表示します。 • length : ユーザーが指定したタイプ 6 プライマリ キーの長さを表示します。 • protection-type : 保存されたタイプ 6 プライマリ キーの保護タイプを表示します。

パスワード暗号化の設定例

次の例は、プライマリ キーを作成し、AES パスワード暗号化機能を有効にして、TACACS+アプリケーションのためのタイプ 6 暗号化パスワードを構成する方法を示しています。

```
key config-key ascii
  New Master Key:
  Retype Master Key:
configure terminal
feature password encryption aes tam
show encryption service status
  Encryption service is enabled.
  Master Encryption Key is configured.
  Type-6 encryption is being used.
feature tacacs+
tacacs-server key Cisc0123
show running-config tacacs+
  feature tacacs+
  logging level tacacs 5
  tacacs-server key 6
"JDYkqyIFWeBvzpljSfWmRZrmRSRE8syxKlOSjP9RCckFinZbJI3GD5c6rckJR/Qju2PKLmOewbheAA=="
```

「show encryption mkey info」コマンドの構成例

次に、**show encryption mkey info [all | hash-prefix | last-updated | length | protection-type]** コマンドのさまざまなオプションの出力例を示します。

- **all**

```
switch# show encryption mkey info all
Master-Key ID : 1
-----
Type                               : Running (Active)
Key-Hash(first 16 chars)           : SHA512: TNESx81zL5C1fRpb
Protection-Type                     : Hardware
Length                             : 20
Last updated                       : 2024-11-03 16:35:26.074 IST
-----
```

- **hash-prefix: [key-Hash]** は、プライマリ キーの SHA-512 ダイジェストの base64 エンコーディングの最初の16文字です。

```
switch# show encryption mkey info hash-prefix
Master-Key ID : 1
-----
Key-Hash(first 16 chars)           : SHA512: TNESx81zL5C1fRpb
-----
```

- **last-updated : [Last updated]** 属性は、最後の変更のタイムスタンプを提供します。

```
switch# show encryption mkey info last-updated
Master-Key ID : 1
-----
Last updated                       : 2024-11-03 16:35:26.074 IST
-----
```

- **length** : **[Length]** は、構成されたプライマリ キーの長さを示しています。

```
switch# show encryption mkey info length
Master-Key ID : 1
```

```
-----
Length                               :          23
-----
```

- **protection-type** : **[protection-type]** は、プライマリキーの保護方法を示します。プライマリ キーは、**[Hardware]** (TAM 暗号化サービスを使用) または **[Software]** (内部ハッシュを使用) のいずれかによって保護されます。

Protection type : Hardware

```
switch(config)# feature password encryption aes tam
switch# show encryption mkey info all
Master-Key ID : 1
```

```
-----
Type                                :      Running (Active)
Key-Hash(first 16 chars)           :      SHA512: TNESx81zL5C1fRpb
Protection-Type                    :      Hardware
Length                             :      20
Last updated                        :      2024-11-03 16:35:26.074 IST
-----
```

Protection type : Software

```
switch# key config ascii
<master-key>
<retype master-key>
switch# show encryption mkey info all
Master-Key ID : 1
```

```
-----
Type                                :      Running (Active)
Key-Hash(first 16 chars)           :      SHA512: TNESx81zL5C1fRpb
Protection-Type                    :      Software
Length                             :      20
Last updated                        :      2024-11-03 16:35:26.074 IST
-----
```

プライマリキーでは、**Type** と **Protection-Type** を除く、その前のすべての属性は変更されません。次の使用例では、これらの操作のいずれか（「copy run start」、「no key config ascii」、「write erase」、またはプライマリ キーが変更された場合）が次にハイライトされているように実行される場合に、これらの **[Type]** および **[Protection-Type]** フィールドの値がどのように変更されるかを説明します。

- **ケース 1** : プライマリ キーが初めて構成された場合、プライマリ キーは現在「アクティブ」であり、タイプ 6 暗号化サービスに使用できます。

```
switch# key config ascii
<master-key>
<retype master-key>
switch# show encryption mkey info all
Master-Key ID : 1
```

```
-----
Type                                :      Running (Active)
-----
```



```

Key-Hash(first 16 chars) : SHA512: TNESx81zL5C1fRpb
Protection-Type          : Software
Length                   : 20
Last updated              : 2024-11-03 16:35:26.074 IST

```



(注) 構成は、スタートアップ構成に保存されていないため (copy run start を使用)、デバイスのリロード後は存在しません。

- **ケース 2**：プライマリ キーがタイプ 6 暗号化コマンドを使用して暗号化されている場合、**[Protection-type]** が **Hardware** に変更されます。これは、保存されたマスター キーがトラストアンカーモジュール (TAM) で提供される暗号化アルゴリズムを使用して暗号化されたことを示します。

```

switch(config)# feature password encryption aes tam
switch# show encryption mkey info all
Master-Key ID : 1

```

```

Type                : Running (Active)
Key-Hash(first 16 chars) : SHA512: TNESx81zL5C1fRpb
Protection-Type      : Hardware
Length               : 20
Last updated         : 2024-11-03 16:35:26.074 IST

```

- **ケース-3**：プライマリ キーが変更された場合、次の 2 つのシナリオが発生します。

1. アクティブな「Running」のプライマリキーがすでに存在する場合、既存のプライマリキーは、同じタイプ（実行中な場合）の新しく設定されたプライマリキーに置き換えられます。

```

switch# key config ascii
<current master-key>
<new master-key>
<retype new master-key>
switch# show encryption mkey info all
Master-Key ID : 1

```

```

Type                : Running (Active)
Key-Hash(first 16 chars) : SHA512: PWEQJonK0xzt21NJ
Protection-Type      : Hardware
Length               : 26
Last updated         : 2024-11-05 05:33:37.626IST

```

2. アクティブな「Running & Startup」プライマリ キーがある場合、既存のプライマリキーは新しく構成されたプライマリ キーに置き換えられます。show コマンドは、次の 2 つの独立したプライマリ キーを表示します。

- 「Startup」という新しいタイプに設定され、「Inactive」としてマークされている古いプライマリ キー用に 1 つ。このプライマリ キーは、次のデバイスのリロード後にのみ使用できます。

- その他 新しく構成されたプライマリ キーは「Running」タイプで、現在アクティブであり、（デバイスがリロードされるまで）新しいセッションで使用できます。

```
switch# show encryption mkey info all
```

```
Master-key ID : 1
```

```
-----
Type                : Startup (Inactive)
Key-Hash(first 16 chars) : SHA512: TNESx8lzL5C1fRpb
Protection-Type      : Hardware
Length              : 20
Last updated        : 2024-11-03 16:35:26.074 IST
-----
```

```
Master-Key ID : 2
```

```
-----
Type                : Running (Active)
Key-Hash(first 16 chars) : SHA512: PWEQJonK0xzt21NJ
Protection-Type      : Hardware
Length              : 26
Last updated        : 2024-11-05 05:33:37.626IST
-----
```

- ケース 4： 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーすると、現在構成されているプライマリ キー（running-config 内）が startup-config に保存され、そのタイプが「Running & Startup」に変更されます。つまり、このプライマリ キーは現在「アクティブ」で、タイプ 6 暗号化サービスに使用できます。

```
switch# copy r s
```

```
switch# show encryption mkey info all
```

```
Master-key ID : 1
```

```
-----
Type                : Running & Startup (Active)
Key-Hash(first 16 chars) : SHA512: TNESx8lzL5C1fRpb
Protection-Type      : Hardware
Length              : 20
Last updated        : 2024-11-03 16:35:26.074 IST
-----
```



- (注)
- 構成は、スタートアップ構成に保存されているため（copy run start を使用）、デバイスのリロード後は存在しません。
 - デバイス リロード前にコピー実行の開始が実行されない場合、プライマリ キーが失われる可能性があります。または、スタートアップコンフィギュレーションに既存のプライマリ キーがあった場合は、そのプライマリ キーの最後に保存された状態がリロード後も保持されます。

- ケース 5： running-config からプライマリ キーが削除されると、次の 2 つのシナリオが発生します。

1. 「Running」プライマリ キーのみがある場合、現在構成されているプライマリ キーは running-config から削除され、対応するエントリが削除されます。したがって、show コマンドの出力は空です。

```
switch# no key config ascii
switch# show encryption mkey info all
switch#
```

2. 「Running & Startup」プライマリ キーがある場合、**no key config ascii** コマンドの実行後のタイプは「Startup」に変わります。これは、プライマリ キーが running-config から削除されますが、startup-config にはまだ存在することを意味します。ただし、この「Startup」プライマリ キーはこのセッションではアクティブではなく、デバイスのリロード後にのみ使用できます。また、現在システムにアクティブなタイプ 6 プライマリ キーがないと表記された警告メッセージが生成されます。

```
switch# no key config ascii
switch# show encryption mkey info all
Master-key ID : 1
```

```
-----
Type                               :      Startup (Inactive)
Key-Hash(first 16 chars)           :      SHA512: TNESx81zL5C1fRpb
Protection-Type                     :      Hardware
Length                             :      20
Last updated                       :      2024-11-03 16:35:26.074 IST
-----
```

Warning: There is no "Running" master-key in the system as it may have been removed from running-config.



第 21 章

キーチェーン管理の設定

この章では、Cisco NX-OS デバイスでキーチェーン管理を設定する手順について説明します。

この章は、次の項で構成されています。

- キーチェーン管理について, [on page 631](#)
- キーチェーン管理の前提条件, [on page 632](#)
- キーチェーン管理の注意事項と制約事項 (632 ページ)
- キーチェーン管理のデフォルト設定, [on page 633](#)
- キーチェーン管理の設定, [on page 633](#)
- アクティブなキーのライフタイムの確認, [on page 642](#)
- キーチェーン管理の設定の確認, [on page 642](#)
- キーチェーン管理の設定例, [on page 642](#)
- 次の作業, [on page 643](#)
- キーチェーン管理に関する追加情報, [on page 643](#)

キーチェーン管理について

キーチェーン管理を使用すると、キーチェーンの作成と管理を行えます。キーチェーンはキーのシーケンスを意味します（共有秘密ともいいます）。キーチェーンは、他のデバイスとの通信をキーベース認証を使用して保護する機能と合わせて使用できます。デバイスでは複数のキーチェーンを設定できます。

キーベース認証をサポートするルーティング プロトコルの中には、キーチェーンを使用してヒットレス キー ロールオーバーによる認証を実装できるものがあります。詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

キーのライフタイム

安定した通信を維持するためには、キーベース認証で保護されるプロトコルを使用する各デバイスに、1つの機能に対して同時に複数のキーを保存し使用できる必要があります。キーチェーン管理は、キーの送信および受け入れライフタイムに基づいて、キーロールオーバーを処理するセキュアなメカニズムを提供します。デバイスはキーのライフタイムを使用して、キーチェーン内のアクティブなキーを判断します。

キーチェーンの各キーには次に示す 2 つのライフタイムがあります。

受け入れライフタイム

別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。

送信ライフタイム

別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

キーの送信ライフタイムおよび受け入れライフタイムは、次のパラメータを使用して定義します。

Start-time

ライフタイムが開始する絶対時間。

End-time

次のいずれかの方法で定義できる終了時。

- ライフタイムが終了する絶対時間
- 開始時からライフタイムが終了するまでの経過秒数
- 無限のライフタイム（終了時なし）

キーの送信ライフタイム中、デバイスはルーティング アップデート パケットをキーとともに送信します。送信されたキーがデバイス上のキーの受け入れライフタイム期間内でない場合、そのデバイスはキーを送信したデバイスからの通信を受け入れません。

どのキーチェーンも、キーのライフタイムが重なるように設定することを推奨します。このようにすると、アクティブなキーがないことによるネイバー認証の失敗を避けることができます。

キーチェーン管理の前提条件

キーチェーン管理には前提条件はありません。

キーチェーン管理の注意事項と制約事項

キーチェーン管理に関する注意事項と制約事項は次のとおりです。

- システム クロックを変更すると、キーがアクティブになる時期に影響が生じます。
- キーチェーンの設定タイプは、クライアントプロトコル内でリンクされているタイプと一致する必要があります。これらのタイプの不一致がある状態で試行されると、ユーザーに通知するための syslog メッセージが生成されます。

たとえば、**keychain_abc** という名前のキーチェーンが Macsec キーチェーンとして設定されていても、OSPF でクラシック キーチェーンとして関連付けられている場合はサポートされません。同様に、キーチェーンが最初にクライアントに関連付けられ（前方参照と呼

ばれるプロセス)、別のキーチェーン タイプとして設定される場合もサポートされません。

- ネイバー/テンプレートのパスワードをプログラマ的に (restconf/Netconfなどで) 設定する場合は、ユーザーのパスワードのタイプとパスワードを指定することを強くお勧めします。プログラムの呼び出しでどちらかのプロパティが欠落している場合、BGPは欠落しているプロパティについて、すでに使用可能な (またはデフォルトの) 値を使用して、ネイバー/テンプレートのパスワードを構成します。

ユーザーがプロパティを指定せずに構成する必要がある場合、ユーザーは両方のピアルータで同じ手順を実行する必要があります。

キーチェーン管理のデフォルト設定

次の表に、Cisco NX-OS キーチェーン管理パラメータのデフォルト設定を示します。

Table 36: キーチェーン管理パラメータのデフォルト値

パラメータ	デフォルト
キー チェーン	デフォルトではキーチェーンはありません。
キー	デフォルトでは新しいキーチェーンの作成時にキーは作成されません。
受け入れライフタイム	常に有効です。
送信ライフタイム	常に有効です。
キースtringing入力の暗号化	暗号化されません。

キーチェーン管理の設定

キーチェーンの作成

デバイスにキーチェーンを作成できます。新しいキーチェーンには、キーは含まれていません。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example:	グローバル構成モードを開始します。

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	key chain name Example: switch(config)# key chain bgp-keys switch(config-keychain)#	キーチェーンを作成し、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	(Optional) show key chain name Example: switch(config-keychain)# show key chain bgp-keys	キーチェーンの設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config-keychain)# copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。

キーチェーンの削除

デバイスのキーチェーンを削除できます。



Note キーチェーンを削除すると、キーチェーン内のキーはどれも削除されます。

Before you begin

キーチェーンを削除する場合は、そのキーチェーンを使用している機能がないことを確認してください。削除するキーチェーンを使用するように設定されている機能がある場合、その機能は他のデバイスとの通信に失敗する可能性が高くなります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル構成モードを開始します。
ステップ 2	no key chain name Example: switch(config)# no key chain bgp-keys	キーチェーンおよびそのキーチェーンに 含まれているすべてのキーを削除しま す。

	Command or Action	Purpose
ステップ 3	(Optional) show key chain <i>name</i> Example: switch(config-keychain)# show key chain bgp-keys	そのキーチェーンが実行コンフィギュレーション内にないことを確認します。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config-keychain)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

プライマリ キーの設定および AES パスワード暗号化機能の有効化

タイプ 6 暗号化用のプライマリ キーを構成し、高度暗号化規格（AES）パスワード暗号化機能を有効にすることができます。

Cisco NX-OS リリース 10.3(3)F 以降では、RPM レガシー キーチェーンでタイプ 6 暗号化がサポートされています。

Procedure

	Command or Action	Purpose
ステップ 1	[no] key config-key ascii [<new_key> old <old_master_key>] Example: switch# key config-key ascii New Master Key: Retype Master Key:	プライマリ キー（マスター キー）を、AES パスワード暗号化機能で使用するよう設定します。プライマリ キーは、16 ～ 32 文字の英数字を使用できます。このコマンドの no 形式を使用すると、いつでもプライマリ キーを削除できます。 プライマリ キーを設定する前に AES パスワード暗号化機能を有効にすると、プライマリ キーが設定されていない限りパスワード暗号化が実行されないことを示すメッセージが表示されます。プライマリ キーがすでに設定されている場合は、新しいプライマリ キーを入力する前に現在のプライマリ キーを入力するように求められます。 Note Cisco NX-OS リリース 10.3(2)F 以降、DME ペイロードおよび非インタラクティブ モードを使用して、プライマリ キーを構成できます。

	Command or Action	Purpose
ステップ 2	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 3	[no] feature password encryption aes tam Example: <pre>switch(config)# feature password encryption aes tam</pre>	AES パスワード暗号化機能を有効化または無効化します。
ステップ 4	encryption re-encrypt obfuscated Example: <pre>switch(config)# encryption re-encrypt obfuscated</pre>	既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換します。
ステップ 5	(Optional) show encryption service stat Example: <pre>switch(config)# show encryption service stat</pre>	AES パスワード暗号化機能とプライマリ キーの設定ステータスを表示します。
ステップ 6	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 Note このコマンドは、実行コンフィギュレーションとスタートアップ コンフィギュレーションのプライマリ キーを同期するために必要です。

Related Topics

- [AES パスワード暗号化およびプライマリ暗号キーについて \(617 ページ\)](#)
- [AES パスワード暗号化およびプライマリ暗号キーについて \(617 ページ\)](#)
- [キーのテキストの設定 \(636 ページ\)](#)
- [キーの受け入れライフタイムおよび送信ライフタイムの設定 \(639 ページ\)](#)

キーのテキストの設定

キーのテキストを設定できます。テキストは共有秘密です。デバイスはこのテキストをセキュアな形式で保存します。

MACsec および RPM レガシー キーチェーンの場合、AES パスワード暗号化機能が有効になっており、プライマリ キーが構成されている場合、テキストはタイプ 6 形式で暗号化されて保存されます。それ以外の場合は、タイプ 7 暗号化形式で保存されます。

デフォルトでは、受け入れライフタイムおよび送信ライフタイムは無限になり、キーは常に有効です。キーにテキストを設定してから、そのキーの受け入れライフタイムと送信ライフタイムを設定します。

Before you begin

そのキーのテキストを決めます。テキストは、暗号化されていないテキストとして入力できます。また、**show key chain** コマンド使用時に Cisco NX-OS がキー テキストの表示に使用する暗号形式で入力することもできます。特に、別のデバイスから **show key chain** コマンドを実行し、その出力に表示されるキーと同じキーテキストを作成する場合には、暗号化形式での入力が便利です。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル構成モードを開始します。
ステップ 2	key chain name Example: switch(config)# key chain bgp-keys switch(config-keychain)#	指定したキーチェーンのキーチェーン 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 key-ID Example: switch(config-keychain)# key 13 switch(config-keychain-key)#	指定したキーのキー コンフィギュレーション モードを開始します。 <i>key-ID</i> 引数は、0 ～ 65535 の整数で指定する必要があります。
ステップ 4	key-string [encryption-type] text-string Example: switch(config-keychain-key)# key-string 0 AS3cureStr1ng	そのキーのテキスト スtring を設定します。 <i>key-ID</i> 引数は、大文字と小文字を区別して、英数字で指定します。特殊文字も使用できます。 <i>Encryption-type</i> 引数に、次のいずれかの値を指定します。 • 0 : 入力した <i>text-string</i> 引数は、暗号化されていないテキスト文字列です。これがデフォルトです。 • 6 : Cisco NX-OS リリース 10.3(3)F 以降、Cisco Nexus 9000 シリーズ プラットフォーム スイッチでシスコ独自の（タイプ 6 暗号化）方式がサポートされています。

	Command or Action	Purpose																
		7: 入力した <i>text-string</i> 引数は、暗号化されています。シスコ固有の暗号方式で暗号化されます。このオプションは、別の Cisco NX-OS デバイス上で実行した show key chain コマンドの暗号化出力に基づいて、テキスト文字列を入力する場合に役立ちます。 key-string コマンドには、<i>text-string</i> での次の特殊文字の使用に関する制限があります。 <table><tr><th>特殊文字</th><th>説明</th></tr><tr><td> </td><td>縦棒</td></tr><tr><td>></td><td>右辺</td></tr><tr><td>\</td><td>バックslash</td></tr><tr><td>(</td><td>左丸括弧</td></tr><tr><td>'</td><td>アポストロフィ</td></tr><tr><td>"</td><td>引用符</td></tr><tr><td>?</td><td>疑問符</td></tr></table> コマンドでの特殊文字の使用方法の詳細については、「コマンドラインインターフェイスについて」セクションを参照してください。	特殊文字	説明		縦棒	>	右辺	\	バックslash	(	左丸括弧	'	アポストロフィ	"	引用符	?	疑問符
特殊文字	説明																	
	縦棒																	
>	右辺																	
\	バックslash																	
(	左丸括弧																	
'	アポストロフィ																	
"	引用符																	
?	疑問符																	
ステップ 5	(Optional) show key chain name [mode decrypt] Example: switch(config-keychain-key)# show key chain bgp-keys	キー テキストの設定も含めて、キーチェーンの設定を表示します。デバイス管理者だけが使用できる mode decrypt オプションを使用すると、キーはクリアテキストで表示されます。																

	Command or Action	Purpose
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config-keychain-key)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[プライマリ キーの設定および AES パスワード暗号化機能の有効化](#) (620 ページ)

キーの受け入れライフタイムおよび送信ライフタイムの設定

キーの受け入れライフタイムおよび送信ライフタイムを設定できます。デフォルトでは、受け入れライフタイムおよび送信ライフタイムは無限になり、キーは常に有効です。



Note

キーチェーン内のキーのライフタイムが重複するように設定することを推奨します。このようにすると、アクティブなキーがないために、キーによるセキュア通信の切断を避けることができます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	key chain name Example: <pre>switch(config)# key chain bgp-keys switch(config-keychain)#</pre>	指定したキーチェーンのキーチェーン 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 key-ID Example: <pre>switch(config-keychain)# key 13 switch(config-keychain-key)#</pre>	指定したキーのキー 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	accept-lifetime [local] start-time [duration duration-value infinite end-time] Example: <pre>switch(config-keychain-key)# accept-lifetime 00:00:00 Jun 13 2013 23:59:59 Sep 12 2013</pre>	キーの受け入れライフタイムを設定します。デフォルトでは、デバイスは start-time および end-time 引数を UTC として扱います。 local キーワードを指定すると、デバイスはこれらの時間を現地時間として扱います。

	Command or Action	Purpose
		<i>start-time</i> 引数は、キーがアクティブになる日時です。 ライフタイムの終了時は次のいずれかのオプションで指定できます。 • duration <i>duration-value</i> : ライフタイムの長さ（秒）。最大値は 2147483646 秒（約 68 年）です。 • infinite : キーの受け入れライフタイムは期限切れになりません。 • end-time : The <i>end-time</i> 引数はキーがアクティブでなくなる日時です。
ステップ 5	send-lifetime [local] <i>start-time</i> [duration <i>duration-value</i> infinite <i>end-time</i>] Example: <pre>switch(config-keychain-key)# send-lifetime 00:00:00 Jun 13 2013 23:59:59 Aug 12 2013</pre>	キーの送信ライフタイムを設定します。デフォルトでは、デバイスは <i>start-time</i> および <i>end-time</i> 引数を UTC として扱います。 local キーワードを指定すると、デバイスはこれらの時間を現地時間として扱います。 <i>start-time</i> 引数は、キーがアクティブになる日時です。 送信ライフタイムの終了時は次のいずれかのオプションで指定できます。 • duration <i>duration-value</i> : ライフタイムの長さ（秒）。最大値は 2147483646 秒（約 68 年）です。 • infinite : キーの送信ライフタイムは期限切れになりません。 • end-time : The <i>end-time</i> 引数はキーがアクティブでなくなる日時です。
ステップ 6	(Optional) show key chain <i>name</i> [mode decrypt] Example: <pre>switch(config-keychain-key)# show key chain bgp-keys</pre>	キー テキストの設定も含めて、キーチェーンの設定を表示します。デバイス管理者だけが使用できる mode decrypt オプションを使用すると、キーはクリアテキストで表示されます。

	Command or Action	Purpose
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config-keychain-key) # copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[プライマリ キーの設定および AES パスワード暗号化機能の有効化](#) (620 ページ)

OSPFv2 暗号化認証用のキーの設定

OSPFv2のメッセージダイジェスト5 (MD5) またはハッシュベースのメッセージ認証コードセキュアハッシュアルゴリズム (HMAC-SHA) 認証を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config) #</pre>	グローバル構成モードを開始します。
ステップ 2	key chain name 例 : <pre>switch(config) # key chain bgp-keys switch(config-keychain) #</pre>	指定したキーチェーンのキーチェーン 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 key-ID 例 : <pre>switch(config-keychain) # key 13 switch(config-keychain-key) #</pre>	指定したキーのキー コンフィギュレーション モードを開始します。 <i>key-ID</i> 引数は、0 ～ 65535 の整数で指定する必要があります。 (注) OSPFv2 の場合、 <i>key key-id</i> コマンドのキー ID の値は 0 ～ 255 です。
ステップ 4	[no] cryptographic-algorithm {HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 MD5} 例 : <pre>switch(config-keychain-key) # cryptographic-algorithm HMAC-SHA-1</pre>	指定キーに使用される OSPFv2 暗号アルゴリズムを設定します。1つのキーに設定できる暗号化アルゴリズムは1つだけです。

	コマンドまたはアクション	目的
ステップ 5	(任意) show key chain name 例： switch(config-keychain-key)# show key chain bgp-keys	キーチェーンの設定を表示します。
ステップ 6	(任意) copy running-config startup-config 例： switch(config-keychain-key)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

アクティブなキーのライフタイムの確認

キーチェーン内のキーのうち、受け入れライフタイムまたは送信ライフタイムがアクティブなキーを確認するには、次の表のコマンドを使用します。

コマンド	目的
show key chain	デバイスで設定されたキーチェーンを表示します。

キーチェーン管理の設定の確認

キーチェーン管理の設定情報を表示するには、次の作業を行います。

コマンド	目的
show key chain name	デバイスに設定されているキーチェーンを表示します。

キーチェーン管理の設定例

「ospf-keys」という名前のキーチェーンを構成する例を示します。各キー テキスト スtring は暗号化されています。キーは、暗号化アルゴリズムとして MD5 を使用するように構成されます。各キーの受け入れライフタイムは送信ライフタイムよりも長いため、キーのペア間で重複が発生します。この例では、キー 1 とキー 2、およびキー 2 とキー 3 の間にオーバーラップが設定されています。これにより、アクティブなキーがない期間が回避され、基盤となるプロトコルの通信の中断を回避できます。

```
key chain ospf-keys
key 1
  key-string 7 070c285f4d0658544541
  accept-lifetime local 00:00:00 May 13 2024 12:00:00 Sep 14 2024
  send-lifetime local 00:00:00 May 13 2024 00:00:00 Sep 14 2024
```



```
cryptographic-algorithm MD5
key 2
key-string 7 070c285f4d0658574446
accept-lifetime local 00:00:00 Sep 13 2024 12:00:00 Jan 15 2025
send-lifetime local 10:00:00 Sep 13 2024 12:00:00 Jan 15 2025
cryptographic-algorithm MD5
key 3
key-string 7 070c285fad0622474941
accept-lifetime local 00:00:00 Jan 15 2025 12:00:00 Jun 15 2025
send-lifetime local 10:00:00 Jan 15 2025 12:00:00 Jun 15 2025
cryptographic-algorithm MD5
```

次に、タイプ 6 暗号を使用する「bgp-keys」という名前のキーチェーンを構成する例を示します。この暗号化モードは、feature password encryption aes が有効になっている場合に使用できません。

```
key chain bgp-keys
key 1
key-string 6
JDYkbN6ZTz3Hqrv5ZWliyxqlYiQXYc0wWpOnK7epMGoHK6qVJPeJtSYAGhQ9V+QKG4ZrcWeuunTtAA==
accept-lifetime local 00:00:00 May 13 2024 12:00:00 Sep 14 2024
send-lifetime local 00:00:00 May 13 2024 00:00:00 Sep 14 2024
key 2
key-string 6
JDYkO6Di45BulikPja/r8VJNoSTa4I4QMxtzzG3DQzal9G9LJA6F1WNGX8GRgn95SPuf4naoTZCtAA==
accept-lifetime local 00:00:00 Sep 13 2024 12:00:00 Jan 15 2025
send-lifetime local 10:00:00 Sep 13 2024 12:00:00 Jan 15 2025
key 3
key-string 6
JDYk8DJ15ZdOQ/O7vnj2M921RiR2x8VrL0Muj/30TN1IK5f+JMFH0Wy0Rfuy827G/H10w2it7eVAA==
accept-lifetime local 00:00:00 Jan 15 2025 12:00:00 Jun 15 2025
send-lifetime local 10:00:00 Jan 15 2025 12:00:00 Jun 15 2025
```

次の作業

キーチェーンを使用するルーティング機能については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

キーチェーン管理に関する追加情報

関連資料

関連項目	マニュアル タイトル
ボーダー ゲートウェイ プロトコル	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』
OSPFv2	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—



CHAPTER 22

トラフィック ストーム制御の設定

この章では、Cisco NX-OS デバイスに、トラフィック ストーム制御機能を設定する手順について説明します。

この章は、次の項で構成されています。

- [トラフィック ストーム制御について, on page 645](#)
- [トラフィック ストーム制御のライセンス要件, on page 647](#)
- [トラフィック ストーム制御のガイドラインと制約事項 \(647 ページ\)](#)
- [トラフィック ストーム制御のデフォルト設定, on page 652](#)
- [ワンレベルのしきい値のトラフィック ストーム制御の設定, on page 652](#)
- [CoPP ポリサーよりもストーム制御ポリサーを優先する \(653 ページ\)](#)
- [ツーレベルのしきい値のトラフィック ストーム制御の設定 \(654 ページ\)](#)
- [トラフィック ストーム制御の設定の確認, on page 656](#)
- [トラフィック ストーム制御カウンタのモニタリング \(656 ページ\)](#)
- [トラフィック ストーム制御の設定例, on page 657](#)
- [トラフィック ストーム制御のシステム ログの例 \(657 ページ\)](#)
- [トラフィック ストーム制御に関する追加情報, on page 658](#)

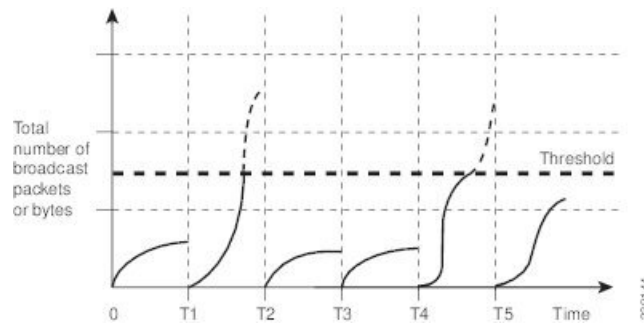
トラフィック ストーム制御について

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能を使用すると、物理インターフェイスにおけるブロードキャスト、マルチキャスト、またはユニキャストトラフィック ストームによって、レイヤ 2 またはレイヤ 3 ポート経由の通信が妨害されるのを防げます。

トラフィック ストーム制御（トラフィック抑制ともいう）では、ブロードキャスト、マルチキャスト、ユニキャストの着信トラフィックのレベルを 3.9 ミリ秒間隔でモニターできます。この間、トラフィック レベル（ポートの使用可能合計帯域幅に対するパーセンテージ）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

次の表に、指定したインターバルでのレイヤ2またはレイヤ3 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ます。この例では、トラフィック ストーム制御が T1 と T2 時間の間、および T4 と T5 時間の間で発生します。これらの間隔中に、ブロードキャストトラフィックの量が設定済みのしきい値を超過したためです。

Figure 20: ブロードキャストの抑制



トラフィック ストーム制御しきい値の数値と期間の組み合わせにより、トラフィック ストーム制御アルゴリズムがさまざまな粒度で機能します。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。

Cisco Nexus 9000v デバイスのトラフィック ストーム制御はハードウェアに実装されています。トラフィック ストーム制御は、レイヤ2 またはレイヤ3 インターフェイスからスイッチングバスに渡されるパケットをモニタします。システムはパケットの宛先アドレスに設定されている Individual/Group ビットを使用して、パケットがユニキャストかブロードキャストかを判断し、3.9 ミリ秒以内の間隔で現在のパケット数を追跡します。パケット数がしきい値に到達したら、後続のパケットをすべて破棄します。

トラフィック ストーム制御では、トラフィック量の計測に帯域幅方式を使用します。制御対象のトラフィックが使用できる、利用可能な合計帯域幅に対するパーセンテージを設定します。パケットは一定間隔で着信するわけではないので、3.9 ミリ秒の間隔はトラフィック ストーム制御の動作に影響を及ぼす可能性があります。

次に、トラフィック ストーム制御の動作がどのような影響を受けるかを示します。

- ブロードキャストトラフィック ストーム制御をイネーブルにした場合、ブロードキャストトラフィックが3.9 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまですべてのブロードキャストトラフィックがドロップされます。
- ブロードキャストとマルチキャストのトラフィック ストーム制御をイネーブルにした場合、ブロードキャストとマルチキャストの混合トラフィックが3.9 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまでブロードキャストとマルチキャストのすべてのトラフィックがドロップされます。
- ブロードキャストとマルチキャストのトラフィック ストーム制御をイネーブルにした場合、ブロードキャストトラフィックが3.9 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまでブロードキャストとマルチキャストのすべてのトラフィックがドロップされます。

- ブロードキャストとマルチキャストのトラフィック ストーム制御をイネーブルにした場合、マルチキャスト トラフィックが 3.9 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまでブロードキャストとマルチキャストのすべてのトラフィックがドロップされます。

トラフィックが設定レベルを超過する場合、トラフィック ストーム制御を設定して次のオプションの修正措置を実行することができます。

- シャットダウン：入力トラフィックがポートに対して設定されたトラフィック ストーム制御レベルを超えると、トラフィック ストーム制御がポートを **errdisable** ステートにします。このポートを再度イネーブルにするために、設定されたインターフェイス上で **shutdown** と **no shutdown** オプションを使用することも、**error-disable** 検出および回復機能を使用することもできます。**error-disable** 検出および回復用の **errdisable recovery cause storm-control** コマンドは回復間隔を定義する **errdisable recovery interval** コマンドと一緒に使用することをお勧めします。この間隔は 30 ～ 65535 秒の範囲にすることができます。
- トラップ：入力トラフィックが設定されたトラフィック ストーム制御レベルを超えたときに **SNMP** トラップを生成するようにトラフィック ストーム制御を設定できます。**SNMP** トラップアクションはデフォルトでイネーブルになっています。ただし、ストーム制御トラップはデフォルトでレート制限されません。コマンドを使用して、1分あたりに生成されるトラップの数を制御できます。**snmp-server enable traps storm-control trap-rate**

デフォルトで、Cisco NX-OS は、トラフィックが設定済みレベルを超えても是正のための処理を行いません。

トラフィック ストーム制御のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	トラフィック ストーム制御にはライセンスは必要ありません。ライセンスパッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。Cisco NX-OS ライセンス方式の詳細については、『 <i>Cisco NX-OS Licensing Guide</i> 』を参照してください。

トラフィック ストーム制御のガイドラインと制約事項

トラフィック ストーム制御には、次の設定時のガイドラインおよび制約事項があります。

- sFlow も有効になっているインターフェイスでストーム制御を有効にした場合、ストーム制御機能は動作しません。

- ストーム制御 PPS オプションは、Cisco Nexus 9300-FX2 プラットフォーム スイッチでのみサポートされていました。Cisco NX-OS Release 10.3(2)F 以降では、Cisco Nexus 9300-FX3、9300-GX、および 9300-GX2 プラットフォーム スイッチでもサポートされています。
- Cisco Nexus NFE2対応デバイスの場合、ストーム制御CPUを使用してCPUに送信されるARPパケットの数を制御できます。
- ストーム制御は、物理インターフェイス、ポートチャネルインターフェイス、およびブレイクアウトインターフェイスで設定できます。
- トラフィック ストーム制御レベルをインターフェイスの帯域幅全体に対する割合として指定します。
 - pps の範囲は 0 ～ 2000000000 です。
 - 任意で、レベルの小数部を 0 ～ 99 の範囲で指定できます。
 - 100% は、トラフィック ストーム制御がないことを意味します。
 - 0.0% は、すべてのトラフィックを抑制します。
- 9400 シリーズ ライン カードを搭載した Cisco Nexus 9300 シリーズ スイッチでは、ストーム制御 CLI を使用して、帯域幅レベルをポート容量のパーセンテージまたは 1 秒あたりのパケット数として指定できます。
- Cisco Nexus リリース 9.2 (1) 以降では、ストーム制御パケット/秒を次のように設定すると、エラーマージンが 1% を超えます。
 - 60 秒未満のトラフィック期間
 - ストーム制御 pps が 1000 未満
 - ストーム制御 pps が 5 未満の場合はサポート対象外
 - 5～1000 pps の場合、60 秒未満でストーム制御をヒットさせるには追加の pps が 20 必要
 - 1000 pps を超える場合、60 秒未満でストーム制御をヒットさせるには、2.5～3% の追加の pps が必要です。
- Cisco Nexus リリース 9.2(1) 以降では、Cisco Nexus 9336C-FX2、Cisco Nexus 93300YC-FX2、および Cisco Nexus 93240YC-FX2-Z スイッチのポート容量または 1 秒あたりのパケット数の割合を使用できます。
- N9K-X9700-FX3 ラインカードで VLAN の SVI を設定している場合、ストーム制御ブロードキャストは ARP トラフィック (ARP 要求) に対して機能しません。
- ストーム制御ドロップが個別にカウントされるを防ぐ、ローカルリンクおよびハードウェアの制約事項があります。代わりに、ストーム制御ドロップは discards カウンタの他のドロップとともにカウントされます。

- ハードウェアの制限およびサイズの異なるパケットがカウントされる方式のため、トラフィック ストーム制御レベルの割合は概数になります。着信トラフィックを構成するフレームのサイズに応じて、実際に適用されるパーセンテージ レベルと設定したパーセンテージ レベルの間には、数パーセントの誤差がある可能性があります。
- ハードウェアの制限により、**show interface counters storm-control** の出力は次のとおりです。コマンドは、ストーム制御が設定され、インターフェイスが実際にARPブロードキャストトラフィックを抑制している場合、ARP 抑制を表示しません。この制限によって、設定されたアクションがトリガーされない可能性があります。入力 ARP ブロードキャストトラフィックは正しくストーム抑制されます。
- ハードウェアの制限により、ストーム制御は、Cisco Nexus GX シリーズプラットフォームスイッチのポート帯域幅の 70% を超える 400G ポートではサポートされません。
- ハードウェアの制限のため、パケット ドロップ カウンタは、トラフィック ストームが原因のパケット ドロップパケット ドロップによって発生その他の破棄された入力フレームとを区別できません。この制限によって、トラフィック ストームが発生していなくても、設定されたアクションがトリガーされる可能性があります。
- ハードウェアの制限により、ストーム抑制パケットの統計情報はアップリンクポートではサポートされません。
- ハードウェアの制限により、ストーム抑制パケット統計情報には、アクティブなSwitched Virtual Interface (SVI) を備えたVLAN上のブロードキャストトラフィックは含まれません。
- 設計上の制限により、設定されたレベルが0.0の場合、ストーム抑制パケットの統計情報は機能しません。これは、すべての着信ストームパケットを抑制することを意味します。
- トラフィック ストーム制御は、Cisco Nexus 9300 シリーズスイッチおよびX97160YC-EX、9700-FX ライン カードを搭載した Cisco Nexus 9500 シリーズ スwitchでサポートされます。
- トラフィックストーム制御は、Cisco N9K-M4PC-CFP2ではサポートされていません。
- トラフィックストーム制御は、FEXインターフェイスではサポートされません。
- トラフィックストーム制御は、未知のユニキャスト、未知のマルチキャスト、ブロードキャスト トラフィックなどの入力トラフィック専用です。



(注) Cisco Nexus 9000 シリーズスイッチでは、トラフィックストーム制御は不明なユニキャストトラフィックと不明なユニキャストトラフィックに適用されます。

- 設定されたアクションによってポートチャネルメンバーがエラーディセーブルになった場合、すべての個々のメンバーポートをフラップして、エラーディセーブル状態から回復する必要があります。

- Cisco Nexusリリース9.2 (1) のトラフィックストーム制御機能は、N9K-X96136YC-RラインカードおよびN9K-C9504-FM-Rファブリックモジュールを搭載したCisco Nexus 9500プラットフォームスイッチではサポートされません。
- Cisco Nexusリリース9.2 (4) 以降、トラフィックストーム制御機能は、N9K-X96136YC-RラインカードおよびN9K-C9504-FM-Rファブリックモジュールを搭載したCisco Nexus 9500プラットフォームスイッチでサポートされます。インターフェイスがブロードキャストトラフィックでフラッディングされた場合、トラフィックストーム制御カウンタは増加しません。
- Cisco Nexusリリース9.3(2)以降では、N9K-X96136YC-R、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RXラインカード、およびN9K-C9504-FM-RおよびN9K-C9508-FM-Rファブリックモジュール。トラフィックストーム制御カウンタおよびストーム制御アクションはサポートされていません。
- Cisco NX-OS リリース10.1(2) 以降では、N9K-X9624D-R2 およびN9K-C9508-FM-R2 プラットフォーム スイッチで ストーム制御機能がサポートされます。
- Cisco Nexusリリース10.1(2) 以降、Cisco Nexus N9300-FXおよびN9300-FX2シリーズスイッチでは、ブロードキャスト、不明なユニキャスト、およびマルチキャスト (BUM) トラフィックの2レベルのしきい値とロギングのサポートを設定できます。各しきい値レベルのトラップまたはシャットダウンアクション。既存のストーム制御設定は、1レベルのしきい値にのみ使用されるようになりました。
- 次のガイドラインと制限事項は、Cisco Nexus 10.1(2) リリースのBUMトラフィック機能の2レベルしきい値およびロギングに適用されます。
 - Cisco Nexus リリース 10.1(2) の新しいトラフィック ストーム制御機能は、Cisco Nexus N9300-FX では最大 62 ポート (単一スライスとして) 、Cisco Nexus N9300-FX2 では合計 124 ポート (2 スライスとして) をサポートします。
 - トラフィックストーム制御は、一度に1つのストーム制御モード (1レベルまたは2レベルのしきい値) にあるデバイスのみをサポートします。一度に1レベルのしきい値と2レベルのしきい値ストーム制御モードを混在させることはできません。
 - トラフィックストーム制御は、トラフィック統計情報をモニタし、Cisco Nexusリリース10.1 (2) からの各レベル (下位および上位) およびトラフィックタイプ (不明なユニキャスト、マルチキャスト、およびブロードキャスト) のシステムログを生成します。
 - 2レベルしきい値トラフィックストーム制御機能では、固定サイズ512の新しいTernary Content Addressable Memory (TCAM) リージョンのカービングと、デバイスのリロードが必要です。
 - 2レベルしきい値のトラフィックストーム制御は、L2 Netflow機能、つまりconfig layer2 スイッチドフローモニタCLIと共存できません。これは、TCAMリソースの制限によるものです。
 - トラフィックストーム制御の2レベルしきい値機能は、非IPMCフラッドトラフィック (IPヘッダーのないパケット) およびパケット/秒モードをサポートしません。

- トラフィック ストーム制御は、Generic Online Diagnostics (GOLD) パッケージおよびサブインターフェイスレベルではサポートされません。
- 以前のリリースで10.1 (2) にアップグレードし、2レベルのストーム制御機能を使用する場合は、新しいストーム制御コマンドを使用してスイッチを設定してください。
- バージョン10.1 (2) で2レベルストーム制御機能を設定しており、以前のバージョンにダウングレードする場合、新しい機能はダウングレードをサポートしません。ダウングレードするには、設定を削除します。
- Cisco Nexusリリース10.2 (1) 以降、ストーム制御では、1つのインターフェイスに複数のアクションを設定できません。以前のアクション値が上書きされると、設定されている最新のアクション値が考慮されます。
- Cisco NX-OS リリース 10.2(2)F 以降、ストーム制御機能は Cisco N9K-9332D-GX2B プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.3(2)F 以降、トラフィック ストーム制御はレイヤ3 インターフェイスでサポートされ、次の注意事項と制限事項が適用されます。
 - トラフィック ストーム制御は、1 つのしきい値ストーム制御モードにあるデバイスのみをサポートします。
 - ARPブロードキャストなど、制御プレーンに向けられるレイヤ3制御パケットは、ストーム制御によって抑制されず、CoPP ポリサーによってポリシングされます。ただし、ストーム制御違反アクションがトリガーされます。
 - この機能は、Cisco Nexus 9300-FX、9300-FX2、9300-FX3、9300-GX、9300-GX2 プラットフォーム スイッチ、および FX と GX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチでサポートされます
- Cisco NX-OS リリース 10.3(3)F 以降では、CoPP ポリサーよりもストーム制御ドロップを優先するために **system storm-control priority-policy drop-l3** コマンドが導入され、次の注意事項と制限事項が適用されます。
 - この機能は、レイヤ3 制御フレームに適用されます。
 - この機能は、Cisco Nexus 9300-FX、9300-FX2、9300-FX3、9300-GX、9300-GX2 プラットフォーム スイッチ、および FX と GX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチでサポートされます
 - この機能は、1 レベルのしきい値トラフィック ストーム制御にのみ適用されます。

トラフィック ストーム制御のデフォルト設定

次の表に、トラフィック ストーム制御パラメータのデフォルト設定値を示します。

Table 37: デフォルトのトラフィック ストーム制御パラメータ

パラメータ	デフォルト
トラフィック ストーム制御	無効
しきい値パーセンテージ	100

ワンレベルのしきい値のトラフィック ストーム制御の設定

制御対象のトラフィックがツーレベルしきい値に使用できる、利用可能な合計帯域幅に対するパーセンテージを設定できます。



Note

- トラフィック ストーム制御機能では、トラフィック ストーム制御の動作を 3.9 ミリ秒間隔で変更できます。
- ポートチャネルに storm-control-cpu レートを設定する前に、n9k-arp-acl TCAM リージョンをカービングする必要があります。TCAM リージョン サイズの設定の詳細については、『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』の「*Configuring ACL TCAM Region Sizes*」の章を参照してください。<https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-installation-and-configuration-guides-list.html>

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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 {ethernet slot/port port-channel number} Example:	インターフェイス設定モードを開始します。

	Command or Action	Purpose
	switch# interface ethernet 1/1 switch(config-if)#	
ステップ 3	[no] storm-control {broadcast multicast unicast} level { <level-value %> pps <pps-value > } Example: switch(config-if)# storm-control unicast level 40 Example: switch(config-if)# storm-control broadcast level pps 8000	インターフェイスを通過するトラフィックのトラフィック ストーム制御を設定します。ポート容量または1秒あたりのパケット数の割合として帯域幅レベルを設定することもできます。デフォルトのステートはディセーブルです。
ステップ 4	[no] storm-control action trap Example: switch(config-if)# storm-control action trap	トラフィック ストーム制御の制限に達すると、SNMP トラップ (CISCO-PORT-STORM-CONTROL-MIB で定義) を生成します。
ステップ 5	exit Example: switch(config-if)# exit switch(config)#	インターフェイスコンフィギュレーション モードを終了します。
ステップ 6	(Optional) show running-config interface {ethernet slot/port port-channel number} Example: switch(config)# show running-config interface ethernet 1/1	トラフィック ストーム制御の設定を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

CoPP ポリサーよりもストーム制御ポリサーを優先する

デフォルトでは、ARPブロードキャストなどのレイヤ3制御パケットはストーム制御ポリサーによってドロップされますが、CoPP ポリサーによってポリシングされて CPU に送信されます。これは、制御パケットの場合、ストーム制御ポリサーの優先順位が CoPP ポリサーよりも低いからです。CoPP ポリサー機能よりもストーム ポリサーの優先順位を高くすると、レイヤ3 制御パケットの CoPP ポリサーよりもストーム制御ポリサーの優先順位を高くすることができます。その結果、ARPブロードキャストなどのレイヤ3制御パケットは完全にドロップされます。CoPP ポリサーによってさらにポリシングされるのではなく、ストーム制御ポリサーによってポリシングされます。



- (注) この機能が有効の場合、着信トラフィックが特定のトラフィック タイプ（マルチキャストおよびブロードキャスト）に設定されたしきい値を超えた場合、ストーム制御ポリサは、ドロップされるパケットを制御できなくなる可能性があります。このシナリオでは、その特定のトラフィック タイプ（マルチキャストおよびブロードキャスト）の正規のレイヤ3制御パケットでさえドロップされる可能性があります。

CoPP ポリサよりもストーム制御ポリサを優先するには、次のコマンドを使用します。

[no] system storm-control priority-policy drop-l3

この機能を無効化するには、このコマンドの **no** 形式を使用します。

ツールレベルのしきい値のトラフィック ストーム制御の設定

制御対象のトラフィックがツールレベルしきい値に使用できる、利用可能な合計帯域幅に対するパーセンテージを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	system storm control multi-threshold 例： switch# system storm control multi-threshold	グローバル CLI を入力します。このコマンドはツールレベルしきい値を設定するときにのみ必要です。
ステップ 2	hardware access-list tcam region ing-storm-control 512 例： switch# hardware access-list tcam region ing-storm-control 512	新規 TCAM リージョンは、ツールレベルしきい値向けに固定サイズ 512 でカービングされます。 コマンド実行後、デバイスをリロードしてください。
ステップ 3	configure terminal 例： switch# configure terminal switch(config)#	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	interface {ethernet slot/port port-channel number} 例： switch(config)# interface ethernet 1/1 switch(config-if)#	インターフェイス設定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 5	[no] storm-control multiunicast {level1 <level-value %> level2 <level-value %>} 例 : <pre>switch(config-if)# storm-control multiunicast level1 5 level2 10</pre>	ツールレベルしきい値のインターフェイスを通過するトラフィックのトラフィック ストーム制御を設定します。 ポート容量のパーセンテージとして帯域幅レベルを設定することもできます。デフォルトのステートはディセーブルです。
ステップ 6	[no] storm-control multi action1 {trap shutdown} action2 {trap shutdown} 例 : <pre>switch(config-if)# storm-control multi action1 trap action2 shutdown</pre>	次が生成されます: • SNMP トラップ (CISCO-PORT-STORM-CONTROL-MIB で定義) でストーム制御をモニタします。 • トラフィック ストーム制御が制限に到達すると、シスログ メッセージが生成されます。 ストーム制御しきい値の低/高レベルでトラップおよびシャットダウンアクションを設定することもできます。ただし、ポートの低しきい値 (level1) をシャットダウンに設定する場合、ポートの高しきい値 (level2) にシャットダウンを設定する必要があります。
ステップ 7	exit 例 : <pre>switch(config-if)# exit switch(config)#</pre>	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 8	(任意) show running-config interface {ethernet slot/port port-channel number} 例 : <pre>switch(config)# show running-config interface ethernet 1/1</pre>	トラフィック ストーム制御の設定を表示します。
ステップ 9	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

トラフィック ストーム制御の設定の確認

トラフィック ストーム制御の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config interface	トラフィック ストーム制御の設定を表示します。
show access-list storm-control arp-stats interface [ethernet port-channel] number	インターフェイス上の ARP パケットのストーム制御統計情報を表示します。

トラフィック ストーム制御カウンタのモニタリング

トラフィック ストーム制御動作に関して Cisco NX-OS デバイスが維持するカウンタをモニタリングできます。

コマンド	目的
次の行は、ワンレベルのしきい値にのみ適用されます。	
show interface [ethernet slot/port port-channel number] counters storm-control	トラフィック ストーム制御カウンタを表示します。
次の行は、ツーレベルのしきい値にのみ適用されます。	
show interface [ethernet slot/port port-channel number] counters storm-control multi-threshold	すべてのインターフェイスに設定されたストーム制御値のリストを表示します。
show interface [ethernet slot/port port-channel number] counters storm-control multi-threshold	すべてのインターフェイスに設定されたストーム制御値のリストを表示します。
show interface [ethernet slot/port port-channel number] counters storm-control multi-threshold unicast	level1 と level2 の両方のマルチユニキャストドロップのリストを表示します。
show interface [ethernet slot/port port-channel number] counters storm-control multi-threshold broadcast	level1 と level2 の両方のマルチbroadcastドロップのリストを表示します。
show interface [ethernet slot/port port-channel number] counters storm-control multi-threshold multicast	level1 と level2 の両方のマルチキャストドロップのリストを表示します。

トラフィック ストーム制御の設定例

次に、ワンレベルしきい値のトラフィック ストーム制御の設定例を示します。

```
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# storm-control broadcast level 40
switch(config-if)# storm-control multicast level 40
switch(config-if)# storm-control unicast level 40
```

次に、ツーレベルしきい値のトラフィック ストーム制御の設定例を示します。

```
switch# system storm control multi-threshold
switch# hardware access-list tcam region ing-storm-control 512
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# storm-control multi broadcast level1 5 level2 10
switch(config-if)# storm-control multi multicast level1 5 level2 10
switch(config-if)# storm-control multi unicast level1 5 level2 10
switch(config-if)# storm-control multi action1 trap action2 shutdown
```

次に、プログラムされた設定レートと、ドロップされた ARP パケットの統計情報を確認する例を示します。

```
switch(config)# sh access-list storm-control-cpu arp-stats
interface port-channel 132
slot 1
=====
-----
                        ARP Policer Entry Statistics
-----
Interface port-channel132:
-----
Member Interface    Entry-ID  Rate      RedPacket Count      GreenPacket Count
-----
Ethernet1/35        3976     50         0                     0
-----

slot 7
=====
-----
                        ARP Policer Entry Statistics
-----
Interface port-channel132:
-----
Member Interface    Entry-ID  Rate      RedPacket Count      GreenPacket Count
-----
```

トラフィック ストーム制御のシステム ログの例

次の例は、1レベルのしきい値を持つトラフィックストーム制御のシステムログを示しています。

- %ETHERPORT-5-STORM_CONTROL_ABOVE_THRESHOLD: Traffic in port Ethernet1/5 exceeds the configured threshold , action - Trap

次に、2レベルのしきい値を持つトラフィックストーム制御のシステムログの例を示します。

- %ETHPORT-5-STORM_CONTROL_ABOVE_THRESHOLD: Traffic in port Ethernet1/5 exceeds the configured Broadcast threshold level1[10%], action - Trap
- %ETHPORT-5-STORM_CONTROL_ABOVE_THRESHOLD: Traffic in port Ethernet1/5 exceeds the configured Broadcast threshold level1[15%], action - Shutdown



(注) システムログメッセージには、しきい値を超えた特定のトラフィックタイプと、そのトラフィックタイプがインターフェイスのストーム制御アクションに到達したレベルが含まれます。

トラフィック ストーム制御に関する追加情報

ここでは、トラフィック ストーム制御の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	Cisco NX-OS ライセンス ガイド



第 23 章

ユニキャスト RPF の設定

この章では、Cisco NX-OS デバイスで unicast reverse path forwarding (uRPF) を設定する方法を説明します。

この章は、次の項で構成されています。

- [ユニキャスト RPF について, on page 659](#)
- [ユニキャスト RPF の注意事項と制約事項 \(661 ページ\)](#)
- [ユニキャスト RPF のデフォルト設定, on page 664](#)
- [-R ラインカードを搭載した Cisco Nexus 9500 スイッチのユニキャスト RPF の設定, on page 664](#)
- [Cisco Nexus 9300 スイッチのユニキャスト RPF の設定 \(666 ページ\)](#)
- [ユニキャスト RPF の設定例, on page 668](#)
- [ユニキャスト RPF の設定の確認, on page 669](#)
- [ユニキャスト RPF に関する追加情報, on page 670](#)

ユニキャスト RPF について

ユニキャスト RPF 機能を使用すると、ネットワークに変形または偽造（スプーフィング）された IPv4 または IPv6 ソースアドレスが注入されて引き起こされる問題を、裏付けのない IPv4 または IPv6 パケットを廃棄する方法により緩和します。たとえば、Smurf や Tribal Flood Network (TFN) など、いくつかの一般的なサービス拒絶（DoS）攻撃は、偽造の送信元 IPv4 または IPv6 アドレスやすぐに変更される送信元 IPv4 または IPv6 アドレスを利用して、攻撃を突き止めたりフィルタリングしたりする手段を妨ぐことができます。ユニキャスト RPF では、送信元アドレスが有効で IP ルーティングテーブルと一致するパケットだけを転送することにより、攻撃を回避します。

インターフェイス上でユニキャスト RPF を有効にすると、スイッチはそのインターフェイス上で受信されたすべての入力パケットを検証することにより、送信元アドレスと発信元インターフェイスがルーティングテーブル内に現れ、しかもパケット受信場所のインターフェイスと一致することを確認します。この送信元アドレス検査は転送情報ベース（FIB）に依存しています。



Note ユニキャスト RPF は入力機能であり、接続のアップストリーム エンドにあるスイッチの入力インターフェイスにのみ適用されます。

ユニキャスト RPF は、FIB のリバースルックアップを実行することにより、スイッチインターフェイスでの受信パケットがそのパケットの送信元への最良リターンパス（リターンルート）で着信していることを確認します。パケットが最適なリバースパスルートのいずれかから受信された場合、パケットは通常どおりに転送されます。パケットを受信したインターフェイス上にリバースパスルートがない場合、攻撃者によって送信元アドレスが変更される可能性があります。ユニキャスト RPF がそのパケットのリバースパスを見つけられない場合は、パケットはドロップされます。



Note ユニキャスト RPF では、コストが等しいすべての「最良」リターンパスが有効と見なされます。つまり、複数のリターンパスが存在していても、各パスのルーティングコスト（ホップカウントや重みなど）が他のパスと等しく、そのルートが FIB 内にある限り、ユニキャスト RPF は機能します。ユニキャスト RPF は、Enhanced Interior Gateway Routing Protocol (EIGRP) バリエーションが使用されていて、送信元 IP アドレスに戻る同等でない候補パスが存在する場合にも機能します。

ユニキャスト RPF プロセス

ユニキャスト RPF には、キーの実装原則がいくつかあります。

- パケットは、パケットの送信元に対する最適なリターンパス（ルート）があるインターフェイスで受信される必要があります（このプロセスは対称ルーティングと呼ばれます）。FIB に受信インターフェイスへのルートと一致するルートが存在する必要があります。スタティックルート、ネットワーク文、ダイナミックルーティングによって FIB にルートが追加されます。
- 受信側インターフェイスでの IP 送信元アドレスは、そのインターフェイスのルーティングエントリと一致する必要があります。
- ユニキャスト RPF は入力機能であり、接続のアップストリームエンドのデバイスの入力インターフェイスだけに適用されます。

ダウンストリームネットワークにインターネットへの他の接続があっても、ダウンストリームネットワークにユニキャスト RPF を使用できます。



Caution 攻撃者が送信元アドレスへの最良パスを変更する可能性があるため、加重やローカルプリファレンスなどのオプションの BGP 属性を使用する際には、十分に注意してください。変更によって、ユニキャスト RPF の操作に影響が出ます。

ユニキャスト RPF と ACL を設定したインターフェイスでパケットが受信されると、Cisco NX-OS ソフトウェアは次の動作を行います。

1. インバウンドインターフェイスで入力 ACL をチェックします。
2. ユニキャスト RPF を使用し、FIB テーブル内のリバース ルックアップを実行することにより、そのパケットが送信元への最良リターンパスで着信したことを確認します。
3. パケットの転送を目的として FIB ルックアップを実行します。
4. アウトバウンドインターフェイスで出力 ACL をチェックします。
5. パケットを転送します。

ユニキャスト RPF の注意事項と制約事項

ユニキャスト RPF (uRPF) に関する注意事項と制約事項は次のとおりです。

- uRPF は、次のプラットフォームでサポートされています。
 - N9K-X9636C-R と N9K-X9636Q-R ライン カード搭載の Cisco Nexus 9500 シリーズ スイッチ
 - N9K-X9636C-RX ライン カード搭載の Cisco Nexus 9500 シリーズ スイッチ
 - Cisco Nexus 9300 プラットフォーム スイッチ (9300-FXP スイッチを除く)
- Cisco NX-OS リリース 10.1(2) 以降、uRPF は次でサポートされます。
 - Cisco Nexus 9300-GX/GX2 シリーズ スイッチおよび FX ライン カードを備えた Cisco Nexus 9500 シリーズ スイッチ (IPv4 および IPv6 用)
 - EX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチ (IPv4 専用)
 - vPC をサポートする ToR および EoR スイッチ
- Cisco NX-OS リリース 9.2(1) 以降、uRPF は次でサポートされます。
 - Cisco Nexus 9300-FX/FX2 シリーズ スイッチ (IPv4 および IPv6)
- Cisco NX-OS リリース 9.3(5) 以降、uRPF は Cisco Nexus 9300-FX3 プラットフォーム スイッチ (IPv4 および IPv6) でサポートされます。
- Cisco Nexus リリース 9.3(1) 以降、uRPF はモジュラ EX/FX ライン カード ファミリの Cisco Nexus 9500 シリーズ スイッチでサポートされています (『[Cisco Nexus 9500 Cloud-Scale Line Cards and Fabric Modules Data Sheet](#)』を参照)。



- (注) モジュラ X97160YC-EX、9700-FX ラインカードの uRPF は、DUAL STACK MCAST ルーティングモードでのみサポートされます。
- uRPF をイネーブルにする前に、`system routing template-dual-stack-mcast` の設定を指定します。DUAL STACK MCAST ルーティングモードの設定方法については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
- Cisco NX-OS リリース 10.1(2) 以降、モジュラ X97160YC-EX、9700-FX ラインカードの uRPF はデフォルトルーティングモードでもサポートされます。

- uRPF は、ネットワーク内のより大きな部分からのダウンストリームのインターフェイスで適用する必要があります（ネットワークのエッジに適用するのが望ましい）。
- なるべくダウンストリームで uRPF を適用する方が、アドレススプーフィングの軽減やスプーフされたアドレスの送信元の特定の精度が高くなります。たとえば、集約デバイスで uRPF を適用すると、多くのダウンストリーム ネットワークまたはクライアントからの攻撃を軽減できるとともに、管理が簡単になりますが、攻撃の送信元は特定できません。ネットワーク アクセス サーバに uRPF を適用すると、攻撃の範囲を絞り、攻撃元を追跡しやすくなります。ただし、多数のサイトにユニキャスト RPF を展開すると、ネットワーク運用の管理コストが増加します。
- インターネット、イントラネット、およびエクストラネットのリソースにわたって uRPF を展開するエンティティ数が増えるほど、インターネットコミュニティ全体の大規模なネットワークの中断を軽減できる可能性と、攻撃元を追跡できる可能性が高くなります。
- uRPF は、総称ルーティング カプセル化（GRE）トンネルのようなトンネルでカプセル化された IP パケットは検査しません。トンネリングとカプセル化のレイヤがパケットから除かれてから uRPF がネットワーク トラフィックを処理するように、ホーム ゲートウェイに uRPF を設定する必要があります。
- uRPF は、ネットワークからのアクセス ポイントが 1 つだけ、またはアップストリーム接続が 1 つだけの「単一ホーム」環境で使用できます。アクセス ポイントが 1 つのネットワークは対称ルーティングを提供します。これはつまり、パケットがネットワークに入るインターフェイスはその IP パケットの送信元への最良のリターンパスでもあるということです。
- uRPF は、ネットワーク内部のインターフェイスに使用しないでください。内部インターフェイスは、ルーティングを非対称にする可能性が高く、パケットの送信元へのルートが複数存在する場合があります。uRPF を設定するのは、元々対称であるか、対称に設定されている場合だけにしてください。
- uRPF を使用すると、送信元が 0.0.0.0 で宛先が 255.255.255.255 のパケットを通過させて、ブートストラップ プロトコル（BOOTP）と Dynamic Host Configuration Protocol（DHCP）を正しく動作させることができます。

- uRPF が有効な場合、スイッチがインストールできる null0 へのスタティック ルートの量は、「show hardware internal forwarding table utilization」の「Max V4 Ucast DA TCAM table entries」の値に制限されます。
- Cisco NX-OS リリース 9.2(1) 以降、N9K-X9636C-R および N9K-X96136YC-R スイッチでは、使用可能な IPv4 および IPv6 ユニキャスト RPF コマンドのバージョンは 1 つだけです。ただし、これにより、IPv4 と IPv6 の両方でユニキャスト RPF が有効になります。
- 次のガイドラインと制限は、N9K-X9636C-R、N9K-X9636C-RX、または N9K-X9636Q-R ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチにのみ適用されます。
 - 厳密な uRPF を機能させるには、入力インターフェイスと送信元 IP アドレスが学習されたインターフェイスで有効にします。
 - スイッチ ハードウェアは、設定されたルーティング インターフェイスごとに厳密な uRPF を実装しません。
 - 厳密な uRPF は、厳密な uRPF 対応インターフェイスの学習ルートごとに実装されます。
 - ルートが ECMP として解決されると、strict uRPF はルーズモードにフォールバックします。
 - トラップ解決に関するハードウェアの制限により、uRPF はインバンド経由でスーパーバイザ宛パケットに適用されない場合があります。
 - IP トラフィックの場合は、IPv4 と IPv6 の設定を同時に有効にします。
 - ハードウェアの制限により、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ラインカードは次の組み合わせのみをサポートします。

uRPF の設定		送信元 IP アドレスのトラフィックチェックの適用			
IPv4	IPv6	IP Unipath	IP ECMP	MPLS EncapVPN/ECMP	N9K-X9636C-RX ラインカードの Unipath MPLS VPN
無効	無効	許可	許可	許可	許可
Loose	Loose	uRPF loose	uRPF loose	uRPF loose	uRPF strict
Strict	Strict	uRPF strict	uRPF loose	uRPF loose	uRPF strict

- Strict uRPF は、次のプラットフォームの VxLAN 経由でインターフェイスに送信される ICMP トラフィックをブロックします。
 - Cisco Nexus 9300--FX/GX プラットフォーム スイッチ
 - N9K-X97160YC-EX および N9K-X9700-FX ラインカードを搭載した Nexus 9500 スイッチ

- Strict uRPF が構成されている場合は、サブネットの背後にある未解決のホストに対して `urpf strict` モードが機能するように、次のコマンドを追加します。
 - **`no system multicast dcs-check`**
 - **`hardware profile multicast max-limit lpm-entries 0`**
- Cisco NX-OS リリース 10.5(2)F 以降、uRPF は Cisco Nexus 9800 シリーズ スイッチでサポートされますが、次の制限があります。
 - ルートが ECMP として解決されると、strict uRPF はルーズモードにフォールバックします。
 - uRPF ルーズモードでは、**`allow-default`** キーワードはサポートされません。
 - IPv4 と IPv6 の個別の uRPF 制御はありません。コマンドを使用して uRPF 機能を構成すると、IPv4 と IPv6 の両方のパケットに対して同時に有効になります。
 - uRPF 構成は、トンネル インターフェイスではサポートされていません。
 - uRPF 厳格モード構成は、L3 ポート チャネルと L3 ポート チャネル サブインターフェイスではサポートされません。

ユニキャスト RPF のデフォルト設定

次の表に、ユニキャスト RPF パラメータのデフォルト設定を示します。

Table 38: ユニキャスト RPF パラメータのデフォルト設定

パラメータ	デフォルト
ユニキャスト RPF	無効化

-R ラインカードを搭載した Cisco Nexus 9500 スイッチのユニキャスト RPF の設定

-R ラインカードを使用して Cisco Nexus 9500 シリーズ スイッチの入力インターフェイスにユニキャスト RPF を設定できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interface ethernet slot/port Example: switch(config)# interface ethernet 2/3 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	{ip ipv6} address ip-address/length Example: switch(config-if)# ip address 172.23.231.240/23	インターフェイスの IPv4 または IPv6 アドレスを指定します。
ステップ 4	{ip ipv6} verify unicast source reachable-via any Example: switch(config-if)# ip verify unicast source reachable-via any	IPv4 と IPv6 の両方に対するインターフェイスでユニキャスト RPF を設定します。 Note IPv4 または IPv6 の uRPF をイネーブルにすると (ip または ipv6 キーワードを使用)、uRPF は IPv4 と IPv6 の両方でイネーブルになります。
ステップ 5	(Optional) show ip interface ethernet slot/port Example: switch(config)# show ip interface ethernet 2/3	インターフェイスの IP 情報を表示します。
ステップ 6	(Optional) show running-config interface ethernet slot/port Example: switch(config)# show running-config interface ethernet 2/3	実行コンフィギュレーション内のインターフェイスの情報を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco Nexus 9300 スイッチのユニキャスト RPF の設定

Cisco NX-OS リリース 9.2(1) 以降のリリースを実行する Cisco Nexus 9300 プラットフォーム スイッチ（9300-FXP スイッチを除く）の入力インターフェイスで、次のいずれかのユニキャスト RPF モードを設定できます。

ストリクト ユニキャスト RPF モード

厳格モードでは、ユニキャスト RPF が FIB で一致するパケット送信元アドレスを見つけて、パケットを受信した入力インターフェイスが FIB 内のユニキャスト RPF インターフェイスのいずれかと一致した場合に、チェックに合格します。チェックに合格しないと、パケットは廃棄されます。このタイプのユニキャスト RPF チェックは、パケットフローが対称であると予想される場合に使用できます。

ルーズ ユニキャスト RPF モード

緩和モードでは、FIB でのパケット送信元アドレスのルックアップで一致が戻り、FIB の結果からその送信元が少なくとも 1 つの実インターフェイスで到達可能であることが示された場合に、チェックに合格します。パケットを受信した入力インターフェイスが FIB 内のインターフェイスのいずれかと一致する必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] system urpf disable 例： switch(config)# no system urpf disable	スイッチでユニキャスト RPF を有効にします。 (注) ユニキャスト RPF 設定を適用するには、Cisco NX-OS ボックスをリロードする必要があります。
ステップ 3	interface ethernet slot/port 例： switch(config)# interface ethernet 2/3 switch(config-if)#	イーサネット 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	{ip ipv6} address ip-address/length 例： switch(config-if)# ip address 172.23.231.240/23	インターフェイスの IPv4 または IPv6 アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 5	{ip ipv6} verify unicast source reachable-via {any [allow-default] rx} 例 : <pre>switch(config-if)# ip verify unicast source reachable-via any</pre>	IPv4 および IPv6 用インターフェイスにユニキャスト RPF を設定します。 Cisco Nexus 9300-FX/FX2 シリーズ スイッチでは、IPv4 および IPv6 uRPF を個別に有効にできます。 (注) IPv4 または IPv6 のユニキャスト RPF を有効にすると (ip または ipv6 キーワードを使用)、ユニキャスト RPF は IPv4 と IPv6 の両方で有効になります。 インターフェイスで使用する IPv4 および IPv6 ユニキャスト RPF コマンドのバージョンは1つだけです。1つのバージョンを設定する場合、すべてのモード変更はこのバージョンで行う必要があります、他のすべてのバージョンはそのインターフェイスによってブロックされます。 • any キーワードは緩和モードのユニキャスト RPF を指定します。 • allow-default キーワードを指定すると、送信元アドレスのルックアップでデフォルト ルートと一致させることが可能であり、これを検証に使用できます。 (注) allow-default キーワードは、ALPM ルーティング モードでは適用されません。 (注) allow-default キーワードを指定しない場合、送信元アドレス ルックアップ (ルーズなユニキャスト RPF チェックの場合) はデフォルト ルートと一致しません。 • rx キーワードは厳格モードのユニキャスト RPF を指定します。

	コマンドまたはアクション	目的
ステップ 6	exit 例 : <pre>switch(config-if)# exit switch(config)#</pre>	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	(任意) show ip interface ethernet slot/port 例 : <pre>switch(config)# show ip interface ethernet 1/54 grep -i "unicast reverse path forwarding" IP unicast reverse path forwarding: none</pre>	インターフェイスの IP 情報を表示し、ユニキャスト RPF が有効かどうかを確認します。
ステップ 8	(任意) show running-config interface ethernet slot/port 例 : <pre>switch(config)# show running-config interface ethernet 2/3</pre>	実行コンフィギュレーション内のインターフェイスの情報を表示します。
ステップ 9	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ユニキャスト RPF の設定例

次に、-R ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチで IPv4 パケットの loose ユニキャスト RPF を設定する例を示します。

```
interface Ethernet2/3
 ip address 172.23.231.240/23
 ip verify unicast source reachable-via any
```

次に、-R ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチで IPv6 パケットの loose ユニキャスト RPF を設定する例を示します。

```
interface Ethernet2/1
 ipv6 address 2001:0DB8:c18:1::3/64
 ipv6 verify unicast source reachable-via any
```

次に、Cisco Nexus 9300 プラットフォーム スイッチで IPv4 パケットの loose ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/3
 ip address 172.23.231.240/23
```

```
ip verify unicast source reachable-via any
```

次に、Cisco Nexus 9300 プラットフォーム スイッチで IPv6 パケットの loose ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/1
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via any
```

次に、Cisco Nexus 9300 プラットフォーム スイッチで IPv4 パケットの strict ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/2
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via rx
```

次に、Cisco Nexus 9300 プラットフォーム スイッチで IPv6 パケットの strict ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/4
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via rx
```

ユニキャスト RPF の設定の確認

ユニキャスト RPF の設定情報を表示するには、次のいずれかの操作を行います。

コマンド	目的
show running-config interface ethernet slot/port	実行コンフィギュレーション内のインターフェイスの設定を表示します。
show running-config ip [all]	実行コンフィギュレーション内の IPv4 設定を表示します。
show running-config ipv6 [all]	実行コンフィギュレーション内の IPv6 設定を表示します。
show startup-config interface ethernet slot/port	スタートアップ コンフィギュレーション内のインターフェイスの設定を表示します。
show startup-config ip	スタートアップ コンフィギュレーション内の IP 設定を表示します。

ユニキャスト RPF に関する追加情報

ここでは、ユニキャスト RPF の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
データ管理エンジン (DME) コマンド	Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference (Cisco Nexus 3000 および 9000 シリーズ NX-API REST SDK ユーザ ガイドと API リファレンス)
MPLS VPN	Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング コンフィギュレーション ガイド (Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide)



第 24 章

スイッチポート ブロッキングの設定

この章では、Cisco NX-OS デバイス上でスイッチポート ブロッキングを設定する方法について説明します。

この章は、次の項で構成されています。

- [スイッチポート ブロッキングについて \(671 ページ\)](#)
- [スイッチポート ブロッキングの注意事項および制約事項 \(671 ページ\)](#)
- [スイッチポート ブロッキングのデフォルト設定 \(672 ページ\)](#)
- [スイッチポート ブロッキングの設定 \(672 ページ\)](#)
- [スイッチポート ブロッキング設定の確認 \(673 ページ\)](#)
- [スイッチポート ブロッキングの設定例 \(673 ページ\)](#)

スイッチポート ブロッキングについて

MAC アドレスが期限切れになるか、スイッチによって学習されなかったために、不明のマルチキャストまたはユニキャストトラフィックがスイッチポートにフラッドिंगすることがあります。不明なマルチキャストおよびユニキャストトラフィックがスイッチポートに転送されると、セキュリティ問題が発生する可能性があります。スイッチポート ブロッキングをイネーブルにすると、マルチキャストまたはユニキャストトラフィックのポートへのフラッドिंगを防止できます。

スイッチポート ブロッキングの注意事項および制約事項

スイッチポート ブロッキング設定時の注意事項および制約事項は次のとおりです。

- トラフィック ストーム制御が適用されるのは入力ポートだけであるのに対して、スイッチポート ブロッキングが適用されるのは出力ポートだけです。
- スwitchポート ブロッキングは、すべてのスイッチドポート（PVLAN ポートを含む）でサポートされ、ポートが転送するすべての VLAN に適用されます。
- スwitchポート ブロッキングは FEX ポートではサポートされません。

- ポート チャンネルの不明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 チャンネル グループのすべてのポートでブロックされます。
- スイッチポートブロッキングには制御のレベルは用意されていません。指定されたポートにおける未知の出力マルチキャストまたはユニキャストパケットのフラッディングをすべて防止します。
- スイッチポートブロッキングは、Cisco Nexus 9500 シリーズ スイッチの CPU を発信元とする制御パケットをドロップします。Cisco Nexus 9300 シリーズ スイッチのパケットはドロップしません。

スイッチポート ブロッキングのデフォルト設定

次の表に、スイッチポートブロッキングパラメータのデフォルト設定を示します。

表 39: スイッチポートブロッキングパラメータのデフォルト値

パラメータ	デフォルト
スイッチポートブロッキング	無効化

スイッチポート ブロッキングの設定

デフォルトでは、スイッチは不明の宛先 MAC アドレスを持つパケットをすべてのポートにフラッディングします。それらのトラフィックの転送を防止するには、未知のマルチキャストまたはユニキャストパケットをブロックするポートを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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 {ethernet slot/port port-channel number} 例 : switch# interface ethernet 1/1 switch(config-if)#	インターフェイス設定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] switchport block {multicast unicast} 例 : <pre>switch(config-if)# switchport block unicast</pre>	指定されたポートにおける未知のマルチキャストまたはユニキャストパケットのフラディングを防止します。 ポートで通常の転送を再開するには、このコマンドのno形式を使用します。
ステップ 4	(任意) show interface [ethernet slot/port port-channel number] switchport 例 : <pre>switch(config-if)# show interface ethernet 1/1 switchport</pre>	スイッチポートブロッキング設定を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

スイッチポート ブロッキング設定の確認

スイッチポートブロッキング設定情報を表示するには、次のタスクのいずれかを行います。

コマンド	目的
show interface switchport	すべてのインターフェイスのスイッチポートブロッキング設定を表示します。
show interface {ethernet slot/port port-channel number} switchport	指定したインターフェイスのスイッチポートブロッキング設定を表示します。
show running-config interface [ethernet slot/port port-channel number]	実行コンフィギュレーションのスイッチポートブロッキングコンフィギュレーションを表示します。

スイッチポート ブロッキングの設定例

次に、イーサネットインターフェイス 1/2 上でマルチキャストおよびユニキャストフラディングをブロックし、設定を確認する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# switchport block multicast
switch(config-if)# switchport block unicast
switch(config-if)# show running-config interface ethernet 1/2
!Command: show running-config interface Ethernet1/2
!Time: Wed Apr 15 16:25:48 2015

version 79.2(1)

interface Ethernet1/2
switchport
switchport block multicast
switchport block unicast
```




第 25 章

コントロールプレーンポリシングの設定

この章では、Cisco NX-OS デバイスでコントロールプレーンポリシング (CoPP) を構成する方法について説明します。

- [CoPP について, on page 675](#)
- [CoPP の注意事項と制約事項 \(689 ページ\)](#)
- [CoPP のデフォルト設定, on page 695](#)
- [CoPP の設定, on page 695](#)
- [出力 CoPP のプロトコル ACL フィルタリング \(703 ページ\)](#)
- [CoPP の設定の確認, on page 708](#)
- [CoPP 設定ステータスの表示, on page 711](#)
- [CoPP のモニタリング, on page 712](#)
- [SNMP での CoPP のモニタリング \(713 ページ\)](#)
- [CoPP 統計情報のクリア, on page 713](#)
- [CoPP の設定例, on page 714](#)
- [CoPP に関する追加情報, on page 717](#)

CoPP について

コントロールプレーンポリシング (CoPP) はコントロールプレーンを保護し、それをデータプレーンから分離することによって、ネットワークの安定性、到達可能性、およびパケット配信を保証します。

この機能により、コントロールプレーンにポリシーマップを適用できるようになります。このポリシーマップは、通常の QoS ポリシーに似ており、非管理ポートからスイッチに入るすべてのトラフィックに適用されます。ネットワークデバイスへの一般的な攻撃ベクトルは、過剰なトラフィックがデバイスインターフェイスに転送されるサービス妨害 (DoS) 攻撃です。

Cisco NX-OS デバイスは、DoS 攻撃がパフォーマンスに影響しないようにするために CoPP を提供します。このような攻撃は誤って、または悪意を持って実行される場合があり、通常は、スーパーバイザモジュールまたは CPU 自体に宛てられた大量のトラフィックが含まれます。

スーパーバイザモジュールは、管理対象のトラフィックを次の3つの機能コンポーネント (プレーン) に分類します。

データプレーン

すべてのデータトラフィックを処理します。Cisco NX-OS デバイスの基本的な機能は、インターフェイス間でパケットを転送することです。スイッチ自身に向けられたものでないパケットは、中継パケットと呼ばれます。データプレーンで処理されるのはこれらのパケットです。

コントロールプレーン

ルーティングプロトコルのすべての制御トラフィックを処理します。ボーダーゲートウェイプロトコル（BGP）や Open Shortest Path First（OSPF）プロトコルなどのルーティングプロトコルは、デバイス間で制御パケットを送信します。これらのパケットはルータのアドレスを宛先とし、コントロールプレーンパケットと呼ばれます。

管理プレーン

コマンドラインインターフェイス（CLI）や簡易ネットワーク管理プロトコル（SNMP）など、Cisco NX-OS デバイスを管理する目的のコンポーネントを実行します。

スーパーバイザモジュールには、管理プレーンとコントロールプレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。スーパーバイザモジュールの動作が途絶したり、スーパーバイザモジュールが攻撃されたりすると、重大なネットワークの停止につながります。たとえば、スーパーバイザに過剰なトラフィックが加わると、スーパーバイザモジュールが過負荷になり、Cisco NX-OS デバイス全体のパフォーマンスが低下する可能性があります。たとえば、スーパーバイザモジュールに対する DoS 攻撃は、コントロールプレーンに対して非常に高速に IP トラフィックストリームを生成することがあります。これにより、コントロールプレーンは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

DoS 攻撃の例は次のとおりです。

- インターネット制御メッセージプロトコル（ICMP）エコー要求
- IP フラグメント
- TCP SYN フラッディング

これらの攻撃によりデバイスのパフォーマンスが影響を受け、次のようなマイナスの結果をもたらします。

- サービス品質の低下（音声、ビデオ、または重要なアプリケーショントラフィックの低下など）
- ルートプロセッサまたはスイッチプロセッサの高い CPU 使用率
- ルーティングプロトコルのアップデートまたはキープアライブの消失によるルートフラップ
- 不安定なレイヤ 2 トポロジ
- CLI との低速な、または応答を返さない対話型セッション
- メモリやバッファなどのプロセッサリソースの枯渇
- 着信パケットの無差別のドロップ

**Caution**

コントロールプレーンの保護策を講じることで、スーパーバイザ モジュールを偶発的な攻撃や悪意ある攻撃から確実に保護することが重要です。

コントロールプレーン保護

コントロールプレーンを保護するため、Cisco NX-OS デバイスはコントロールプレーンに向かうさまざまなパケットを異なるクラスに分離します。クラスの識別が終わると、Cisco NX-OS デバイスはパケットをポリシングします。これにより、スーパーバイザモジュールに過剰な負担がかからないようになります。

コントロールプレーンのパケット タイプ

コントロールプレーンには、次のような異なるタイプのパケットが到達します。

受信パケット

ルータの宛先アドレスを持つパケット。宛先アドレスには、レイヤ 2 アドレス（ルータ MAC アドレスなど）やレイヤ 3 アドレス（ルータ インターフェイスの IP アドレスなど）があります。これらのパケットには、ルータ アップデートとキープアライブ メッセージも含まれます。ルータが使用するマルチキャストアドレス宛てに送信されるマルチキャストパケットも、このカテゴリに入ります。

例外パケット

スーパーバイザモジュールによる特殊な処理を必要とするパケット。たとえば、宛先アドレスが Forwarding Information Base（FIB; 転送情報ベース）に存在せず、結果としてミスとなった場合は、スーパーバイザモジュールが送信側に到達不能パケットを返します。他には、IP オプションがセットされたパケットもあります。

次の例外は、ラインカードからのみ発生する可能性があります。

- match exception ip option
- match exception ipv6 option
- match exception ttl-failure

次の例外は、ファブリック モジュールからのみ発生する可能性があります。

- match exception ipv6 icmp unreachable
- match exception ip icmp unreachable

次の例外は、ラインカードとファブリック モジュールから発生する可能性があります。

- match exception mtu-failure

リダイレクトパケット

スーパーバイザ モジュールにリダイレクトされるパケット。

収集パケット

宛先 IP アドレスのレイヤ 2 MAC アドレスが FIB に存在していない場合は、スーパーバイザ モジュールがパケットを受信し、ARP 要求をそのホストに送信します。

これらのさまざまなパケットは、コントロールプレーンへの悪意ある攻撃に利用され、Cisco NX-OS デバイスに過剰な負荷をかける可能性があります。CoPP は、これらのパケットを異なるクラスに分類し、これらのパケットをスーパーバイザが受信する速度を個別に制御するメカニズムを提供します。

CoPP の分類

効果的に保護するために、Cisco NX-OS デバイスはスーパーバイザ モジュールに到達するパケットを分類して、パケットタイプに基づいた異なるレート制御ポリシーを適用できるようにします。たとえば、Hello メッセージなどのプロトコルパケットには厳格さを緩め、IP オプションがセットされているためにスーパーバイザモジュールに送信されるパケットには厳格さを強めることが考えられます。クラスマップとポリシー マップを使用して、パケットの分類およびレート制御ポリシーを設定します。

出力 CoPP

Cisco NX-OS リリース 10.2(3)F 以降、出力 CoPP は Nexus 93180YC-FX、Nexus 93240YC-FX2、Nexus 93360YC-FX2、Nexus 9336C-FX2、Nexus 9336C-FX2-E、Nexus 93180YC-FX3、N9K-C9316D-GX、N9K-C93600CD-GX、Nexus 9364C-GX、N9K-C9332D-GX2B クラウドスケール スイッチでサポートされます。

出力 CoPP は、カスタム/デフォルトの CoPP ポリシーに加えて適用できます。

レート制御メカニズム

パケットの分類が終わると、Cisco NX-OS デバイスにはスーパーバイザモジュールに到達するパケットのレートを制御するメカニズムがあります。スーパーバイザモジュールへのトラフィックのレート制御には 2 つのメカニズムを使用します。1 つはポリシング、もう 1 つはレート制限と呼ばれるものです。

ハードウェアポリサーを使用すると、トラフィックが所定の条件に一致する場合、または違反する場合について異なるアクションを定義できます。このアクションには、パケットの送信、パケットのマーク付け、およびパケットのドロップがあります。

ポリシングには、次のパラメータを設定できます。

認定情報レート (CIR)

望ましい帯域幅を、ビット レート、またはリンク レートの割合として指定します。

認定バースト (BC)

指定した時間枠内に CIR を超過する可能性があるが、スケジューリングには影響を与えないトラフィック バーストのサイズ。

さらに、一致トラフィックおよび違反トラフィックに対して、送信またはドロップなどの異なるアクションを設定できます。

ポリシング パラメータの詳細については、『Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide』を参照してください。

ダイナミックおよびスタティック CoPP ACL

CoPP アクセスコントロールリスト (ACL) は、ダイナミックまたはスタティックに分類されます。Cisco Nexus 9300 および 9500 シリーズ スイッチは、ダイナミック CoPP ACL のみを使用します。

ダイナミック CoPP ACL は、転送情報ベース (FIB) ベースのスーパーバイザリダイレクトパケットに対してのみ機能し、スタティック CoPP ACL は ACL ベースのスーパーバイザリダイレクトパケットに対してのみ機能します。ダイナミック CoPP ACL は myIP およびリンク ローカル マルチキャスト トラフィックでサポートされ、スタティック CoPP ACL は他のすべてのタイプのトラフィックでサポートされます。

スタティック CoPP ACL は、サブストリングによって識別されます。これらのサブストリングのいずれかを持つ ACL は、スタティック CoPP ACL として分類されます。

- MAC ベースのスタティック CoPP ACL サブストリング :
 - acl-mac-cdp-udld-vtp
 - acl-mac-cfsoc
 - acl-mac-dot1x
 - acl-mac-l2-tunnel
 - acl-mac-l3-isis
 - acl-mac-lacp
 - acl-mac-lldp
 - acl-mac-sdp-srp
 - acl-mac-stp
 - acl-mac-undesirable
- プロトコルベースのスタティック CoPP ACL サブストリング :
 - acl-dhcp
 - acl-dhcp-relay-response
 - acl-dhcp6
 - acl-dhcp6-relay-response
 - acl-ptp
- マルチキャストベースのスタティック CoPP ACL サブストリング :
 - acl-igmp

スタティック CoPP ACL の詳細については、を参照してください。[CoPP の注意事項と制約事項 \(689 ページ\)](#)

デフォルトのポリシングポリシー

Cisco NX-OS デバイスの初回起動時に、DoS 攻撃からスーパーバイザ モジュールを保護するためのデフォルトの `copp-system-p-policy-strict` ポリシーが Cisco NX-OS ソフトウェアによりインストールされます。最初のセットアップ ユーティリティで、次のいずれかの CoPP ポリシー オプションを選択することにより、保護レベルを設定できます。

- **Strict** : このポリシーは 1 レート、2 カラーです。
- **Moderate** : このポリシーは 1 レート、2 カラーです。重要クラスのバーストサイズは `strict` ポリシーより大きく、`lenient` ポリシーより小さくなります。
- **Lenient** : このポリシーは 1 レート、2 カラーです。重要クラスのバーストサイズは `moderate` ポリシーより大きく、`dense` ポリシーより小さくなります。
- **Dense** : このポリシーは 1 レート、2 カラーです。ポリサーの CIR 値は、`strict` ポリシーよりも低くなります。
- **Skip** : コントロールプレーン ポリシーは適用されません。（ネットワークのコントロールプレーンに影響するため、Skip オプションの使用は推奨されません）。

オプションを選択しなかった場合や、セットアップ ユーティリティを実行しなかった場合には、`strict` ポリシングが適用されます。`strict` ポリシーから開始し、必要に応じて、CoPP ポリシーを変更することを推奨します。



Note POAP を使用する場合、デフォルトでは厳格なポリシングは適用されないため、CoPP ポリシーを設定する必要があります。

`copp-system-p-policy` ポリシーには、基本的なデバイス操作に最も適した値が設定されています。使用する DoS に対する保護要件に適合するよう、特定のクラスやアクセス コントロール リスト (ACL) を追加する必要があります。デフォルト CoPP ポリシーは、ソフトウェアをアップグレードしても変更されません。



Caution `skip` オプションを選択し、その後に CoPP 保護を設定していない場合、Cisco NX-OS デバイスは DoS 攻撃に対して脆弱な状態になります。

CLI プロンプトから **setup** コマンドを実行して再度セットアップ ユーティリティを起動するか、または **copp profile** コマンドを使用して、CoPP のデフォルト ポリシーを再割り当てできます。

Related Topics

[デフォルトの CoPP ポリシーの変更または再適用](#) (702 ページ)

デフォルト クラス マップ

`copp-system-class-critical` クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-critical
  match access-group name copp-system-p-acl-bgp
  match access-group name copp-system-p-acl-rip
  match access-group name copp-system-p-acl-vpc
  match access-group name copp-system-p-acl-bgp6
  match access-group name copp-system-p-acl-ospf
  match access-group name copp-system-p-acl-rip6
  match access-group name copp-system-p-acl-eigrp
  match access-group name copp-system-p-acl-ospf6
  match access-group name copp-system-p-acl-eigrp6
  match access-group name copp-system-p-acl-auto-rp
  match access-group name copp-system-p-acl-mac-l3-isis
```

copp-system-class-exception クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-exception
  match exception ip option
  match exception ip icmp unreachable
  match exception ipv6 option
  match exception ipv6 icmp unreachable
```

copp-system-class-exception-diag クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-exception-diag
  match exception ttl-failure
  match exception mtu-failure
```

copp-system-class-important クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-important
  match access-group name copp-system-p-acl-hsrp
  match access-group name copp-system-p-acl-vrrp
  match access-group name copp-system-p-acl-hsrp6
  match access-group name copp-system-p-acl-vrrp6
  match access-group name copp-system-p-acl-mac-lldp
```

copp-system-class-l2-default クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l2-default
  match access-group name copp-system-p-acl-mac-undesirable
```

copp-system-class-l2-unpoliced クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l2-unpoliced
  match access-group name copp-system-p-acl-mac-stp
  match access-group name copp-system-p-acl-mac-lacp
  match access-group name copp-system-p-acl-mac-cfsoe
  match access-group name copp-system-p-acl-mac-sdp-srp
  match access-group name copp-system-p-acl-mac-l2-tunnel
  match access-group name copp-system-p-acl-mac-cdp-udld-vtp
```

copp-system-class-l3mc-data クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l3mc-data
  match exception multicast rpf-failure
  match exception multicast dest-miss
```

copp-system-class-l3uc-data クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l3uc-data
  match exception glean
```

copp-system-class-management クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-management
  match access-group name copp-system-p-acl-ftp
  match access-group name copp-system-p-acl-ntp
  match access-group name copp-system-p-acl-ssh
  match access-group name copp-system-p-acl-http
  match access-group name copp-system-p-acl-ntp6
  match access-group name copp-system-p-acl-sftp
  match access-group name copp-system-p-acl-snmp
  match access-group name copp-system-p-acl-ssh6
  match access-group name copp-system-p-acl-tftp
  match access-group name copp-system-p-acl-https
  match access-group name copp-system-p-acl-snmp6
  match access-group name copp-system-p-acl-tftp6
  match access-group name copp-system-p-acl-radius
  match access-group name copp-system-p-acl-tacacs
  match access-group name copp-system-p-acl-telnet
  match access-group name copp-system-p-acl-radius6
  match access-group name copp-system-p-acl-tacacs6
  match access-group name copp-system-p-acl-telnet6
```

copp-system-class-monitoring クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-monitoring
  match access-group name copp-system-p-acl-icmp
  match access-group name copp-system-p-acl-icmp6
  match access-group name copp-system-p-acl-traceroute
```

copp-system-class-multicast-host クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-multicast-host
  match access-group name copp-system-p-acl-mld
```

copp-system-class-multicast-router クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-multicast-router
  match access-group name copp-system-p-acl-pim
  match access-group name copp-system-p-acl-msdp
  match access-group name copp-system-p-acl-pim6
  match access-group name copp-system-p-acl-pim-reg
  match access-group name copp-system-p-acl-pim6-reg
  match access-group name copp-system-p-acl-pim-mdt-join
```

copp-system-class-nat-flow クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-nat-flow
  match exception nat-flow
```

copp-system-class-ndp クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-ndp
  match access-group name copp-system-p-acl-ndp
```

copp-system-class-normal クラスの設定は次のとおりです。


```
class-map type control-plane match-any copp-system-p-class-normal
  match access-group name copp-system-p-acl-mac-dot1x
  match protocol arp
```

copp-system-class-normal-dhcp クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-normal-dhcp
  match access-group name copp-system-p-acl-dhcp
  match access-group name copp-system-p-acl-dhcp6
```

copp-system-class-normal-dhcp-relay-response クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-normal-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp6-relay-response
```

copp-system-class-normal-igmp クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-normal-igmp
  match access-group name copp-system-p-acl-igmp
```

copp-system-class-redirect クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-redirect
  match access-group name copp-system-p-acl-ntp
```

copp-system-class-undesirable クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-undesirable
  match access-group name copp-system-p-acl-undesirable
  match exception multicast sg-rpf-failure
```

copp-system-class-fcoe クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-fcoe
  match access-group name copp-system-p-acl-mac-fcoe
```

strict デフォルト CoPP ポリシー

Cisco Nexus 9300 と 9500 シリーズスイッチの場合、strict CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-strict
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 3000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
```

moderate デフォルト CoPP ポリシー

```

set cos 1
  police cir 2000 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l3mc-data
  set cos 1
  police cir 3000 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal
  set cos 1
  police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-ndp
  set cos 6
  police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 300 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 400 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 6000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 300 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-fcoe
  set cos 6
  police cir 1500 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-nat-flow
  set cos 7
  police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 50 pps bc 32 packets conform transmit violate drop
class class-default
  set cos 0
  police cir 50 pps bc 32 packets conform transmit violate drop

```

moderate デフォルト CoPP ポリシー

Cisco Nexus 9300 と 9500 シリーズ スイッチの場合、moderate CoPP ポリシーの設定は次のとおりです。

```

policy-map type control-plane copp-system-p-policy-moderate
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 192 packets conform transmit violate drop

```

```

class copp-system-p-class-important
  set cos 6
  police cir 3000 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-multicast-router
  set cos 6
  police cir 3000 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-management
  set cos 2
  police cir 3000 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-multicast-host
  set cos 1
  police cir 2000 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-l3mc-data
  set cos 1
  police cir 3000 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal
  set cos 1
  police cir 1500 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-ndp
  set cos 6
  police cir 1500 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 300 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 400 pps bc 96 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 6000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 1500 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 50 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 50 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 300 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-fcoe
  set cos 6
  police cir 1500 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-nat-flow
  set cos 7
  police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 50 pps bc 48 packets conform transmit violate drop
class class-default
  set cos 0
  police cir 50 pps bc 48 packets conform transmit violate drop

```

lenient デフォルト CoPP ポリシー

Cisco Nexus 9300 と 9500 シリーズ スイッチの場合、lenient CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-lenient
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 3000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 3000 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 2000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1500 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1500 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 300 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 400 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 6000 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 50 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 300 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 20000 pps bc 8192 packets conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 15 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 1500 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-nat-flow
```

```

set cos 7
police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
set cos 0
police cir 50 pps bc 64 packets conform transmit violate drop
class class-default
set cos 0
police cir 50 pps bc 64 packets conform transmit violate drop

```

デンス デフォルト CoPP ポリシー

Cisco Nexus 9300 と 9500 シリーズ スイッチの場合、dense CoPP ポリシーの設定は次のとおりです。

```

policy-map type control-plane copp-system-p-policy-dense
class copp-system-p-class-l3uc-data
set cos 1
police cir 250 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-critical
set cos 7
police cir 2500 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-important
set cos 6
police cir 1200 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-multicast-router
set cos 6
police cir 1200 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-management
set cos 2
police cir 1200 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-multicast-host
set cos 2
police cir 1000 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l3mc-data
set cos 1
police cir 1200 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal
set cos 1
police cir 750 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-ndp
set cos 1
police cir 750 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
set cos 1
police cir 150 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
set cos 1
police cir 200 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
set cos 3
police cir 2500 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-redirect
set cos 1
police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception
set cos 1
police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception-diag
set cos 1
police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-monitoring
set cos 1
police cir 50 pps bc 128 packets conform transmit violate drop

```

```

class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-fcoe
  set cos 6
  police cir 750 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop
class class-default
  set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop

```

1 秒間あたりのパケットのクレジット制限

特定のポリシーの 1 秒間あたりのパケット（PPS）の合計（ポリシーの各クラス部分の PPS の合計）の上限は、PPS のクレジット制限（PCL）の上限になります。特定のクラスの PPS が増加して PCL 超過すると、設定が拒否されます。目的の PPS を増やすには、PCL を超える PPS の分を他のクラスから減少させる必要があります。

モジュラ QoS コマンドライン インターフェイス

CoPP は、モジュラ QoS コマンドライン インターフェイス（MQC）を使用します。MQC は CLI の構造を持っています。MQC を使用すると、トラフィック クラスの定義、トラフィック ポリシー（ポリシー マップ）の作成、およびインターフェイスへのトラフィック ポリシーの適用が可能になります。トラフィック ポリシーには、トラフィック クラスに適用する CoPP 機能を含めます。

Procedure

- ステップ 1** **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィック の分類に使用します。

次に、copp-sample-class と呼ばれる新しいマップを作成する例を示します。

```
class-map type control-plane copp-sample-class
```

- ステップ 2** **policy-map** コマンドを使用して、トラフィック ポリシーを定義します。トラフィック ポリシー（ポリシー マップ）には、トラフィック クラスと、トラフィック クラスに適用する 1 つまたは複数の CoPP 機能を含めます。トラフィック ポリシー内の CoPP の機能で、分類されたトラフィック の処理方法が決まります。

- ステップ 3** **control-plane** コマンドおよび **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシー マップ）をコントロールプレーンに適用します。

次に、コントロールプレーンにポリシー マップを適用する例を示します。

```
control-plane
service-policy input copp-system-policy
```

Note

copp-system-policy は常に設定され、適用されます。このコマンドを明示的に使用する必要はありません。

CoPP と管理インターフェイス

Cisco NX-OS デバイスは、管理インターフェイス (mgmt0) をサポートしないハードウェアベースの CoPP だけをサポートします。アウトオブバンド mgmt0 インターフェイスは CPU に直接接続するため、CoPP が実装されているインバンドトラフィックハードウェアは通過しません。

mgmt0 インターフェイスで、ACL を設定して、特定タイプのトラフィックへのアクセスを許可または拒否することができます。

Related Topics

[IP ACL の構成](#) (355 ページ)

[MAC ACL の設定](#) (451 ページ)

CoPP の注意事項と制約事項

CoPP に関する注意事項と制約事項は次のとおりです。

- 最初に strict デフォルト CoPP ポリシーを使用し、後で、データセンターおよびアプリケーションの要件に基づいて CoPP ポリシーを変更することを推奨します。
- 第 1 世代の Cisco Nexus 9000 シリーズ スイッチ (非 FX/FX2) は、送信元ベースの CoPP をサポートしていません。この制限は、クラウド スケールの ASIC ベースの Cisco Nexus スイッチには存在しません。
- **match-all** オプションは CoPP クラスマップではサポートされず、常に **match-any** オプションにはデフォルトになります。
- CoPP のカスタマイズは継続的なプロセスです。CoPP を設定するときには、特定の環境で使用されるプロトコルや機能のみならず、サーバ環境に必要なスーパーバイザ機能を考慮する必要があります。これらのプロトコルや機能に変更されたら、CoPP を変更する必要があります。
- CoPP を継続的にモニタすることを推奨します。ドロップが発生した場合は、CoPP がトラフィックを誤ってドロップしたのか、または誤動作や攻撃に反応してドロップしたのかを判定してください。いずれの場合も、状況を分析し、CoPP ポリシーを変更する必要性を評価します。
- 他のクラス マップで指定しないトラフィックはすべて、最後のクラス (デフォルトクラス) に配置されます。このクラス内のドロップをモニタし、これらのドロップが必要な

いトラフィックに基づいているのか、または設定されていないために追加が必要な機能の結果であるかどうかを調査します。

- アクセス コントロール リスト (ACL) を通してルータ プロセッサにリダイレクトする必要のあるパケット (たとえば、ARP および DHCP) を判定するために、すべてのブロードキャストトラフィックが CoPP ロジックを通して送信されます。リダイレクトする必要のないブロードキャストトラフィックは CoPP ロジックに対して照合され、準拠したパケットと違反したパケットの両方がハードウェア内でカウントされますが、CPU には送信されません。CPU に送信しなければならないブロードキャストトラフィックと、CPU に送信する必要のないブロードキャストトラフィックを異なるクラスに分離する必要があります。
- CoPP を設定した後、古いクラスマップや未使用のルーティングプロトコルなど、使用されていないものはすべて削除してください。
- CoPP ポリシーによって、ルーティングプロトコルなどのクリティカルなトラフィック、またはデバイスへのインタラクティブなアクセスがフィルタリングされないように注意してください。このトラフィックをフィルタリングすると、Cisco NX-OS デバイスへのリモートアクセスが禁止され、コンソール接続が必要になる場合があります。
- Cisco NX-OS ソフトウェアは、出力 CoPP とサイレントモードをサポートしません。CoPP は、入力でのみサポートされます (コントロールプレーン インターフェイスに対して **service-policy output copp** コマンドは使用できません)。
- ハードウェアのアクセス コントロール エントリ (ACE) ヒットカウンタは、ACL 論理だけで使用できます。CPU のトラフィックを評価するには、ソフトウェアの ACE ヒットカウンタと **show access-lists** および **show policy-map type control-plane** コマンドを使用します。
- Cisco NX-OS デバイスのハードウェアは、フォワーディングエンジン単位で CoPP を実行します。CoPP は分散ポリシーをサポートしていません。したがって、レートを選択する場合は、集約トラフィックでスーパーバイザモジュールに過剰な負荷をかけることのない値にしてください。
- 複数のフローが同じクラスにマッピングされる場合、個々のフローの統計情報は使用できません。
- CoPP 機能をサポートする Cisco NX-OS リリースから、新しいプロトコルのその他のクラスを含む CoPP 機能をサポートする Cisco NX-OS リリースにアップグレードする場合は、CoPP の新しいクラスを使用可能にするためにセットアップユーティリティを **setup** コマンドで実行するか **copp profile** コマンドを実行する必要があります。
- コントロールプレーン ポリシング (CoPP) 機能をサポートしている Cisco NX-OS リリースから CoPP 機能をサポートしていない以前の Cisco NX-OS リリースへのダウングレードを実行する前に、**show incompatibility nxos bootflash:filename** コマンドを使用して互換性を確認しておく必要があります。非互換な部分が存在する場合は、ソフトウェアをダウングレードする前に、ダウングレードイメージと互換性がない機能をすべて無効化してください。
- CoPP は無効にできません。これを無効にしようとすると、パケットは 50 パケット/秒。

- スキップ CoPP ポリシー オプションは、ネットワークのコントロールプレーンに影響を与える可能性があるため、Cisco NX-OS 初期設定ユーティリティから削除されました。
- スタティック アCoPP ACL には、次のガイドラインと制限事項が適用されます。
 - スタティック CoPP ACL は、別の CoPP クラスに再マッピングできます。
 - スタティック CoPP ACL のアクセス コントロール エントリ (ACE) は変更または削除できません。
 - CoPP ACL にスタティック ACL のサブストリングがある場合、このタイプのトラフィックに対してマッピングされます。たとえば、ACL に `acl-mac-stp` サブストリングが含まれている場合、STP トラフィックはこの ACL のクラス マップに分類されます。
 - スタティック CoPP ACL は、CoPP ポリシー内での位置、設定される順序、および **show policy-map type control-plane** コマンドの出力での表示に関係なく、ダイナミック CoPP ACL よりも優先されます。
 - CoPP ポリシーにスタティック CoPP ACL が必要です。これを行わないと、CoPP ポリシーは拒否されます。
- Cisco Nexus リリース 9.2(2) 以降、Cisco Nexus 9300-FX シリーズ スイッチ、および Cisco Nexus 9500 プラットフォーム スイッチは、プロトコル ACL フィルタリングをサポートしています。このリリースでは、IPv6 ACL はサポートされていません。
- Cisco NX-OS リリース 9.2(3) 以降では、Cisco Nexus 9300-FX シリーズ スイッチ、および Cisco Nexus 9500 プラットフォーム スイッチのダイナミック CoPP で IPv6 ACL がサポートされています。
- 出力 CoPP 用のプロトコル ACL フィルタリングには、次の制限があります。
 - 出力 CoPP ACL を定義すると、既存のルールを追加または削除できなくなります。これは、出力 CoPP ACL に付加されたすべてのクラスマップとポリシーマップに適用されます。
 - 既存の出力 CoPP を新しいポリシーで上書きすることはできません。新しいポリシーを追加する前に、既存の出力 CoPP を削除する必要があります。
 - 拒否アクションは適用されません。
 - すべてのエントリは TCAM でプログラムされ、同じエントリを持つ2つの MAC または IP ACL が作成され、同じまたは異なるクラスマップにバインドされている場合、異なる TCAM スペースを使用します。
 - 出力 CoPP でサポートされる TCAM カービングの最大数は 128 エントリです。24 エントリは予約済みで、残りの 104 エントリは出力 CoPP 用で、すべて倍幅です。これは、52 (Ipv4、mac、Ipv6) エントリのいずれかになります。
 - ポリサーを使用すると、cir と burst を 0 にして、トラフィックを完全にドロップできます。
 - SNMP MIB は、サポートされません。

- パケットが複数の例外条件を満たしている場合、CoPP は CoPP ACL が設定されている順序に基づいてパケットを照合し、単一のクラスに対してのみ照合します。これは予期された CoPP 動作です。

Cisco NX-OS リリース 9.3 (4) 以降では、UC FIB MISS 例外は CoPP クラス (copp-system-p-class-exception) に対してカウントされます。したがって、パケットに TTL (accounted user class copp-system-p-class-exception-diag) と UC FIB MISS 例外の両方がある場合、UC FIB MISS 例外と見なされます。この動作は、copp-system-p-class-exception クラスの順序が copp-system-p-class-exception-diag クラスよりも高い CoPP クラスの順位のために発生します。NX-OS リリース 9.3(4) より前の NX-OS リリースでは、UC FIB MISS 例外は CoPP ルールによって明示的に処理されませんでした。

- CoPP 処理は 2 つの段階で構成されます。最初の段階では、各クラスポリシーで実際のパケットサイズが再利用されますが、パケットが 2 番目の段階に入ると、44 バイトの内部ヘッダーが追加されます。これにより、すべての CoPP クラスの適合ポリシーまたは違反ポリシーが変更されます。この制限は、Cisco Nexus 9300-FX、Nexus 9300-FX2、および 9300-GX プラットフォームスイッチに適用されます。
- Cisco NX-OS リリース 10.1(2) 以降、CoPP は Cisco Nexus X9624D-R2 ラインカードおよび 9508-FM-R2 スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(2) 以降、CoPP は 9364D-GX2A および 9332D-GX2B スイッチでサポートされます。
- Cloudscale IPv6 リンクローカル BGP のサポートには、512 を超える ing-sup TCAM リージョンを切り分ける必要があります (これを有効にするには、リロードが必要です)。
- Cisco NX-OS リリース 10.3(1)F 以降、CoPP ACL は Cisco Nexus 9808 スイッチでサポートされます。
 - Cisco NX-OS リリース 10.4(1)F 以降、CoPP ACL は、Cisco Nexus X98900CD-A および X9836DM-A ラインカードを搭載した Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、CoPP ACL は、Cisco Nexus 9804 スイッチ、および Cisco Nexus X98900CD-A と X9836DM-A ラインカードでサポートされます。
- Cisco Nexus 9808/9804 スイッチには、SUP CoPP ACL サポートに関する次の制限があります。
 - ポリサー レートは、ステージ 1 で 161 PPS の倍数です。
 - ステージ 0 にはシェーパーがありません。
 - ステージ 2 の出力は LC/モジュール レベルで、ステージ 3 の出力は SUP/CPU レベルです。
 - ファブリック/FM は、インバンドパスに関与しません。
 - ステージ 1、ステージ 2、およびステージ 3 の CoPP ポリシーは PPS です。
 - CoPP ステージ 3 の統計情報は、システムのスイッチオーバー後にゼロにリセットされます。

- カスタム CoPP では、ポリサー レートの変更のみがサポートされます。
- トラフィックの影響時にトラフィック損失を回避するには、Cisco Nexus 9300 GX/FX/FX2/FX3、9504-FM-G および 9508-FM-G スイッチと X9716D-GX ラインカードで CoPP クラスの通常の CIR 値を 2200 kbps に構成します。
- Cisco NX-OS リリース 10.3(2)F 以降、R/RX ラインカードを備えた Cisco Nexus 9504 および 9508 モジュラ シャーシで、CoPP の ソース IP ベースのフィルタリングのサポートが追加されました。



(注) IPv6 の場合、ソース IP ベースのフィルタリングは、24b MSB まですサポートされます。

- Cisco NX-OS リリース 10.4(1)F 以降、CoPP ACL は Cisco Nexus 9332D-H2R スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、CoPP ACL は Cisco Nexus 93400LD-H1、および 93108TC-FX3 スイッチでサポートされます。
- Cisco Nexus リリース 10.4(3)F 以降、CoPP ACL は Cisco Nexus 9364C-H1 スイッチでサポートされます。
- Cisco Nexus 9336C-SE1 スイッチでは、カスタム CoPP またはハードウェア レート リミッタではゼロ CIR はサポートされません。ユーザーがゼロ CIR を構成すると、ハードウェアで可能な最小値に設定されます。

Cisco Nexus 9364E-SG2 スイッチの CoPP のガイドラインと制限事項

- Cisco NX-OS リリース 10.5(3)F 以降、Cisco Nexus 9364E-SG2-Q と 9364E-SG2-O スイッチではカスタム CoPP がサポートされています。以下は機能と制限です。
 - 組み込みクラスのコピーに対するポリサー レートを変更できます。
 - ユーザー定義の一致基準とポリサーレートを使用して、完全にユーザー定義の CoPP クラスを作成できます。
 - ポリサー レートは、パケット/秒 (PPS) でのみ構成できます。
 - ユーザー定義の MAC アクセス リストと送信元 MAC アドレス (SMAC) は、カスタム CoPP 内ではサポートされません。ただし、デフォルトプロファイルの既知の接続先 MAC アドレス (DMAC) を持つ MAC ACL はサポートされています。
 - 少なくとも 1 つの IPv4 ACL がカスタム CoPP 構成に存在する必要があります。
 - すべてのブリッジプロトコル データ ユニット (BPDU) が単一のポリサーにマッピングされます。したがって、Cisco Discovery Protocol (CDP)、Link Layer Discovery Protocol (LLDP)、スパニングツリープロトコル (STP) などのプロトコルに対する個別のポリシング構成はサポートされません。

- CoPP ポリシーで最大 28 のクラス マップを作成できます。
- カスタム CoPP スケール制限（一次元）：TCAM エントリの最大数：
 - IPv4：360
 - IPv6：180
- カスタム CoPP の CoPP 整合性チェッカーはサポートされていません。
- 126 パケットの単一のバースト値のみがサポートされます。
- 宛先 IP 照合は、IPv4 または IPv6 リンクローカル マルチキャスト アドレスをサポートしません。
- OSPF、RIP、EIGRP、AUTO-RP などのリンク ローカル マルチキャスト エントリの IPv4 および IPv6 ACL は、同じ CoPP クラス内に追加する必要があります。同様に、HSRP および VRRP の IPv4 および IPv6 ACL も、デフォルトの CoPP プロファイルと同じ CoPP クラスである必要があります。さらに、リンク ローカル マルチキャスト エントリの ACL 名には、「acl-ospf」や「acl-eigrp」などのデフォルトの CoPP ポリシーの文字列を含める必要があります。

Cisco Nexus 9336C-SE1 スイッチ上の CoPP のガイドラインと制限事項

- ポリサー レートは 1 秒あたりのパケット数（PPS）で指定されます。
- カスタム コントロールプレーンポリシング（CoPP）では、宛先IPベースのアクセスリスト照合はサポートされていません。
- ユーザー定義の MAC アクセス リストはサポートされません。組み込み MAC ACL だけを使用できます。
- カスタム コントロールプレーンポリシング（CoPP）ポリシーでは、最大 28 のクラス マップを構成できます。
- カスタム コントロールプレーンポリシング（CoPP）は、最大 360 の IPv4（一次元）と 180 の IPv6（一次元）の TCAM エントリをサポートします。
- カスタム コントロールプレーンポリシング（CoPP）のコントロールプレーンポリシング（CoPP）整合性チェッカーはサポートされていません。
- ゼロ設定情報レート（CIR）はサポートされていません。ユーザーがゼロ設定情報レート（CIR）が構成されるとハードウェアは、可能な最小値に設定されます。

CoPP のデフォルト設定

次の表に、CoPP パラメータのデフォルト設定を示します。

Table 40: CoPP パラメータのデフォルト設定

パラメータ	デフォルト
デフォルト ポリシー	strict
デフォルト ポリシー	9 ポリシー エントリ Note 関連するクラス マップでサポートされるポリシーの最大数は 128 です。
スケールファクタ値	1.00

CoPP の設定

ここでは、CoPP の設定方法について説明します。

コントロールプレーンクラスマップの設定

コントロールプレーンポリシーのコントロールプレーンクラスマップを設定する必要があります。

トラフィックを分類するには、既存の ACL に基づいてパケットを照合します。ACL キーワードの permit および deny は、照合時には無視されます。

IP バージョン 4 (IPv4) および IP バージョン 6 (IPv6) のパケットに対してポリシーを設定できます。

Before you begin

クラスマップ内で ACE ヒットカウンタを使用する場合は、IP ACL が設定してあることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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

	Command or Action	Purpose
ステップ 2	class-map type control-plane [match-all match-any] class-map-name Example: <pre>switch(config)# class-map type control-plane ClassMapA switch(config-cmap)#</pre>	コントロールプレーン クラス マップを指定し、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。デフォルトのクラス一致は match-any です。名前は最大 64 文字で、大文字と小文字は区別されます。 Note class-default、match-all、または match-any をクラス マップ名に使用できません。
ステップ 3	(Optional) match access-group name access-list-name Example: <pre>switch(config-cmap)# match access-group name MyAccessList</pre>	IP ACL のマッチングを指定します。 Note ACL キーワード permit および deny は、CoPP マッチング時には無視されます。
ステップ 4	(Optional) match exception {ip ipv6} icmp redirect Example: <pre>switch(config-cmap)# match exception ip icmp redirect</pre>	IPv4 または IPv6 ICMP リダイレクト例外パケットのマッチングを指定します。
ステップ 5	(Optional) match exception {ip ipv6} icmp unreachable Example: <pre>switch(config-cmap)# match exception ip icmp unreachable</pre>	IPv4 または IPv6 ICMP 到達不能例外パケットのマッチングを指定します。
ステップ 6	(Optional) match exception {ip ipv6} option Example: <pre>switch(config-cmap)# match exception ip option</pre>	IPv4 または IPv6 ICMP オプション例外パケットのマッチングを指定します。
ステップ 7	match protocol arp Example: <pre>switch(config-cmap)# match protocol arp</pre>	IP アドレス解決プロトコル (ARP) および逆アドレス解決プロトコル (RARP) パケットのマッチングを指定します。
ステップ 8	exit Example: <pre>switch(config-cmap)# exit switch(config)#</pre>	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。

	Command or Action	Purpose
ステップ 9	(Optional) show class-map type control-plane [class-map-name] Example: <pre>switch(config)# show class-map type control-plane</pre>	コントロールプレーン クラス マップ の設定を表示します。
ステップ 10	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

コントロールプレーンポリシーマップの設定

CoPP のポリシーマップを設定する必要があります。ポリシーマップにはポリシーパラメータを含めます。クラスのポリサーを設定しなかった場合、次のデフォルトが設定されます。

- 50 パケット/秒 (pps) 、 32 パケットのバースト (Cisco Nexus 9300 および 9500 シリーズ スイッチの場合)
- 150 キロビット/秒 (kbps) 、 32,000 バイトのバースト

Before you begin

コントロールプレーン クラス マップが設定してあることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	policy-map type control-plane policy-map-name Example: <pre>switch(config)# policy-map type control-plane ClassMapA switch(config-pmap)#</pre>	コントロールプレーン ポリシー マップを指定し、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。ポリシー マップ名は最大 64 文字で、大文字と小文字は区別されます。
ステップ 3	class {class-map-name [insert-before class-map-name2] class-default} Example:	コントロールプレーン クラス マップ 名またはクラスデフォルトを指定し、コントロールプレーンクラスコンフィギュレーションモードを開始します。

	Command or Action	Purpose
	<pre>switch(config-pmap)# class ClassMapA switch(config-pmap-c)#</pre>	class-default クラスマップは、必ずポリシー マップのクラス マップ リストの末尾に位置します。
ステップ 4	次のいずれかのコマンドを入力します。 • police [cir] {cir-rate [rate-type]} • police [cir] {cir-rate [rate-type]} [bc] burst-size [burst-size-type] • police [cir] {cir-rate [rate-type]} conform transmit [violate drop] Example: <pre>switch(config-pmap-c)# police cir 52000 bc 1000 packets</pre> Example: <pre>switch(config-pmap-c)# police cir 3400 kbps bc 200 kbytes</pre>	認定情報レート (CIR) を指定します。レート範囲を次に示します。 • 01 ～ 268435456 pps (Cisco Nexus 9300 および 9500 シリーズ スイッチの場合) • 0 ～ 80000000000 bps/gbps/kbps/mbps Note CIR レートの範囲は 0 から始まりません。以前のリリースでは、CIR レートの範囲は 1 から始まります。0 の値ではパケットがドロップします。 committed burst (BC) 範囲は次のようになります。 • 1 ～ 1073741 パケット (Cisco Nexus 9300 および 9500 シリーズ スイッチの場合) • 1 ～ 512000000 bytes/kbytes/mbytes 適合送信アクションは、パケットを送信します。 Note 同じ CIR に BC と一致 (conform) アクションを指定できます。
ステップ 5	(Optional) logging drop threshold [drop-count [level syslog-level]] Example: <pre>switch(config-pmap-c)# logging drop threshold 100</pre>	ドロップされたパケットのしきい値を指定し、ドロップ数が設定したしきい値を超えた場合、Syslog を生成します。drop-count 引数の範囲は 1 ～ 8000000000 バイトです。syslog-level 引数の範囲は 1 ～ 7 であり、デフォルトレベルは 4 です。
ステップ 6	(Optional) set cos cos-value Example: <pre>switch(config-pmap-c)# set cos 1</pre>	802.1Q CoS 値を指定します。範囲は 0 ～ 7 です。デフォルト値は 0 です。

	Command or Action	Purpose
ステップ 7	exit Example: <pre>switch(config-pmap-c)# exit switch(config-pmap)#</pre>	ポリシー マップ クラス コンフィギュレーション モードを終了します。
ステップ 8	exit Example: <pre>switch(config-pmap)# exit switch(config)#</pre>	ポリシーマップコンフィギュレーション モードを終了します。
ステップ 9	(Optional) show policy-map type control-plane [expand] [name class-map-name] Example: <pre>switch(config)# show policy-map type control-plane</pre>	コントロールプレーン ポリシー マップの設定を表示します。
ステップ 10	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Related Topics

[コントロールプレーン クラス マップの設定](#) (695 ページ)

コントロールプレーン サービス ポリシーの設定

CoPP サービス ポリシーに対して 1 つまたは複数のポリシー マップを設定できます。



Note CoPP ポリシーを変更し CoPP のカスタム ポリシーを適用しようとした場合、ハードウェア内では非アトミックとして設定され、次のメッセージが表示されます。

```
This operation can cause disruption of control traffic. Proceed (y/n)? [no] y
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT24-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT23-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT21-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT25-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT26-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT22-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT4-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
```

Before you begin

コントロールプレーン ポリシー マップが設定してあることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	control-plane Example: <pre>switch(config)# control-plane switch(config-cp)#</pre>	コントロールプレーン 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	[no] service-policy input policy-map-name Example: <pre>switch(config-cp)# service-policy input PolicyMapA</pre>	入トラフィックのポリシー マップを指定します。ポリシー マップが複数ある場合は、このステップを繰り返します。 CoPPはディセーブルにできません。このコマンドの no 形式を入力すると、パケットは 50 パケット/秒。
ステップ 4	exit Example: <pre>switch(config-cp)# exit switch(config)#</pre>	コントロールプレーン コンフィギュレーション モードを終了します。

	Command or Action	Purpose
ステップ 5	(Optional) show running-config copp [all] Example: <pre>switch(config)# show running-config copp</pre>	CoPP 設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

[コントロールプレーン ポリシー マップの設定](#) (697 ページ)

ラインカードごとの CoPP のスケール ファクタの設定

ラインカードごとの CoPP のスケール ファクタを設定できます。

スケール ファクタの設定は、特定のラインカードに適用された CoPP のポリシーのポリサー レートのスケールリングに使用されます。受け入れ値は 0.10 ～ 2.00 です。特定のラインカード に対して現在の CoPP ポリシーを変更せずに、ポリサー レートを増加または削減できます。変更はすぐに有効となるため、CoPP ポリシーを再適用する必要はありません。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	control-plane Example: <pre>switch(config)# control-plane switch(config-cp)#</pre>	コントロールプレーン 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	scale-factor value module multiple-module-range Example: <pre>switch(config-cp)# scale-factor 1.10 module 1-2</pre>	ラインカードごとにポリサー レートを設定します。許可されたスケール ファクタ値は 0.10 ～ 2.00 です。スケール ファクタ値が設定されている場合、ポリシング値にはモジュールの対応するスケール ファクタ値が乗算され、特定のモジュールにプログラミングされます。

	Command or Action	Purpose
		デフォルトのスケールファクタ値 1.00 に戻すには、 no scale-factor value module multiple-module-range コマンドを使用するか、 scale-factor 1 module multiple-module-range コマンドを使用して明示的にデフォルトのスケールファクタである値 1.00 に設定します。
ステップ 4	(Optional) show policy-map interface control-plane Example: <pre>switch(config-cp)# show policy-map interface control-plane</pre>	CoPP ポリシーが適用される場合に適用されるスケールファクタ値を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

デフォルトの CoPP ポリシーの変更または再適用

別のデフォルト CoPP ポリシーに変更したり、同じデフォルト CoPP ポリシーを再適用したりすることができます。

Procedure

	Command or Action	Purpose
ステップ 1	no copp profile strict moderate lenient dense Example: <pre>switch(config)# copp profile moderate</pre>	CoPP ベストプラクティスポリシーを適用します。 CoPP はディセーブルにできません。このコマンドに no フォームを入力する場合、パケットは 1 秒あたり 50 パケットにレート制限されます。
ステップ 2	(Optional) show copp status Example: <pre>switch(config)# show copp status</pre>	最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。このコマンドを実行すると、CoPP ベストプラクティスポリシーがコントロールプレーンにアタッチされていることを確認することもできます。

	Command or Action	Purpose
ステップ 3	(Optional) show running-config copp Example: <pre>switch(config)# show running-config copp</pre>	実行コンフィギュレーション内の CoPP 設定を表示します。

Related Topics

[セットアップユーティリティによるデフォルト CoPP ポリシーの変更または再適用](#) (715 ページ)

CoPP ベスト プラクティス ポリシーのコピー

CoPP ベスト プラクティス ポリシーは読み取り専用です。その設定を変更する場合は、それをコピーする必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	copp copy profile {strict moderate lenient dense} {prefix suffix} string Example: <pre>switch# copp copy profile strict prefix abc</pre>	CoPP ベスト プラクティス ポリシーのコピーを作成します。 CoPP は、指定したプレフィックスまたはサフィックスのすべてのクラス マップおよびポリシー マップの名前を変更します。
ステップ 2	(Optional) show copp status Example: <pre>switch# show copp status</pre>	最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。このコマンドを実行すると、コピーされたポリシーがコントロールプレーンにアタッチされていないことを確認することもできます。
ステップ 3	(Optional) show running-config copp Example: <pre>switch# show running-config copp</pre>	コピーされたポリシー設定を含む、実行コンフィギュレーション内の CoPP 設定を表示します。

出力 CoPP のプロトコル ACL フィルタリング

出力 CoPP のプロトコル ACL フィルタリングにより、NX-OS スイッチは、ホスト MAC、IPv4、および IPv6 アドレスに基づいてコントロールプレーンへのすべてのトラフィックをフィルタリングできます。

出力 CoPP の ARP ACL フィルタリングの構成

出力 CoPP で、MAC ACL フィルタリングを構成できます。

Before you begin

コントロールプレーン ポリシー マップが設定してあることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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] hardware access-list tcam region erg-copp size Example: switch(config)# hardware access-list tcam region erg-copp 128	CoPP TCAM リージョン サイズを設定します。
ステップ 3	copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。
ステップ 4	reload Example: switch(config)# reload	デバイスがリロードされます。 Note 新しいサイズの値は、 copy running-config startup-config + reload を入力するか、すべてのラインカードモジュールをリロードした後にのみ有効になります。
ステップ 5	configure terminal Example: switch# configure terminal switch(config)#	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	mac access-list mac-foo-1 Example: switch# mac access-list mac-foo-1 switch(config-mac-acl)#	

	Command or Action	Purpose
ステップ 7	class-map type control-plane [match-all match-any] class-map-name Example: <pre>switch(config)# class-map type control-plane match-any c-map2 switch(config-cmap)#</pre>	コントロールプレーン クラス マップを指定し、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。デフォルトのクラス一致は match-any です。名前は最大 64 文字で、大文字と小文字は区別されます。
ステップ 8	(Optional) match access-group name access-list-name Example: <pre>switch(config-cmap)# match access-group name IP-foo-1</pre>	
ステップ 9	policy-map type control-plane policy-map-name Example: <pre>switch(config)# policy-map type control-plane ClassMapA switch(config-pmap)#</pre>	コントロールプレーン ポリシー マップを指定し、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。ポリシー マップ名は最大 64 文字で、大文字と小文字は区別されます。
ステップ 10	class {class-map-name [insert-before class-map-name2] class-default} Example: <pre>switch(config-pmap)# class ClassMap2 switch(config-pmap-c)#</pre>	コントロールプレーン クラス マップ名またはクラスデフォルトを指定し、コントロールプレーンクラスコンフィギュレーションモードを開始します。 class-default クラスマップは、必ずポリシー マップのクラス マップ リストの末尾に位置します。
ステップ 11	次のいずれかのコマンドを入力します。 • police [cir] {cir-rate [rate-type]} • police [cir] {cir-rate [rate-type]} [bc] burst-size [burst-size-type] • police [cir] {cir-rate [rate-type]} conform transmit [violate drop] Example: <pre>switch(config-pmap-c)# police cir 52000 bc 1000 packets</pre>	認定情報レート (CIR) を指定します。レート範囲を次に示します。 認定バースト (BC) の範囲は次のとおりです。
ステップ 12	control-plane Dynamic mode Example: <pre>switch(config)# control-plane dynamic switch(config-cp-dyn)#</pre>	制御プレーン動的コンフィギュレーション モードに入ります。

	Command or Action	Purpose
ステップ 13	service-policy-dynamic input <i>policy-map-name</i> Example: <pre>switch(config-cp-dyn)# service-policy-dynamic input PolicyMap1</pre>	入トラフィックのポリシーマップを指定します。

出力 CoPP の IP ACL フィルタリングの構成

出力 CoPP で IP ACL フィルタリングを設定できます。

始める前に

コントロールプレーン ポリシー マップが設定してあ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 例 : <pre>switch# configure terminal switch(config)#</pre>	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] hardware access-list tcam region erg-copp size 例 : <pre>switch(config)# hardware access-list tcam region erg-copp 128</pre>	CoPP TCAM リージョンの出力サイズを設定します。
ステップ 3	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。
ステップ 4	reload 例 : <pre>switch(config)# reload</pre>	デバイスがリロードされます。 (注) 新しいサイズの値は、 copy running-config startup-config + reload を入力するか、すべてのラインカードモジュールをリロードした後にのみ有効になります。
ステップ 5	configure terminal 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
	switch# configure terminal switch(config)#	
ステップ 6	ip access-list IP-foo-1 例 : switch# ip access-list mac-foo-1 switch(config-acl)#	
ステップ 7	permit tcp access-list IP-foo-1 eq bgp 例 : switch(config-acl)# 10 permit tcp 10.1.1.1/32 10.1.1.2/32 eq bgp	
ステップ 8	class-map type control-plane [match-all match-any] class-map-name 例 : switch(config)# class-map type control-plane match-any c-map2 switch(config-cmap)#	コントロールプレーン クラス マップを指定し、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。デフォルトのクラス一致は match-any です。名前は最大 64 文字で、大文字と小文字は区別されます。
ステップ 9	match access-group name access-list-name 例 : switch(config-cmap)# match access-group name IP-foo-1	
ステップ 10	policy-map type control-plane policy-map-name 例 : switch(config)# policy-map type control-plane ClassMapA switch(config-pmap)#	コントロールプレーン ポリシー マップを指定し、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。ポリシー マップ名は最大 64 文字で、大文字と小文字は区別されます。
ステップ 11	class {class-map-name [insert-before class-map-name2] class-default} 例 : switch(config-pmap)# class ClassMap2 switch(config-pmap-c)#	コントロールプレーン クラス マップ名またはクラスデフォルトを指定し、コントロールプレーンクラスコンフィギュレーションモードを開始します。 class-default クラスマップは、必ずポリシー マップのクラス マップ リストの末尾に位置します。
ステップ 12	次のいずれかのコマンドを入力します。 • police [cir] {cir-rate [rate-type]} • police [cir] {cir-rate [rate-type]} [bc] burst-size [burst-size-type]	認定情報レート (CIR) を指定します。レート範囲を次に示します。 認定バースト (BC) の範囲は次のとおりです。

	コマンドまたはアクション	目的
	• police [cir] {cir-rate [rate-type]} conform transmit [violate drop] 例 : <pre>switch(config-pmap-c)# police cir 52000 bc 1000 packets</pre> 例 : <pre>switch(config-pmap-c)# police cir 3400 kbps bc 200 kbytes</pre>	
ステップ 13	control-plane Dynamic mode 例 : <pre>switch(config)# control-plane dynamic switch(config-cp-dyn)#</pre>	制御プレーン動的コンフィギュレーション モードに入ります。
ステップ 14	service-policy-dynamic input <i>policy-map-name</i> 例 : <pre>switch(config-cp-dyn)# service-policy-dynamic input PolicyMap1</pre>	入トラフィックのポリシーマップを指定します。終了

CoPP の設定の確認

CoPP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show policy-map type control-plane [expand] [name policy-map-name]	コントロールプレーン ポリシー マップと関連するクラス マップ、および CIR と BC の値を表示します。

コマンド	目的
show policy-map interface control-plane	ポリシーの値と関連するクラス マップ、およびポリシーごとまたはクラス マップごとのドロップが表示されます。また、CoPP ポリシーが適用されている場合は、スケール ファクタ値も表示されます。スケール ファクタ値がデフォルト (1.00) の場合は表示されません。 Note スケール ファクタは、CIR と BC の値を各モジュールで内部的に変更しますが、ディスプレイに表示されるのは、設定された CIR と BC の値のみです。モジュールに実際に適用される値は、スケール ファクタに設定値を掛けた値です。
show class-map type control-plane <i>[class-map-name]</i>	このクラス マップにバインドされている ACL を含め、コントロールプレーンクラス マップの設定を表示します。

コマンド	目的
show copp diff profile {strict moderate lenient dense} [prior-ver] profile {strict moderate lenient dense} show copp diff profile	2つの CoPP ベスト プラクティス ポリシーの違いを表示します。 prior-ver オプションを指定しない場合、このコマンドは、現在適用されている2つのデフォルトの CoPP のベスト プラクティス ポリシー（現在適用されている厳密なポリシーと現在適用されている中程度のポリシーなど）の差異を表示します。 prior-ver オプションを指定した場合、このコマンドは、現在適用されているデフォルトの CoPP ベスト プラクティス ポリシーと以前に適用したデフォルトの CoPP ベスト プラクティス ポリシーの違いを表示します（現在適用されている厳密なポリシーと以前適用した緩いポリシーなど）。
show copp profile {strict moderate lenient dense}	クラスおよびポリサー値とともに、CoPP ベスト プラクティス ポリシーの詳細を表示します。
show running-config aclmgr [all]	実行コンフィギュレーションのユーザ設定によるアクセスコントロール リスト (ACL) を表示します。 all オプションを使用すると、実行コンフィギュレーションのデフォルト (CoPP 設定) とユーザ定義による ACL の両方が表示されます。
show running-config copp [all]	実行コンフィギュレーション内の CoPP 設定を表示します。

コマンド	目的
show startup-config aclmgr [all]	スタートアップ コンフィギュレーションのユーザ設定によるアクセスコントロールリスト (ACL) を表示します。 all オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト (CoPP 設定) とユーザ定義による ACL の両方が表示されます。

CoPP 設定ステータスの表示

Procedure

	Command or Action	Purpose
ステップ 1	switch# show copp status	CoPP 機能の設定ステータスを表示します。

Example

次に、CoPP 設定ステータスを表示する例を示します。

```
switch# show copp status
```

CoPP 整合性チェッカー

Cisco NX-OS リリース 10.5(2)F 以降、ソフトウェア、HAL、およびハードウェア レイヤ全体で、すべての SUP 関連の ACL の一貫性を確保するために CoPP 整合性チェッカーが導入されました。この機能は、Cisco Nexus 9300-FX3/GX/GX2/HX、Nexus 9808、および Nexus 9804 シリーズ スイッチでサポートされます。



- (注) Cisco NX-OS リリース 10.5(3)F 以降、**show consistency-checker copp extended module** コマンドは廃止されました。CoPP 整合性チェッカーの詳細については、『Cisco Nexus 9000 シリーズ NX-OS トラブルシューティング ガイド、リリース 10.5 (x)』の「整合性チェッカー コマンド」の項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	<code>switch#<module_no>[brief detail]show consistency-checker copp extended module</code>	CoPP 整合性検査を実行します。 brief : 整合性チェッカーの簡潔な構造化された出力を表示します。 detail : 整合性チェッカーの構造化された出力の詳細を表示します。

CoPP のモニタリング

Procedure

	Command or Action	Purpose
ステップ 1	<code>switch# show policy-map interface control-plane</code>	適用された CoPP ポリシーの一部であるすべてのクラスに関して、パケットレベルの統計情報を表示します。 統計情報は、OutPackets（コントロールプレーンに対して許可されたパケット）と DropPackets（レート制限によってドロップされたパケット）に関して指定します。

Example

次に、CoPP をモニタする例を示します。

```
switch# show policy-map interface control-plane
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-critical (match-any)
  set cos 7
  police cir 19000 pps , bc 128 packets
  module 4 :
    transmitted 373977 packets;
    dropped 0 packets;
```

SNMP での CoPP のモニタリング

Cisco Nexus リリース 9.2(3) 以降、CoPP は Cisco クラスベース QoS MIB (cbQoS MIB) をサポートします。CoPP 要素はすべて、SNMP を使用してモニタできるようになりました（ただし変更は不可）。この機能は、コントロールプレーンにアタッチされたポリシーとサブ要素（クラス、一致ルール、セット アクションなど）にのみ適用されます。コントロールプレーンで使用されていないポリシーの要素は、SNMP では見えません。

次の cbQoS MIB テーブルがサポートされます。

- ccbQoSServicePolicy
- cbQoSInterfacePolicy
- cbQoSObjects
- cbQoSPolicyMapCfg
- cbQoSClassMapCfg
- cbQoSMatchStmtCfg
- cbQoSPoliceCfg
- cbQoSSetCfg



(注) SNMP MIB は、ダイナミック CoPP ではサポートされていません。

CoPP 統計情報のクリア

Procedure

	Command or Action	Purpose
ステップ 1	(Optional) switch# show policy-map interface control-plane	現在適用されている CoPP ポリシーおよびクラスごとの統計情報を表示します。
ステップ 2	switch# clear copp statistics	CoPP 統計情報をクリアします。 Note N9K-X9836DM-A および N9K-X98900CD-A ライン カード、N9K-C9232E-B1、9364E-SG2、および N9324C-SE1U スイッチを備えた Cisco Nexus 9800 シリーズ スイッチで、 clear copp statistics コマンドは、ハードウェア

	Command or Action	Purpose
		アラートリミッタ ポリサー以外の全てのポリサーの CoPP 統計をクリアします。

Example

次に、インターフェイス環境で、CoPP 統計情報をクリアする例を示します。

```
switch# show policy-map interface control-plane
switch# clear copp statistics
```

CoPP の設定例

ここでは、CoPP の設定例を示します。

CoPP の設定例

次に、IP ACL と MAC ACL を使用する CoPP を設定する例を示します。

```
configure terminal
ip access-list copp-system-p-acl-igmp
permit igmp any 10.0.0.0/24

ip access-list copp-system-p-acl-msdp
permit tcp any any eq 639

mac access-list copp-system-p-acl-arp
permit any any 0x0806

ip access-list copp-system-p-acl-tacas
permit udp any any eq 49

ip access-list copp-system-p-acl-ntp
permit udp any 10.0.1.1/23 eq 123

ip access-list copp-system-p-acl-icmp
permit icmp any any

class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-igmp
match access-group name copp-system-p-acl-msdp

class-map type control-plane match-any copp-system-p-class-normal
match access-group name copp-system-p-acl-icmp
match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option

policy-map type control-plane copp-system-p-policy

class copp-system-p-class-critical
```



```
police cir 19000 pps bc 128 packets conform transmit violate drop

class copp-system-p-class-important
police cir 500 pps bc 128 packets conform transmit violate drop

class copp-system-p-class-normal
police cir 300 pps bc 32 packets conform transmit violate drop

class class-default
police cir 50 pps bc 32 packets conform transmit violate drop

control-plane
service-policy input copp-system-p-policy
```

CoPP クラスを作成し、ACL を関連付けるには、次のようにします。

```
class-map type control-plane copp-arp-class
match access-group name copp-arp-acl
```

CoPP ポリシーにクラスを追加するには、次のようにします。

```
policy-map type control-plane copp-system-policy
class copp-arp-class
police pps 500
```

次に、COPP 制限をカスタマイズする例を示します。

```
copp copy profile strict suffix CUSTOMIZED-COPP
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
class copp-class-redirect-CUSTOMIZED-COPP
police cir 1500 mbps bc 125 mbytes conform transmit violate drop
control-plane
service-policy input copp-policy-strict-CUSTOMIZED-COPP
```

セットアップユーティリティによるデフォルト CoPP ポリシーの変更または再適用

セットアップユーティリティを使用して CoPP のデフォルト ポリシーを再適用する例を次に示します。

```
switch# setup

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

```

Do you want to enforce secure password standard (yes/no) [y]: <CR>

Create another login account (yes/no) [n]: n

Configure read-only SNMP community string (yes/no) [n]: n

Configure read-write SNMP community string (yes/no) [n]: n

Enter the switch name : <CR>

Enable license grace period? (yes/no) [n]: n

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

Configure the default gateway? (yes/no) [y]: n

Configure advanced IP options? (yes/no) [n]: <CR>

Enable the telnet service? (yes/no) [n]: y

Enable the ssh service? (yes/no) [y]: <CR>

Type of ssh key you would like to generate (dsa/rsa) : <CR>

Configure the ntp server? (yes/no) [n]: n

Configure default interface layer (L3/L2) [L3]: <CR>

Configure default switchport interface state (shut/noshut) [shut]: <CR>

Configure best practices CoPP profile (strict/moderate/lenient/dense/skip) [strict]:
strict

The following configuration will be applied:
password strength-check
no license grace-period
no telnet server enable
no system default switchport
system default switchport shutdown
policy-map type control-plane copp-system-p-policy

Would you like to edit the configuration? (yes/no) [n]: <CR>

Use this configuration and save it? (yes/no) [y]: y

switch#

```

CoPP ポリシー制限の変更

次の例では、CoPP 制限を変更して、PTP インターフェイス全体で PTP 状態を安定させます。

```

copp copy profile strict suffix CUSTOMIZED-COPP
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
class copp-class-redirect-CUSTOMIZED-COPP
police cir 1500 mbytes bc 125 mbytes conform transmit violate drop
control-plane
service-policy input copp-policy-strict-CUSTOMIZED-COPP

```

CoPP に関する追加情報

ここでは、CoPP の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
ライセンス	Cisco NX-OS ライセンス ガイド

標準

標準	タイトル
RFC 2698	『A Two Rate Three Color Marker』



第 26 章

レート制限の設定

この章では、Cisco NX-OS デバイスでスーパーバイザ宛のトラフィックのレート制限を設定する手順について説明します。

この章は、次の項で構成されています。

- [レート制限について, on page 719](#)
- [レート制限の注意事項と制約事項 \(720 ページ\)](#)
- [レート制限のデフォルト設定, on page 721](#)
- [レート制限の設定, on page 722](#)
- [レート制限のモニタリング, on page 724](#)
- [レート制限統計情報のクリア, on page 724](#)
- [レート制限の設定の確認, on page 725](#)
- [レート制限の設定例, on page 725](#)
- [レート制限に関する追加情報, on page 726](#)

レート制限について

レート制限を行うことで、例外のリダイレクトパケットにより Cisco NX-OS デバイス上のスーパーバイザ モジュールに過剰な負荷がかかるのを回避できます。

次のタイプのリダイレクト パケットに対してレート制限を設定できます。

- アクセス リスト ログ パケット
- 双方向フォワーディング検出 (BFD) パケット
- キャッチオール例外トラフィック
- ファブリック エクステンダ (FEX) トラフィック
- レイヤ 3 収集パケット
- レイヤ 3 マルチキャスト データ パケット
- SPAN 出力トラフィック

Cisco Nexus 9300-FX/FXP/FX2/FX3、9300-GX プラットフォーム スイッチ、および X97160YC-EX、9700-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチの場合、CoPP ポリサー レートはキロビット/秒です。他の Cisco Nexus 9000 シリーズ スイッチの場合、CoPP ポリサー レートはパケット/秒です。ただし、SPAN 出力トラフィックではキロビット/秒です。

レート制限の注意事項と制約事項

レート制限に関する注意事項と制約事項は次のとおりです。

- スーパーバイザ宛の例外トラフィックおよびリダイレクトされたトラフィックに対してレート制限を設定できます。スーパーバイザ宛の他のタイプのトラフィックには、コントロールプレーン ポリシング (CoPP) を使用します。



(注) ハードウェア レート制限は、スーパーバイザの CPU を過剰な入力トラフィックから保護します。ハードウェアレート制限によって許容されるトラフィック レートは、グローバルに設定され、個々の I/O モジュールのそれぞれに適用されます。結果的に許容されるレートは、システム内の I/O モジュールの数によって異なります。CoPP では、Modular Quality-of-Service CLI (MQC) を利用して、スーパーバイザの CPU をさらに細かく保護することができます。

- ハードウェア レートリミッタを設定して、SPAN 出力ポートの発信トラフィックの統計情報を表示できます。レート リミッタは、すべての Cisco Nexus 9000、9300 と 9500 シリーズ スイッチでサポートされます。
- 出力ポートのレート リミッタは、Cisco Nexus 9300 および 9500 シリーズ スイッチではパイプごとに制限されます。
- Cisco Nexus 9300 および 9500 シリーズ スイッチは、ローカルと ERSPAN の両方をサポートします。ただし、レート リミッタは ERSPAN にのみ適用されます。これらのスイッチでレート リミッタを有効にするには、[e-racl ACL TCAM リージョンを設定する必要があります](#)。詳細については、Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイドの「[ACL TCAM リージョン サイズの設定](#)」セクションを参照してください。
- Cisco Nexus 9348GC-FXP、93108TC-FX、93180YC-FX シリーズ スイッチの場合、sFlow と ERSPAN の両方を設定しないでください。
- ロギングレート制限はデフォルトでイネーブルになっています。デフォルト設定は、**show running-config** および **show running-config all** には表示されません。レート制限が有効になっているかどうかを確認するには、**show logging** を使用します。レート制限が有効か無効かを確認するための専用フィールドがあります。

ロギングレート制限の設定が適用されない場合は、実行コンフィギュレーションに表示され、show loggingの出力に表示されます。

- **rate-limit cpu direction {input | output | both} pps** パケットの **action log** コマンドは、Cisco Nexus 9000 シリーズスイッチではサポートされていません。



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

レート制限のデフォルト設定

次の表に、レート制限パラメータのデフォルト設定を示します。

Table 41: レート制限パラメータのデフォルト設定

パラメータ	デフォルト
アクセス リスト ロギング パケットのレート制限	100 pps
BFD パケットのレート制限	10000 pps
例外パケットのレート制限	50パケット/秒
FEXパケットレート制限	12000 パケット/秒
レイヤ3 収集パケットのレート制限	100 pps
レイヤ3 マルチキャストデータ パケットのレート制限	3000パケット/秒
SPAN 出力レート制限	制限なし
RL クラス パケット レート制限	100 pps
SPAN パケット レート制限	50パケット/秒
sFLOW パケット レート制限	40000 キロビット/秒
VXLAN-OAM パケット レート制限	1000 pps
100M-ethports パケット レート制限	10000 pps
SPAN 出力無効 dot1x パケット レート制限	3000パケット/秒
MPLS-OAM パケット レート制限	300 パケット/秒
Netflow パケット レート制限	120000 パケット/秒

パラメータ	デフォルト
SSX パケット レート制限	120000 パケット/秒
UCS-mgmt パケット レート制限	120000 パケット/秒
MDNS パケット レート制限	1024 パケット/秒

レート制限の設定

スーパーバイザ宛トラフィックにレート制限を設定できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	hardware rate-limiter access-list-log {packets disable} [module module [port start end]] Example: switch(config)# hardware rate-limiter access-list-log 200	アクセス リスト ロギングのためにスーパーバイザモジュールにコピーされるパケットのレート制限を設定します。範囲は 0 ～ 10,000 です。
ステップ 3	hardware rate-limiter bfd packets [module module [port start end]] Example: switch(config)# hardware rate-limiter bfd 500	双方向フォワーディング検出 (BFD) パケットのレート制限を設定します。範囲は 0 ～ 10,000 です。
ステップ 4	hardware rate-limiter exception packets [module module [port start end]] Example: switch(config)# hardware rate-limiter exception 500	コントロールプレーン ポリシング (CoPP) ポリシーで分類されないシステムのすべての例外トラフィックのレート制限を設定します。範囲は 0 ～ 10,000 です。
ステップ 5	hardware rate-limiter fex packets [module module [port start end]] Example: switch(config)# hardware rate-limiter fex 500	スーパーバイザ宛 FEX トラフィックのレート制限を設定します。範囲は 0 ～ 10,000 です。

	Command or Action	Purpose
ステップ 6	hardware rate-limiter layer-3 glean packets [module module [port start end]] Example: <pre>switch(config)# hardware rate-limiter layer-3 glean 500</pre>	レイヤ 3 収集パケットのレート制限を設定します。範囲は 0 ～ 10,000 です。 特定の宛先へのトラフィックを受信するノードは、書き換え情報または宛先の背後にある物理層インターフェイスを認識しないため、トラフィックを転送できないことがあります。この間に、その宛先のデータパスに収集エントリをインストールすることができます。これはグローバルパント隣接関係へのポインタではない可能性があるため、予約済みモジュールまたはポート値を使用して、このようなパケットをスーパーバイザにパントします。この収集レートは、特定のレトリミッタを使用して制御できます。 Note CoPP ポリシーは、グローバルパント隣接のヒットにより CPU に転送される収集パケットのレートを制御します。レイヤ 3 収集ハードウェアレートリミッタは、sup-redirect access-list によって CPU にリダイレクトされる収集パケットの数を制限します。これは、パケットが不明な VTEP から受信される VXLAN 環境などの特殊なケースで使用されます。
ステップ 7	hardware rate-limiter layer-3 multicast local-groups packets [module module [port start end]] Example: <pre>switch(config)# hardware rate-limiter layer-3 multicast local-groups 300</pre>	最短パスツリー (SPT) の参加開始用にパントされたレイヤ 3 マルチキャストデータパケットのレート制限を設定します。0 ～ 10,000 です。
ステップ 8	hardware rate-limiter span-egress rate [module module] Example: <pre>switch(config)# hardware rate-limiter span-egress 123</pre>	出力トラフィックの SPAN のレート制限を設定します。範囲は 0 ～ 100000000 です。 Note sFlow と SPAN 出力レートリミッタの両方を設定しないでください。

	Command or Action	Purpose
ステップ 9	(Optional) show hardware rate-limiter [access-list-log bfd exception fex layer-3 glean layer-3 multicast local-groups module module] Example: switch# show hardware rate-limiter	レート制限の設定を表示します。モジュールの範囲は1 ～ 30 です。
ステップ 10	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

レート制限のモニタリング

レート制限をモニタリングできます。

Procedure

	Command or Action	Purpose
ステップ 1	show hardware rate-limiter [access-list-log bfd exception fex layer-3 glean layer-3 multicast local-groups span-egress module module] Example: switch# show hardware rate-limiter access-list-log	レート制限統計情報を表示します。

レート制限統計情報のクリア

レート制限統計情報をクリアできます。

Procedure

	Command or Action	Purpose
ステップ 1	clear hardware rate-limiter { all access-list-log bfd exception fex layer-3 glean layer-3 multicast local-groups span-egress [module module]} }	レート制限統計情報をクリアします。

	Command or Action	Purpose
	Example: switch# clear hardware rate-limiter access-list-log	

レート制限の設定の確認

レート制限の設定情報を表示するには、次の作業を行います。

コマンド	目的
show hardware rate-limiter [access-list-log bfd exception fex layer-3 glean layer-3 multicast local-groups span-egress module module]	レート制限の設定を表示します。

レート制限の設定例

次に、アクセス リスト ロギングのためにスーパーバイザ モジュールにコピーされるパケットのレート制限を設定する例を示します。

```
switch(config)# hardware rate-limiter access-list-log
switch(config)# show hardware rate-limiter access-list-log
Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated since last clear counters
```

```
Module: 4
R-L Class          Config          Allowed          Dropped          Total
+-----+-----+-----+-----+-----+
+
+ access-list-log   100             0                 0                 0

Port group with configuration same as default configuration
Eth4/1-36
```

```
Module: 22
R-L Class          Config          Allowed          Dropped          Total
+-----+-----+-----+-----+-----+
+
+ access-list-log   100             0                 0                 0

Port group with configuration same as default configuration
Eth22/1-0
```

次に、SPAN 出力レート リミッタが sFlow と競合する例を示します。

```
switch(config)# hardware rate-limiter span-egress 123
Warning: This span-egress rate-limiter might affect functionality of sFlow
switch(config)# show hardware rate-limiter span-egress
Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated since Module: 1
R-L Class          Config          Allowed          Dropped          Total
+-----+-----+-----+-----+-----+
+
+ L3 glean          100             0                 0                 0
```

```

L3 mcast loc-grp      3000      0      0      0
access-list-log       100        0      0      0
bfd                   10000      0      0      0
exception             50         0      0      0
fex                   3000      0      0      0
span                  50         0      0      0
dpss                  6400      0      0      0
span-egress           123        0      0      0
<<configured

```

レート制限に関する追加情報

ここでは、レート制限の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	Cisco NX-OS ライセンス ガイド



第 27 章

MACsec を構成します

この章では、Cisco NX-OS デバイスで MACsec を構成する方法について説明します。

- [MACsec について \(727 ページ\)](#)
- [MACsec のライセンス要件 \(729 ページ\)](#)
- [MACsec の注意事項と制約事項 \(729 ページ\)](#)
- [MACsec の有効化 \(736 ページ\)](#)
- [MACsec の無効化 \(737 ページ\)](#)
- [MACsec キーチェーンとキーの設定 \(737 ページ\)](#)
- [MACsec パケット番号の消耗 \(740 ページ\)](#)
- [MACsec フォールバック キーの設定 \(740 ページ\)](#)
- [MACsec ポリシーの設定 \(741 ページ\)](#)
- [MACsec EAP の構成 \(744 ページ\)](#)
- [QKD と MACsec での SKIP の統合 \(745 ページ\)](#)
- [設定可能な EAPOL の宛先とイーサネット タイプについて \(754 ページ\)](#)
- [MACsec 設定の確認 \(756 ページ\)](#)
- [MACsec 統計の表示 \(758 ページ\)](#)
- [MACsec の設定例 \(761 ページ\)](#)
- [XML の例 \(765 ページ\)](#)
- [MIB \(773 ページ\)](#)
- [関連資料 \(773 ページ\)](#)

MACsec について

Media Access Control Security (MACsec) である IEEE 802.1AE と MACsec Key Agreement (MKA) プロトコルは、イーサネットリンク上でセキュアな通信を提供します。次の機能があります。

- ライン レート暗号化機能を提供します。
- レイヤ 2 で強力な暗号化を提供することで、データの機密性を確保します。
- 整合性チェックを行い、転送中にデータを変更できないことを保証します。

- 中央集中型ポリシーを使用して選択的に有効にでき、MACsec 非対応コンポーネントがネットワークにアクセスできるようにしながら、必要に応じて適用することができます。
- レイヤ 2 ではホップバイホップ ベースでパケットを暗号化します。これにより、ネットワークは、既存のポリシーに従って、トラフィックを検査、モニタ、マーク、転送できます（エンドツーエンド レイヤ 3 暗号化技術とは異なり、パケットの内容をネットワーク デバイスから非表示にします）

キー ライフタイムおよびヒットレス キー ロールオーバー

MACsec キー チェーンには、キー ID とオプションのライフタイムが設定された複数の事前共有キー（PSK）を含めることができます。キーのライフタイムでは、キーがいつ有効になり、いつ期限切れになるかが指定されます。ライフタイム設定が存在しない場合は、無期限のデフォルトライフタイムが使用されます。ライフタイムが設定されていて、ライフタイムの期限が切れると、MKA はキー チェーン内で次に設定された事前共有キーにロールオーバーします。キーのタイム ゾーンは、ローカルまたは UTC を指定できます。デフォルトの時間帯は UTC です。

MACsec キーチェーンを設定するには、[MACsec キーチェーンとキーの設定（737 ページ）](#)を参照してください。

（キーチェーン内で）2 番目のキーを設定し、最初のキーのライフタイムを設定することで、そのキーチェーン内の 2 番目のキーにロールオーバーできます。最初のキーのライフタイムが期限切れになると、リスト内の次のキーに自動的にロールオーバーします。同一のキーがリンクの両側で同時に設定されていた場合、キーのロールオーバーはヒットレスになります。つまり、キーはトラフィックを中断せずにロールオーバーされます。

フォールバック キー

MACsec セッションは、キー/キー名（CKN）のミスマッチで、またはスイッチとピア間のキーの期限が切れて、失敗する可能性があります。MACsec セッションが失敗した場合、フォールバック キーが設定されていれば、フォールバック セッションが引き継ぐことができます。フォールバック セッションは、プライマリ セッションの障害によるダウンタイムを防止し、ユーザが障害の原因となっている主要な問題を修正できるようにします。フォールバック キーは、プライマリ セッションの開始に失敗した場合のバックアップ セッションも提供します。この機能はオプションです。

MACsec フォールバックキーを設定するには、[MACsec フォールバック キーの設定（740 ページ）](#)を参照してください。

MACsec のライセンス要件

製品	ライセンス要件
Cisco NX-OS	MACsec にはセキュリティ ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細の取得および適用の方法については、 Cisco NX-OS ライセンス ガイド を参照してください。

MACSec の注意事項と制約事項

MACsec に関する注意事項と制約事項は次のとおりです。

- MACsec は、次のインターフェイス タイプでサポートされます。
 - レイヤ 2 スイッチポート（アクセスとトランク）
 - レイヤ 3 ルーテッド インターフェイス（サブインターフェイスなし）



(注) レイヤ 3 ルーテッド インターフェイスで MACsec を有効にすると、そのインターフェイスで定義されているすべてのサブインターフェイスでも暗号化が有効になります。ただし、同じレイヤ 3 ルーテッド インターフェイスのサブインターフェイスのサブセットで MACsec を選択的に有効にすることはサポートされていません。

- レイヤ 2 およびレイヤ 3 ポート チャネル（サブインターフェイスなし）
- Cisco Nexus リリース 10.2 (1) F以降では、Cisco Nexus 9000 ToR スイッチの MACSec セキュリティタグ（SecTAG）からセキュアチャネル識別子（SCI）を無効にできます。
 - FX2 および FX3 プラットフォームでサポートされています。
 - XPN 暗号スイートを使用する FX プラットフォームでのみサポートされます。
- Cisco Nexus ToR スイッチを Cisco NX-OS リリース 9.3.7 から Cisco NX-OS リリース 9.3.6 以前のリリースにダウングレードする場合、MACsec はサポートされません。
- MKA は、MACsec でサポートされている唯一のキー交換プロトコルです。Security Association Protocol（SAP）はサポートされていません。
- リンクレベルフロー制御（LLFC）およびプライオリティフロー制御（PFC）は、MACsec ではサポートされません。
- 同じインターフェイスに対する複数の MACsec ピア（異なる SCI 値）はサポートされません。

- **macsec shutdown** コマンドを使用して MACsec を無効にすると、MACsec 設定を保持できません。
- MACsec セッションは、最新の Rx および最新の Tx フラグが Tx SA のインストール後に最初に廃止されたキーサーバからのパケットを受け入れるのに寛容です。MACsec セッションは、セキュアな状態に収束します。
- Cisco NX-OS リリース 9.2(1) 以降では、次の設定が可能です。
 - ポリシーがインターフェイスによって参照されている間に、MACsec ポリシーを変更できるようにします。
 - ブレークアウト ポートの異なるレーン間で異なる MACsec ポリシーを許可します。
- Cisco Nexus リリース 9.2(1) 以降、MACsec は Cisco Nexus 93180YC-FX スイッチでサポートされます。
- Cisco Nexus リリース 9.3(1) 以降、MACsec は Cisco Nexus 9348GC-FXP スイッチでサポートされます。これらのスイッチで MACsec を使用する場合は、次の制限が適用されます。
 - Cisco Nexus 9348GC-FXP : MACsec は 6 ポート（ポート 49 ～ 54）でサポートされません。
- Cisco Nexus リリース 9.3(1) 以降では、ポートチャネル インターフェイスに MACsec 設定を直接適用することはできません。ただし、MACsec 設定をポートチャネルメンバー ポートに直接適用できます。これは、NX-OS と vPC ポートチャネルの両方に適用されます。
- Cisco Nexus リリース 9.3(3) 以降、MACsec は Cisco Nexus 93216TC-FX2、Cisco Nexus 93360YC-FX2 でサポートされています。
- Cisco NX-OS リリース 9.3(5) 以降、MACsec は次のスイッチおよびライン カードでサポートされます。
 - Cisco Nexus 93180YC-FX3S スイッチ : MACsec はすべてのポートでサポートされません。
 - Cisco Nexus X9732C-FX および X9788TC-FX ライン カード
- Cisco Nexus 9300-FX スイッチおよび 9700-FX ライン カード
 - MACsec は 1G ポートではサポートされていません。
 - さらに、MAC ブロックに 1G ポートが含まれている場合、MACsec はその MAC ブロック内のポートではサポートされません。
 - MACsec 対応の 9700-FX ライン カードで 1G 光ファイバを使用する場合は、診断モードを「最小」に変更することを推奨します。診断の詳細については、『**Cisco Nexus 9000 シリーズ NX-OS システム管理コンフィギュレーション ガイド**』の「[起動時の診断](#)」のセクションを参照してください。
- Cisco Nexus 9300-FX2 スイッチの場合 :

- MACsec は、1G ポートでサポートされます（ポートが非 BV または非リタイマー ポートである場合）。

リタイマー ポートの詳細については、『Cisco Nexus 9000 シリーズ NX-OS インターフェイス構成ガイド』の「サポートされているリタイマー ポート」セクションを参照してください。

- Cisco NX-OS リリース 10.1(1)以降、Cisco Nexus 93180YC-FX3 および 93108TC-FX3P スイッチは、1G および 10G ポート速度を含むすべてのポート速度で MACsec をサポートします。
- MACsec は、Cisco Nexus 93240YC-FX2、9336C-FX2、93108TC-FX、93180YC-FX スイッチ、および X9736C-FX および X9732C-EXM ライン カードでサポートされています。
- 1G は BV ポートまたはリタイマー ポートではサポートされません。リタイマー ポートの詳細については、『Cisco Nexus 9000 シリーズ NX-OS インターフェイス構成ガイド』の「サポートされているリタイマー ポート」セクションを参照してください。
- Cisco NX-OS リリース 9.3(7)以降、QSA が使用されている場合、MACsec は Cisco Nexus 9336C-FX2 スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(1)以降、QSA が使用されている場合、MACsec は Cisco Nexus 9336C-FX2、9336C-FX2-E スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(2)以降では、QSA が使用されている場合、MACsec は Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされます。
- Cisco Nexus リリース 10.1(1)以降、MACsec は Cisco Nexus 9336C-FX2-E でサポートされます。
- Cisco Nexus リリース 10.2(1)F 以降、MACsec は Cisco Nexus X9716D-GX でサポートされます。
- Cisco NX-OS リリース 10.2(1q)F 以降、MACsec は Cisco Nexus 9332D-GX2B スイッチのポート 25 ～ 32 でサポートされます。
- Cisco NX-OS リリース 10.2(2)F 以降、MACsec は Cisco Nexus N9K-C9348D-GX2A スイッチの 1 ～ 48 ポートでサポートされます。
- Cisco NX-OS リリース 10.2(2)F 以降、MACsec は 10G QSA リンクを備えた Cisco Nexus X9736C-FX、および X9736Q-FX ラインカードをサポートします。
- Cisco NX-OS リリース 10.2(2)F 以降、MACsec は Cisco Nexus 9364D-GX2A スイッチのポート 1 ～ 16 でサポートされます。
- Cisco Nexus 9332D-GX2B、9364D-GX2A および 9348D-GX2A スイッチ と Cisco Nexus X9836DM-A ライン カードでは、ポートで MACsec が設定されていても設定されていなくても、MACsec セキュリティ ポリシー タイプに関係なくポートフラップが発生します。
- Cisco NX-OS リリース 10.3(1)F 以降、MACsec は Cisco Nexus 9800 プラットフォーム スイッチの Cisco Nexus X9836DM-A ライン カードでサポートされます。

- Cisco NX-OS リリース 10.3(2)F 以降、MACsec は、LEM モジュール X9400-16W および X9400-8D を搭載した Cisco Nexus 9408 スイッチのサポートされているすべてのリンクでサポートされます。
- Cisco Nexus リリース 10.3(3)F 以降、暗号キーの適用機能には、Cisco Nexus 9332D-GX2B、9336C-FX2、93180YC-FX、および 93180YC-FX3 スイッチで、最も優先される暗号スイートから最も優先されない暗号スイートまでを定義するオプションを提供します。ただし、以下の制限があります。
 - 暗号キーの適用機能は、キーサーバとして優先順位が付けられている場合にのみ効果的に機能します。それ以外の場合は、**init** または **pending** 状態のセッションになります。
 - 暗号キーの適用機能は、2つのピア間の直接接続でのみサポートされます。MKA セッションが複数のピアとの間で行われている場合、この機能は正常に動作しません。
 - ピア暗号スイート許可の変更中、最も優先されるサポートされている暗号スイートでセッションが保護されない場合があります。
 - 任意のセキュリティで保護された MACsec セッションで使用されるポリシーで暗号を **any** から強制ピア暗号に変更する場合は、期待される動作が実現されるよう、暗号を変更した後にポートをフラップすることをお勧めします。フラッピングが行われない場合、セッションはスイッチ上保護されていると表示されますが、ピアセッションではサポートされていない暗号で保留中と表示されます。また、サポートされている暗号が強制ピア暗号スイートに存在する場合でも、セッションがすぐに保護されない可能性があります。
 - 許可されたピア暗号スイート (APSC) を空にすることはできません。また、重複させることはできません。
 - **cipher-suite** コマンドと **cipher-suite enforce-peer** コマンドは、同じポリシーの下で共存できません。
 - **SAK** 暗号適用タイマーがタイムアウトして次の暗号スイートを試行するのを待機している間、データおよび制御トラフィックでは、セキュアモードであっても、一方向のトラフィックの中断が発生する可能性があります。中断は、セッションが保護された場合にのみ回復します。
- Cisco Nexus リリース 10.4(1)F 以降、MACsec は Cisco Nexus 9348GC-FX3 および 9348GC-FX3PH スイッチのポート 49 ~ 54 でサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、MACsec は Cisco Nexus 9332D-H2R プラットフォームスイッチのすべての前面パネルポート（ポート 1 ~ 32）でサポートされます。ただし、MACsec は Ethernet1/33 および Ethernet1/34 ではサポートされません。
- Cisco Nexus リリース 10.4(2)F 以降、MACsec は以下のスイッチでサポートされます。
 - Cisco Nexus 93400LD-H1 のすべてのポート。
 - Cisco Nexus 93108TC-FX3 のポート 49 ~ 54

- Cisco Nexus リリース 10.4(3)F 以降、MACsec は Cisco Nexus 9364C-H1 スイッチのポート 49 ～ 64 でサポートされます。
- MACsec は、Nexus 9600-R/R2 ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチではサポートされません。
- MACsec 機能が設定されている場合、無停止 ISSU はサポートされません。

キーチェーンの制限：

- MACsec キーのオクテット文字列は上書きできません。代わりに、新しいキーまたは新しいキーチェーンを作成する必要があります。
- **end** または **exit** を入力すると、キーチェーンの新しいキーが設定されます。エディタモードのデフォルトのタイムアウト値は 6 秒です。キーがキー オクテット文字列または 6 秒間の送信ライフタイムで設定されていない場合、MACsec セッションを起動するために不完全な情報が使用され、セッションが承認保留状態のままになる可能性があります。設定の完了後に MACsec セッションがコンバージされない場合は、ポートをシャットダウン/非シャットダウンすることをお勧めします。
- 指定したキーチェーンでは、キーの有効期間を重複させて、有効なキーの不在期間を避ける必要があります。キーがアクティブ化されない期間が発生すると、セッション ネゴシエーションが失敗し、トラフィックがドロップされる可能性があります。MACsec キーロールオーバーでは、現在アクティブなキーの中で最も遅い開始時刻のキーが優先されます。
- セキュリティ アドオン ライセンスを使用するためには、MACsec 機能を有効にすることに加えて、少なくとも 1 つのインターフェイスで MACsec キーチェーンを設定する必要があります。

フォールバックの制限：

- MACsec セッションが古いプライマリキーで保護されている場合、最新のアクティブなプライマリキーが一致しない場合、フォールバックセッションには進みません。そのため、セッションは古いプライマリキーで保護されたままになり、ステータスが古い CA のキー再生成として表示されます。プライマリ PSK の新しいキーの MACsec セッションは init 状態になります。
- フォールバック キーチェーンでは、無期限のキーを 1 つだけ使用します。複数のキーはサポートされていません。
- フォールバック キーチェーンで使用されるキー ID (CKN) は、プライマリ キーチェーンで使用されるキー ID (CKN) のいずれとも一致しないようにしてください。
- 一度設定すると、インターフェイスのすべての MACsec 設定が削除されない限り、インターフェイスのフォールバック設定は削除できません。

MACsec ポリシーの制限：

- MACsec セッションがセキュアになる前に、BPDU パケットを送信できます。

レイヤ 2 トンネリング プロトコル (L2TP) の制約事項 :

- MACsec は、dot1q トンネリング (スイッチポート モード dot1q-tunnel) または L2TP 用に設定されたポートではサポートされません。
- 非ネイティブ VLAN のトランク ポートで STP が有効になっている場合、L2TP は機能しません。

統計情報の制限 :

- MACsec モードと非 MACsec モード (通常のポート シャットダウン/非シャットダウン) の間の移行中に発生する CRC エラーはほとんどありません。
- Secy 統計情報は累積され、30 秒ごとにポーリングされます。
- IEEE8021-SECY-MIB OID secyRxSASStatsOKPkts、secyTxSASStatsProtectedPkts、および secyTxSASStatsEncryptedPkts は最大 32 ビットのカウンタ値しか伝送できませんが、トラフィックは 32 ビットを超える可能性があります。
- Cisco Nexus 9300-FX3 プラットフォーム スイッチでは、**show macsec secy statistics** コマンドは、レート統計情報と、Cisco NX-OS リリース 10.4(2)F 以降のレート関連の「CISCO-SECY-EXT-MIB」OID をサポートします。
 - cseSecyIfRxUncontrolledPktRate、
 - cseSecyIfRxControlledPktRate、
 - cseSecyIfTxUncontrolledPktRate、
 - cseSecyIfTxControlledPktRate
 - cseSecyIfRxControlledOctetRate
 - cseSecyIfTxControlledOctetRate
 - cseSecyIfRxUnControlledOctetRate
 - cseSecyIfTxUnControlledOctetRate

相互運用性の制限 :

- N9K-X9732C-EXM と他のピア スイッチ (他のシスコおよびシスコ以外のスイッチ) の相互運用性は、XPN 暗号スイートでのみサポートされます。
- MACsec ピアは、AES_128_CMAC 暗号化アルゴリズムを使用するために同じ Cisco NX-OS リリースを実行する必要があります。以前のリリースと Cisco NX-OS リリース 9.2(1) の間の相互運用性のために、AES_256_CMAC 暗号化アルゴリズムでキーを使用する必要があります。
- 以前のリリースと Cisco NX-OS リリース 9.2(1) の間の相互運用性を確保するために、MACsec キーが 32 オクテット未満の場合は、MACsec キーにゼロを付加します。
- Cisco NX-OS スイッチでは、すべてのインターフェイスで代替 MAC アドレスとイーサネット タイプの一意の組み合わせを 1 つだけ設定できます。

- Cisco NX-OS リリース 9.3(1) から、ポートチャネル メンバーごとの MACsec 設定サポートのない Cisco NX-OS リリースにダウングレードしようとした場合、スイッチの同じポートチャネル インターフェイスのメンバーに、相互に異なる MACsec 設定があった場合、次のエラー メッセージが表示されることがあります。

ポートチャネル メンバーに非対称 macsec 設定が存在します。メンバー間で対称 macsec 設定を使用して、中断のない ISSU を実行してください。

- MACsec のソフトウェア サポートは、Cisco Nexus X9400-22L LEM カードでは使用できません。

EAPOl には、次の注意事項と制約事項があります。

- 転送エンジンの同じスライス内では、EAPOl ethertype と dot1q ethertype に同じ値を指定することはできません。
- EAPOl 設定を有効にするには、0 ～ 0x599 の範囲のイーサネット タイプの範囲が無効です。
- EAPOl 設定を有効にする場合、N9K-X9836DM-A ラインカードでサポートされる EAPOl mac アドレスは、0x0180c2000000 ～ 0x0180c20000ff の範囲のみです。
- EAPOl パケットの設定中は、次の組み合わせを使用しないでください。
 - MAC アドレス 0100.0ccd.cdd0 と ethertype
 - MAC アドレスと ethertype : 0xffff0、0x800、0x86dd
 - デフォルトの宛先 MAC アドレス 0180.c200.0003 とデフォルトのイーサネット タイプ 0x888e
 - 両方の MACsec ピアで異なる EAPOl DMAC アドレス。MACsec セッションは、MACsec ピアがローカルに設定された DMAC を使用して MKAPDU を送信している場合にのみ機能します。
- Cisco NX-OS リリース 10.2(1)F 以降、EAPOl は Cisco Nexus 9300-FX3 シリーズ スイッチでサポートされます。

Cisco Nexus 9336C-SE1 スイッチ上の MACsec のガイドラインと制限事項

Cisco Nexus 9336C-SE1 スイッチで MACsec 機能を使用する場合は、次のガイドラインと制限事項を確認してください。

Supported Features

- Cisco Nexus リリース 10.6 (1) F 以降、Cisco Nexus 9336C-SE1 スイッチは、40G/100G ポートで MACsec 機能をサポートします。
- スイッチの 36 個のポートはすべてインターフェイスブレイクアウトをサポートしており、MACsec 用に個別に構成できます。

制限事項

- Macsec SecY 統計情報は、出力セキュアアソシエーション (SA) カウンタに関連する統計情報をサポートしていません。出力統計データは常にゼロとして表示されます。

EAPOL 構成要件

- EAPOL 構成では、次の要件が満たされていることを確認します。
 - EAPOL MAC アドレスの範囲は 0180.C200.0000 ～ 0180.C200.00FF（最後のバイトは 0x00 ～ 0xFF）、EtherType は 0x600 ～ 0xFFFF の任意の値にできます。
 - EtherType がデフォルト値の 0x888E に設定されている場合、任意の MAC アドレスが許可されます。
 - ブロードキャスト MAC アドレスは、0x600 ～ 0xFFFF の範囲内の任意の EtherType 値で使用できます。

MACsec の有効化

MACsec および MKA コマンドにアクセスする前に、MACsec 機能を有効に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 例 : <pre>switch# configure terminal switch(config)#</pre>	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	feature macsec 例 : <pre>switch(config)# feature macsec</pre>	デバイスで MACsec および MKA を有効にします。
ステップ 3	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MACsec の無効化

Cisco NX-OS リリース 9.2(1) 以降では、MACsec 機能を無効にしても、この機能が非アクティブ化されるだけで、関連する MACsec 設定は削除されません。

MACsec の無効化には、次の条件があります。

- MACsec shutdown はグローバルコマンドであり、インターフェイス レベルでは使用できません。
- macsec shutdown、show macsec mka session/summary、show macsec mka session detail、および show macsec mka/secy statistics コマンドは、「Macsec is shutdown」メッセージを表示します。ただし、show macsec policy および show key chain コマンドは出力を表示します。
- 連続する MACsec ステータスが macsec shutdown から no macsec shutdown に変更された場合、またはその逆の場合は、ステータス変更の間に 30 秒の間隔が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	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	macsec shutdown 例 : switch(config)# macsec shutdown	デバイスの MACsec 設定を無効にします。 no オプションは、MACsec 機能を復元します。
ステップ 3	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。この手順は、スイッチのリロード後に MACsec をシャットダウン状態に維持する場合にのみ必要です。

MACsec キーチェーンとキーの設定

デバイスに MACsec キーチェーンとキーを作成できます。



(注) MACsec キーチェーンのみが MKA セッションをコンバージします。

始める前に

MACsec が有効であ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 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	(任意) [no] key-chain macsec-psk no-show 例 : <pre>switch(config)# key-chain macsec-psk no-show</pre>	show running-config および show startup-config コマンドの出力で、暗号化されたキーオクテット文字列をワイルドカード文字に置き換えて非表示にします。デフォルトでは、PSK キーは暗号化形式で表示され、簡単に復号化できます。このコマンドは、MACsec キーチェーンにのみ適用されます。 (注) キーオクテット文字列は、設定をファイルに保存するときに非表示になります (アスタリスクに変更)。その結果、このコマンドを設定して ASCII リロードまたは設定置換を実行すると、「key-octet-string」設定は保持されません。
ステップ 3	key chain name macsec 例 : <pre>switch(config)# key chain 1 macsec switch(config-macseckeychain)#</pre>	MACSec キーチェーンを作成して MACSec キーのセットを保持し、MACSec キーチェーン設定モードを開始します。
ステップ 4	key key-id 例 : <pre>switch(config-macseckeychain)# key 1000 switch(config-macseckeychain-macseckey)#</pre>	MACsec キーを作成し、MACsec キー設定モードを開始します。範囲は1〜32 オクテットで、最大サイズは 64 です。 (注) キーの文字数は偶数でなければなりません。
ステップ 5	key-octet-string octet-string cryptographic-algorithm {AES_128_CMAC AES_256_CMAC}	そのキーのオクテット スtring を設定します。octet-string 引数には、最大 64 文字の 16 進数文字を含めることがで

	コマンドまたはアクション	目的
	例 : <pre>switch(config-macseckeychain-macseckey) # key-octet-string abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm AES_256_CMAC</pre>	きます。オクテット キーは内部でエンコードされるため、show running-config macsec コマンドの出力にクリア テキストのキーが現れることはありません。 キーオクテット文字列には、次のものが含まれます。 • 0 暗号化タイプ - 暗号化なし（デフォルト） • 6 暗号化タイプ - 独自仕様（タイプ 6 暗号化）。詳細については、MACsec キーでのタイプ 6 暗号化の有効化（622 ページ）を参照してください。 • 7 暗号化タイプ - 最大 64 文字の、独自仕様 WORD キー オクテット 文 列 (注) AES_128_CMAC 暗号化アルゴリズムを使用するためには、MACsec ピアは同じ Cisco NX-OS リリースを実行する必要があります。以前のリリースと、Cisco NX-OS リリース 7.0(3)I7(2)以降のリリース間で相互運用できるようにするには、キーを AES_256_CMAC 暗号化アルゴリズムで使用する必要があります。
ステップ 6	send-lifetime 開始時間 duration 長さ 例 : <pre>switch(config-macseckeychain-macseckey) # send-lifetime 00:00:00 Oct 04 2016 duration 100000</pre>	キーの送信ライフタイムを設定します。デフォルトでは、デバイスは開始時間を UTC として扱います。 start-time 引数は、キーがアクティブになる日時です。duration 引数はライフタイムの長さ（秒）です。最大値は 2147483646 秒（約 68 年）です。
ステップ 7	(任意) show key chain name 例 : <pre>switch(config-macseckeychain-macseckey) # show key chain 1</pre>	キーチェーンの設定を表示します。

	コマンドまたはアクション	目的
ステップ 8	(任意) copy running-config startup-config 例 : <pre>switch(config-macseckeychain-macseckey) # copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MACsec パケット番号の消耗

各 MACsec フレームには 32 ビット パケット番号 (PN) が含まれており、特定のセキュリティ アソシエーション キー (SAK) に対して一意です。PN 消耗後 ($2^{32}-1$ の 75% に達した後)、SAK リキーは自動的に行われ、データ プレーン キーを更新し、PN を周囲に配置します。

たとえば、64 バイトの 10G フルライン レートでは、PN の枯渇により 216 秒ごとに SAK キー再生成が発生します。

これは、GCM-AES-PN-128 または GCM-AES-PN-256 暗号スイートを使用する場合に適用されます。

GCM-AES-XPB-128 または GCM-AES-XPB-256 暗号スイートが使用されている場合、SAK キー再生成は $2^{64}-1$ の 75% に達すると自動的に行われます (パケットの番号付けを消耗するのに数年かかります)。暗号スイートは macsec ポリシーで設定可能で、動作する暗号スイートはキー サーバ デバイスによって決定されます。

N9K-X9732C-EXM ライン カードで XPB 暗号スイートを使用することを推奨します。

MACsec フォールバック キーの設定

Cisco NX-OS リリース 9.2(1)以降では、プライマリセッションがスイッチとピア間のキー/キー名 (CKN) のミスマッチまたはキーの有効期限の結果として失敗した場合にバックアップセッションを開始するようにデバイスのフォールバック キーを設定できます。

始める前に

MACsec が有効になっており、プライマリおよびフォールバック キーチェーンとキー ID が設定されていることを確認します。「[MACsec キーチェーンとキーの設定](#)」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 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
	switch# configure terminal switch(config)#	
ステップ 2	interface <i>name</i> 例 : <pre>switch(config)# interface ethernet 1/1 switch(config-if)#</pre>	設定するインターフェイスを指定します。インターフェイスタイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。
ステップ 3	macsec keychain <i>keychain-name</i> policy <i>policy-name</i> fallback-keychain <i>keychain-name</i> 例 : <pre>switch(config-if)# macsec keychain kc2 policy abc fallback-keychain fb_kc2</pre>	キー/キー ID のミスマッチまたはキーの期限切れによる MACsec セッションの失敗後に使用するフォールバック キーチェーンを指定します。フォールバック キー ID は、プライマリ キーチェーンのキー ID と一致してはなりません。 フォールバック キーチェーン名を変更して同じコマンドを再発行することで、MACsec 設定を削除せずに、各インターフェイスのフォールバック キーチェーン設定を対応するインターフェイスで変更できます。 (注) コマンドは、フォールバック キーチェーン名を除き、インターフェイスの既存のコンフィギュレーション コマンドとまったく同じように入力する必要があります。 「MACsec キーチェーンとキーの設定」を参照してください。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MACsec ポリシーの設定

異なるパラメータを使用して複数の MACsec ポリシーを作成できます。しかし、1 つのインターフェイスでアクティブにできるポリシーは 1 つのみです。

始める前に

MACsec が有効であ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 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル構成モードを開始します。
ステップ 2	macsec policy name 例 : <pre>switch(config)# macsec policy abc switch(config-macsec-policy)#</pre>	MACsec ポリシーを作成します。
ステップ 3	(任意) [no] cipher-suite { { enforce-peer <allowed-peer-cipher-suite1> [allowed-peer-cipher-suite2> [allowed-peer-cipher-suite3> [allowed-peer-cipher-suite4>]] } <suite> } 例 : <pre>switch(config-macsec-policy)# cipher-suite enforce-peer GCM-AES-256 GCM-AES-256 GCM-AES-256 GCM-AES-256</pre>	次の暗号スイートの順序を、最も優先度の高いものから最も低いものへと構成します。セッションは、ピアでサポートされている最も優先される暗号スイート（GCM-AES-128、GCM-AES-256、GCM-AES-256、GCM-AES-256）で保護されます。 構成を解除するには、no フォームを使用するか、必要な順序設定で既存の順序を上書きします。 (注) - この機能を動作させるには、Cisco NX-OS スイッチがキー サーバーとして設定されていることを確認します。 cipher-suite enforce-peer コマンドで定義された暗号スイートのセットに含まれていない暗号スイートをピアがサポートしている場合、MKA セッション状態は保護されず、保留状態になります。

	コマンドまたはアクション	目的
ステップ 4	(任意) [no] include-sci 例 : <pre>switch(config-macsec-policy)# no include-sci</pre>	SecTAG の SCI を無効にします。デフォルトでは、SCI は常に有効になっています。 (注) パケットのドロップを防ぐには、SCI タギング設定が入力ポイントと出力ポイントの両方で一貫していることを確認します。
ステップ 5	(任意) no protocol lldp encrypted 例 : <pre>switch(config-macsec-policy)# no protocol lldp encrypted</pre>	must-secure ポリシーが設定されたポートの MACsec 構成がセキュアでない場合でも、LLDP パケットを許可します。Cisco NX-OS リリース 10.5(3)F より前では、must-secure ポリシーを備えたポートの MACsec 構成がセキュアな状態でない場合、LLDP パケットはドロップされていました。 (注) このコマンドは、Cisco Nexus 9300-GX2、H2R、H1 シリーズ スイッチのみでサポートされます。
ステップ 6	(任意) key-server-priority number 例 : <pre>switch(config-macsec-policy)# key-server-priority 0</pre>	キー交換中はピア間の接続が解除されるように、キー サーバのプライオリティを設定します。範囲は0（最高）〜255（最低）で、デフォルト値は16です。
ステップ 7	(任意) security-policy name 例 : <pre>switch(config-macsec-policy)# security-policy should-secure</pre>	次のいずれかのセキュリティポリシーを設定して、データおよび制御パケットの処理を定義します。 • must-secure : MACsec をヘッダー持たないパケットはドロップされます。 • should-secure : MACsec ヘッダーを持たないパケットも許可されます。これはデフォルト値です。
ステップ 8	(任意) window-size number 例 :	インターフェイスが、設定されたウィンドウサイズ未満のパケットを受け入れないように、再生保護ウィンドウを

	コマンドまたはアクション	目的
	<code>switch(config-macsec-policy) # window-size 512</code>	設定します。範囲は 0 ～ 596000000 です。
ステップ 9	(任意) sak-expiry-time time 例 : <pre>switch(config-macsec-policy) # sak-expiry-time 100</pre>	SAK キー再生成を強制する時間を秒単位で設定します。このコマンドを使用して、セッションキーを予測可能な時間間隔に変更できます。デフォルトは 0 です。 (注) 10.5(3)F リリースより前は、SAK の有効期限の最小時間は 60 秒でした。 10.5(3)F リリース以降、最小時間 30 秒がサポートされています。
ステップ 10	(任意) conf-offset name 例 : <pre>switch(config-macsec-policy) # conf-offset CONF-OFFSET-0</pre>	暗号化を開始するレイヤ 2 フレームの機密性オフセットの 1 つとして、CONF-OFFSET-0、CONF-OFFSET-30、または CONF-OFFSET-50 のいずれかを設定します。このコマンドは、中間スイッチがパケットヘッダー {dmac、smac、etype} を MPLS タグのように使用するために必要です。
ステップ 11	(任意) show macsec policy 例 : <pre>switch(config-macsec-policy) # show macsec policy</pre>	MACSec ポリシー設定を表示します。
ステップ 12	(任意) copy running-config startup-config 例 : <pre>switch(config-macsec-policy) # copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

MACsec EAP の構成

Cisco NX-OS リリース 10.4(1)F 以降では、802.1X 認証に MACsec EAP プロファイルを使用できます。

始める前に

- Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

- MACsec コマンドを設定し、should-secure（デフォルト）または must-secure macsec ポリシーを指定します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 ethernet slot/port 例 : <pre>switch(config)# interface ethernet 1/30 switch(config-if)#</pre>	設定するインターフェイスを選択し、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] macsec eap policy policy name 例 : <pre>switch(config-if)# macsec eap policy P1 switch(config-eap-profile)#</pre>	MACsec eap プロファイルを作成します。 コマンドの no フォームは、MACsec eap プロファイルを無効にするために使用されます。
ステップ 4	[no] dot1x supplicant eap profile eap profile name } 例 : <pre>switch(config-if)# dot1x supplicant eap profile</pre>	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。 サプリカントが使用する eap プロファイルを設定します。

QKD と MACsec での SKIP の統合

量子安全暗号化について

量子コンピューティングの最近の進歩により、さまざまな暗号化アルゴリズムの脆弱性が明らかになっており、将来のアプリケーションでの安全性は保証されていません。計算の複雑さに依存する RSA（素因数分解）および DHE（離散対数）公開鍵アルゴリズムには、現在、Shor または Grover のアルゴリズムを使用する量子コンピュータによって解決されるリスクがあります。

その結果、通信する当事者間で共有秘密キーを確立することが、重要な課題になっています。この問題を回避するには、量子安全アルゴリズムを構成するか、量子キー配布（QKD）を実装します。

QKD と Secure Key Integration Protocol の統合について

Secure Key Integration Protocol (SKIP) プロトコルをスイッチに統合すると、外部量子デバイスとの通信を確立できます。この機能強化により、スイッチ間でMACsec暗号キーを交換する際に Quantum Key Distribution (QKD) デバイスを使用できるようになります。

QKD は量子物理学の原理に基づいて動作し、光子の量子状態を利用して光リンク経由で情報をエンコードおよび共有します。さらに、認証された従来のチャネルが、測定値の共有に使用されます。量子状態の変化は、通信チャネルの2つのエンドパーティがキーの傍受を検出するのに役立ちます。

QKDは、暗号解読や量子コンピューティングが将来的に進歩しても、量子攻撃に対抗できる、セキュアなキー交換メカニズムです。QKD は、検出された脆弱性に基づく継続的な更新を必要としません。

ポスト量子事前共有キー (PPK)

事前共有キーに十分なエントロピーがあり、疑似乱数関数 (PRF) 、暗号化、および認証変換が量子セキュアである場合、事前共有キーに基づくセッションキーは、量子攻撃に対して脆弱ではありません。このようにして得られるシステムは、今日の古典的な攻撃者や量子コンピュータを使用する将来の攻撃者に対してセキュアであると考えられます。

注意事項と制約事項

QKD と MACsec 通信用の SKIP の統合には、次の注意事項と制限事項があります。

- Cisco NX-OS リリース 10.4 (3) F 以降では、次の Cisco Nexus スイッチで Secure Key Integration Protocol がサポートされています。
 - N9K-C9348GC-FXP
 - N9K-C93216TC-FX2
 - N9K-C93360YC-FX2
 - N9K-C9336C-FX2
 - N9K-C9348GC-FX3
 - N9K-C9348D-GX2A
 - N9K-C9332D-H2R
- SKIP プロトコルは、ポイントツーポイント MACsec リンク暗号化のシナリオでのみ使用できます。
- SKIP プロトコルは、MACsec 暗号化をサポートするインターフェイスでのみ使用できます。
- スイッチに HTTPS 接続が確立されている場合は、管理インターフェイスを介して QKD サーバーにアクセスできることを確認します。

- MACsec ピアが 2 つの異なる QKD サーバに接続されている場合、QKD サーバはキーを同期して MKA セッションを確立します。この同期により、MACsec キー（CKN）とキー 스트リング（CAK）が両端で同じになります。
- セキュアな Transport Layer Security（TLS）接続を確立し、相互認証を有効にするには、スイッチにトラストポイント証明書をインストールする必要があります。これらの証明書により、スイッチはサーバからキーを取得できます。詳細については、『Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド』の [PKI の構成](#) を参照してください。
- MACsec PPK セッションと EAP-TLS セッションは、同じのインターフェイスではサポートされません。
- スイッチは、スイッチごとに 1 つの QKD サーバーと 1 つの QKD プロファイルにのみ接続できます。
- SKIP プロトコルの場合、1 つの remoteSystemID のみがサポートされます。
- QKD 接続の場合、IPv6 はサポートされていません。
- QKD キーを交換する MACsec ピアは、Cisco NX-OS スイッチである必要があります。
- MACsec セッションが確立されると、QKD プロファイルを変更すると、**MUST SECURE MACSEC** モードでトラフィックが失われます。
- KME サーバーから取得された QKD キーを使用して MACsec セッションが確立されると、QKD プロファイルの一部であるトラストポイントの変更は、現在のセッションに影響しません。
- 機能応答では、remoteSystemID 属性は必須です。
- Cisco NX-OS リリース 10.5（2）F 以降では、以下の注意事項と制限事項を持つプライマリ PPK に障害が発生した場合にセキュアな MKA セッションを確立するために、PSK サポートへの QKD MACsec フォールバックが提供されます。
 - PPK が構成されている場合は、PSK が最初に構成されていることを確認します。
 - PPK モードは、PSK のキーチェーン フォールバック メソッドをサポートしていません。
 - MACsec セッションが PPK モードで保護されている場合、QKD サーバがダウンしたり切断されたりした場合、または cryptopqc 機能が削除された場合、SAK の有効期限のタイムアウトまたは PN の枯渇などキー再生成イベントがトリガされるまで、現在の PPK セッションとキーが引き続き維持され、使用されます。その後、PPK セッションはセキュアな PSK モードにフォールバックします。ただし、PPK 暗号化 QKD プロファイルが MACsec ポリシーから削除されると、PPK セッションはすぐに PSK モードにフォールバックします。

SKIP を使用したポイントツーポイント MACsec リンク暗号化の設定

ポイントツーポイント MACsec リンク暗号化では、スイッチで SKIP を使用してセキュアな暗号化を確立します。この暗号化は、ピアスイッチの2つのインターフェイス間で設定されるもので、QKD デバイスネットワークの支援を必要とします。スイッチネットワークの代わりに、QKD ネットワークが MACsec 暗号キーを共有します。したがって、スイッチがピア スイッチ インターフェイス間に MACsec リンクを作成する必要がある場合、スイッチは外部 QKD デバイスに接続し、キーを要求します。外部 QKD デバイスは、キー ID とキーで構成されるキーペアを生成します。

キー ID は、キーの一意の ID 文字列として機能します（共有秘密）。QKD デバイスはキー ID とキーの両方をスイッチと共有しますが、スイッチはキー ID のみをピアと共有します。ピアスイッチは、このキー ID を使用して、QKD デバイスから暗号キーを取得します。したがって、量子ネットワークは常に暗号キーをセキュアに通信します。

ポスト量子暗号化の有効化

始める前に

- MACsec 事前共有キー（PSK）を設定します。
- PPK モードで MACsec を設定します。
- 外部 QKD デバイス ネットワーク。
- QKD サーバー CA をスイッチのトラストポイントに追加し、QKD サーバー ルート CA 証明書をスイッチにインポートします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal 例： switch# configure terminal switch(config)#	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	switch(config)# feature cryptopqc 例： switch(config)# feature cryptopqc	スイッチでポスト量子暗号化（cryptopqc）を有効にします。
ステップ 3	（任意） switch(config)# copy running-config startup-config 例： switch(config)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

MACsec および MKA 機能の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal 例 : switch# configure terminal switch(config)#	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	switch(config)# feature macsec 例 : switch(config)# feature macsec	スイッチで MACsec および MKA を有効にします。
ステップ 3	(任意) switch(config)# copy running-config startup-config 例 : switch(config)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

量子キー配布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	switch (config)# crypto qkd profilename 例 : switch(config)# crypto qkd profile ppk1	ppk1 という名前の QKD プロファイルを作成します。
ステップ 2	switch (config)# kme server<hostname/IP> port portnumber 例 : switch(config-crypto-qkd-profile)# kme server 172.0.0.2 port 6000	キー管理エンジン (KME) /QKD サーバーの IP と TCP ポート番号を設定します。 (注) ポート番号はオプションです。デフォルトでは、ポート番号は 443 です。
ステップ 3	switch(config)# transport tls authentication-type trustpoint<trustpoint name> 例 :	CA (認証局) トラストポイントを設定します。トラストポイントを作成するには、「PKI の設定」の項を参照してください。

	コマンドまたはアクション	目的
	<code>switch(config-crypto-qkd-profile) # transport tls authentication-type trustpoint tp1</code>	
ステップ 4	(任意) <code>switch(config) # copy running-config startup-config</code> 例 : <code>switch(config) # copy running-config startup-config</code>	リブートおよびリスタート時に実行コン フィギュレーションをスタートアップ コンフィギュレーションにコピーして、 変更を継続的に保存します。

MACsec および MKA 機能の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch(config) # macsec policy<name></code> 例 : <code>switch(config) # [no] macsec policy test-policy</code>	MACsec ポリシーを作成します。
ステップ 2	<code>switch(config) # ppk crypto-qkd-profile<name></code> 例 : <code>switch(config-macsec-policy) # [no] ppk crypto-qkd-profile ppk1</code>	PPK プロファイル名を構成します。
ステップ 3	(任意) <code>switch(config) # copy running-config startup-config</code> 例 : <code>switch(config) # copy running-config startup-config</code>	リブートおよびリスタート時に実行コン フィギュレーションをスタートアップ コンフィギュレーションにコピーして、 変更を継続的に保存します。

設定例

次に、QKD プロファイルの設定と、設定された詳細の表示の例を示します。

• QKD プロファイルの設定

```
switch(config) # feature cryptopqc
switch(config) #
switch(config) # crypto qkd profile ppk1
switch(config-crypto-qkd-profile) # kme server 168.20.1.2 port 5000
switch(config-crypto-qkd-profile) # transport tls authentication-type trustpoint tp1
switch(config-crypto-qkd-profile) # end
switch#
```

- QKD 設定の表示

```
switch# show running-config cryptopqc
!Command: show running-config cryptopqc
!Running configuration last done at: Mon Jan 29 22:19:16 2024
!Time: Mon Jan 29 22:19:35 2024
version 10.4(3) Bios:version 05.51
feature cryptopqc
crypto qkd profile ppk1
kme server 168.20.1.2 port 5000
transport tls authentication-type trustpoint tp1
switch#
```

次に、MACsec ポリシーの PPK プロファイルの設定と、設定された詳細の表示の例を示します。

- MACsec ポリシー上の PPK プロファイルの設定

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# macsec policy test
switch(config-macsec-policy) # ppk crypto-qkd-profile ppk1
switch(config-macsec-policy) # sak-expiry-time 1800
switch(config-macsec-policy) # exit
switch(config) # end
```

- 設定された MACsec ポリシーの表示

```
switch# show macsec policy test
MACSec Cipher      Pri Window Offset Security      SAKRekey    timeICV      Policy
Indicator          Include-SCI
-----
test      GCM-AES-XPN-256 16      148809600 0      should-secure 1800      FALSE
              TRUE
MACSec Policy      PPK Crypto-QKD-Profile Name
-----
test              ppk1
switch#
```

次に、キー チェーンの設定、インターフェイスでの MACsec ポリシー、および設定された詳細の表示の例を示します。

- キー チェーンの設定

```
switch(config)# key chain KC1 macsec
switch(config-macseckeychain) #key 10100000
switch(config-macseckeychain-macseckey) #key-octet-string
F123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF
cryptographic-algorithm AES_256_CMAC
switch(config-macseckeychain-macseckey) #exit
```

- インターフェイスへの MACsec ポリシーの設定

```
switch(config)# interface Ethernet 1/21
switch(config-if) # macsec keychain KC1 policy test
```

- MACsec セッションの表示

```
switch(config)# show macsec mka session
Interface      Local-TxSCI #      Peers      Status      Key-Server Auth Mode
-----
```

```
-----
Ethernet1/21  6cb2.ae9f.e766/0001 1      Secured      No      PRIMARY-PPK
```

次に、ポイントツーポイント MACsec QKD プロファイルを設定し、QKD プロファイルを MACsec ポリシーにバインドし、MACsec ポリシーをインターフェイスにバインドする例を示します。



(注) 管理ポートを介した接続に対して、KME1 および KME2 サーバーがアクティブである必要があります。

スイッチ 1 の設定

```
switch1# configure terminal
switch1(config)# crypto ca trustpoint tp1
switch1(config-trustpoint)# end
switch1#

switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)# feature cryptopqc
switch1(config)#
switch1(config)# crypto qkd profile PPK1
switch1(config-crypto-qkd-profile)# kme server KME1 port 7010
switch1(config-crypto-qkd-profile)# transport tls authentication-type trustpoint tp1
switch1(config-crypto-qkd-profile)# end
switch1#

switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)# feature macsec
switch1(config)#

switch1(config)# macsec policy MP1
switch1(config-macsec-policy)# ppk crypto-qkd-profile PPK1
switch1(config-macsec-policy)# exit
switch1(config-if)# interface Ethernet1/21
switch1(config-if)# macsec keychain KC1 policy MP1
switch1(config-if)#

switch1(config-if)# interface Ethernet1/22
switch1(config-if)# macsec keychain KC1 policy MP1
switch1(config-if)#
switch1(config-if)# end
switch1#
```

スイッチ 2 の設定

```
switch2# configure terminal
switch2(config)# crypto ca trustpoint tp1
switch2(config-trustpoint)# end
switch2#

switch2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch2(config)# feature cryptopqc
switch2(config)#
switch2(config)# crypto qkd profile PPK1
switch2(config-crypto-qkd-profile)# kme server KME2 port 7010
```

```

switch2(config-crypto-qkd-profile)# transport tls authentication-type trustpoint tp1
switch2(config-crypto-qkd-profile)#
switch2(config-crypto-qkd-profile)# end
switch2#

switch2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch2(config)# feature macsec
switch2(config)#

switch2(config)# macsec policy MP1
switch2(config-macsec-policy)# ppk crypto-qkd-profile PPK1
switch2(config-macsec-policy)# exit

switch2(config-if)# interface Ethernet1/53
switch2(config-if)# macsec keychain KC1 policy MP1
switch2(config-if)#
switch2(config-if)# interface Ethernet1/54
switch2(config-if)# macsec keychain KC1 policy MP1
switch2(config-if)# end
switch2#

```

次に、スイッチ 1 とスイッチ 2 の設定の出力を示します。

Switch 1

```

switch1#
switch1# show macsec mka session

```

Interface	Local-TxSCI #	Peers	Status	Key-Server	Auth Mode
Ethernet1/22	3c8b.7ffe.0244/0001	1	Secured	Yes	PRIMARY-PPK
Ethernet1/21	3c8b.7ffe.0240/0001	1	Secured	Yes	PRIMARY-PPK

```

N9K3K STANDARD TEMPLATE FOR FEATURE REVIEWS

Total Number of Sessions : 2
Secured Sessions : 2
Pending Sessions : 0
switch1#

```

スイッチ 2

```

switch2#
switch2# show macsec mka session

```

Interface	Local-TxSCI #	Peers	Status	Key-Server	Auth Mode
Ethernet1/53	5451.deb8.62b4/0001	1	Secured	No	PRIMARY-PPK
Ethernet1/54	5451.deb8.62b8/0001	1	Secured	No	PRIMARY-PPK

```

Total Number of Sessions : 2
Secured Sessions : 2
Pending Sessions : 0
switch2#

```

設定可能な EAPOL の宛先とイーサネットタイプについて

Cisco NX-OS リリース 9.2(2) 以降では、WAN MACsec を使用するネットワークで、Extensible Authentication Protocol (EAP) over LAN (EAPOL) プロトコルの宛先アドレスとイーサネットタイプの値を非標準値に変更できます。

設定可能な EAPOL MAC およびイーサネットタイプでは、標準 MKA パケットを消費するイーサネットネットワーク上で CE デバイスが MKA セッションを形成できるように、MKA パケットの MAC アドレスとイーサネットタイプを変更できます。

EAPOL 宛先イーサネットタイプは、デフォルトのイーサネットタイプ 0x888E から代替値に変更できます。または、EAPOL 宛先 MAC アドレスは、デフォルト DMAC の 01:80:C2:00:00:03 から代替値に変更できます。プロバイダーブリッジによって消費されないようにします。

この機能はインターフェイスレベルで使用でき、代替 EAPOL 設定は、次のように任意のインターフェイスでいつでも変更できます。

- MACsec がインターフェイスですでに設定されている場合、セッションは新しい代替 EAPOL 設定で起動します。
- MACsec がインターフェイスで設定されていない場合、EAPOL 設定はインターフェイスに適用され、MACsec がそのインターフェイスで設定されている場合に有効になります。

EAPOL 設定の有効化

EAPOL 設定は、使用可能な任意のインターフェイスで有効にできます。

始める前に

MACsec が有効であ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 例 : switch# configure terminal switch(config)#	グローバル構成モードを開始します。
ステップ 2	interface name 例 : switch(config)# interface ethernet 1/1 switch(config-if)#	設定するインターフェイスを指定します。インターフェイスタイプと ID を指定できます。イーサネットポートの場合は、「ethernet slot / port」を使用します。

	コマンドまたはアクション	目的
ステップ 3	eapol mac-address <i>mac_address</i> [ethertype <i>eth_type</i>]	指定されたインターフェイス タイプおよび ID で EAPOL 設定を有効にします。 (注) イーサネット タイプが指定されていない場合、MKA パケットのデフォルトイーサネット タイプ (0x888e) であると見なします。
ステップ 4	eapol mac-address broadcast-address [ethertype <i>eth_type</i>]	ブロードキャストアドレスを代替 MAC アドレスとして有効にします。
ステップ 5	(任意) copy running-config startup-config 例 : switch(config-macseckeychain-macseckey) # copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 6	show macsec mka session detail	EAPOL 設定を表示します。

EAPOL 設定の無効化

使用可能なインターフェイスで EAPOL 設定を無効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config) #	グローバル構成モードを開始します。
ステップ 2	interface <i>name</i> 例 : switch(config) # interface ethernet 1/1 switch(config-if) #	設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。
ステップ 3	[no] eapol mac-address <i>mac_address</i> [ethertype <i>eth_type</i>]	指定されたインターフェイス タイプおよび ID で EAPOL 設定を無効にします。
ステップ 4	(任意) copy running-config startup-config 例 :	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
	switch(config-macseckeychain-macseckey) # copy running-config startup-config	

MACsec 設定の確認

MACsec 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show key chain name	キーチェーンの設定を表示します。
show macsec mka session [interface type slot/port] [detail]	特定のインターフェイスまたはすべてのインターフェイスの MACsec MKA セッションに関する情報を表示します。
show macsec mka session details	すべての EAPOL パケットのインターフェイスで現在使用されている MAC アドレスおよびイーサネット タイプに関する情報を表示します。
show macsec mka summary	MACsec MKA 設定を表示します。
show macsec policy [policy-name]	特定の MACsec ポリシーまたはすべての MACsec ポリシーの設定を表示します。
show running-config macsec	MACsec の実行コンフィギュレーション情報を表示します。

次に、すべてのインターフェイスの MACsec MKA セッションに関する情報を表示する例を示します。

```
switch# show macsec mka session
Interface          Local-TxSCI          #Peers      Status
  Key-Server      Auth Mode
-----
Ethernet2/2        2c33.11b8.7d14/0001    1           Secured
  Yes              PRIMARY-PSK
Ethernet2/3        2c33.11b8.7d18/0001    1           Secured
  Yes              PRIMARY-PSK
-----
Total Number of Sessions : 2
      Secured Sessions : 2
      Pending Sessions : 0
```

次に、特定のインターフェイスの MACsec MKA セッションに関する情報を表示する例を示します。前の例で説明したテーブルの一般的な要素に加えて、現在の MACsec セッション タイプを定義する認証モードも示します。

```
switch# show macsec mka session interface ethernet 1/1

Interface          Local-TxSCI          # Peers      Status          Key-Server      Auth Mode
```

```

-----
Ethernet1/1    70df.2fdc.baf4/0001    0    Pending    Yes    PRIMARY-PSK
Ethernet1/1    70df.2fdc.baf4/0001    1    Secured    No    FALLBACK-PSK

```

次に、特定のイーサネットインターフェイスの MACsec MKA セッションに関する詳細情報を表示する例を示します。

```

Interface Name      : Ethernet2/2
  Session Status      : SECURED - Secured MKA Session with MACsec
  Local Tx-SCI        : 2c33.11b8.7d14/0001
  Local Tx-SSCI       : 2
  MKA Port Identifier : 2
  CAK Name (CKN)      : 12
  CA Authentication Mode : PRIMARY-PSK
  Member Identifier (MI) : B54263EF7949A561E25CE617
  Message Number (MN)  : 523
  MKA Policy Name     : tests2
  Key Server Priority  : 16
  Key Server          : Yes
  Include ICV         : No
  SAK Cipher Suite    : GCM-AES-XPB-256
  SAK Cipher Suite (Operational) : GCM-AES-XPB-256
  Replay Window Size  : 148809600
  Confidentiality Offset : CONF-OFFSET-0
  Confidentiality Offset (Operational) : CONF-OFFSET-0
  Latest SAK Status    : Rx & TX
  Latest SAK AN       : 0
  Latest SAK KI       : B54263EF7949A561E25CE61700000001
  Latest SAK KN       : 1
  Last SAK key time    : 12:59:38 PST Tue Mar 19 2019
  CA Peer Count       : 1
  Eapol dest mac      : 0180.c200.0003
  Ether-type          : 0x888e
Peer Status:
  Peer MI             : 2C2C090E62A96F4D6E018210
  RxSCI              : 2c33.11b8.8b88/0001
  Peer CAK            : Match
  Latest Rx MKPDU     : 13:16:54 PST Tue Mar 19 2019

```

次に、MACsec MKA 設定を表示する例を示します。

```

switch# show macsec mka summary
Interface      MACSEC-policy      Keychain
-----
Ethernet2/13   1                      1/10000000000000000000
Ethernet2/14   1                      1/10000000000000000000

```

次に、すべての MACsec ポリシーの設定を表示する例を示します。

```

switch# show macsec policy
MACSec Policy      Cipher      Pri  Window      Offset      Security      SAK Rekey time
ICV Indicator      Include-SCI
-----
KC256-Pol17b      GCM-AES-256    16   148809600    0           should-secure  pn-rollover
  FALSE          True
poll              GCM-AES-XPB-256 100  148809600    30          must-secure    60
  FALSE          True
pol256-Fan0       GCM-AES-XPB-256 16   148809600    0           must-secure    60
  FALSE          True
pol256-MCT        GCM-AES-XPB-256 16   148809600    0           should-secure  60
  FALSE          FALSE

```

```

system-default-
macsec-policy      GCM-AES-XPB-256  16  148809600  0  should-secure  pn-rollover
FALSE              FALSE
test1              GCM-AES-XPB-256  16  148809600  0  should-secure  pn-rollover
FALSE              True

```

次の例では、**show running-config** および **show startup-config** コマンドの出力にキー オクテット文字列が表示されることを示しています。ただし、**key-chain macsec-psk no-show** コマンドが設定されている場合を除きます。

```

key chain KC256-1 macsec
  key 2000
  key-octet-string 7
075e701e1c5a4a5143475e5a527d7c7c706a6c724306170103555a5c57510b051e47080
a05000101005e0e50510f005c4b5f5d0b5b070e234e4d0a1d0112175b5e cryptographic-algorithm
AES_256_CMAC

```

次の例では、**show running-config** および **show startup-config** コマンドの出力にキー オクテット文字列が表示されることを示しています。こちらは、**key-chain macsec-psk no-show** コマンドが設定されている場合です。

```

key chain KC256-1 macsec
  key 2000
  key-octet-string 7 ***** cryptographic-algorithm AES_256_CMAC

```

MACsec 統計の表示

次のコマンドを使用して、MACsec 統計情報を表示できます。

コマンド	説明
show macsec mka statistics [interface type slot/port]	MACsec MKA 統計情報を表示します。
show macsec secy statistics [interface type slot/port]	MACsec セキュリティ統計情報を表示します。

次に、特定のイーサネット インターフェイスの MACsec MKA 統計情報の例を示します。

```

switch# show macsec mka statistics interface ethernet 2/2

Per-CA MKA Statistics for Session on interface (Ethernet2/2) with CKN 0x10
=====
CA Statistics
  Pairwise CAK Rekeys..... 0

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

MKPDU Statistics
  MKPDUs Transmitted..... 1096
  "Distributed SAK".. 0

  MKPDUs Validated & Rx... 0
  "Distributed SAK".. 0

```

```

MKA Statistics for Session on interface (Ethernet2/2)
=====
CA Statistics
  Pairwise CAK Rekeys..... 0

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

MKPDU Statistics
  MKPDUs Transmitted..... 1096
  "Distributed SAK".. 0
  MKPDUs Validated & Rx... 0
  "Distributed SAK".. 0
  MKPDUs Tx Success..... 1096
  MKPDUs Tx Fail..... 0
  MKPDUS Tx Pkt build fail... 0
  MKPDUS No Tx on intf down.. 0
  MKPDUS No Rx on intf down.. 0
  MKPDUs Rx CA Not found..... 0
  MKPDUs Rx Error..... 0
  MKPDUs Rx Success..... 0

MKPDU Failures
  MKPDU Rx Validation ..... 0
  MKPDU Rx Bad Peer MN..... 0
  MKPDU Rx Non-recent Peerlist MN..... 0
  MKPDU Rx Drop SAKUSE, KN mismatch..... 0
  MKPDU Rx Drop SAKUSE, Rx Not Set..... 0
  MKPDU Rx Drop SAKUSE, Key MI mismatch.... 0
  MKPDU Rx Drop SAKUSE, AN Not in Use..... 0
  MKPDU Rx Drop SAKUSE, KS Rx/Tx Not Set... 0
  MKPDU Rx Drop Packet, Ethertype Mismatch. 0

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

CA Failures
  ICK Derivation..... 0
  KEK Derivation..... 0
  Invalid Peer MACsec Capability... 0

MACsec Failures
  Rx SA Installation..... 0
  Tx SA Installation..... 0

```

次に、特定のイーサネットインターフェイスの MACsec セキュリティ統計情報を表示する例を示します。



(注) Rx および Tx 統計情報の非制御パケットと制御パケットには、次の違いがあります。

- Rx 統計
 - 非制御=暗号化および非暗号化
 - 制御 = 非暗号化
- TX 統計情報 :
 - 非制御 = 非暗号化
 - 制御 = 暗号化
 - 共通 = 暗号化および非暗号化

```
switch(config)# show macsec secy statistics interface e2/28/1

Interface Ethernet2/28/1 MACSEC SecY Statistics:
-----
Interface Rx Statistics:
  Unicast Uncontrolled Pkts: 14987
  Multicast Uncontrolled Pkts: 1190444
  Broadcast Uncontrolled Pkts: 4
  Uncontrolled Pkts - Rx Drop: 0
  Uncontrolled Pkts - Rx Error: 0
  Unicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Multicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Broadcast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Controlled Pkts: 247583
  Controlled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
  Controlled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
  In-Octets Uncontrolled: 169853963 bytes
  In-Octets Controlled: 55027017 bytes
  Input rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Input rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Input rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Input rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)

Interface Tx Statistics:
  Unicast Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Multicast Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Broadcast Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Uncontrolled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
  Uncontrolled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
  Unicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Multicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Broadcast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Controlled Pkts: 205429
  Controlled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
  Controlled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
  Out-Octets Uncontrolled: N/A (N9K-X9736C-FX not supported)
  Out-Octets Controlled: 20612648 bytes
  Out-Octets Common: 151787484 bytes
  Output rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Output rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Output rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Output rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)
```

```

SECY Rx Statistics:
  Transform Error Pkts: N/A (N9K-X9736C-FX not supported)
  Control Pkts: 952284
  Untagged Pkts: N/A (N9K-X9736C-FX not supported)
  No Tag Pkts: 0
  Bad Tag Pkts: 0
  No SCI Pkts: 0
  Unknown SCI Pkts: 0
  Tagged Control Pkts: N/A (N9K-X9736C-FX not supported)

SECY Tx Statistics:
  Transform Error Pkts: N/A (N9K-X9736C-FX not supported)
  Control Pkts: 967904
  Untagged Pkts: N/A (N9K-X9736C-FX not supported)

SAK Rx Statistics for AN [3]:
  Unchecked Pkts: 0
  Delayed Pkts: 0
  Late Pkts: 0
  OK Pkts: 1
  Invalid Pkts: 0
  Not Valid Pkts: 0
  Not-Using-SA Pkts: 0
  Unused-SA Pkts: 0
  Decrypted In-Octets: 235 bytes
  Validated In-Octets: 0 bytes

SAK Tx Statistics for AN [3]:
  Encrypted Protected Pkts: 2
  Too Long Pkts: N/A (N9K-X9736C-FX not supported)
  SA-not-in-use Pkts: N/A (N9K-X9736C-FX not supported)
  Encrypted Protected Out-Octets: 334 bytes
switch(config)#

```

MACsec の設定例

次に、ユーザ定義のMACsecポリシーを設定し、そのポリシーをインターフェイスに適用する例を示します。

```

switch(config)# macsec policy 1
switch(config-macsec-policy)# cipher-suite GCM-AES-256
switch(config-macsec-policy)# window-size 512
switch(config-macsec-policy)# key-server-priority 0
switch(config-macsec-policy)# conf-offset CONF-OFFSET-0
switch(config-macsec-policy)# security-policy should-secure
switch(config-macsec-policy)# exit

```

```

switch(config)# int e2/13-14
switch(config-if-range)# macsec keychain 1 policy 1
switch(config-if-range)# exit
switch(config)# show macsec mka summary

```

Interface	MACSEC-policy	Keychain
Ethernet2/13	1	1/100000000000000000
Ethernet2/14	1	1/100000000000000000

```

switch(config)# show macsec mka session

```

Interface	Local-TxSCI	# Peers	Status	Key-Server
Ethernet2/13	006b.f1be.d31c/0001	1	Secured	Yes

```
Ethernet2/14    006b.flbe.d320/0001  1          Secured    No
```

```
switch(config)# show running-config macsec
!Command: show running-config macsec
!Time: Mon Dec  5 04:53:40 2016
```

```
version 9.2(1)feature macsec
macsec policy 1
  cipher-suite GCM-AES-256
  key-server-priority 0
  window-size 512
  conf-offset CONF-OFFSET-0
  security-policy should-secure
```

```
interface Ethernet2/13
  macsec keychain 1 policy 1
```

```
interface Ethernet2/14
  macsec keychain 1 policy 1
```

次に、MACsec キーチェーンを設定し、インターフェイスにシステムデフォルトの MACsec ポリシーを追加する例を示します。

```
switch(config)# key chain 1 macsec
switch(config-macseckeychain)# key 1000
switch(config-macseckeychain-macseckey)# key-octet-string
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm
aes_256_CMAC
switch(config-macseckeychain-macseckey)# exit
```

```
switch(config)# int e2/13-14
switch(config-if-range)# macsec keychain 1
switch(config-if-range)# exit
switch(config)#
```

```
switch(config)# show running-config macsec
!Command: show running-config macsec
!Time: Mon Dec  5 04:50:16 2016
version 7.0(3)I4(5)
feature macsec
interface Ethernet2/13
  macsec keychain 1 policy system-default-macsec-policy
interface Ethernet2/14
  macsec keychain 1 policy system-default-macsec-policy
```

```
switch(config)# show macsec mka session
```

Interface	Local-TxSCI	# Peers	Status
Key-Server	Auth Mode		
Ethernet2/2	2c33.11b8.7d14/0001	1	Secured
Yes	PRIMARY-PSK		
Ethernet2/3	2c33.11b8.7d18/0001	1	Secured
Yes	PRIMARY-PSK		

```
-----
Total Number of Sessions : 2
  Secured Sessions : 2
  Pending Sessions : 0
```

```
switch(config)# show macsec mka summary
Interface      Status  Cipher (Operational)  Key-Server  MACSEC-policy  Keychain
Fallback-keychain
```



```

-----
-----
Ethernet2/1      down      -          -          tests1      keych1
  no keychain
Ethernet2/2      Secured   GCM-AES-XP-256   Yes        tests2      keych2
  no keychain
Ethernet2/3      Secured   GCM-AES-256      Yes        tests3      keyc3
  no keychain

```

次に、Peer Enforce Cipher 設定機能 MACsec の設定と出力の例を示します。

```

switch# show key chain
Key-Chain KC1 Macsec
Key 10000000 -- text 7
"0729701e1d534c53404a522d26090f010e63647040534355560e007971772a263e30080a0407070303530227257b73213556550958525a771b165038273
4362e2a"
cryptographic-algorithm AES_256_CMAC
send lifetime (always valid) [active]

Key-Chain KC2 Macsec
Key 10100000 -- text 7
"0729701e1d534c53404a522d26090f010e63647040534355560e007971772a263e30080a0407070303530227257b73213556550958525a771b165038273
4362e2a"
cryptographic-algorithm AES_256_CMAC
send lifetime (always valid) [active]

switch#
switch# show run macsec

!Command: show running-config macsec
!Running configuration last done at: Mon Apr 17 16:49:57 2023
!Time: Mon Apr 17 16:50:09 2023

version 10.3(3) Bios:version 05.47
feature macsec

macsec policy MP1
no protocol lldp encrypted
cipher-suite enforce-peer GCM-AES-XP-256 GCM-AES-XP-128
macsec policy MP2
no protocol lldp encrypted
cipher-suite enforce-peer GCM-AES-256
interface Ethernet1/97/1
macsec keychain KC1 policy MP1

interface Ethernet1/97/2
macsec keychain KC2 policy MP2

switch#

switch# show macsec policy
MACSec Policy Cipher Pri Window Offset Security SAK Rekey time ICV Indicator Include-SCI
-----
-----
MP1 Enforce-Peer 16 148809600 0 should-secure pn-rollover FALSE TRUE
MP2 Enforce-Peer 16 148809600 0 should-secure pn-rollover FALSE TRUE
system-default-macsec-policy GCM-AES-XP-256 16 148809600 0 should-secure pn-rollover
FALSE TRUE

MACSec Policy                               Lldp-bypass
-----
MP1                                           True
MP2                                           True
system-default-macsec-policy                 FALSE

```

```
MACSec Policy PPK Crypto-QKD-Profile Name
```

```
MACSec Policy Cipher-Suite Enforce-Peer
```

```
MP1 GCM-AES-XPB-256 GCM-AES-XPB-128
```

```
MP2 GCM-AES-256
```

```
switch#
```

次の例は、**show macsec mka session detail** コマンドのサンプル出力を示しています。

```
switch# show macsec mka session details
```

```
Detailed Status for MKA Session
```

```
-----
```

```
Interface Name : Ethernet1/97/1
```

```
Session Status : SECURED - Secured MKA Session with MACsec
```

```
Local Tx-SCI : c4f7.d530.1484/0001
```

```
Local Tx-SSCI : 1
```

```
MKA Port Identifier : 1
```

```
CAK Name (CKN) : 10000000
```

```
CA Authentication Mode : PRIMARY-PSK
```

```
Member Identifier (MI) : D94B90E3FDB111CE583E7158
```

```
Message Number (MN) : 111
```

```
MKA Policy Name : MP1
```

```
Key Server Priority : 16
```

```
Key Server : Yes
```

```
Include ICV : No
```

```
SAK Cipher Suite : GCM-AES-XPB-128
```

```
SAK Cipher Suite (Operational) : GCM-AES-XPB-128
```

```
Replay Window Size : 148809600
```

```
Confidentiality Offset : CONF-OFFSET-0
```

```
Confidentiality Offset (Operational): CONF-OFFSET-0
```

```
Latest SAK Status : Rx & TX
```

```
Latest SAK AN : 1
```

```
Latest SAK KI : D94B90E3FDB111CE583E715800000001
```

```
Latest SAK KN : 1
```

```
Last SAK key time : 16:48:41 PST Mon Apr 17 2023
```

```
CA Peer Count : 1
```

```
Eapol dest mac : 0180.c200.0003
```

```
Ether-type : 0x888e
```

```
Peer Status:
```

```
Peer MI : 0011000000010001000000001
```

```
RxSCI : 0011.0000.0001/0001
```

```
Peer CAK : Match
```

```
Latest Rx MKPDU : 16:52:07 PST Mon Apr 17 2023
```

```
Interface Name : Ethernet1/97/2
```

```
Session Status : SECURED - Secured MKA Session with MACsec
```

```
Local Tx-SCI : c4f7.d530.1485/0001
```

```
Local Tx-SSCI : 1
```

```
MKA Port Identifier : 1
```

```
CAK Name (CKN) : 10100000
```

```
CA Authentication Mode : PRIMARY-PSK
```

```
Member Identifier (MI) : 43AE54C19982238C298E0241
```

```
Message Number (MN) : 107
```

```
MKA Policy Name : MP2
```

```
Key Server Priority : 16
```

```
Key Server : Yes
```

```
Include ICV : No
```

```
SAK Cipher Suite : GCM-AES-256
```

```
SAK Cipher Suite (Operational) : GCM-AES-256
```

```
Replay Window Size : 148809600
```

```
Confidentiality Offset : CONF-OFFSET-0
```

```
Confidentiality Offset (Operational): CONF-OFFSET-0
```

```

Latest SAK Status : Rx & TX
Latest SAK AN : 0
Latest SAK KI : 43AE54C19982238C298E024100000001
Latest SAK KN : 1
Last SAK key time : 16:48:42 PST Mon Apr 17 2023
CA Peer Count : 1
Eapol dest mac : 0180.c200.0003
Ether-type : 0x888e
Peer Status:
Peer MI : 002700000001000100000001
RxSCI : 0027.0000.0001/0001
Peer CAK : Match
Latest Rx MKPDU : 16:52:06 PST Mon Apr 17 2023
switch#

```

XML の例

MACsec は、`| xml` を使用したスクリプト用に次の **show** コマンドの XML 出力をサポートします。

- **show key chain name | xml**
- **show macsec mka session interface interface slot/port details | xml**
- **show macsec mka statistics interface interface slot/port | xml**
- **show macsec mka summary | xml**
- **show macsec policy name | xml**
- **show macsec secy statistics interface interface slot/port | xml**
- **show running-config macsec | xml**

次に、上記の各 **show** コマンドの出力例を示します。

例 1：キーチェーンの設定を表示します

```

switch# show key chain "Kc2" | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0:rpm">
  <nf:data>
    <show>
      <key>
        <chain>
          <__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
            <keychain>Kc2</keychain>
          </__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
        </chain>
      </key>
    </show>
  </nf:data>
</nf:rpc-reply>
]]>]]>

```

例 2：特定のインターフェイスの MACsec MKA セッションに関する情報を表示します。

例 3 : MACsec MKA 統計情報を表示します。

```
switch# show macsec mka statistics interface ethernet 4/31 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0">
```

```

<nf:data>
  <show>
<macsec>
  <mka>
    <statistics>
      <__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
        <interface>
          <__XML__INTF_ifname>
            <__XML__PARAM_value>
              <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
              <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
            </__XML__PARAM_value>
          </__XML__INTF_ifname>
        </interface>
      <__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
        <__readonly__>
          <TABLE_mka_intf_stats>
            <ROW_mka_intf_stats>
              <TABLE_ca_stats>
                <ROW_ca_stats>
                  <ca_stat_ckn>0x2</ca_stat_ckn>
                  <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
                  <sa_stat_sak_generated>0</sa_stat_sak_generated>
                  <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
                  <sa_stat_sak_received>91</sa_stat_sak_received>
                  <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
                  <mkpdu_stat_mkpdu_tx>2808</mkpdu_stat_mkpdu_tx>
                  <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
                  <mkpdu_stat_mkpdu_rx>2714</mkpdu_stat_mkpdu_rx>
                  <mkpdu_stat_mkpdu_rx_distsak>91</mkpdu_stat_mkpdu_rx_distsak>
                </ROW_ca_stats>
              </TABLE_ca_stats>
            </ROW_mka_intf_stats>
          </TABLE_mka_intf_stats>
        </__readonly__>
      </__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
    </interface>
    <__XML__INTF_ifname>
      <__XML__PARAM_value>
        <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
      </__XML__PARAM_value>
    </__XML__INTF_ifname>
  </interface>
  <__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
    <__readonly__>
      <TABLE_mka_intf_stats>
        <ROW_mka_intf_stats>
          <TABLE_idb_stats>
            <ROW_idb_stats>
              <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
              <sa_stat_sak_generated>0</sa_stat_sak_generated>
              <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
              <sa_stat_sak_received>91</sa_stat_sak_received>
              <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
              <mkpdu_stat_mkpdu_tx>2808</mkpdu_stat_mkpdu_tx>
              <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
              <mkpdu_stat_mkpdu_rx>2714</mkpdu_stat_mkpdu_rx>
              <mkpdu_stat_mkpdu_rx_distsak>91</mkpdu_stat_mkpdu_rx_distsak>
              <idb_stat_mkpdu_tx_success>2808</idb_stat_mkpdu_tx_success>
              <idb_stat_mkpdu_tx_fail>0</idb_stat_mkpdu_tx_fail>
              <idb_stat_mkpdu_tx_pkt_build_fail>0</idb_stat_mkpdu_tx_pkt_build_fail>
              <idb_stat_mkpdu_no_tx_on_intf_down>0</idb_stat_mkpdu_no_tx_on_intf_down>
              <idb_stat_mkpdu_no_rx_on_intf_down>0</idb_stat_mkpdu_no_rx_on_intf_down>
              <idb_stat_mkpdu_rx_ca_notfound>0</idb_stat_mkpdu_rx_ca_notfound>
            </ROW_idb_stats>
          </TABLE_idb_stats>
        </ROW_mka_intf_stats>
      </TABLE_mka_intf_stats>
    </__readonly__>
  </__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>

```

```

        <idb_stat_mkpdu_rx_error>0</idb_stat_mkpdu_rx_error>
        <idb_stat_mkpdu_rx_success>2714</idb_stat_mkpdu_rx_success>
        <idb_stat_mkpdu_failure_rx_integrity_check_error>0</idb_stat_mkpdu_
failure_rx_integrity_check_error>
        <idb_stat_mkpdu_failure_invalid_peer_mn_error>0</idb_stat_mkpdu_fai
lure_invalid_peer_mn_error>
        <idb_stat_mkpdu_failure_nonrecent_peerlist_mn_error>1</idb_stat_mkp
du_failure_nonrecent_peerlist_mn_error>
        <idb_stat_mkpdu_failure_sakuse_kn_mismatch_error>0</idb_stat_mkpdu_
failure_sakuse_kn_mismatch_error>
        <idb_stat_mkpdu_failure_sakuse_rx_not_set_error>0</idb_stat_mkpdu_f
ailure_sakuse_rx_not_set_error>
        <idb_stat_mkpdu_failure_sakuse_key_mi_mismatch_error>0</idb_stat_mk
pdu_failure_sakuse_key_mi_mismatch_error>
        <idb_stat_mkpdu_failure_sakuse_an_not_in_use_error>0</idb_stat_mkpdu
failure_sakuse_an_not_in_use_error>
        <idb_stat_mkpdu_failure_sakuse_ks_rx_tx_not_set_error>0</idb_stat_m
kpdu_failure_sakuse_ks_rx_tx_not_set_error>
        <idb_stat_mkpdu_failure_sakuse_eapol_ethertype_mismatch_error>0</id
b_stat_mkpdu_failure_sakuse_eapol_ethertype_mismatch_error>
        <idb_stat_sak_failure_sak_generate_error>0</idb_stat_sak_failure_sa
k_generate_error>
        <idb_stat_sak_failure_hash_generate_error>0</idb_stat_sak_failure_h
ash_generate_error>
        <idb_stat_sak_failure_sak_encryption_error>0</idb_stat_sak_failure_
sak_encryption_error>
        <idb_stat_sak_failure_sak_decryption_error>0</idb_stat_sak_failure_
sak_decryption_error>
        <idb_stat_sak_failure_ick_derivation_error>0</idb_stat_sak_failure_
ick_derivation_error>
        <idb_stat_sak_failure_kek_derivation_error>0</idb_stat_sak_failure_
kek_derivation_error>
        <idb_stat_sak_failure_invalid_macsec_capability_error>0</idb_stat_s
ak_failure_invalid_macsec_capability_error>
        <idb_stat_macsec_failure_rx_sa_create_error>0</idb_stat_macsec_fail
ure_rx_sa_create_error>
        <idb_stat_macsec_failure_tx_sa_create_error>0</idb_stat_macsec_fail
ure_tx_sa_create_error>
    </ROW_idb_stats>
</TABLE_idb_stats>
</ROW_mka_intf_stats>
</TABLE_mka_intf_stats>
</__readonly__>
</__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
</__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
</statistics>
</mka>
</macsec>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>

```

例 4 : MACsec MKA 設定を表示します。

```

switch# show macsec mka summary | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:1.0">
  <nf:data>
    <show>
      <macsec>
        <mka>
          <__XML__OPT_Cmd_some_macsec_summary>

```

```
<__XML__OPT_Cmd_some_macsec___readonly__>  
  <__readonly__>  
    <TABLE_mka_summary>  
      <ROW_mka_summary>  
        <ifname>Ethernet2/1</ifname>  
        <policy>am2</policy>  
<keychain>kc2/0200000000000000000000000000000000000000000000000000000000000000  
00000000</keychain>  
      </ROW_mka_summary>  
      <ROW_mka_summary>  
        <ifname>Ethernet3/1</ifname>  
        <policy>am2</policy>  
        <keychain>kc2/0200000000000000000000000000000000000000000000000000000000000000  
00000000</keychain>  
      </ROW_mka_summary>  
  
[TRUNCATED FOR READABILITY]  
  
<ROW_mka_summary>  
  <ifname>Ethernet3/32</ifname>  
  <policy>am2</policy>  
  <keychain>kc2/0200000000000000000000000000000000000000000000000000000000000000  
00000000</keychain>  
  </ROW_mka_summary>  
</TABLE_mka_summary>  
</__readonly__>  
</__XML__OPT_Cmd_some_macsec___readonly__>  
</__XML__OPT_Cmd_some_macsec_summary>  
</mka>  
</macsec>  
</show>  
</nf:data>  
</nf:rpc-reply>  
]]>]]>
```

例 5：特定の MACsec ポリシーの設定を表示します。

```
switch# show macsec policy am2 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0">
  <nf:data>
    <show>
      <macsec>
        <policy>
          <__XML__OPT_Cmd_some_macsec_policy_name>
            <policy_name>am2</policy_name>
            <__XML__OPT_Cmd_some_macsec__readonly__>
              <__readonly__>
                <TABLE_macsec_policy>
                  <ROW_macsec_policy>
                    <name>am2</name>
                    <cipher_suite>GCM-AES-256</cipher_suite>
                    <keyserver_priority>0</keyserver_priority>
                    <window_size>512</window_size>
                    <conf_offset>0</conf_offset>
                    <security_policy>must-secure</security_policy>
                    <sak-expiry-time>60</sak-expiry-time>
                  </ROW_macsec_policy>
                </TABLE_macsec_policy>
              </__readonly__>
            </__XML__OPT_Cmd_some_macsec__readonly__>
          </__XML__OPT_Cmd_some_macsec_policy_name>
        </policy>
      </show>
    </nf:data>
  </nf:rpc-reply>
</show>
```

```

    </macsec>
  </show>
</nf:data>
</nf:rpc-reply>
]]>]]>

```

例 6 : MACsec セキュリティ統計情報を表示します。

```

switch# show macsec secy statistics interface ethernet 4/31 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0">
  <nf:data>
    <show>
      <macsec>
        <secy>
          <statistics>
            <interface>
              <__XML__ INTF_ifname>
                <__XML__ PARAM_value>
                  <__XML__ INTF_output>Ethernet4/31</__XML__ INTF_output>
                </__XML__ PARAM_value>
              <__XML__ OPT_Cmd_some_macsec_secy_statistics__readonly__>
                <__readonly__>
                  <TABLE_statistics>
                    <ROW_statistics>
                      <in_pkts_unicast_uncontrolled>0</in_pkts_unicast_uncontrolled>
                      <in_pkts_multicast_uncontrolled>42</in_pkts_multicast_uncontrolled>
                      <in_pkts_broadcast_uncontrolled>0</in_pkts_broadcast_uncontrolled>
                      <in_rx_drop_pkts_uncontrolled>0</in_rx_drop_pkts_uncontrolled>
                      <in_rx_err_pkts_uncontrolled>0</in_rx_err_pkts_uncontrolled>
                      <in_pkts_unicast_controlled>0</in_pkts_unicast_controlled>
                      <in_pkts_multicast_controlled>2</in_pkts_multicast_controlled>
                      <in_pkts_broadcast_controlled>0</in_pkts_broadcast_controlled>
                      <in_rx_drop_pkts_controlled>0</in_rx_drop_pkts_controlled>
                      <in_rx_err_pkts_controlled>0</in_rx_err_pkts_controlled>
                      <in_octets_uncontrolled>7230</in_octets_uncontrolled>
                      <in_octets_controlled>470</in_octets_controlled>
                      <input_rate_uncontrolled_pps>0</input_rate_uncontrolled_pps>
                      <input_rate_uncontrolled_bps>9</input_rate_uncontrolled_bps>
                      <input_rate_controlled_pps>0</input_rate_controlled_pps>
                      <input_rate_controlled_bps>23</input_rate_controlled_bps>
                      <out_pkts_unicast_uncontrolled>0</out_pkts_unicast_uncontrolled>
                      <out_pkts_multicast_uncontrolled>41</out_pkts_multicast_uncontrolled>
                      <out_pkts_broadcast_uncontrolled>0</out_pkts_broadcast_uncontrolled>
                      <out_rx_drop_pkts_uncontrolled>0</out_rx_drop_pkts_uncontrolled>
                      <out_rx_err_pkts_uncontrolled>0</out_rx_err_pkts_uncontrolled>
                      <out_pkts_unicast_controlled>0</out_pkts_unicast_controlled>
                      <out_pkts_multicast_controlled>2</out_pkts_multicast_controlled>
                      <out_pkts_broadcast_controlled>0</out_pkts_broadcast_controlled>
                      <out_rx_drop_pkts_controlled>0</out_rx_drop_pkts_controlled>
                      <out_rx_err_pkts_controlled>0</out_rx_err_pkts_controlled>
                      <out_octets_uncontrolled>6806</out_octets_uncontrolled>
                      <out_octets_controlled>470</out_octets_controlled>
                      <out_octets_common>7340</out_octets_common>
                      <output_rate_uncontrolled_pps>2598190092</output_rate_uncontrolled_pps>
                      <output_rate_uncontrolled_bps>2598190076</output_rate_uncontrolled_bps>
                      <output_rate_controlled_pps>0</output_rate_controlled_pps>
                      <output_rate_controlled_bps>23</output_rate_controlled_bps>
                      <in_pkts_transform_error>0</in_pkts_transform_error>
                      <in_pkts_control>40</in_pkts_control>
                      <in_pkts_untagged>0</in_pkts_untagged>
                      <in_pkts_no_tag>0</in_pkts_no_tag>
                      <in_pkts_badtag>0</in_pkts_badtag>
                    </ROW_statistics>
                  </TABLE_statistics>
                </__readonly__>
              </__XML__ OPT_Cmd_some_macsec_secy_statistics__readonly__>
            </__XML__ PARAM_value>
          </__XML__ INTF_output>
        </interface>
      </statistics>
    </secy>
  </macsec>
</show>
</nf:data>
</nf:rpc-reply>

```



```

<in_pkts_no_sci>0</in_pkts_no_sci>
<in_pkts_unknown_sci>0</in_pkts_unknown_sci>
<in_pkts_tagged_ctrl>0</in_pkts_tagged_ctrl>
<out_pkts_transform_error>0</out_pkts_transform_error>
<out_pkts_control>41</out_pkts_control>
<out_pkts_untagged>0</out_pkts_untagged>
<rx_sa_an>1</rx_sa_an>
<in_pkts_unchecked>0</in_pkts_unchecked>
<in_pkts_delayed>0</in_pkts_delayed>
<in_pkts_late>0</in_pkts_late>
<in_pkts_ok>1</in_pkts_ok>
<in_pkts_invalid>0</in_pkts_invalid>
<in_pkts_not_valid>0</in_pkts_not_valid>
<in_pkts_not_using_sa>0</in_pkts_not_using_sa>
<in_pkts_unused_sa>0</in_pkts_unused_sa>
<in_octets_decrypted>223</in_octets_decrypted>
<in_octets_validated>0</in_octets_validated>
<tx_sa_an>1</tx_sa_an>
<out_pkts_encrypted_protected>1</out_pkts_encrypted_protected>
<out_pkts_too_long>0</out_pkts_too_long>
<out_pkts_sa_not_inuse>0</out_pkts_sa_not_inuse>
<out_octets_encrypted_protected>223</out_octets_encrypted_protected>
</ROW_statistics>
</TABLE_statistics>
</__readonly__>
</__XML__OPT_Cmd_some_macsec_secy_statistics__readonly__>
</__XML__INTF_ifname>
</interface>
</statistics>
</secy>
</macsec>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>

```

例 7 : MACsec の実行コンフィギュレーション情報を表示します。

```
switch# show running-config macsec | xml
```

```
!Command: show running-config macsec
!Time: Fri Jan 20 07:12:34 2017
```

```

version 7.0(3)I4(6)
*****
This may take time. Please be patient.
*****
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cis
co.com/nxos:7.0.3.I4.6.:configure " xmlns:m="http://www.cisco.com/nxos:7.0.3.I4.
6.:_exec" xmlns:ml="http://www.cisco.com/nxos:7.0.3.I4.6.:configure__macsec-poli
cy" xmlns:m2="http://www.cisco.com/nxos:7.0.3.I4.6.:configure__if-eth-non-member
" message-id="1">
  <nf:get-config>
    <nf:source>
      <nf:running/>
    </nf:source>
    <nf:filter>
      <m:configure>
        <m:terminal>
          <feature>
            <macsec/>
          </feature>
        <macsec>

```

```

<policy>
  <__XML__PARAM__policy_name>
    <__XML__value>am2</__XML__value>
    <m1:cipher-suite>
      <m1:__XML__PARAM__suite>
        <m1:__XML__value>GCM-AES-XPB-256</m1:__XML__value>
      </m1:__XML__PARAM__suite>
    </m1:cipher-suite>
    <m1:key-server-priority>
      <m1:__XML__PARAM__pri>
        <m1:__XML__value>0</m1:__XML__value>
      </m1:__XML__PARAM__pri>
    </m1:key-server-priority>
  <m1>window-size>
    <m1:__XML__PARAM__size>
      <m1:__XML__value>512</m1:__XML__value>
    </m1:__XML__PARAM__size>
  </m1>window-size>
  <m1:conf-offset>
    <m1:__XML__PARAM__offset>
      <m1:__XML__value>CONF-OFFSET-0</m1:__XML__value>
    </m1:__XML__PARAM__offset>
  </m1:conf-offset>
  <m1:security-policy>
    <m1:__XML__PARAM__policy>
      <m1:__XML__value>must-secure</m1:__XML__value>
    </m1:__XML__PARAM__policy>
  </m1:security-policy>
  <m1:sak-expiry-time>
    <m1:__XML__PARAM__ts>
      <m1:__XML__value>60</m1:__XML__value>
    </m1:__XML__PARAM__ts>
  </m1:sak-expiry-time>
</__XML__PARAM__policy_name>
</policy>
</macsec>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet2/1</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>kc2</m2:__XML__value>
        <m2:policy>
          <m2:__XML__PARAM__policy_name>
            <m2:__XML__value>am2</m2:__XML__value>
          </m2:__XML__PARAM__policy_name>
        </m2:policy>
      </m2:__XML__PARAM__keychain_name>
    </m2:keychain>
  </m2:macsec>
</__XML__PARAM__interface>
</interface>

```

[TRUNCATED FOR READABILITY]

```

<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet4/31</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>kc2</m2:__XML__value>
        <m2:policy>

```

```

        <m2:__XML__PARAM__policy_name>
        <m2:__XML__value>am2</m2:__XML__value>
        </m2:__XML__PARAM__policy_name>
    </m2:policy>
    </m2:__XML__PARAM__keychain_name>
</m2:keychain>
</m2:macsec>
</__XML__PARAM__interface>
</interface>
</m:terminal>
</m:configure>
</nf:filter>
</nf:get-config>
</nf:rpc>
]]>]]>

```

MIB

MACsec は次の MIB をサポートします。

- IEEE8021-SECY-MIB
- CISCO-SECY-EXT-MIB

サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください：<https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html>。

関連資料

関連項目	マニュアル タイトル
キーチェーン管理	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
システム メッセージ	Cisco Nexus 9000 シリーズ NX-OS システム メッセージ リファレンス



第 28 章

Cisco Live Protect による NX-OS のセキュア化

この章では、NXSecure 構成が有効な場合に NX-OS をセキュアにする Cisco Live Protect 機能について説明します。この章は、次の項で構成されています。

- [Cisco Live Protect \(775 ページ\)](#)
- [Cisco Live Protect の注意事項と制約事項 \(776 ページ\)](#)
- [Cisco Live Protect の NXSecure 機能の有効化 \(776 ページ\)](#)
- [Cisco Live Protect の NXSecure 設定の確認 \(777 ページ\)](#)
- [イベント ログ \(777 ページ\)](#)

Cisco Live Protect

Cisco Live Protect は：

- シスコネットワークデバイスのコントロールプレーンを保護するセキュリティ機能です。
- NX-OS デバイスで NXSecure 設定を有効にする必要があります。
- リアルタイムのセキュリティイベントの検出と分析により、包括的なセキュリティのオペラビリティを提供します。

Cisco NX-OS リリース 10.6(1)F では、NX-OS を保護する Cisco Live Protect 機能が導入されており、NX-OS デバイス コントロールプレーンのセキュリティとソフトウェア完全性のアシュアランスが強化されています。このリリースではモニタリングモードのみがサポートされています。

NXSecure：NXSecure は、Nexus スイッチ向けのセキュリティ設定ツールです。コントロールプレーンをセキュリティの脆弱性から保護します。NXSecure は、拡張バークレイ パケット フィルタ (eBPF) と呼ばれるテクノロジーを内部的に使用して、セキュリティ イベントをリアルタイムに追跡、検出、レポートします。NXSecure は、ファイルの監視、プロセスの追跡、システム コールの追跡も行います。

トレース ポリシー：Cisco Live Protect 機能では、トレース ポリシーを使用してセキュリティのオプザバビリティを提供します。これらのポリシーは、NX-OS イメージにパッケージ化されています。

モニタリング モード：設定されたポリシーに基づいて、モニタリング モードはシステムが各異常イベントのログ ファイルを検出して生成できるようにします。

イベントログ：イベントログはモニタリングモードで生成されます。NXSecure の正しいセンサーパスが構成されている場合は、テレメトリを使用してイベント ログをエクスポートできます。

Cisco Live Protect の注意事項と制約事項

Cisco Live Protect を使用する場合は、ご使用のソフトウェアリリースでプラットフォームと機能がサポートされていることを必ず確認してください。次の注意事項と制約事項に従って、互換性を確保し、サポートされていない展開を回避してください。

- **プラットフォーム サポート**：Cisco NX-OS リリース 10.6(1)F 以降で、この機能には以下の特徴があります：
 - 24G 以上の RAM を搭載した Cisco Nexus 9300-FX、-FX2、-FX3、-GX、-GX2、-H1、および -H2R スイッチでサポートされます。
 - Nexus 9800 および N9324C-SE1U を含む SiliconOne スイッチではサポートされていません。
- **他の機能との互換性**：アプリケーション ホスティングまたは AuditD 機能ではサポートされていません。

Cisco Live Protect の NXSecure 機能の有効化

NXSecure 機能を有効にするには、次の手順を実行します。

手順

NXSecure 機能を有効にするには、**feature nxsecure** コマンドを使用します。

例：

```
switch(config)# feature nxsecure
```

NXSecure 機能を無効にするには、このコマンドの **no** 形式を使用します。

NXSecure 機能が有効になっていること。Docker および NXSecure コンテナが開始されます。

Cisco Live Protect の NXSecure 設定の確認

Cisco Live Protect 機能の NXSecure 設定のステータスを確認するには、次の show コマンドを使用します。

コマンド	目的
show nxsecure status	NXSecure のステータスを表示します。
show nxsecure logfiles	生成されたログ ファイルの現在のセットを表示します。
show tech-support nxsecure	NXSecure のデバッグ ログを表示します。
show telemetry transport sessions	テレメトリ トランスポートセッションをループし、そのようなセッションに関する情報を表示します

検証コマンドの出力例

参考のために、リストされている show コマンドの出力例をここに示します。

- **show nxsecure status**

```
switch# show nxsecure status
Tetragon Agent Status: Running
```

- **show nxsecure logfiles**

```
switch# show nxsecure logfiles
tetragon-2025-03-17T22-17-32.948.log
tetragon-2025-03-17T22-21-59.194.log
tetragon-2025-03-17T22-25-58.694.log
tetragon.log
```

- **show telemetry transport sessions**

```
switch# show telemetry transport sessions
Session Id: 0
Dst Grp Id: 1000
IP Address:Port <ip address>
Transport: EVTLOG
Status: Connected
Last Connected: Tue Jun 24 14:33:32.577 IST
Last Disconnected: Tue Jun 24 14:33:32.570 IST
Tx Error Count: 0
Last Tx Error: None
```

イベント ログ

イベント ログは、以下のようなログ ファイルです：

- セキュリティ異常ごとに NXSecure モニタリング モードで生成されます。

- JSON 形式で出力されます。
- テレメトリを使用してエクスポートされます。

JSON ログ ファイル：NXSecure は、カーネル プログラムから受信した JSON イベントとアラートを含むログ ファイルを、プレーン JSON データとして生成します。システムは、最大 5 つの JSON イベント ファイルを生成するように設定されています。各ファイルには、サイズ制限（3 MB）または時間制限（120 秒）があり、どちらか早い方が適用されます。

テレメトリを使用したログ ファイルのエクスポート：テレメトリ トランスポートは、NXSecure ログ ファイルをリモート HTTPS サーバにエクスポートするために使用されます。これは、**path event-nxsecure** センサータイプが設定されている場合にのみ可能です。

テレメトリ パス センサー タイプを構成します

テレメトリを構成するときに、パス センサー タイプが構成されます。**event-history** や **event-monitor** などの既存のパス センサー タイプに加えて、NX-OS リリース 10.6(1)F では、新しいテレメトリ パス センサー タイプである **event-nxsecure** が導入されています。このセンサー タイプは、ログ ファイルを外部の受信者にエクスポートするために使用されます。新しい **path event-nxsecure** センサー タイプを設定するには、設定例を参考にしてください。

パス センサー タイプの設定の詳細については、該当するバージョンの『[Cisco Nexus 9000 シリーズ NX-OS プログラマビリティ ガイド](#)』の「テレメトリ」の章を参照してください。

設定例

```
switch(config)# telemetry
switch(config-telemetry)# certificate /bootflash/server.pem <ip address>
switch(config-telemetry)# destination-group 1
switch(conf-tm-dest)# ip address <ip address> port 8083 protocol HTTP encoding Form-data
switch(conf-tm-dest)# sensor-group 1
switch(conf-tm-sensor)# path event-nxsecure
switch(conf-tm-sensor)# data-source native
switch(conf-tm-sensor)# subscription 1
switch(conf-tm-sub)# dst-grp 1
switch(conf-tm-sub)# snsr-grp 1 sample-interval 0
```




第 29 章

TCP 認証オプションの設定

本書では、Cisco NX-OS デバイスに TCP 認証オプションを設定する手順について説明します。

- [TCP 認証オプションについて \(779 ページ\)](#)
- [TCP-AO キー チェーン \(780 ページ\)](#)
- [TCP-AO キー ロールオーバー \(782 ページ\)](#)
- [注意事項と制約事項 \(782 ページ\)](#)
- [TCP キーチェーンおよびキーの設定 \(783 ページ\)](#)
- [TCP キーチェーンの確認 \(786 ページ\)](#)
- [TCP キーチェーンの構成例 \(787 ページ\)](#)

TCP 認証オプションについて

RFC 5925 で定義されている TCP 認証オプション (TCP-AO) を使用すると、より強力なメッセージ認証コード (MAC) を使用して、長期間の TCP 接続をリプレイから保護できます。

TCP-AO は、RFC 2385 で定義されている TCP MD5 の代替案です。TCP MD5 とは異なり、TCP-AO はコリジョン攻撃に対する耐性があり、アルゴリズム的俊敏性とキー管理のサポートを提供します。

TCP-AO には次のような顕著な特徴があります。

- TCP-AO は、長時間の TCP 接続のセキュリティを強化するために、より強力なメッセージ認証コード (MAC) の使用をサポートしています。
- TCP-AO は、長期的な TCP 接続のリプレイから保護し、より明示的なキー管理を提供することで、エンドポイント間のキー変更を調整します。

TCP-AO 機能により TCP MD5 は廃止されます。Cisco NX-OS デバイスは、レガシー BGP ピアの TCP-MD5 オプションを引き続きサポートします。ただし、一方の端がデバイスに TCP MD5 オプションが構成され、もう一方のピアリングに TCP-AO オプションが構成されている構成はサポートされていません。

TCP-AO キー チェーン

TCP-AO は、トラフィック キー、およびキーと MAC アルゴリズムを使用して生成されたメッセージ認証コード (MAC) に基づいています。トラフィック キーは、TCP-AO キー チェーンで設定できるマスター キーから導出されます。TCP-AO キー チェーンを作成し、チェーン内のキーを設定するには、グローバルコンフィギュレーションモードで **key chain key-chain-name tcp** コマンドを使用します。TCP 接続を介して通信する両方のピアで TCP-AO キー チェーンを設定する必要があります。

TCP-AO キー チェーンのキーには、次の設定可能なプロパティがあります。

設定可能なプロパティ	説明 (Description)
send-id	発信セグメントの TCP-AO オプションのキー識別子。 ルータで構成された送信識別子は、ピアで構成された受信識別子と一致する必要があります。
recv-id	認証時に着信セグメントの TCP-AO キー識別子と比較されるキー識別子。 ルータで構成された受信識別子は、ピアで構成された送信識別子と一致する必要があります。
cryptographic-algorithm	発信セグメントの MAC を作成するために使用される MAC アルゴリズム。アルゴリズムは次のいずれかになります。 • AES-128-CMAC 認証アルゴリズム • HMAC-SHA-1 認証アルゴリズム • HMAC-SHA-256 認証アルゴリズム
include-tcp-options	このフラグは、MAC の計算に TCP-AO 以外の TCP オプションを使用するかどうかを示します。 このフラグを有効にすると、すべてのオプションの内容とゼロで埋められた認証オプションが MAC の計算に使用されます。 フラグを無効にすると、TCP-AO 以外のすべてのオプションが MAC 計算から除外されます。 このフラグはデフォルトでは無効になっています。 (注) このフラグの設定は、アプリケーション設定を使用可能にすると、アプリケーション設定によって上書きされます。

設定可能なプロパティ	説明 (Description)
send-lifetime	この設定は、キーが有効であり、TCP セグメントの TCP-AO ベースの認証に使用できる時間を決定します。キーのライフタイムが経過し、キーが期限切れになると、ライフタイムが最も若い次のキーが選択されます。
key-string	キー文字列は、両方のピアで設定された事前共有マスターキーであり、トラフィック キーを導出するために使用されます。

TCP-AO 形式

```

+-----+-----+-----+-----+
| Kind=29 | Length | KeyID | RNextKeyID |
+-----+-----+-----+-----+
|                                     MAC      ...
+-----+-----+-----+-----+
...-----+
...  MAC (con't) |
...-----+

```

TLV 形式のフィールドは、次のとおりです。

- Kind : TCP-AO を示す 29 という値。
- Length : TCP-AO シーケンスの長さを示します。
- KeyID : トラフィック キーの生成に使用されるマスター キー タプル (MKT) の送信識別子。
- RNextKeyID : 受信したセグメントの認証に使用できる MKT の受信識別子。
- MAC : TCP セグメント データとプレフィックス付き疑似ヘッダーに対して計算された MAC。

マスター キー タプル

トラフィック キーは、個々の TCP セグメントのメッセージ認証コードを計算するために使用されるキー情報です。

マスター キー タプル (MKT) を使用すると、一意のトラフィック キーを導出し、それらのトラフィック キーの生成に必要なキーマテリアルを含めることができます。MKT は、トラフィック キーが設定されるパラメータを示します。パラメータには、TCP オプションが認証されているかどうか、そしてトラフィック キーの導出および MAC 計算に使用されるアルゴリズムの指示子が含まれます。

各 MKT には、次の 2 つの識別子があります：

- **SendID** : SendID 識別子は、発信セグメントの TCP AO オプションの KeyID 識別子として挿入されます。

- **RecvID** : **RecvID** は、着信セグメントの TCP AO キー ID と照合されます。

TCP-AO キー ロールオーバー

TCP-AO キーは、**send-lifetime** を使用して設定された定義済みの期間有効です。**send-lifetime** が設定されていない場合、キーは非アクティブと見なされます。キーロールオーバーは、キーの送信ライフタイムに基づいて開始されます。

TCP-AO は、TCP-AO オプションフィールドの **RNextKeyID** および **KeyID** フィールドを使用して、新しい **MKT** の使用を調整します。ヒットレスキーロールオーバーの場合、キーチェーン設定の新しいキーと古いキーには、少なくとも 15 分間のオーバーラップが必要です。これは、TCP-AO が新しい **MKT** の使用を調整するのに十分な時間を確保するために必要です。

キーロールオーバーが開始されると、ピアルータの 1 つ（たとえばルータ A）が、ロールオーバーが必要であることを示します。ロールオーバーが必要であることを示すために、ルータ A は使用する新しい **MKT** の受信識別子（**recv-id**）に **RNextKeyID** を設定します。TCP セグメントを受信すると、ピアルータ（たとえばルータ B）は、データベースで送信識別子（**send-id**）を検索して、TCP-AO ペイロードの **RNextKeyID** によって示される **MKT** を見つけます。キーが使用可能で有効な場合、ルータ B は現在のキーを新しい **MKT** に設定します。ルータ B がロールオーバーした後、ルータ A も現在のキーを新しいプライマリ キータプルに設定します。

送信ライフタイムと送信ライフタイムの有効期限が重複してキーロールオーバーが開始されます。

現在のキーの有効期限が切れる前にアクティブ化できる新しいキーを設定しないと、キーがタイムアウトして期限切れになる可能性があります。このような期限が切れると、ピアルータが期限切れのキーで認証されたセグメントを拒否し、再送信が発生することがあります。再送信タイムアウト（**RTO**）が原因で接続が失敗する可能性があります。新しい有効なキーが構成済みで使用可能な場合、接続を再確立することができます。

注意事項と制約事項

- キーチェーン内の各キーの **send-id** と **recv-id** は一意である必要があります。**send-id** と **recv-id** は 0 ～ 255 の範囲から選択する必要があるため、TCP-AO キーチェーンに含められるのは最大 256 個のキーです。
- アプリケーション接続に関連付けられるキーチェーンは 1 つだけです。ロールオーバーは、常にこのキーチェーンのキー内で実行されます。
- 使用中のキーが期限切れになった場合は、有効なライフタイムを持つ新しいキーがそれぞれの側で設定されます。キーがロールオーバーするまで、セグメントの損失が予想されます。
- TCP-AO キーチェーン キーをアクティブと見なすには、**send-id**、**recv-id**、**key-string**、**send-lifetime**、および **cryptographic-algorithm** のすべての設定を行う必要があります。

- キーチェーンソフトウェアプロセスでは、送信ライフタイム構成に基づいて最新のキーが使用されます。または、同じキーチェーンの2つの異なるキーに同じ send-lifetime が設定されている場合は、最後に設定されたキーを選択します。同じ送信ライフタイムを持つ2つのキーを設定することは、ベストプラクティスではなく、推奨されません。
- ユーザーは、重複する2つのキー間の重複時間を15分以上に設定する必要があります。
- key-string、send-id、recv-id、cryptographic-algorithm、send-lifetime など使用中のキーの設定を変更すると、TCP 接続フラップが発生します。
- キーチェーンの設定タイプは、クライアントプロトコル内でリンクされているタイプと一致している必要があります。これらのタイプの不一致がある状態で試行されると、ユーザーに通知するための syslog メッセージが生成されます。たとえば、keychain_abc という名前のキーチェーンが Macsec キーチェーンとして設定されていても、BGP で TCP キーチェーンとして関連付けられている場合はサポートされません。同様に、キーチェーンが最初にクライアントに関連付けられ（前方参照と呼ばれるプロセス）、別のキーチェーンタイプとして設定される場合もサポートされません。

TCP キーチェーンおよびキーの設定

始める前に

- キー文字列、送信ライフタイム、暗号化アルゴリズム、およびキーの ID が両方のピアで一致することを確認します。
- ルータの送信 ID がピアルータの受信 ID と一致していることを確認します。個別のキースペースを使用する必要がある場合を除き、両方のパラメータに同じ ID を使用することをお勧めします。
- キーの送信 ID と受信 ID を同じキーチェーン内の別のキーに再利用することはできません。
- AES パスワード暗号化機能が有効になっており、プライマリ キーが構成されている場合、キースtringは暗号化され、タイプ6形式で保存されます。それ以外の場合、パスワードはタイプ7暗号化形式で保存されます。
- 詳細については、「[プライマリ キーの設定および AES パスワード暗号化機能のイネーブル化](#)」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 例： switch# configure terminal	グローバル構成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	key chain <i>name</i> tcp 例 : <pre>switch(config)# key chain bgp-keys tcp</pre>	指定したキーチェーンのキーチェーン 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 <i>key-ID</i> 例 : <pre>switch(config-tcpkeychain)# key 13</pre>	指定したキーのキー コンフィギュレーション モードを開始します。 <i>key-ID</i> 引数は、0 ～ 65535 の整数で指定する必要があります。
ステップ 4	send-id <i>send-ID</i> 例 : <pre>switch(config-tcpkeychain-tcpkey)# send-id 2</pre>	キーの送信 ID を指定します。 <i>send-ID</i> は、0 ～ 255 の範囲内で、キーチェーンごとに一意の値である必要があります。
ステップ 5	recv-id <i>recv-ID</i> 例 : <pre>switch(config-tcpkeychain-tcpkey)# recv-id 2</pre>	キーの受信 ID を指定します。 <i>recv-ID</i> は、0 ～ 255 の範囲内で、キーチェーンごとに一意の値である必要があります。
ステップ 6	key-string [<i>encryption-type</i>] <i>text-string</i> 例 : <pre>switch(config-tcpkeychain-tcpkey)# key-string 0 AS3cureStr1ng</pre>	そのキーのテキスト スtring を設定します。<i>text-string</i> 引数は英数字で指定します。特殊文字も使用できます。大文字と小文字は区別されます。 Encryption-type 引数に、次のいずれかの値を指定します。 • 0 : 入力した <i>text-string</i> 引数は、暗号化されていないテキスト文字列です。これがデフォルトです。 • 6 : Cisco NX-OS リリース 10.3(3)F 以降、Cisco Nexus 9000 シリーズプラットフォーム スイッチでシスコ独自の（タイプ 6 暗号化）方式がサポートされています。 • 7 : 入力した <i>text-string</i> 引数は、暗号化されています。シスコ固有の暗号方式で暗号化されます。このオプションは、別の Cisco NX-OS デバイス上で実行した show key chain コマンドの暗号化出力に基づいて、テキスト文字列を入力する場合に役立ちます。

	コマンドまたはアクション	目的																								
		key-string コマンドには、<i>text-string</i> での次の特殊文字の使用に関する制限があります。 <table border="1" data-bbox="1052 405 1520 1480"> <thead> <tr> <th data-bbox="1052 405 1105 562">特殊文字</th><th data-bbox="1105 405 1284 562">説明 (Description)</th><th data-bbox="1284 405 1520 562">注</th></tr> </thead> <tbody> <tr> <td data-bbox="1052 562 1105 688"> </td><td data-bbox="1105 562 1284 688">縦棒またはパイプ</td><td data-bbox="1284 562 1520 688">キー文字列の先頭ではサポートされていません</td></tr> <tr> <td data-bbox="1052 688 1105 814">></td><td data-bbox="1105 688 1284 814">右辺と比較して大きい</td><td data-bbox="1284 688 1520 814">キー文字列の先頭ではサポートされていません</td></tr> <tr> <td data-bbox="1052 814 1105 940">\</td><td data-bbox="1105 814 1284 940">バックスラッシュ</td><td data-bbox="1284 814 1520 940">キー文字列の先頭または末尾ではサポートされていません</td></tr> <tr> <td data-bbox="1052 940 1105 1066">(</td><td data-bbox="1105 940 1284 1066">左丸かっこ</td><td data-bbox="1284 940 1520 1066">キー文字列の先頭ではサポートされていません</td></tr> <tr> <td data-bbox="1052 1066 1105 1192">'</td><td data-bbox="1105 1066 1284 1192">アポストロフィ</td><td data-bbox="1284 1066 1520 1192">キー文字列の先頭ではサポートされていません</td></tr> <tr> <td data-bbox="1052 1192 1105 1318">"</td><td data-bbox="1105 1192 1284 1318">引用符</td><td data-bbox="1284 1192 1520 1318">キー文字列の先頭ではサポートされていません</td></tr> <tr> <td data-bbox="1052 1318 1105 1480">?</td><td data-bbox="1105 1318 1284 1480">疑問符</td><td data-bbox="1284 1318 1520 1480">サポート。ただし、疑問符 (?) を入力する前に Ctrl+V を押します。</td></tr> </tbody> </table> コマンドでの特殊文字の使用方法の詳細については、「コマンドラインインターフェイスについて」セクションを参照してください。	特殊文字	説明 (Description)	注		縦棒またはパイプ	キー文字列の先頭ではサポートされていません	>	右辺と比較して大きい	キー文字列の先頭ではサポートされていません	\	バックスラッシュ	キー文字列の先頭または末尾ではサポートされていません	(	左丸かっこ	キー文字列の先頭ではサポートされていません	'	アポストロフィ	キー文字列の先頭ではサポートされていません	"	引用符	キー文字列の先頭ではサポートされていません	?	疑問符	サポート。ただし、疑問符 (?) を入力する前に Ctrl+V を押します。
特殊文字	説明 (Description)	注																								
	縦棒またはパイプ	キー文字列の先頭ではサポートされていません																								
>	右辺と比較して大きい	キー文字列の先頭ではサポートされていません																								
\	バックスラッシュ	キー文字列の先頭または末尾ではサポートされていません																								
(	左丸かっこ	キー文字列の先頭ではサポートされていません																								
'	アポストロフィ	キー文字列の先頭ではサポートされていません																								
"	引用符	キー文字列の先頭ではサポートされていません																								
?	疑問符	サポート。ただし、疑問符 (?) を入力する前に Ctrl+V を押します。																								
ステップ 7	[no] cryptographic-algorithm {HMAC-SHA-1 HMAC-SHA-256 AES-128-CMAC } 例 :	TCP セグメントの MAC の計算に使用するアルゴリズムを指定します。1 つのキーに設定できる暗号化アルゴリズムは 1 つだけです。																								

	コマンドまたはアクション	目的
ステップ 8	switch(config-tcpkeychain-tcpkey) # cryptographic-algorithm HMAC-SHA-1 send-lifetime [local] start-time duration [duration-value infinite end-time] 例 : <pre>switch(config-tcpkeychain-tcpkey) # send-lifetime local 01:01:01 Jan 01 2023 01:01:01 Jan 10 2023</pre>	キーの送信ライフタイムを設定します。デフォルトでは、デバイスは start-time および end-time 引数を UTC として扱います。local キーワードを指定すると、デバイスはこれらの時間を現地時間として扱います。 start-time 引数は、キーがアクティブになる日時です。 送信ライフタイムの終了時は次のいずれかのオプションで指定できます。 • duration duration-value : ライフタイムの長さ (秒)。最大値は 2147483646 秒 (約 68 年) です。 • infinite : キーの送信ライフタイムは期限切れになりません。 • end-time : end-time 引数はキーがアクティブでなくなる日時です。
ステップ 9	(任意) include-tcp-options 例 : <pre>switch(config-tcpkeychain-tcpkey) # include-tcp-options</pre>	パケットの「MAC」ダイジェストを計算中に TCP ヘッダー (TCP AO オプション以外) の一部の「TCP オプション」全体を含める必要があるかどうかを指定するためのオプションの構成です。

TCP キーチェーンの確認

コマンド	目的
show key chain [name] [detail]	デバイスに設定されているキーチェーンを表示します。

```
switch# show key chain
Key-Chain bgp_keys tcp
  Key 2 -- text 7 "070e234f"
    send-id 2
    recv-id 2
    cryptographic-algorithm AES_128_CMAC
    send lifetime UTC (08:17:00 May 29 2023)-(08:21:00 May 29 2023)
    include-tcp-options
  Key 3 -- text 7 "070c2058"
    send-id 3
    recv-id 4
```



```
cryptographic-algorithm HMAC-SHA-1
send lifetime UTC (08:20:00 May 29 2023)-(always valid) [active]
include-tcp-options
Key 12 -- text ""
send lifetime UTC (08:20:00 May 29 2023)-(always valid)
```



(注) [active] は、キーが有効でアクティブであることを示します。それ以外の場合、キーは非アクティブです。上記の例では、キー 3 のみがアクティブで使用可能です。

show key chain detail コマンドは、アクティブなキーと非アクティブなキーを明示的に表示します。タイプ 6 暗号化の場合、**show key chain detail** コマンドを実行すると、タイプ 6 キー文字列が復号化可能かどうか也表示されます。また、クライアントがパケットを認証するために現在使用している最も新しいアクティブな送信キー也表示されます。

```
switch# show key chain detail
Key-Chain bgp_keys tcp
Key 1 -- text 6 "JDYk9k4kmaciqah6Eu2+9C0tmCRl9k7JAMys/fXGbw1lmHP88PAA=="
Type6 Decryptable: yes
send-id 1
recv-id 1
cryptographic-algorithm HMAC-SHA-1
send lifetime local (18:15:42 May 15 2023)-(always valid) [active]
include-tcp-options
accept-ao-mismatch
Key 2 -- text 6 "JDYkB+Fs8u3ujRDpFSu4tH6H7iTS45JJA6sKeGsBD0L3HjGDeg9AA=="
Type6 Decryptable: yes
send-id 2
recv-id 2
cryptographic-algorithm AES_128_CMACE
send lifetime local (17:10:47 May 15 2023)-(18:15:42 May 15 2023) [inactive]

youngest active send key: 1
```

TCP キーチェーンの構成例

bgp_keys という名前の TCP キーチェーンを設定する例を示します。各キー テキストストリングは暗号化されています。キーのライフタイム設定は重複しています。

```
key chain bgp_keys tcp
key 1
send-id 1
recv-id 1
key-string 7 070e234f
send-lifetime 01:00:00 Oct 10 2023 01:00:00 Oct 11 2023
cryptographic-algorithm AES-128-CMAC
key 2
send-id 2
recv-id 2
key-string 7 075e731f
send-lifetime 00:45:00 Oct 11 2023 01:00:00 Oct 12 2023
cryptographic-algorithm HMAC-SHA-256
include-tcp-options
```




索引

数字

- 802.1X [301, 304–305, 307, 310–311, 317–318, 344, 351](#)
 - MAC 認証バイパス [305](#)
 - オーセンティケータ PAE [304](#)
 - ガイドライン [311](#)
 - サポートされるトポロジ [307](#)
 - シングルホストのサポート [307](#)
 - デフォルト設定 [317](#)
 - マルチホストのサポート [307](#)
 - 機能のイネーブル化 [318](#)
 - 構成 [318](#)
 - 構成の確認 [344](#)
 - 制限事項 [311](#)
 - 設定例 [351](#)
 - 説明 [301](#)
 - 前提条件 [310](#)
- 802.1X サブリカント [329](#)
 - 手動による再認証 [329](#)
- 802.1X 再認証 [343](#)
 - インターフェイスでの最大再試行回数の設定 [343](#)
- 802.1X 認証 [303–304, 341](#)
 - RADIUS アカウンティングのイネーブル化 [341](#)
 - ポートの許可ステート [304](#)
 - 開始 [303](#)

A

- aa アカウンティングの表示 [58](#)
- aaa accounting default [24](#)
- aaa accounting default group [47](#)
- aaa accounting default local [47](#)
- aaa accounting dot1x default group [342](#)
- aaa authentication dot1x default group [319](#)
- aaa authentication login {mschap | mschapv2} enable [43](#)
- aaa authentication login ascii-authentication [125](#)
- aaa authentication login chap enable [42](#)
- aaa authentication login console [24, 31–32](#)
- aaa authentication login console group [31–32](#)
- aaa authentication login console local [31–32](#)
- aaa authentication login console none [31–32](#)
- aaa authentication login default [23](#)

- aaa authentication login error-enable [36](#)
- aaa authorization {commands | config-commands} {console | default} {group} [126](#)
- aaa authorization {group | local} [157](#)
- aaa authorization {ssh-certificate | ssh-publickey} [157](#)
- aaa authorization default [157](#)
- aaa authorization ssh-certificate default [44, 46](#)
- aaa group server ldap [148](#)
- aaa group server radius [81](#)
- aaa group server tacacs+ [114](#)
- aaa user default-role [36](#)
- accept-lifetime [639](#)
- aclog match-log-level [426](#)
- action {drop | forward | redirect} [469](#)
- authentication (bind-first | compare) [149](#)

B

- BGP [660](#)
 - ユニキャスト RPF との使用 [660](#)

C

- CA [207–208, 212–213, 215, 223, 226, 228, 233, 236, 239](#)
 - identity [208](#)
 - multiple [213](#)
 - アイデンティティ証明書のインストール [228](#)
 - アイデンティティ証明書要求の作成 [226](#)
 - カットアンドペーストによる登録 [212](#)
 - ピア証明書 [213](#)
 - 構成 [215](#)
 - 構成の表示 [236](#)
 - 証明書のダウンロードの例 [239](#)
 - 証明書の削除 [233](#)
 - 設定例 [236](#)
 - 説明 [207](#)
 - 認証 [223](#)
 - 複数のトラストポイント [212](#)
 - 目的 [207](#)
- CA トラストポイント [219](#)
 - PKI のアソシエーションの作成 [219](#)
- chgrp [173](#)
- chown [173](#)

class 697
 class class-default 697
 class insert-before 697
 class-map 688
 class-map type control-plane {match-all | match-any} 696, 705, 707
 clear access-list ipsg stats 614
 clear copp statistics 713
 clear hardware rate-limiter {all | access-list-log | bfd | exception | fex |
 layer-3 glean | layer-3 multicast local-groups |
 span-egress} 724
 clear hardware rate-limiter module 724
 clear ip access-list counters 434
 clear ip arp inspection log 602
 clear ip arp inspection statistics 602
 clear ip dhcp global statistics 563
 clear ip dhcp relay statistics interface 563
 clear ip dhcp snooping binding interface ethernet 562
 clear ip dhcp snooping binding interface port-channel 562
 clear ip dhcp snooping binding vlan 562
 clear ip dhcp snooping statistics 562
 clear ip dhcp snooping statistics vlan 562
 clear ipv6 access-list counters 434
 clear ipv6 dhcp relay statistics interface 563
 clear ldap-server statistics 160
 clear line 197, 199
 clear mac access-list counters 464
 clear port-security dynamic 490
 clear port-security dynamic address 489
 clear radius-server statistics 97
 clear ssh hosts 195
 clear tacacs-server statistics 134
 conf-offset 744
 control-plane 688, 700–701
 copp copy profile {strict | Moderate | lenient | 高密度} 703
 copp copy profile prefix {サフィックス} 703
 copp profile 702
 copp profile dense 702
 copp profile lenient 702
 copp profile Moderate 702
 copp profile strict 702
 copy scp: 180, 203
 copy sftp: 203
 CRL 214, 232, 262, 264, 269
 インポートの例 269
 ダウンロード 264
 パブリッシュ 262
 構成 232
 生成 262
 説明 214
 crypto ca aauthenticate 186
 crypto ca crt request 186
 crypto ca trustpoint 186

D

deadtime 82
 deny 391, 393, 395
 description 290
 DHCP リレー オンスタック 569
 説明 569
 DoS 攻撃 661
 ユニキャスト RPF、配置 661
 dot1x default 340
 dot1x host-mode {multi-host | single-host} 337
 dot1x max-req 341
 dot1x port-control {auto | force-authorized | forced-unauthorized} 321
 dot1x re-authentication 328
 dot1x timeout quiet-period 330
 dot1x timeout ratelimit-period 331
 dot1x timeout re-authperiod 328
 dot1x timeout server-timeout 331
 dot1x timeout supp-timeout 331
 dot1x timeout tx-period 331

E

enable Cert-DN-match 149
 enable user-server-group 149
 encryption decrypt type6 622
 encryption delete type6 624
 encryption re-encrypt obfuscated 621–622, 636
 encryption-algorithm {HMAC-SHA-1 | HMAC-SHA-256 |
 HMAC-SHA-384 | HMAC-SHA-512 | MD5} 641

F

feature 291
 feature dhcp 518
 feature dot1x 319
 feature macsec 736–737
 feature password encryption aes tam 621, 636
 feature port-security 483
 feature scp-server 184
 feature sftp-server 184
 feature ssh 176, 194
 feature tacacs+ 109
 feature telnet 198
 FIPS 13, 16–17, 19
 セルフテスト 13
 設定例 19
 無効化 17
 有効化 16
 fragments {permit-all | deny-all} 390, 393

G

generate type7_encrypted_secret 54, 73, 75, 111, 113

H

hardware access-list team region 398, 706
 hardware access-list team region ing-ifacl qualify udf 418, 455
 hardware profile team resource service-template 410
 hardware profile team resource template 410
 hardware rate-limiter access-list-log 426, 722
 hardware rate-limiter bfd 722
 hardware rate-limiter exception 722
 hardware rate-limiter fex 722
 hardware rate-limiter layer-3 glean 723
 hardware rate-limiter layer-3 multicast local-groups 723
 hardware rate-limiter span-egress 723

I

ID 証明書 226, 228, 233
 PKI の削除 233
 インストール 228
 要求の作成 226
 interface policy dent 292
 ip access-class 395
 ip access-group 421, 425
 ip access-list 390, 393, 395, 419, 428
 ip arp inspection log-buffer entries 600
 ip arp inspection trust 597
 ip arp inspection validate 599
 ip arp inspection validate dst-mac 599
 ip arp inspection validate ip 599
 ip arp inspection validate src-mac 599
 ip arp inspection vlan 596, 600
 ip dhcp packet strict-validation 504, 524
 ip dhcp relay 529, 532
 ip dhcp relay address 535
 ip dhcp relay address use-vrf 535
 ip dhcp relay information option 530
 ip dhcp relay information option server-id-override-disable 533
 ip dhcp relay information option trust 526
 ip dhcp relay information option vpn 532
 ip dhcp relay information trust-all 528
 ip dhcp relay information trusted 527
 ip dhcp relay sub-option circuit-id customized 530
 ip dhcp relay sub-option circuit-id format-type string 531
 ip dhcp relay sub-option type cisco 532
 ip dhcp smart-relay 538
 ip dhcp smart-relay global 537
 ip dhcp snooping information option 522
 ip dhcp snooping ipsg-excluded vlan 614
 ip dhcp snooping trust 525
 ip dhcp snooping verify mac-address 520
 ip dhcp snooping vlan 520
 ip port accessgroup 422
 ip radius source-interface 83
 ip source binding 613
 ip tacacs source-interface 115

ip verify source dhcp-snooping-vlan 612
 ip verify unicast source reachable-via 667
 ip verify unicast source reachable-via any 665
 IP ドメイン名 216
 PKI での設定 216
 ipdhcprelayscale-interface 536
 ipv6 access-class 395
 ipv6 access-list 390, 393, 395
 ipv6 address use-link-local-only 554
 ipv6 dhcp relay 540
 ipv6 dhcp relay address 545
 ipv6 dhcp relay option type cisco 542
 ipv6 dhcp relay option vpn 542
 ipv6 dhcp relay source-interface 547
 ipv6 dhcp smart-relay 544
 ipv6 dhcp smart-relay global 543
 ipv6 port traffic-filter 422
 ipv6 traffic-filter 421
 ipv6 verify unicast source reachable-via 667
 ipv6 verify unicast source reachable-via any 665

K

key-chain macsec-psk no-show 738
 key-octet-string 738
 key-server-priority 743
 key-string 637

L

ldap search-map 153
 ldap-server deadtime 155–156
 ldap-server host 146, 151–152, 155
 ldap-server host idle-time 155
 ldap-server host password 147, 155
 ldap-server host port 147, 152
 ldap-server host rootDN 147
 ldap-server host test rootDN 155
 ldap-server host timeout 147, 152
 ldap-server host username 155
 ldap-server timeout 150
 line vty 395
 logging drop threshold 698
 logging ip access-list cache entries 426
 logging ip access-list cache interval 425
 logging ip access-list cache threshold 426
 logging ip access-list detailed 426
 login block-for 50
 login block-for attempts 50
 login on-failure log 37
 login on-success log 38
 login quiet-mode access-class 51

M

mac access-list 453, 456–457
 mac packet-classify 461
 mac port access-group 456, 460
 MAC アドレス 474
 ラーニング 474
 MAC 認証 305
 802.1X のバイパス 305
 macsec policy 742
 match {ip | ipv6} address 469
 match access-group name 696, 705, 707
 match exception {ip | ipv6} icmp redirect 696
 match exception {ip | ipv6} icmp unreachable 696
 match exception {ip | ipv6} option 696
 match mac address 469
 match protocol arp 696

N

no {periodic | absolute} 447
 no aaa authentication login {console | default | fallback error local 24, 35
 no aaa authentication login ascii-authentication 41, 43
 no dot1x system-auth-control 338
 no feature dot1x 339
 no feature ssh 175, 194–196
 no feature tacacs+ 133
 no host 441–442
 no ip access-list 397
 no ipv6 access-list 397
 no key chain 634
 no mac access-list 459
 no object-group {ip address | ipv6 address | ip port} 444
 no ssh key dsa 196
 no ssh key rsa 196
 no time-range 448
 no vlan access-map 470

O

object-group ip address 440
 object-group ip port 442
 object-group ipv6 address 441

P

password prompt username 53
 password strength-check 283
 permit 395
 permit | deny 453
 permit http-method 428
 permit interface 292
 permit ip 419
 permit mac 456

permit udf 419
 permit vlan 294
 permit vrf 295
 PKI 207, 212–217, 236
 IP ドメイン名の設定 216
 RSA キー ペアの生成 217
 ガイドライン 214
 デフォルト設定 215
 ホスト名の設定 216
 構成の表示 236
 証明書失効確認 213
 制限事項 214
 設定例 236
 説明 207
 登録のサポート 212
 police 698, 705, 707
 police cir 698, 705, 707
 policy-map 688
 policy-map type control-plane 697

R

RADIUS アカウンティング 341
 802.1X 認証のイネーブル化 341
 radius-server deadtime 90–92
 radius-server directed-request 84
 radius-server host 54, 72, 74, 82, 86–87, 91
 radius-server host accounting 88
 radius-server host acct-port 87
 radius-server host auth-port 88
 radius-server host authentication 88
 radius-server host idle-time 91
 radius-server host password 91
 radius-server host retransmit 86
 radius-server host test 91
 radius-server host timeout 86
 radius-server host username 91
 radius-server key 54, 73
 radius-server retransmit 85
 radius-server test {idle-time} 89
 radius-server test {password} 89
 radius-server test {username} 89
 radius-server timeout 85
 reload 406, 411, 419, 455, 704, 706
 resequence {ip | ipv6} access-list 396
 resequence mac access-list 458
 resequence time-range 449
 role feature-group name 291
 role name 289, 292–293, 295
 role name priv 131
 RSA キー ペア 210, 213–214, 217, 230–231, 235–236
 Cisco NX-OS デバイスからの削除 235
 multiple 213
 PKI に生成 217

RSA キー ペア (続き)

インポート 214, 231

エクスポート 214, 230

構成の表示 236

説明 210

rule {deny | permit} command 289

rule {deny | permit} {read | read-write} 289

rule {deny | permit} {read | read-write} feature 289

rule {deny | permit} {read | read-write} feature-group 289

rule {deny | permit} {read | read-write} oid 290

rule {deny | permit} command 131

S

sak-expiry-time 744

security-policy 743

send-lifetime 640, 739

service-policy 688

service-policy input 700

set cos 698

show {ip | ipv6 | access-lists} 444

show aaa accounting 48, 343

show aaa authentication 32, 34–35, 37, 59

show aaa authentication login {ascii-authentication | chap | error-enable
| mschap | mschapv2} 59

show aaa authentication login {mschap | mschapv2} 44

show aaa authentication login chap 42

show aaa authorization 45, 127, 157

show aaa authorization all 45

show aaa groups 59

show aaa user default-role 36

show class-map type control-plane 697, 709

show cli syntax roles network-admin 297

show cli syntax roles network-operator 297

show copp profile 710

show copp status 702–703, 711

show crypto ca certificates 187, 200

show crypto ca crt 187, 200

show dot1x 319, 338

show dot1x {all | interface ethernet} 351

show dot1x all 321, 328, 331, 337, 340–341

show dot1x interface ethernet 321

show encryption service stat 621, 636

show hardware access-list interface input entries detail 433

show hardware access-list team region 406, 431

show hardware access-list team template 411, 431

show hardware rate-limiter 724–725

show hardware rate-limiter access-list-log 724–725

show hardware rate-limiter bfd 724–725

show hardware rate-limiter exception 724–725

show hardware rate-limiter fex 724–725

show hardware rate-limiter layer-3 glean 724–725

show hardware rate-limiter layer-3 multicast local-groups 724–725

show hardware rate-limiter module 724–725

show hardware rate-limiter span-egress 724–725

show incompatibility nxos bootflash: 690

show interface counters storm-control 649, 656

show interface ethernet counters storm-control 656

show interface port-channel counters storm-control 656

show interface port-channel counters storm-control multi-threshold 656

show interface port-channel counters storm-control multi-threshold
broadcast 656show interface port-channel counters storm-control multi-threshold
multicast 656show interface port-channel counters storm-control multi-threshold
unicast 656

show interface switchport 673

show ip access-lists 392, 394–396, 429, 431, 433

show ip access-lists summary 397

show ip arp inspection 602

show ip arp inspection interface 598

show ip arp inspection interfaces 602

show ip arp inspection log 602

show ip arp inspection statistics 602

show ip arp inspection vlan 596, 602

show ip dhcp relay 526, 529, 531, 536–537, 539, 558

show ip dhcp relay address 560

show ip dhcp relay information trusted-sources 526–528

show ip dhcp relay statistics 562

show ip dhcp snooping binding 561, 613

show ip interface 665

show ip ver source 614

show ip ver source ethernet 614

show ip ver source port-channel 614

show ipv6 access-lists 392, 394–395, 431, 434

show ipv6 access-lists summary 397

show ipv6 dhcp relay 541–544, 548, 558

show ipv6 dhcp relay interface 542

show ipv6 dhcp relay statistics 562

show key chain 634–635, 638, 640, 642, 739

show key chain mode decrypt 638, 640

show ldap-search-map 154, 161

show ldap-server 146, 148, 150–152, 155–156, 161

show ldap-server groups 149, 161

show ldap-server statistics 159–161

show logging ip access-list cache 427, 432

show logging ip access-list status 432

show login 51, 59

show login failures 51

show login on-failure log 38

show login on-successful log 38

show mac access-lists 454, 457–459, 463–464

show macsec mka session 756

show macsec mka statistics 758

show macsec mka summary 756

show macsec policy 744, 756

show macsec secy statistics 758

show object-group 441–444

show password strength-check 283

show policy-map interface control-plane 702, 709, 712–713

show policy-map type control-plane 699, 708

- show policy-map type control-plane expand 699
- show policy-map type control-plane name 699
- show port-security 483, 494
- show port-security address 490, 494
- show port-security address interface 489
- show port-security interface 494
- show radius {status | pending | pending-diff} 96
- show radius-server 72, 74–75, 83, 86–88, 90–92, 96, 320
- show radius-server directed-request 85
- show radius-server groups 82, 320
- show radius-server statistics 97
- show role 286, 290, 293–295, 297
- show role feature 298
- show role feature-group 291, 298
- show run interface 429
- show running-config aaa 59
- show running-config acllog 432
- show running-config aclmgr 421–422, 432, 444, 460, 463, 469–471, 710
- show running-config aclmgr all 432, 463
- show running-config all | i max-login 52, 59
- show running-config copp 701, 703, 710
- show running-config copp all 701
- show running-config dhcp 518, 520, 523–526, 528–529, 531–532, 535–537, 539, 541–544, 546, 599–602, 612
- show running-config interface 561, 656, 673
- show running-config interface {ethernet | port-channel} 653, 655
- show running-config interface ethernet 461, 554, 669, 673
- show running-config interface mgmt0 554
- show running-config interface port-channel 461, 673
- show running-config interface vlan 554
- show running-config ip 669
- show running-config ipv6 669
- show running-config ldap 160
- show running-config macsec 756
- show running-config port-security 485–488, 492–494
- show running-config radius 96
- show running-config security 184, 200, 298
- show running-config security all 179, 200, 298
- show running-config tacacs 134
- show running-config tacacs all 134
- show ssh key 176, 197, 200
- show ssh key dsa 200
- show ssh key md5 200
- show ssh key rsa 200
- show ssh server 196, 200
- show startup-config aaa 59
- show startup-config acllog 432
- show startup-config aclmgr 433, 463, 471, 711
- show startup-config aclmgr all 433, 463, 471
- show startup-config dhcp 561
- show startup-config dhcp all 561
- show startup-config interface ethernet 669
- show startup-config ip 669
- show startup-config ldap 161
- show startup-config radius 96
- show startup-config security 298
- show startup-config tacacs 134
- show system login 51
- show system login failures 51
- show tacacs-server 110, 112–113, 115, 118–119, 121, 123–125, 134
- show tacacs-server directed-request 117, 134
- show tacacs-server groups 114, 134
- show tacacs-server sorted 134
- show tacacs-server statistics 133–134
- show tacacs+ {pending | pending-diff} 110, 116, 118–119, 124–125, 127
- show tacacs+ {status | pending | pending-diff} 134
- show telnet server 198, 200
- show time-range 447–449
- show user-account 177–178, 187, 200, 288, 297–298
- show username 181
- show username keypair 200
- show userpassphrase {length | max-length | min-length} 53, 59
- show users 187, 197, 199–200
- show vlan access-map 472
- show vlan filter 472
- ssh 180
- ssh login-attempts 179
- ssh vrf 180
- ssh6 180
- ssh6 vrf 180
- statistics per-entry 391, 394, 454, 457, 469
- storm-control {broadcast | multicast | unicast} 653
- storm-control action trap 653, 655
- storm-control multi unicast 655
- switchport 485–486
- switchport block {multicast | unicast} 673
- switchport block ethernet switchport 673
- switchport block port-channel switchport 673
- switchport port-security 485
- switchport port-security aging time 493
- switchport port-security aging type 492
- switchport port-security mac-address 487–488
- switchport port-security mac-address sticky 486, 489
- switchport port-security maximum 491
- switchport port-security violation 494
- system login block-for 50
- system login block-for attempts 50
- system login block-for within 50
- system login quiet-mode access-class 51

T

- tacacs-server dead-time 121–122
- tacacs-server deadtime 123
- tacacs-server directed-request 116
- tacacs-server host 54, 110, 112, 114, 117, 119, 122
- tacacs-server host port 119
- tacacs-server host timeout 117
- tacacs-server key 54, 111
- tacacs-server test 120
- tacacs-server test idle-time 120

tacacs-server test username 120
 tacacs+ commit 110, 116, 118–119, 124–125, 127
 telnet 199
 telnet vrf 199
 telnet6 199
 telnet6 vrf 199
 terminal no verify-only 129
 terminal no verify-only username 129
 terminal verify-only 129
 terminal verify-only username 129
 test aaa authorization command-type {commands | config-commands}
 user command 128
 test aaa group 94, 132
 test aaa server radius 94
 test aaa server radius vrf 94
 test aaa server tacacs + 132
 time-range 446

U

udf 417, 454
 use-vrf 82, 149
 username keypair export 182
 username keypair export {rsa | dsa} 182
 username keypair generate 181
 username keypair import 182
 username keypair import {rsa | dsa} 182
 username password 185, 286
 username sshkey 178
 username sshkey file bootflash 177
 userpassphrase max-length 53
 userpassphrase min-length 53

V

vlan access-map 468
 vlan filter 471
 vlan policy deny 293
 vPC ファーストホップセキュリティ設定 569
 説明 569
 VPC レッグでの DHCP リレー 570
 説明 570
 vrf policy deny 295

W

window-size 743

あ

アカウンティング ログの表示 58
 あかうんていんぐろぐのしょうきよ 58

お

オーセンティケータ PAE 304, 324
 インターフェイスからの削除 324
 インターフェイスの作成 324
 説明 304

か

ガイドライン 481
 ポートセキュリティ 481

き

キー 623, 637, 639, 641, 738
 キーチェーン 634, 637, 639, 641, 738

さ

サーバ (Server) 82, 114, 149
 サービス拒絶攻撃 661
 IP アドレス スプーフィング、軽減 661

す

スケールファクタ 701

せ

セキュア MAC アドレス 474
 ラーニング 474
 セキュリティ 474
 port 474
 MAC address learning 474

た

ダイナミック モード 705, 708

て

デジタル証明書 207, 213–215
 peers 213
 インポート 214
 エクスポート 214
 構成 215
 説明 207, 214
 目的 207
 デバイスの役割 302
 802.1X の説明 302

デフォルト設定 [215, 317, 481](#)
802.1X [317](#)
PKI [215](#)
ポート セキュリティ [481](#)

と

トラスト ポイント [208, 212, 229](#)
multiple [212](#)
リブート後の設定の保存 [229](#)
説明 [208](#)

ほ

ポート [304](#)
802.1X の許可ステート [304](#)
ポート セキュリティ [473–474, 476, 481](#)
MAC address learning [474](#)
MAC 移動 [476](#)
ガイドライン [481](#)
デフォルト設定 [481](#)
制限事項 [481](#)
説明 [473](#)
判別 [476](#)
ホスト [440–441](#)

ホスト名 [216](#)
PKI での設定 [216](#)

ゆ

ユーザ 最大ログイン数 [51](#)
ユーザー単位の DACL [316](#)
ガイドライン [316](#)
制限事項 [316](#)
ユーザ名 [177](#)
ユニキャスト RPF [659–661, 664, 668–669](#)
BGP 属性 [660](#)
BOOTP [661](#)
DHCP [661](#)
FIB [659](#)
ガイドライン [661](#)
デフォルト設定 [664](#)
トンネリング [661](#)
構成の確認 [669](#)
実装 [660](#)
制限事項 [661](#)
設定例 [668](#)
説明 [659](#)
展開 [661](#)

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。