



Cisco Nexus 3000 シリーズ NX-OS セキュリティ コンフィギュレーションガイド リリース 7.x

初版：2015年08月18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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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: <http://www.cisco.com/go/trademarks>. 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. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



目次

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

概要 3

Authentication, Authorization, and Accounting (認証、許可、およびアカウントिंग) 3

RADIUS および TACACS+ セキュリティ プロトコル 4

SSH および Telnet 5

IP ACL 5

認証、許可、アカウントिंगの設定 7

AAA の概要 7

AAA セキュリティ サービス 7

AAA を使用する利点 8

リモート AAA サービス 8

AAA Server Groups 9

AAA サービス設定オプション 9

ユーザ ログインの認証および許可プロセス 10

リモート AAA の前提条件 12

AAA の注意事項と制約事項 12

AAA の設定 12

コンソール ログイン認証方式の設定 12

デフォルトのログイン認証方式の設定 14

ログイン認証失敗メッセージのイネーブル化 15

AAA コマンド許可の設定 15

MSCHAP 認証のイネーブル化 17

デフォルトの AAA アカウントिंग方式の設定 19

AAA サーバの VSA の使用 20

VSA 20

VSA の形式 21

AAA サーバ上でのスイッチのユーザ ロールと SNMPv3 パラメータの指定	21
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	22
AAA 設定の確認	22
AAA の設定例	23
デフォルトの AAA 設定	23
RADIUS の設定	25
RADIUS の概要	25
RADIUS ネットワーク環境	25
RADIUS の操作について	26
RADIUS サーバのモニタリング	27
ベンダー固有属性	28
RADIUS の前提条件	28
RADIUS の注意事項と制約事項	28
RADIUS サーバの設定	29
RADIUS サーバ ホストの設定	29
RADIUS のグローバルな事前共有キーの設定	30
RADIUS サーバの事前共有キーの設定	31
RADIUS サーバ グループの設定	32
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	34
ログイン時にユーザによる RADIUS サーバの指定を許可	34
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	35
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	36
RADIUS サーバのアカウントingおよび認証属性の設定	37
RADIUS サーバの定期的モニタリングの設定	39
デッドタイム間隔の設定	40
RADIUS サーバまたはサーバ グループの手動モニタリング	41
RADIUS 設定の確認	41
RADIUS サーバ統計情報の表示	42
RADIUS サーバ統計情報のクリア	42
RADIUS の設定例	43
RADIUS のデフォルト設定	43
RADIUS の機能の履歴	43

TACACS+ の設定	45
TACACS+ の設定に関する情報	45
TACACS+ の利点	46
TACACS+ を使用したユーザ ログイン	46
デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー	47
TACACS+ サーバのモニタリング	47
TACACS+ の前提条件	48
TACACS+ の注意事項と制約事項	48
TACACS+ の設定	49
TACACS+ サーバの設定プロセス	49
TACACS+ のイネーブル化	49
TACACS+ サーバホストの設定	50
TACACS+ のグローバルな事前共有キーの設定	51
TACACS+ サーバの事前共有キーの設定	52
TACACS+ サーバグループの設定	52
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	54
ログイン時の TACACS+ サーバの指定	54
グローバルな TACACS+ タイムアウト間隔の設定	55
サーバのタイムアウト間隔の設定	56
TCP ポートの設定	56
TACACS+ サーバの定期的モニタリングの設定	57
デッドタイム間隔の設定	58
TACACS+ サーバまたはサーバグループの手動モニタリング	59
TACACS+ のディセーブル化	59
TACACS+ 統計情報の表示	60
TACACS+ の設定の確認	60
TACACS+ の設定例	61
TACACS+ のデフォルト設定	61
SSH および Telnet の設定	63
SSH および Telnet の概要	63
SSH サーバ	63

SSH クライアント	63
SSH サーバ キー	64
Telnet サーバ	64
SSH の注意事項および制約事項	65
SSH の設定	65
SSH サーバ キーの生成	65
ユーザアカウント用 SSH 公開キーの指定	66
Open SSH 形式による SSH 公開キーの指定	66
IETF SECSH 形式による SSH 公開キーの指定	67
PEM フォーマット化された公開キー証明書形式による SSH 公開キーの指定	67
SSH ソース インターフェイスの設定	68
リモート デバイスとの SSH セッションの開始	69
SSH ホストのクリア	69
SSH サーバのディセーブル化	70
SSH サーバ キーの削除	70
SSH セッションのクリア	71
SSH の設定例	71
Telnet の設定	72
Telnet サーバのディセーブル化	72
Telnet サーバの再イネーブル化	73
Telnet ソース インターフェイスの設定	73
リモート デバイスとの Telnet セッションの開始	74
Telnet セッションのクリア	74
SSH および Telnet の設定の確認	75
SSH のデフォルト設定	75
PKI の設定	77
PKI の概要	77
CA とデジタル証明書	77
信頼モデル、トラストポイント、アイデンティティ CA	78
RSA のキー ペアとアイデンティティ証明書	78
複数の信頼できる CA のサポート	79

PKI の登録のサポート	80
カットアンドペーストによる手動での登録	80
複数の RSA キー ペアとアイデンティティ CA のサポート	80
ピア証明書の検証	81
証明書の取消確認	81
CRL のサポート	81
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	82
PKI のライセンス要件	82
PKI の注意事項と制約事項	82
PKI のデフォルト設定	83
CA の設定とデジタル証明書	83
ホスト名と IP ドメイン名の設定	83
RSA キー ペアの生成	84
トラストポイント CA のアソシエーションの作成	86
CA の認証	87
証明書取消確認方法の設定	89
証明書要求の作成	90
アイデンティティ証明書のインストール	92
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	93
PKCS 12 形式でのアイデンティティ情報のエクスポート	94
PKCS 12 形式でのアイデンティティ情報のインポート	95
CRL の設定	96
CA の設定からの証明書の削除	97
Cisco NX-OS デバイスからの RSA キー ペアの削除	98
PKI の設定の確認	99
PKI の設定例	100
Cisco NX-OS デバイスでの証明書の設定	100
CA 証明書のダウンロード	103
アイデンティティ証明書の要求	109
証明書の取り消し	123
CRL の作成と公開	126
CRL のダウンロード	128

CRL のインポート	131
アクセス コントロール リストの設定	135
ACL の概要	135
IP ACL のタイプと適用	136
適用順序	137
ルール	137
送信元と宛先	137
プロトコル	138
暗黙のルール	138
その他のフィルタリング オプション	138
シーケンス番号	139
論理演算子と論理演算ユニット	140
ACL TCAM リージョン	141
ACL のライセンス要件	143
ACL の前提条件	143
ACL の注意事項と制約事項	143
デフォルトの ACL 設定	145
ACL ロギング	145
IP ACL の設定	145
IP ACL の作成	145
IP ACL の変更	146
IP ACL の削除	148
IP ACL 内のシーケンス番号の変更	148
mgmt0 への IP-ACL の適用	149
ポート ACL としての IP ACL の適用	150
ルータ ACL としての IP ACL の適用	151
IP ACL の設定の確認	152
IP ACL の統計情報のモニタリングとクリア	153
RACL 整合性チェッカーのトリガー	153
ACL ロギングの設定	154
ACL ロギング キャッシュの設定	154
インターフェイスへの ACL ロギングの適用	155

ACL ログの一致レベルの適用	156
ログ ファイルのクリア	156
ACL ロギング設定の確認	156
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	157
VLAN ACL の概要	159
VACL とアクセス マップ	160
VACL とアクション	160
統計情報	160
VACL の設定	160
VACL の作成または変更	160
VACL の削除	161
VACL の VLAN への適用	162
VACL の設定の確認	163
VACL 統計情報の表示と消去	163
VACL の設定例	163
LOU しきい値の設定	163
ACL TCAM リージョン サイズの設定	164
デフォルトの TCAM リージョン サイズに戻す	167
仮想端末回線の ACL の設定	167
VTY 回線の ACL の確認	169
VTY 回線の ACL の設定例	169
DHCP スヌーピングの設定	171
DHCP スヌーピングの概要	171
機能のイネーブル化とグローバルなイネーブル化	172
信頼できる送信元と信頼できない送信元	173
DHCP スヌーピング バインディング データベース	173
DHCPv6 リレー エージェントの概要	174
DHCPv6 リレー エージェント	174
DHCPv6 リレー エージェントに対する VRF サポート	174
DHCP スヌーピングのライセンス要件	174
DHCP スヌーピングの前提条件	175
DHCP スヌーピングの注意事項および制約事項	175

DHCP スヌーピングのデフォルト設定	175
DHCP スヌーピングの設定	176
DHCP スヌーピングの最小設定	176
DHCP スヌーピング機能のイネーブル化またはディセーブル化	177
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	178
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	179
Option 82 データの挿入および削除のイネーブル化またはディセーブル化	180
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	180
インターフェイスの信頼状態の設定	181
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	182
DHCP リレー エージェントに対する Option 82 のイネーブル化またはディセーブル化	183
インターフェイスへの DHCP サーバアドレスの設定	184
DHCP スタティック バインディングの作成	186
DHCPv6 リレー エージェントの設定	187
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	187
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	188
DHCPv6 リレー送信元インターフェイスの設定	190
DHCP スヌーピング設定の確認	191
DHCP バインディングの表示	191
DHCP スヌーピング バインディング データベースのクリア	192
DHCP リレー統計情報のクリア	193
DHCPv6 リレー統計情報のクリア	193
DHCP のモニタリング	193
DHCP スヌーピングの設定例	194
ダイナミック ARP インспекションの設定	195
DAI の概要	195
ARP	195
ARP スプーフィング攻撃	196
DAI および ARP スプーフィング攻撃	197
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	197

DAI パケットのロギング	199
DAI のライセンス要件	199
DAI の前提条件	199
DAI の注意事項と制約事項	200
DAI のデフォルト設定	201
DAI の設定	201
VLAN での DAI のイネーブル化とディセーブル化	201
レイヤ 2 インターフェイスの DAI 信頼状態の設定	202
追加検証のイネーブル化またはディセーブル化	203
DAI のログ バッファ サイズの設定	205
DAI のログ フィルタリングの設定	205
DAI の設定の確認	206
DAI の統計情報のモニタリングとクリア	207
DAI の設定例	207
例 1 : 2 つのデバイスが DAI をサポートする場合	207
デバイス A の設定	208
デバイス B の設定	210
ユニキャスト RPF の設定	213
ユニキャスト RPF の概要	213
ユニキャスト RPF プロセス	214
グローバル統計情報	215
ユニキャスト RPF のライセンス要件	215
ユニキャスト RPF の注意事項と制約事項	215
ユニキャスト RPF のデフォルト設定	216
ユニキャスト RPF の設定	217
ユニキャスト RPF の設定例	219
ユニキャスト RPF の設定の確認	219
コントロールプレーン ポリシングの設定	221
CoPP の概要	222
コントロールプレーン保護	223
コントロールプレーンのパケット タイプ	223
CoPP の分類	224

レート制御メカニズム	224
CoPP ポリシー テンプレート	225
デフォルト CoPP ポリシー	225
レイヤ 2 CoPP ポリシー	226
レイヤ 3 CoPP ポリシー	228
スタティック CoPP クラス	229
CoPP クラス マップ	232
1 秒間あたりのパケットのクレジット制限	232
CoPP と管理インターフェイス	232
CoPP のライセンス要件	233
CoPP の注意事項と制約事項	233
CoPP のアップグレードに関する注意事項	234
CoPP の設定	235
コントロールプレーン クラス マップの設定	235
コントロールプレーン ポリシー マップの設定	236
コントロールプレーン サービス ポリシーの設定	238
CoPP show コマンド	239
CoPP 設定ステータスの表示	240
CoPP のモニタリング	240
CoPP クラスに対するレート制限のディセーブル化と再イネーブル化	241
CoPP 統計情報のクリア	243
CoPP の設定例	243
CoPP の設定例	245
例：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	248
CoPP に関する追加情報	248



第 1 章

新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

- [新機能および変更された機能に関する情報, 1 ページ](#)

新機能および変更された機能に関する情報

次の表は、この最新リリースに関するガイドでの主な変更点の概要を示したものです。ただし、この表はコンフィギュレーションガイドへのすべての変更の詳細や、このリリースの新機能のリストを提供するものではありません。

機能	説明	追加または変更されたリリース	参照先
送信元 MAC または DMAC による ACE	オープンフローは POLICY_MGR プロセスによって処理され、タップアグリゲーションは ACLMGR プロセスによって処理されるようになりました。この機能拡張のために、オープンフロー固有のオプションは、タップアグリゲーションに関して使用できません。このため、送信元 MAC または DMAC によって ACE を作成できません。	7.0(3)I2(1)	ACL の注意事項と制約事項, (143 ページ)

機能	説明	追加または変更されたリリース	参照先
HTTP メソッドとの一致に関する機能拡張	HTTP メソッドとの一致に関する機能拡張として、パケットで TCP オプションのヘッダーの長さを指定するために、ACE シンタックスに <code>tcp-option-length</code> オプションが追加されました。	7.0(3)I2(1)	ACL の注意事項と制約事項 , (143 ページ) 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 , (157 ページ)
copp-s-igmp キューでパケットを取得するための PIM の有効化	PIM が有効になっている場合にのみ、ポートで <code>PIM_IGMP class-id</code> が設定されます。PIM が有効になっていない場合はレイヤ 3 ポートで CPU に IGMP パケットをパントする必要がないため、 <code>feature pim</code> を設定し、 <code>copp-s-igmp</code> キューでパケットを取得するポートの PIM を有効にする必要があります。	7.0(3)I2(1)	CoPP の注意事項と制約事項 , (233 ページ)
複数の IP およびポートにわたるスタティック DHCP バインディングでの同じ MAC アドレスの許可	7.0(3)I2(1) より前のリリースでは、サポートされない DHCP スタティック バインディング設定は拒否され、エラーになっていましたが、複数の IP およびポートにわたるスタティック DHCP バインディングで同じ MAC アドレスが許可されるようになりました。	7.0(3)I2(1)	DHCP スヌーピングの注意事項および制約事項 , (175 ページ)



第 2 章

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。

- [Authentication, Authorization, and Accounting \(認証、許可、およびアカウントिंग\)](#) , 3 ページ
- [RADIUS および TACACS+ セキュリティ プロトコル](#), 4 ページ
- [SSH および Telnet](#), 5 ページ
- [IP ACL](#), 5 ページ

Authentication, Authorization, and Accounting (認証、許可、およびアカウントिंग)

認証、許可、アカウントिंग (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。

認証

ワンタイム許可またはサービスごとの許可、ユーザ単位のアカウントリストとプロフィール、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。

Accounting

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。



(注) 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+ を使用する場合は、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。

関連トピック

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、アカウンティング機能が提供されます。

関連トピック

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、市販の一般的な SSH クライアントと相互運用ができます。

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。

関連トピック

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 ソフトウェアがパケットに IP 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は、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の処理を継続し、拒否されたパケットをドロップします。

関連トピック



第 3 章

認証、許可、アカウントिंगの設定

この章の内容は、次のとおりです。

- [AAA の概要, 7 ページ](#)
- [リモート AAA の前提条件, 12 ページ](#)
- [AAA の注意事項と制約事項, 12 ページ](#)
- [AAA の設定, 12 ページ](#)
- [ローカル AAA アカウントング ログのモニタリングとクリア, 22 ページ](#)
- [AAA 設定の確認, 22 ページ](#)
- [AAA の設定例, 23 ページ](#)
- [デフォルトの AAA 設定, 23 ページ](#)

AAA の概要

AAA セキュリティ サービス

認証、許可、アカウントング（AAA）機能では、Cisco Nexus デバイスを管理するユーザの ID 確認、アクセス権付与、およびアクション追跡を実行できます。Cisco Nexus 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 device Plus（TACACS+）プロトコルをサポートします。

ユーザが入力したユーザ ID とパスワードに基づいて、スイッチは、ローカル データベースを使用してローカル認証/ローカル許可を実行するか、1つまたは複数の AAA サーバを使用してリモート認証/リモート許可を実行します。スイッチと AAA サーバ間の通信は、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 サーバ専用共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：ユーザを識別します。選択したセキュリティプロトコルに応じて、ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージングサポート、暗号化などが行われます。
- 許可：アクセスコントロールを実行します。

Cisco Nexus デバイスにアクセスする許可は、AAA サーバからダウンロードされる属性によって提供されます。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。

- アカウンティング：課金、監査、レポートのための情報収集、ローカルでの情報のログイン、および AAA サーバへの情報の送信の方式を提供します。



(注) Cisco NX-OS ソフトウェアは、認証、許可、アカウントティングをそれぞれ個別にサポートします。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スイッチに関するユーザパスワードリストを簡単に管理できます。
- 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スイッチのアカウントティングログを集中管理できます。
- スイッチ上のローカルデータベースを使用する方法に比べて、ファブリック内の各スイッチのユーザ属性は管理が簡単です。

AAA Server Groups

認証、許可、アカウント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。リモート AAA サーバが応答しなかった場合、サーバグループは、フェールオーバーサーバを提供します。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 オプションに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。スイッチが最初のグループ内のサーバからエラーを受信すると、次のサーバグループのサーバが試行されます。

AAA サービス設定オプション

Cisco Nexus デバイスでは、次のサービスに個別の AAA 設定を使用できます。

- 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 アカウントング

次の表に、AAA サービス設定オプションの CLI コマンドを示します。

表 1: 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	aaa authentication login default
コンソール ログイン	aaa authentication login console
ユーザセッション アカウントング	aaa accounting default

AAA サービスには、次の認証方式を指定できます。

- RADIUS サーバグループ：RADIUS サーバのグローバルプールを認証に使用します。
- 特定のサーバグループ：指定した RADIUS または TACACS+ サーバグループを認証に使用します。
- ローカル：ユーザ名またはパスワードのローカルデータベースを認証に使用します。
- なし：ユーザ名だけを使用します。



(注) 方式がすべて RADIUS サーバになっており、特定のサーバグループが指定されていない場合、Cisco Nexus デバイスは、設定されている RADIUS サーバのグローバルプールから、設定された順序で 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 Nexus 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 サービスに対して設定できる AAA 認証方式を示します。

表 2: 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



(注) 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 アカウンティングでは、Cisco Nexus 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。

ユーザ ログインの認証および許可プロセス

ユーザ ログインの認証および許可プロセスは、次のように実行されます。

- 目的の Cisco Nexus デバイスにログインする際、Telnet、SSH、Fabric Manager または Device Manager、コンソール ログインのいずれかのオプションを使用できます。
- サーバグループ認証方式を使用して AAA サーバグループが設定してある場合は、Cisco Nexus デバイスが、グループ内の最初の AAA サーバに認証要求を送信し、次のように処理されます。

その AAA サーバが応答しなかった場合、リモートのいずれかの AAA サーバが認証要求に回答するまで、試行が継続されます。

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。

設定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 Nexus デバイスがリモート AAA サーバで正常に認証できた場合は、次の条件が適用されます。

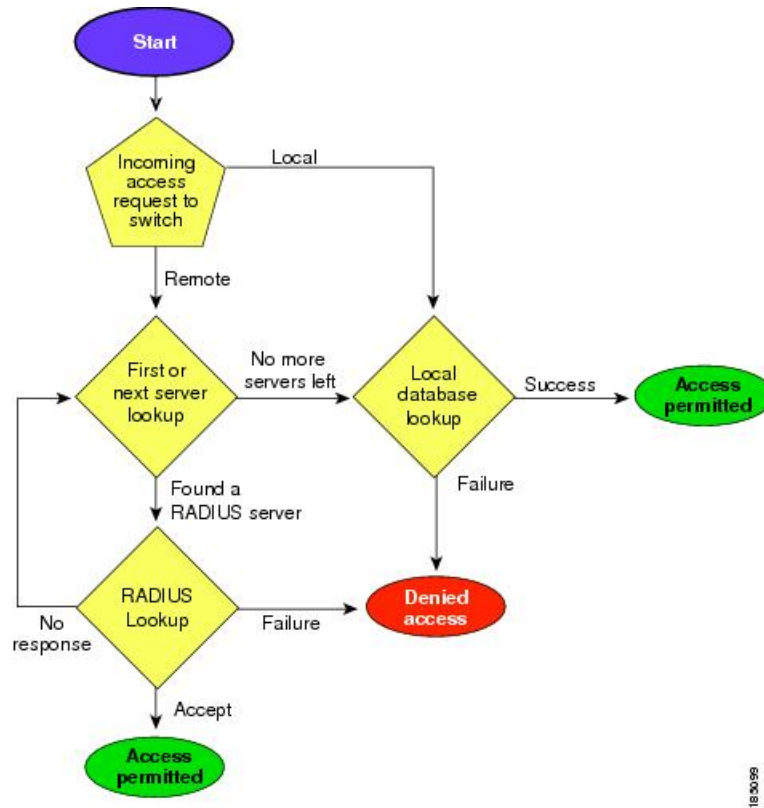
AAA サーバプロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザ ロールが認証応答とともにダウンロードされます。

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。

- ユーザ名とパスワードがローカルで正常に認証された場合は、Cisco Nexus デバイスにログインでき、ローカル データベース内で設定されているロールが割り当てられます。

次の図に、認証および許可プロセスのフローチャートを示します。

図 1: ユーザ ログインの認証および許可のフロー



(注) この図は、ユーザ名とパスワードによる SSH 認証にのみ該当します。公開キー SSH 認証には適用されません。ユーザ名とパスワードによる SSH 認証は、常に AAA を介して行われます。

この図に示されている「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。

リモート 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 サーバまたは TACACS+ サーバが、IP で到達可能であること。
- Cisco Nexus 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。
- 事前に共有された秘密キーが Cisco Nexus デバイス上およびリモート AAA サーバ上で設定されている。
- リモート サーバが Cisco Nexus デバイスからの AAA 要求に応答する。

AAA の注意事項と制約事項

そのユーザ名が TACACS+ または RADIUS で作成されたのか、ローカルで作成されたのかに関係なく、Cisco Nexus デバイスでは、すべて数値のユーザ名はサポートされません。AAA サーバに数字だけのユーザ名が存在し、ログイン時にその名前を入力した場合でも、ユーザは Cisco Nexus デバイスにログインを許可されます。



注意

すべて数字のユーザ名でユーザ アカウントを作成しないでください。

AAA の設定

コンソール 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 サーバまたは TACACS+ サーバの名前付きサブセット
- Cisco Nexus デバイス上のローカル 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。



(注) 事前に設定されている一連の RADIUS サーバに関しては、**aaa authentication** コマンドの **group radius** 形式および **groupserver-name** 形式を使用します。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。

必要に応じて、コンソール ログイン認証方式を設定する前に RADIUS または TACACS+ サーバグループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# aaa authentication login console {groupgroup-list [none] local none}	<p>コンソールのログイン認証方式を設定します。</p> <p><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。</p> <ul style="list-style-type: none"> • radius を指定すると、RADIUS サーバのグローバルプールが認証に使用されます。 • <i>named-group</i> を指定すると、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが認証に使用されます。 <p>local 方式では、ローカルデータベースが認証に使用されます。none 方式では、ユーザ名のみが使用されます。</p> <p>デフォルトのコンソール ログイン方式は local です。この方式は、方式が一切設定されていない場合、および設定済みのどの方式でも応答が得られなかった場合に使用されます。</p>
ステップ 3	switch(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# show aaa authentication	(任意) 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	switch# copy running-config startup-config	(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。

次に、コンソール ログインの認証方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authentication login console group radius
switch(config)# exit
switch# show aaa authentication
switch# copy running-config startup-config
```

デフォルトのログイン認証方式の設定

デフォルトの方式は、ローカルです。

必要に応じて、デフォルトのログイン認証方式を設定する前に RADIUS または TACACS+ サーバグループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# aaa authentication login default {groupgroup-list [none] local none}	<p>デフォルト認証方式を設定します。</p> <p><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。</p> <ul style="list-style-type: none"> • radius を指定すると、RADIUS サーバのグローバル プールが認証に使用されます。 • named-group を指定すると、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが認証に使用されます。 <p>local 方式では、ローカル データベースが認証に使用されます。none 方式では、ユーザ名のみが使用されます。</p> <p>デフォルトのログイン方式は local です。これは、方式が一切設定されていない場合、および設定済みのどの方式でも応答が得られなかった場合に使用されます。</p>
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show aaa authentication	(任意) デフォルトのログイン認証方式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 5	switch# copy running-config startup-config	(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。

ログイン認証失敗メッセージのイネーブル化

ユーザがログインして、リモート AAA サーバが応答しなかった場合は、ローカルユーザデータベースによってログインが処理されます。ログイン失敗メッセージの表示をイネーブルにしている場合は、次のようなメッセージが表示されます。

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

手順

	コマンドまたはアクション	目的
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)# aaa authentication login error-enable	ログイン認証失敗メッセージ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	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show aaa authentication	(任意) 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	switch# copy running-config startup-config	(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。

AAA コマンド許可の設定

TACACS+ サーバの許可方式が設定されている場合は、ユーザが TACACS+ サーバで実行するすべてのコマンド（すべての EXEC モード コマンドおよびすべてのコンフィギュレーションモード コマンドを含む）を許可できます。

許可方式には、次のものがあります。

- Group : TACACS+ サーバグループ
- Local : ローカル ロールベース許可
- None : 許可は実行されません

デフォルトの方式は、Local です。



(注) コンソールセッション上の許可はありません。

はじめる前に

AAA コマンドの許可を設定する前に、TACACS+ 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 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} {default} {[groupgroup-name] [local]} [groupgroup-name] [none]} 例： switch(config)# aaa authorization config-commands default group tac1 例： switch# aaa authorization commands default group tac1	許可パラメータを設定します。 EXEC モード コマンドを許可するには、 commands キーワードを使用します。 コンフィギュレーション モード コマンドの許可には、 config-commands キーワードを使用します。 許可方式を指定するには、 group 、 local 、または none キーワードを使用します。

次に、TACACS+ サーバグループ *tac1* で EXEC モード コマンドを許可する例を示します。

```
switch# aaa authorization commands default group tac1
```

次に、TACACS+ サーバグループ *tac1* でコンフィギュレーション モード コマンドを許可する例を示します。

```
switch(config)# aaa authorization config-commands default group tac1
```

次に、TACACS+ サーバグループ *tac1* でコンフィギュレーション モード コマンドを許可する例を示します。

- サーバが到達可能である場合、コマンドはサーバ応答に基づいて許可され、または許可されません。
- サーバに到達する際にエラーが生じた場合、コマンドはユーザのローカルロールに基づいて許可されます。

```
switch(config)# aaa authorization config-commands default group tac1 local
```

次に、TACACS+ サーバグループ *tac1* でコンフィギュレーションモードコマンドを許可する例を示します。

- サーバが到達可能である場合、コマンドはサーバ応答に基づいて許可され、または許可されません。
- サーバに到達する際にエラーが生じた場合は、ローカルロールにかかわらずコマンドを許可します。

```
switch# aaa authorization commands default group tac1 none
```

次に、ローカルロールにかかわらず EXEC モードコマンドを許可する例を示します。

```
switch# aaa authorization commands default none
```

次に、ローカルロールを使用して EXEC モードコマンドを許可する例を示します。

```
switch# aaa authorization commands default local
```

MSCHAP 認証のイネーブル化

マイクロソフトチャレンジハンドシェイク認証プロトコル (MSCHAP) は、マイクロソフト版の CHAP です。リモート認証サーバ (RADIUS または TACACS+) を通じて、Cisco Nexus デバイスへのユーザログインに MSCHAP を使用できます。

デフォルトでは、Cisco Nexus デバイスはスイッチ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 がイネーブルの場合は、MSCHAP VSA (Vendor-Specific Attribute; ベンダー固有属性) 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。

表 3: MSCHAP 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 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 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。

手順

	コマンドまたはアクション	目的
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)# aaa authentication login mschap enable	MS-CHAP 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	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show aaa authentication login mschap	(任意) MS-CHAP 設定を表示します。
ステップ 5	switch# copy running-config startup-config	(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。

関連トピック

[VSA, \(20 ページ\)](#)

デフォルトの AAA アカウントング方式の設定

Cisco Nexus デバイスは、アカウントングに TACACS+ 方式と RADIUS 方式をサポートします。スイッチは、ユーザアクティビティをアカウントングレコードの形で TACACS+ セキュリティサーバまたは RADIUS セキュリティサーバに報告します。各アカウントングレコードに、アカウントング属性値 (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 アカウントングをアクティブにすると、Cisco Nexus デバイスは、これらの属性をアカウントングレコードとして報告します。そのアカウントングレコードは、セキュリティサーバ上のアカウントングログに格納されます。

特定のアカウントング方式を定義するデフォルト方式のリストを作成できます。それには次の方式があります。

- RADIUS サーバグループ：RADIUS サーバのグローバルプールをアカウントングに使用します。
- 特定のサーバグループ：指定した RADIUS または TACACS+ サーバグループをアカウントングに使用します。
- ローカル：ユーザ名またはパスワードのローカルデータベースをアカウントングに使用します。



(注) 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。

はじめる前に

必要に応じて、AAA アカウントングのデフォルト方式を設定する前に RADIUS または TACACS+ サーバグループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	<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。
ステップ 2	<code>switch(config)# aaa accounting default {groupgroup-list local}</code>	デフォルトのアカウントング方式を設定します。スペースで区切ったリストで、1 つまたは複数のサーバグループ名を指定できます。 <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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • radius を指定すると、RADIUS サーバのグローバルプールがアカウントングに使用されます。 • named-group を指定すると、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トングに使用されます。 <p>local 方式では、アカウントングにローカル データベースが使用されます。</p> <p>デフォルトの方式は local です。サーバグループが設定されていないとき、または設定済みのすべてのサーバグループから応答がないときに、このデフォルト方式が使用されます。</p>
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show aaa accounting	(任意) デフォルトの AAA アカウントング方式の設定を表示します。
ステップ 5	switch# copy running-config startup-config	(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。

AAA サーバの VSA の使用

VSA

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

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 seperator value *

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号 (=) で、アスタリスク (*) は任意属性を示します。

Cisco Nexus 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 Nexus デバイス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ます。
- **Accounting** : `accounting-request` パケットで使用されます。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 Nexus デバイスでサポートされています。

- **roles** : ユーザに割り当てるすべてのロールをリストします。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。
- **accountinginfo** : 標準の RADIUS アカウンティングプロトコルで処理される属性に加えて、追加のアカウンティング情報が格納されます。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 サーバ上でのスイッチのユーザ ロールと 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 Nexus 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。



- (注) Cisco Unified Wireless Network TACACS+ 設定と、ユーザ ロールの変更については、『[Cisco Unified Wireless Network TACACS+ Configuration](#)』を参照してください。

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。

```
shell:roles="roleA roleB..." 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。

追加情報については、Cisco Nexus デバイスの『[System Management Configuration Guide](#)』の「[Configuring User Accounts and RBAC](#)」の章を参照してください。

ローカル AAA アカウントティング ログのモニタリングとクリア

Cisco Nexus デバイスは、AAA アカウントティング アクティビティのローカル ログを保持しています。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# show accounting log [size] [start-time year month day hh:mm:ss]	アカウントティング 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 バイトのアカウントティング ログが表示されます。サイズ引数を指定すれば、コマンドの出力を制限できます。指定できる範囲は 0 ~ 250000 バイトです。ログ出力の開始時刻を指定することもできます。
ステップ 2	switch# clear accounting log	(任意) アカウントティング ログの内容をクリアします。

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 アカウントティングの設定を表示します。
show aaa authentication [login {error-enable mschap}]	AAA 認証情報を表示します。
show aaa authorization	AAA 許可の情報を表示します。
show aaa groups	AAA サーバグループの設定を表示します。
show 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 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。

AAA の設定例

次に、AAA を設定する例を示します。

```
switch(config)# aaa authentication login default group radius
switch(config)# aaa authentication login console group radius
switch(config)# aaa accounting default group radius
```

デフォルトの AAA 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。

表 4: デフォルトの AAA パラメータ

パラメータ	デフォルト
コンソール認証方式	local
デフォルト認証方式	local
ログイン認証失敗メッセージ	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	local
アカウンティング ログの表示サイズ	250 KB



第 4 章

RADIUS の設定

この章の内容は、次のとおりです。

- [RADIUS の概要, 25 ページ](#)
- [RADIUS の前提条件, 28 ページ](#)
- [RADIUS の注意事項と制約事項, 28 ページ](#)
- [RADIUS サーバの設定, 29 ページ](#)
- [RADIUS 設定の確認, 41 ページ](#)
- [RADIUS サーバ統計情報の表示, 42 ページ](#)
- [RADIUS サーバ統計情報のクリア, 42 ページ](#)
- [RADIUS の設定例, 43 ページ](#)
- [RADIUS のデフォルト設定, 43 ページ](#)
- [RADIUS の機能の履歴, 43 ページ](#)

RADIUS の概要

Remote Access Dial-In User Service (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 Nexus 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アカウンティンギング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 Nexus 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 アカウンティンギングが必要なネットワーク。
RADIUS アカウンティンギングは、RADIUS 認証または RADIUS 認可とは個別に使用できます。RADIUS アカウンティンギ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ギ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できます。ユーザごとのプロファイルにより、Cisco Nexus 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 レベル契約を提供できます。

RADIUS の操作について

ユーザがログインを試行し、RADIUS を使用して Cisco Nexus デバイスに対する認証を行う際には、次のプロセスが実行されます。

- 1 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。
- 2 ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
- 3 ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
 - ACCEPT : ユーザが認証されたことを表します。
 - REJECT : ユーザは認証されず、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対して新しいパスワードの選択を求める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。

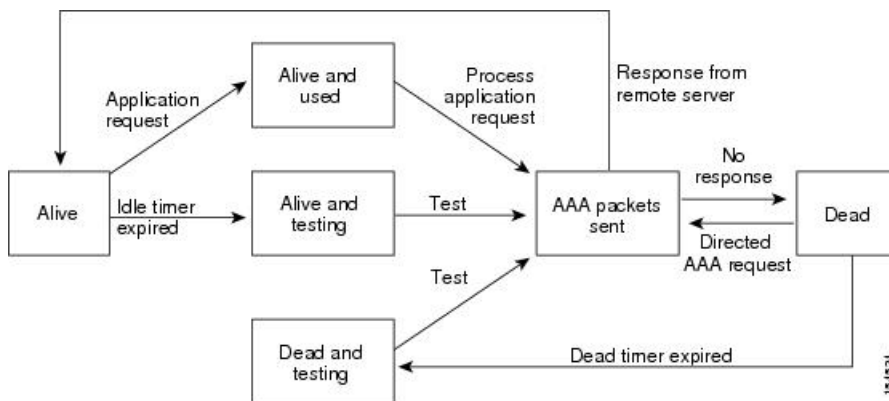
- ユーザがアクセス可能なサービス (Telnet、rlogin、またはローカルエリア トランスポート (LAT) 接続、ポイントツーポイントプロトコル (PPP)、シリアルラインインターネットプロトコル (SLIP)、EXEC サービスなど)
- 接続パラメータ (ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセス リスト、ユーザ タイムアウト)

RADIUS サーバのモニタリング

応答を返さない RADIUS 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 (アライブ状態である) かどうかを調べるよう、スイッチを設定できます。スイッチは、応答を返さない RADIUS サーバをデッド (dead) 状態としてマークし、デッド RADIUS サーバには AAA 要求を送信しません。また、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。このプロセスにより、RADIUS サーバが稼働状態であることを確認してから、実際の AAA 要求がサーバに送信されます。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、障害が発生したことを知らせるエラーメッセージがスイッチによって表示されます。

次の図に、さまざまな RADIUS サーバの状態を示します。

図 2: RADIUS サーバの状態



(注) 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 サーバの間でのベンダー固有属性 (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 *

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号 (=) で、アスタリスク (*) は任意属性を示します。

Cisco Nexus デバイスでの認証に RADIUS サーバを使用する場合は、認証結果とともに許可情報などのユーザ属性を返すよう、RADIUS プロトコルが RADIUS サーバに指示します。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 Nexus デバイス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ます。
- **Accounting** : `accounting-request` パケットで使用されます。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 Nexus デバイスでは、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複数のロール名をリストするストリングです。
- **accountinginfo** : 標準の RADIUS アカウンティングプロトコルで処理される属性に加えて、アカウンティング情報が格納されます。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 の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IP アドレス (IPv4 または IPv6) またはホスト名を取得すること。
- RADIUS サーバから事前共有キーを取得すること。
- Cisco Nexus 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 設定時の注意事項と制限事項は次のとおりです。

- 上に設定できる RADIUS サーバの最大数は 64 です。Cisco Nexus デバイス

RADIUS サーバの設定

ここでは、RADIUS サーバの設定方法について説明します。

手順

-
- ステップ 1** Cisco Nexus デバイスと RADIUS サーバとの接続を確立します。
- ステップ 2** RADIUS サーバの事前共有秘密キーを設定します。
- ステップ 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。
- ステップ 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
 - ログイン時に RADIUS サーバの指定を許可
 - 送信リトライ回数とタイムアウト間隔
 - アカウンティングおよび認証属性
- ステップ 5** 必要に応じて、定期的に RADIUS サーバをモニタリングするよう設定します。
-

RADIUS サーバホストの設定

認証に使用する各 RADIUS サーバについて、IP アドレス (IPv4 または IPv6)、またはホスト名を設定する必要があります。すべての RADIUS サーバホストは、デフォルトの RADIUS サーバグループに追加されます。最大 64 の RADIUS サーバを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i> }	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	switch(config)# exit	設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	switch# show radius-server	(任意) RADIUS サーバの設定を表示します。
ステップ 5	switch# copy running-config startup-config	(任意) 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。

次に、RADIUS サーバとしてホスト 10.10.1.1 を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1
switch(config)# exit
switch# copy running-config startup-config
```

RADIUS のグローバルな事前共有キーの設定

Cisco Nexus 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事前共有キーを設定できます。事前共有キーとは、スイッチと RADIUS サーバホスト間の共有秘密テキストストリングです。

はじめる前に

リモートの RADIUS サーバの事前共有キー値を取得していること。

手順

	コマンドまたはアクション	目的
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)# radius-server key [0 7] key-value	すべての RADIUS サーバで使用する事前共有キーを指定します。クリアテキスト形式 (0) または暗号化形式 (7) 事前共有キーを指定できます。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、事前共有キーは設定されません。
ステップ 3	switch(config)# exit	設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	switch# show radius-server	(任意) RADIUS サーバの設定を表示します。 (注) 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有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	switch# copy running-config startup-config	(任意) 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。

次に、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事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 0 QsEfThUkO
switch(config)# exit
switch# copy running-config startup-config
```

RADIUS サーバの事前共有キーの設定

事前共有キーとは、Cisco Nexus デバイスと RADIUS サーバ ホスト間の共有秘密テキスト ストリングです。

はじめる前に

リモートの RADIUS サーバの事前共有キー値を取得していること。

手順

	コマンドまたはアクション	目的
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)# radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i> } key [0 7] <i>key-value</i>	特定の RADIUS サーバの事前共有キーを指定します。クリア テキスト形式 (0) または暗号化形式 (7) 事前共有キーを指定できます。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。

	コマンドまたはアクション	目的
		この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show radius-server	(任意) RADIUS サーバの設定を表示します。 (注) 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有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	switch# copy running-config startup-config	(任意) 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。

次に、RADIUS 事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

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。

手順

	コマンドまたはアクション	目的
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)# aaa group server radiusgroup-name	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
ステップ 3	<code>switch (config-radius)# server {ipv4-address ipv6-address server-name}</code>	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	<code>switch (config-radius)# deadtimeminutes</code>	(任意) 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。 (注) 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	<code>switch(config-radius)# source-interfaceinterface</code>	(任意) 特定の RADIUS サーバグループに発信元インターフェイスを割り当てます。 サポートされているインターフェイスのタイプは管理および VLAN です。 (注) source-interface コマンドを使用して、 ip radius source-interface コマンドによって割り当てられたグローバルソースインターフェイスをオーバーライドします。
ステップ 6	<code>switch(config-radius)# exit</code>	設定モードを終了します。
ステップ 7	<code>switch(config)# show radius-server group [group-name]</code>	(任意) RADIUS サーバグループの設定を表示します。
ステップ 8	<code>switch(config)# copy running-config startup-config</code>	(任意) 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。

次に、RADIUS サーバグループを設定する例を示します。

```
switch# configure terminal
switch (config)# aaa group server radius RadServer
switch (config-radius)# server 10.10.1.1
switch (config-radius)# deadtime 30
switch (config-radius)# use-vrf management
switch (config-radius)# exit
switch (config)# show radius-server group
switch (config)# copy running-config startup-config
```

次の作業

AAA サービスに RADIUS サーバグループを適用します。

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。

手順

	コマンドまたはアクション	目的
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)# ip radius source-interface interface	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。発信元インターフェイスは、管理または VLAN インターフェイスにすることができます。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show radius-server	(任意) RADIUS サーバの設定情報を表示します。
ステップ 5	switch# copy running-config startup-config	(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。

次に、RADIUS サーバグループのグローバル発信元インターフェイスとして、`mgmt 0` インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# ip radius source-interface mgmt 0
switch(config)# exit
switch# copy running-config startup-config
```

ログイン時にユーザによる RADIUS サーバの指定を許可

ログイン時に RADIUS サーバを指定することをユーザに許可できます。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# radius-server directed-request	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	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show radius-server directed-request	(任意) directed request の設定を表示します。
ステップ 5	switch# copy running-config startup-config	(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。

次に、ネットワークにログインしたときに、ユーザが RADIUS サーバを選択できるようにする例を示します。

```
switch# configure terminal
switch(config)# radius-server directed-request
switch# exit
switch# copy running-config startup-config
```

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、スイッチ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。タイムアウト間隔は、Cisco Nexus 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時間を決定します。

手順

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

	コマンドまたはアクション	目的
ステップ 2	switch(config)# radius-server retransmitcount	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	switch(config)# radius-server timeoutseconds	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	switch(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ます。
ステップ 5	switch# show radius-server	(任意) RADIUS サーバの設定を表示します。
ステップ 6	switch# copy running-config startup-config	(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。

次に、RADIUS サーバで、リトライ回数を 3、伝送タイムアウト間隔を 5 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server retransmit 3
switch(config)# radius-server timeout 5
switch(config)# exit
switch# copy running-config startup-config
```

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 Nexus スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再実行します。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。また、スイッチ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を設定することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# radius-server host {ipv4-address ipv6-address host-name} retransmitcount	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。

	コマンドまたはアクション	目的
		(注) 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	<code>switch(config)#radius-server host {ipv4-address ipv6-address host-name} timeoutseconds</code>	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。 (注) 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	<code>switch(config)# exit</code>	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	<code>switch# show radius-server</code>	(任意) RADIUS サーバの設定を表示します。
ステップ 6	<code>switch# copy running-config startup-config</code>	(任意) 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。

次に、RADIUS ホストサーバ server1 で、RADIUS 送信リトライ回数を 3、タイムアウト間隔を 10 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host server1 retransmit 3
switch(config)# radius-server host server1 timeout 10
switch(config)# exit
switch# copy running-config startup-config
```

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。RADIUS のアカウントングおよび認証メッセージの宛先 UDP ポート番号も指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	<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	switch(config)# radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i> } acct-port <i>udp-port</i>	(任意) 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 1812 です。 範囲は 0 ~ 65535 です。
ステップ 3	switch(config)# radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i> } accounting	(任意) 特定の RADIUS サーバをアカウントング用のみ使用することを指定します。デフォルトでは、アカウントングと認証の両方に使用されます。
ステップ 4	switch(config)# radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i> } auth-port <i>udp-port</i>	(任意) 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	switch(config)# radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i> } authentication	(任意) 特定の RADIUS サーバを認証用のみ使用することを指定します。デフォルトでは、アカウントングと認証の両方に使用されます。
ステップ 6	switch(config)# exit	設定モードを終了します。
ステップ 7	switch(config)# show radius-server	(任意) RADIUS サーバの設定を表示します。
ステップ 8	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。

次に、RADIUS サーバのアカウントング属性と認証属性を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 acct-port 2004
switch(config)# radius-server host 10.10.1.1 accounting
switch(config)# radius-server host 10.10.2.2 auth-port 2005
switch(config)# radius-server host 10.10.2.2 authentication
switch # exit
switch # copy running-config startup-config
switch #
```

RADIUS サーバの定期的モニタリングの設定

RADIUS サーバの可用性をモニタリングできます。パラメータとして、サーバに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することで、サーバを定期的にテストできます。



(注) 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。

テスト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スイッチがテストパケットを送信するかを指定します。

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、スイッチは RADIUS サーバの定期的なモニタリングを実行しません。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# radius-server host <i>{ipv4-address ipv6-address host-name}</i> test <i>{idle-timeminutes passwordpassword [idle-timeminutes] usernamename [passwordpassword [idle-timeminutes]]}</i>	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。 デフォルトのアイドルタイマー値は 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 3	switch(config)# radius-server deadtimeminutes	スイッチが、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	switch(config)# exit	設定モードを終了します。
ステップ 5	switch# show radius-server	(任意) 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
ステップ 6	switch# copy running-config startup-config	(任意) 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。

次に、ユーザ名 (user1) およびパスワード (Ur2Gd2BH) と、3 分のアイドルタイマーおよび 5 分のデッドタイムで、RADIUS サーバホスト 10.10.1.1 を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# copy running-config startup-config
```

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 Nexus 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。デフォルト値は 0 分です。



(注) 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。

手順

	コマンドまたはアクション	目的
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)# radius-server deadtime	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	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show radius-server	(任意) 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
ステップ 5	switch# copy running-config startup-config	(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。

次に、RADIUS サーバに 5 分間のデッドタイムを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# copy running-config startup-config
```

RADIUS サーバまたはサーバグループの手動モニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	switch# test aaa server radius {ipv4-address ipv6-address server-name} [vrf vrf-name] username password switch# test aaa server radius {ipv4-address ipv6-address server-name} [vrf vrf-name] username password	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	switch# test aaa group group-name username password	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。

次に、可用性を確認するために、RADIUS サーバとサーバグループにテストメッセージを送信する例を示します。

```
switch# test aaa server radius 10.10.1.1 user 1 Ur2Gd2BH
switch# test aaa group RadGroup user2 As3He3CI
```

RADIUS 設定の確認

AAA 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 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

コマンド	目的
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 [<i>server-name</i> <i>ipv4-address</i> <i>ipv6-address</i>] [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 サーバ統計情報の表示

手順

	コマンドまたはアクション	目的
ステップ 1	switch# show radius-server statistics { <i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i> }	RADIUS 統計情報を表示します。

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。

はじめる前に

Cisco NX-OS デバイスに RADIUS 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	switch# show radius-server statistics { <i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i> }	(任意) Cisco NX-OS デバイスでの RADIUS サーバ統計情報を表示します。
ステップ 2	switch# clear radius-server statistics { <i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i> }	RADIUS サーバ統計情報をクリアします。

RADIUS の設定例

次に、RADIUS を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 7 "ToIkLhPpG"
switch(config)# radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# exit
switch(config-radius)# use-vrf management
```

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。

表 5: デフォルトの RADIUS パラメータ

パラメータ	デフォルト
サーバの役割	認証とアカウントिंग
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
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	test

RADIUS の機能の履歴

表 6: RADIUS の機能の履歴

機能名	リリース	機能情報
RADIUS	5.0(3)U1(1)	この機能が導入されました。
IPv6	5.0(3)U3(1)	IPv6 サポートが追加されました。



第 5 章

TACACS+ の設定

この章の内容は、次のとおりです。

- [TACACS+ の設定に関する情報, 45 ページ](#)
- [TACACS+ の前提条件, 48 ページ](#)
- [TACACS+ の注意事項と制約事項, 48 ページ](#)
- [TACACS+ の設定, 49 ページ](#)
- [TACACS+ 統計情報の表示, 60 ページ](#)
- [TACACS+ の設定の確認, 60 ページ](#)
- [TACACS+ の設定例, 61 ページ](#)
- [TACACS+ のデフォルト設定, 61 ページ](#)

TACACS+ の設定に関する情報

Terminal Access Controller Access Control System Plus (TACACS+) セキュリティプロトコルは、Cisco Nexus 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。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稼働する TACACS+ デーモンのデータベースで管理されます。設定済みの TACACS+ 機能を Cisco Nexus デバイス上で使用するには、TACACS+ サーバへのアクセス権を持ち、このサーバを設定する必要があります。

TACACS+ では、認証、許可、アカウントिंगの各ファシリティを個別に提供します。TACACS+ を使用すると、単一のアクセスコントロールサーバ (TACACS+ デーモン) で、各サービス (認証、許可、アカウントING) を個別に提供できます。各サービスは固有のデータベースにアソシエートされており、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上で使用可能な他のサービスを利用できます。

TACACS+ 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 TCP (TCP ポート 49) を使用します。Cisco Nexus 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。

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 Nexus 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暗号化して、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暗号化します。

TACACS+ を使用したユーザ ログイン

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

- 1 Cisco Nexus 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。



(注) 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。この動作では通常、ユーザ名とパスワードの入力が要求されますが、ユーザの母親の旧姓など、その他の項目の入力が要求されることもあります。

- 2 Cisco Nexus デバイスが、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 Nexus 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** : 認証中に、デーモン内、またはデーモンと Cisco Nexus デバイス間のネットワーク接続でエラーが発生しました。Cisco Nexus デバイスが **ERROR** 応答を受信した場合、スイッチは代替りのユーザ認証方式の使用を試みます。

Cisco Nexus デバイスで許可がイネーブルになっている場合は、この後、許可フェーズの処理が実行されます。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 Nexus 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)、アクセス リスト、ユーザ タイムアウト)

デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー

TACACS+ サーバに対してスイッチを認証するには、TACACS+ 事前共有キーを設定する必要があります。事前共有キーとは、Cisco Nexus 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 Nexus 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事前共有秘密キーを設定できます。

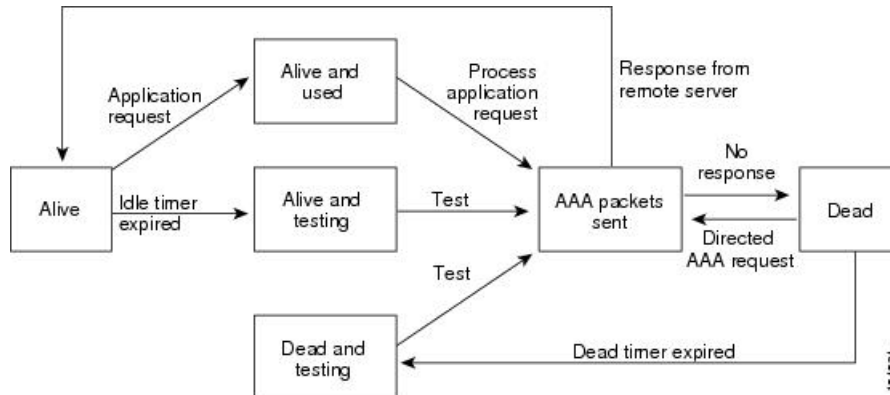
グローバルな事前共有キーの設定は、個々の TACACS+ サーバの設定時に **key** オプションを使用することによって無効にできます。

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 Nexus 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 Nexus 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 Nexus デバイスは定期的にデッド TACACS+ サーバをモニタリングし、それらのサーバが応答を返すようになった時点でアライブ状態に戻します。このプロセスでは、TACACS+ サーバが稼働状態であることを確認してから、実際の AAA 要求がサーバに送信されます。TACACS+ サーバの状態がデッドまたはアライブになると、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 Nexus 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。

次の図に、さまざまな TACACS+ サーバの状態を示します。

図 3: TACACS+ サーバの状態



(注) 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+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバの IPv4 アドレスまたはホスト名を取得すること。
- TACACS+ サーバから事前共有キーを取得していること。
- Cisco Nexus 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+ の注意事項と制約事項

TACACS+ に関する注意事項と制約事項は次のとおりです。

- Cisco Nexus デバイス上に設定できる TACACS+ サーバの最大数は 64 です。

TACACS+ の設定

TACACS+ サーバの設定プロセス

ここでは、TACACS+ サーバを設定する方法について説明します。

手順

-
- 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 Nexus デバイスとの接続を確立します。
- ステップ 3** TACACS+ サーバの事前共有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** 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
 - ログイン時に TACACS+ サーバの指定を許可
 - タイムアウト間隔
 - TCP ポート
- ステップ 6** 必要に応じて、定期的に TACACS+ サーバをモニタリングするよう設定します。
-

TACACS+ のイネーブル化

デフォルトでは、Cisco Nexus デバイスで TACACS+ 機能はディセーブルに設定されています。TACACS+ 機能をイネーブルに設定すると、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	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)# feature tacacs+	TACACS+ をイネーブルにします。
ステップ 3	switch(config)# exit	設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	switch# copy running-config startup-config	(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。

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、TACACS+ サーバの IP アドレス (IPv4) またはホスト名を Cisco Nexus デバイスで設定する必要があります。すべての TACACS+ サーバホストは、デフォルトの TACACS+ サーバグループに追加されます。最大 64 の TACACS+ サーバを設定できます。

設定済みの TACACS+ サーバに事前共有キーが設定されておらず、グローバル キーも設定されていない場合は、警告メッセージが表示されます。TACACS+ サーバキーが設定されていない場合は、グローバル キー (設定されている場合) が該当サーバで使用されます。

TACACS+ サーバホストを設定する前に、次の点を確認してください。

- TACACS+ をイネーブルにします。
- リモート TACACS+ サーバの IP アドレス (IPv4) またはホスト名を取得していること。

手順

	コマンドまたはアクション	目的
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)# exit	設定モードを終了します。
ステップ 3	switch# show tacacs-server	(任意) TACACS+ サーバの設定を表示します。
ステップ 4	switch# copy running-config startup-config	(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。

サーバグループから TACACS+ サーバホストを削除できます。

TACACS+ のグローバルな事前共有キーの設定

Cisco Nexus 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事前共有キーを設定できます。事前共有キーとは、Cisco Nexus 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。

事前共有キーを設定する前に、次の点を確認してください。

- TACACS+ をイネーブルにします。
- リモートの TACACS+ サーバの事前共有キー値を取得していること。

手順

	コマンドまたはアクション	目的
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)# tacacs-server key [0 7] key-value	すべての TACACS+ サーバで使用する事前共有キーを指定します。クリア テキスト形式 (0) または暗号化形式 (7) 事前共有キーを指定できます。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、事前共有キーは設定されません。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show tacacs-server	(任意) TACACS+ サーバの設定を表示します。 (注) 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有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	switch# copy running-config startup-config	(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。

次に、グローバルな事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server key 0 QsEfThUkO
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバの事前共有キーの設定

TACACS+ サーバの事前共有キーを設定できます。事前共有キーとは、Cisco Nexus 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。

手順

	コマンドまたはアクション	目的
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)# exit	設定モードを終了します。
ステップ 3	switch# show tacacs-server	(任意) TACACS+ サーバの設定を表示します。 (注) 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有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 4	switch# copy running-config startup-config	(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。

次に、TACACS+ 事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

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。

はじめる前に

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用して、TACACS+ 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	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)# aaa group server tacacs+group-name	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	switch(config-tacacs+)# deadtimeminutes	(任意) 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0～1440です。 (注) TACACS+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、そ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 4	switch(config-tacacs+)# source-interfaceinterface	(任意) 特定の TACACS+ サーバグループに発信元インターフェイスを割り当てます。 サポートされているインターフェイスのタイプは管理および VLAN です。 (注) source-interface コマンドを使用して、 ip tacacs source-interface コマンドによって割り当てられたグローバルソースインターフェイスをオーバーライドします。
ステップ 5	switch(config-tacacs+)# exit	設定モードを終了します。
ステップ 6	switch(config)# show tacacs-server groups	(任意) TACACS+ サーバグループの設定を表示します。
ステップ 7	switch(config)# copy running-config startup-config	(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。

次に、TACACS+ サーバグループを設定する例を示します。

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# deadtime 30
switch(config-tacacs+)# exit
switch(config)# show tacacs-server groups
switch(config)# copy running-config startup-config
```

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。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip tacacs source-interface interface 例： switch(config)# ip tacacs source-interface mgmt 0	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。発信元インターフェイスは、管理または VLAN インターフェイスにすることができます。
ステップ 3	exit 例： switch(config)# exit switch#	設定モードを終了します。
ステップ 4	show tacacs-server 例： switch# show tacacs-server	(任意) TACACS+ サーバの設定情報を表示します。
ステップ 5	copy running-config startup config 例： switch# copy running-config startup-config	(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。

ログイン時の TACACS+ サーバの指定

認証要求の送信先 TACACS+ サーバをユーザが指定できるようにスイッチを設定するには、`directed-request` オプションをイネーブルにします。デフォルトでは、Cisco Nexus 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。このオプションをイネーブルにすると、ユーザは `username@hostname` としてログインできます。ここで、`hostname` は設定済みの RADIUS サーバの名前です。



(注) ユーザ指定のログインは、Telnet セッションでのみサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# tacacs-server directed-request	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	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show tacacs-server directed-request	(任意) TACACS+ の directed request の設定を表示します。
ステップ 5	switch# copy running-config startup-config	(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。

グローバルな TACACS+ タイムアウト間隔の設定

Cisco Nexus デバイスが、タイムアウトエラーを宣言する前に、すべての TACACS+ サーバからの応答を待機するグローバルなタイムアウト間隔も設定できます。タイムアウト間隔には、スイッチが 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。

手順

	コマンドまたはアクション	目的
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)# tacacs-server timeoutseconds	TACACS+ 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、範囲は 1 ~ 60 秒です。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show tacacs-server	(任意) TACACS+ 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
ステップ 5	switch# copy running-config startup-config	(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。

サーバのタイムアウト間隔の設定

Cisco Nexus 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。タイムアウト間隔は、スイッチ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時間を決定します。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# exit	設定モードを終了します。
ステップ 3	switch# show tacacs-server	(任意) TACACS+ サーバの設定を表示します。
ステップ 4	switch# copy running-config startup-config	(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。

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 Nexus デバイスは、すべての TACACS+ 要求にポート 49 を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グ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	switch(config)# exit	設定モードを終了します。
ステップ 3	switch# show tacacs-server	(任意) TACACS+ サーバの設定を表示します。
ステップ 4	switch# copy running-config startup-config	(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。

次に、TCP ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 port 2
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバの定期的モニタリングの設定

TACACS+ サーバの可用性をモニタリングできます。パラメータとして、サーバに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 Nexus 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、サーバを定期的にテストしたり、1回だけテストを実行できます。



(注) 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。

テスト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 Nexus デバイスがテストパケットを送信するかを指定します。



(注) 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。

手順

	コマンドまたはアクション	目的
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)# tacacs-server dead-time <i>minutes</i>	Cisco Nexus 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、指定できる範囲は 0 ~ 1440 分です。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show tacacs-server	(任意) TACACS+ サーバの設定を表示します。
ステップ 5	switch# copy running-config startup-config	(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。

次に、TACACS+ サーバの定期的モニタリングを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time
3
switch(config)# tacacs-server dead-time 5
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

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 Nexus 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。



(注) 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。デッドタイム間隔はグループ単位で設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# tacacs-server deadtimeminutes	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。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show tacacs-server	(任意) TACACS+ サーバの設定を表示します。
ステップ 5	switch# copy running-config startup-config	(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。

TACACS+ サーバまたはサーバグループの手動モニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	switch# test aaa server tacacs+ {ipv4-address ipv6-address host-name} [vrfvrf-name] usernamepassword	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	switch# test aaa groupgroup-name username password	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。

次に、手動でテストメッセージを送信する例を示します。

```
switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group TacGroup user2 As3He3CI
```

TACACS+ のディセーブル化

TACACS+ をディセーブルにできます。



注意

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。

手順

	コマンドまたはアクション	目的
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 feature tacacs+	TACACS+ をディセーブルにします。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# copy running-config startup-config	(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。

TACACS+ 統計情報の表示

スイッチが TACACS+ のアクティビティについて保持している統計情報を表示するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# show tacacs-server statistics {hostname ipv4-address ipv6-address}	TACACS+ 統計情報を表示します。

このコマンドの出力フィールドの詳細については、Nexus スイッチの『*Command Reference*』を参照してください。

TACACS+ の設定の確認

TACACS+ の情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
<code>show tacacs+ {status pending pending-diff}</code>	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。
<code>show running-config tacacs [all]</code>	実行コンフィギュレーションの TACACS+ 設定を表示します。
<code>show startup-config tacacs</code>	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。
<code>show tacacs-serve [host-name ipv4-address ipv6-address] [directed-request groups sorted statistics]</code>	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+ を設定する例を示します。

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ToIkLhPpG"
switch(config)# tacacs-server host 10.10.2.2 key 7 "ShMoMhT1"
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# use-vrf management
```

次に、TACACS+ をイネーブルにし、TACACS+ サーバの事前共有キーを設定して、サーバグループ TacServer1 を認証するためにリモート AAA サーバを指定する例を示します。

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ikvhw10"
switch(config)# tacacs-server host 1.1.1.1
switch(config)# tacacs-server host 1.1.1.2

switch(config)# aaa group server tacacs+ TacServer1
switch(config-tacacs+)# server 1.1.1.1
switch(config-tacacs+)# server 1.1.1.2
```

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を示します。

表 7: TACACS+ のデフォルトパラメータ

パラメータ	デフォルト
TACACS+	ディセーブル

パラメータ	デフォルト
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	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	test



第 6 章

SSH および Telnet の設定

この章の内容は、次のとおりです。

- [SSH および Telnet の概要, 63 ページ](#)
- [SSH の注意事項および制約事項, 65 ページ](#)
- [SSH の設定, 65 ページ](#)
- [SSH の設定例, 71 ページ](#)
- [Telnet の設定, 72 ページ](#)
- [SSH および Telnet の設定の確認, 75 ページ](#)
- [SSH のデフォルト設定, 75 ページ](#)

SSH および Telnet の概要

SSH サーバ

セキュアシェル (SSH) プロトコルサーバ機能を使用すると、SSH クライアントは Cisco Nexus デバイスとの間で、暗号化されたセキュアな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 Nexus デバイススイッチの SSH サーバは、無償あるいは商用の SSH クライアントと連携して動作します。

SSH がサポートするユーザ認証メカニズムには、RADIUS、TACACS+、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 クライアント機能は、SSH プロトコルを介して実行されるアプリケーションで、認証と暗号化を行います。SSH クライアントを使用すると、スイッチは、別の Cisco Nexus デバイススイッチ

との間、または SSH サーバを稼働している他の任意の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。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 Nexus デバイスの SSH クライアントは、無償あるいは商用の SSH サーバと連係して動作します。

SSH サーバキー

SSH では、Cisco Nexus デバイス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 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

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 2 とおりのキー ペアを使用できます。

- `dsa` オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キーペアが生成されます。
- `rsa` オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キーペアが生成されます。

デフォルトでは、Cisco Nexus デバイスは 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)



注意

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。

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サイトのログインサーバとの TCP 接続を確立して、システム間でキーストロークをやり取りできます。Telnet は、リモートシステムのアドレスとして、IP アドレスまたはドメイン名を受け取ります。

Cisco Nexus デバイスでは、デフォルトで Telnet サーバがイネーブルになっています。

SSH の注意事項および制約事項

SSH には、次の注意事項および制限事項があります。

- Cisco Nexus デバイスは、SSH バージョン 2 (SSHv2) だけをサポートしています。

SSH の設定

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。

手順

	コマンドまたはアクション	目的
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)# ssh key {dsa [force] rsa [bits [force]]}	SSH サーバ キーを生成します。 <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 ~ 2048 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、キーワード force を使用します。
ステップ 3	switch(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# show ssh key	(任意) SSH サーバ キーを表示します。
ステップ 5	switch# copy running-config startup-config	(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。

次に、SSH サーバ キーを生成する例を示します。

```
switch# configure terminal
switch(config)# ssh key rsa 2048
switch(config)# exit
switch# show ssh key
switch# copy running-config startup-config
```

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 3 種類のいずれかの形式で指定できます。

- Open SSH 形式
- Internet Engineering Task Force (IETF) SECSH 形式
- Privacy Enhanced Mail (PEM) 形式の公開キー証明書

Open SSH 形式による SSH 公開キーの指定

ユーザアカウント用に SSH 形式で SSH 公開キーを指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# username username sshkey ssh-key	SSH 形式で SSH 公開キーを設定します。
ステップ 3	switch(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# show user-account	(任意) ユーザアカウントの設定を表示します。
ステップ 5	switch# copy running-config startup-config	(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。

次に、Open SSH 形式で SSH 公開キーを指定する例を示します。

```
switch# configure terminal
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwFZcTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rz0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```



(注) 上記の例の **username** コマンドは、読みやすくするために改行されていますが、単一行です。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# copy server-file bootflash:filename	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。File Transfer Protocol (FTP)、SCP、SSH File Transfer Protocol (SFTP)、または Trivial File Transfer Protocol (TFTP) サーバを利用できます。
ステップ 2	switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 3	switch(config)# username username sshkey file filename	SSH 形式で SSH 公開キーを設定します。
ステップ 4	switch(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ます。
ステップ 5	switch# show user-account	(任意) ユーザアカウントの設定を表示します。
ステップ 6	switch# copy running-config startup-config	(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。

次に、IETF SECSH 形式で SSH 公開キーを指定する例を示します。

```
switch#copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
switch# configure terminal
switch(config)# username User1 sshkey file bootflash:secsh_file.pub
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

PEM フォーマット化された公開キー証明書形式による SSH 公開キーの指定

ユーザアカウント用に PEM フォーマット化された公開キー証明書形式で SSH 公開キーを指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# copy server-file bootflash:filename	サーバから PEM フォーマット化された公開キー証明書形式の SSH キーを含むファイルをダウンロードします。FTP、SCP、SFTP、または TFTP サーバを利用できます。
ステップ 2	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	switch# show user-account	(任意) ユーザ アカウントの設定を表示します。
ステップ 4	switch# copy running-config startup-config	(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。

次に、PEM フォーマット化された公開キー証明書形式で SSH 公開キーを指定する例を示します。

```
switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem
switch# configure terminal
switch# show user-account
switch# copy running-config startup-config
```

SSH ソース インターフェイスの設定

特定のインターフェイスを使用するよう SSH 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	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)# ipsshsource-interface typeslot/port	すべての SSH パケットに対してソース インターフェイスを設定します。次のリストに、 <i>interface</i> として有効な値を示します。 <ul style="list-style-type: none"> • ethernet • loopback • mgmt • port-channel • vlan

	コマンドまたはアクション	目的
ステップ 3	switch(config)# show ip ssh source-interface	設定済みの SSH ソース インターフェイスを表示します。

次に、SSH ソース インターフェイスを設定する例を示します。

```
switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip ssh source-interface ethernet 1/7
switch(config)# show ip ssh source-interface
VRF Name                               Interface
default                                 Ethernet1/7
```

リモート デバイスとの SSH セッションの開始

Cisco Nexus デバイスからリモート デバイスに接続する SSH セッションを開始できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# ssh {hostname username@hostname} [vrfvrf-name]	リモート デバイスとの SSH セッションを作成します。引数 <i>hostname</i> には、IPv4 アドレス、またはホスト名を指定します。

SSH ホストのクリア

SCP または SFTP を使用してサーバからファイルをダウンロードする場合は、サーバと信頼性のある SSH 関係を確立します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# clear ssh hosts	SSH ホストセッションをクリアします。

SSH サーバのディセーブル化

SSH サーバは、デフォルトでCisco Nexus デバイスでイネーブルになっています。

手順

	コマンドまたはアクション	目的
ステップ 1	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] feature ssh	SSH サーバをイネーブル/ディセーブルにします。デフォルトではイネーブルになっています。
ステップ 3	switch(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# show ssh server	(任意) SSH サーバの設定を表示します。
ステップ 5	switch# copy running-config startup-config	(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 サーバ キーの削除

SSH サーバをディセーブルにした後、SSH サーバ キーを削除できます。



(注) 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。

手順

	コマンドまたはアクション	目的
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 feature ssh	SSH サーバをディセーブルにします。
ステップ 3	switch(config)# no ssh key [dsa rsa]	SSH サーバ キーを削除します。

	コマンドまたはアクション	目的
		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	switch(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 5	switch# show ssh key	(任意) SSH サーバの設定を表示します。
ステップ 6	switch# copy running-config startup-config	(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 セッションのクリア

Cisco Nexus デバイスから SSH セッションをクリアできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# show users	ユーザ セッション情報を表示します。
ステップ 2	switch# clear linevty-line	ユーザ SSH セッションをクリアします。

SSH の設定例

次に、SSH を設定する例を示します。

手順

- ステップ 1 SSH サーバ キーを生成します。
- ```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

ステップ 2 SSH サーバをイネーブルにします。

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

(注) SSH サーバはデフォルトでイネーブルになっているため、この手順は必要ありません。

ステップ 3 SSH サーバ キーを表示します。

```
switch(config)# show ssh key
rsa Keys generated:Fri May 8 22:09:47 2009

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4WlAV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/
cTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4ZXIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5/
Ninn0Mc=

bitcount:1024

fingerprint:
4b:d:f6:b9:42:e9:d9:71:3c:bd:09:94:4a:93:ac:ca

could not retrieve dsa key information

```

ステップ 4 Open SSH 形式による SSH 公開キーを指定します。

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4WlAV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
```

ステップ 5 設定を保存します。

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

## Telnet の設定

### Telnet サーバのディセーブル化

デフォルトでは、Telnet サーバはイネーブルに設定されています。Cisco Nexus デバイスの Telnet サーバをディセーブルにできます。

## 手順

|        | コマンドまたはアクション                               | 目的                                               |
|--------|--------------------------------------------|--------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>          | グローバル 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)# <b>[no] feature telnet</b> | Telnet サーバをイネーブル/ディセーブルにします。デフォルトではイネーブルになっています。 |

## Telnet サーバの再イネーブル化

Cisco Nexus デバイスの Telnet サーバがディセーブルにされた場合は、再度イネーブルにできます。

## 手順

|        | コマンドまたはアクション                               | 目的                      |
|--------|--------------------------------------------|-------------------------|
| ステップ 1 | switch(config)# <b>[no] feature telnet</b> | Telnet サーバを再度イネーブルにします。 |

## Telnet ソース インターフェイスの設定

特定のインターフェイスを使用するよう Telnet 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 | switch# <b>configure terminal</b>                                      | グローバル 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)# <b>ip telnet source-interface</b> <i>typeslot/port</i> | すべての Telnet パケットに対してソースインターフェイスを設定します。次のリストに、 <i>interface</i> として有効な値を示します。 <ul style="list-style-type: none"> <li>• ethernet</li> <li>• loopback</li> <li>• mgmt</li> </ul> |

|  | コマンドまたはアクション | 目的                                                                               |
|--|--------------|----------------------------------------------------------------------------------|
|  |              | <ul style="list-style-type: none"> <li>• port-channel</li> <li>• vlan</li> </ul> |

次に、Telnet ソース インターフェイスを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip telnet source-interface ethernet 1/6
switch(config)# show ip telnet source-interface
VRF Name Interface
default Ethernet1/6
switch(config)#
```

## リモート デバイスとの Telnet セッションの開始

Telnet セッションを開始してリモート デバイスに接続する前に、次の作業を行う必要があります。

- リモート デバイスのホスト名を取得します。必要に応じて、リモート デバイスのユーザ名も取得します。
- Cisco Nexus デバイス上で Telnet サーバをイネーブルにします。
- リモート デバイス上で Telnet 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 | switch# <i>telnethostname</i> | リモート デバイスとの Telnet セッションを作成します。引数 <i>hostname</i> には、IPv4 アドレス、IPv6 アドレス、またはデバイス名を指定します。 |

次に、Telnet セッションを開始してリモート デバイスに接続する例を示します。

```
switch# telnet 10.10.1.1
Trying 10.10.1.1...
Connected to 10.10.1.1.
Escape character is '^]'.
switch login:
```

## Telnet セッションのクリア

Cisco Nexus デバイスから Telnet セッションをクリアできます。

## 手順

|        | コマンドまたはアクション                      | 目的                       |
|--------|-----------------------------------|--------------------------|
| ステップ 1 | switch# <b>show users</b>         | ユーザ セッション情報を表示します。       |
| ステップ 2 | switch# <b>clear linevty-line</b> | 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 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。

| コマンドまたはアクション                                      | 目的                                                                                              |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------|
| switch# <b>show ssh key [dsa   rsa]</b>           | SSH サーバ キー ペアの情報を表示します。                                                                         |
| switch# <b>show running-config security [all]</b> | 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。キーワード <b>all</b> 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。 |
| switch# <b>show ssh server</b>                    | SSH サーバの設定を表示します。                                                                               |
| switch# <b>show user-account</b>                  | ユーザ アカウント情報を表示します。                                                                              |

## SSH のデフォルト設定

次の表に、SSH パラメータのデフォルト設定を示します。

表 8: デフォルトの SSH 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                  |
| Telnet サーバ   | イネーブル                 |







## 第 7 章

# PKI の設定

この章の内容は、次のとおりです。

- [PKI の概要, 77 ページ](#)
- [PKI のライセンス要件, 82 ページ](#)
- [PKI の注意事項と制約事項, 82 ページ](#)
- [PKI のデフォルト設定, 83 ページ](#)
- [CA の設定とデジタル証明書, 83 ページ](#)
- [PKI の設定の確認, 99 ページ](#)
- [PKI の設定例, 100 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。

## 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 デバイスは多数のトラストポイントを持つことができ、デバイス上のすべてのアプリケーションがあらゆるトラストポイント CA で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 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 ペアを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、同じ名前でも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 が同じ名前でも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。



(注) 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 ソフトウェアでは、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。選択肢には、CRL、none、これらの方式の組み合わせがあります。

### 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。

## 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 | PKI 機能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すべて Cisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。 |

## 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 ソフトウェアでは、OSCP をサポートしていません。



(注) 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。

## 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。

表 9: 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。



**注意** 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。

## 手順

|        | コマンドまたはアクション                                                                                            | 目的                                                              |
|--------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>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 | <b>hostnamehostname</b><br><br>例：<br>switch(config)# hostname DeviceA                                   | デバイスのホスト名を設定します。                                                |
| ステップ 3 | <b>ip domain-namename [use-vrfrvf-name]</b><br><br>例：<br>DeviceA(config)# ip domain-name<br>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 | <b>exit</b><br><br>例：<br>switch(config)# exit<br>switch#                                                | 設定モードを終了します。                                                    |
| ステップ 5 | <b>show hosts</b><br><br>例：<br>switch# show hosts                                                       | (任意)<br>IP ドメイン名を表示します。                                         |
| ステップ 6 | <b>copy running-config startup-config</b><br><br>例：<br>switch# copy running-config<br>startup-config    | (任意)<br>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。



## 手順

|        | コマンドまたはアクション                                                                                                                                                                  | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例 :<br><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 | <b>crypto key generate rsa</b><br><b>[labellabel-string] [exportable]</b><br><b>[modulussize]</b><br><br>例 :<br><pre>switch(config)# crypto key generate rsa exportable</pre> | <p>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。</p> <p>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。</p> <p>有効なモジュラスの値は 512、768、1024、1536、および 2048 です。デフォルトのモジュラスのサイズは 512 です。</p> <p>(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。</p> <p>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。</p> <p><b>注意</b> キー ペアのエクスポートの可否は変更できません。</p> |
| ステップ 3 | <b>exit</b><br><br>例 :<br><pre>switch(config)# exit switch#</pre>                                                                                                             | 設定モードを終了します。                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ステップ 4 | <b>show crypto key mypubkey rsa</b><br><br>例 :<br><pre>switch# show crypto key mypubkey rsa</pre>                                                                             | (任意)<br>作成したキーを表示します。                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ステップ 5 | <b>copy running-config</b><br><b>startup-config</b><br><br>例 :<br><pre>switch# copy running-config startup-config</pre>                                                       | (任意)<br>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。

はじめる前に

RSA キー ペアを作成します。

手順

|        | コマンドまたはアクション                                                                                                                | 目的                                                                                                                            |
|--------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>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 | <b>crypto ca trustpointname</b><br><br>例：<br>switch(config)# crypto ca<br>trustpoint admin-ca<br>switch(config-trustpoint)# | 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。<br><br>(注) デバイスに設定できるトラストポイントの最大数は 16 です。                           |
| ステップ 3 | <b>enrollment terminal</b><br><br>例：<br>switch(config-trustpoint)#<br>enrollment terminal                                   | 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す。<br><br>(注) 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 4 | <b>rsakeypairlabel</b><br><br>例：<br>switch(config-trustpoint)#<br>rsakeypair SwitchA                                        | 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。<br><br>(注) CA ごとに 1 つの RSA キー ペアだけを指定できます。                                          |
| ステップ 5 | <b>exit</b><br><br>例：<br>switch(config-trustpoint)# exit<br>switch(config)#                                                 | 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 | <b>show crypto ca trustpoints</b><br><br>例：<br>switch(config)# show crypto ca<br>trustpoints                                | (任意)<br>トラストポイントの情報を表示します。                                                                                                    |

|        | コマンドまたはアクション                                                                                                          | 目的                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| ステップ 7 | <b>copy running-config startup-config</b><br><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre> | (任意)<br>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力し、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 が自身の証明書を署名したもの) 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。



(注) 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。

### はじめる前に

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力します。

### 手順

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                                                                                                                                    | 目的                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例 :<br><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 | <b>crypto ca authenticatename</b><br><br>例 :<br><pre>switch(config)# crypto ca authenticate admin-ca input (cut &amp; paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : -----BEGIN CERTIFICATE----- MIIC4jCCAoygAwIBAgIQBWDsiay0GZRPSRI1jK0ZejanBgkqhkiG9w0BAQUFADCB kDEgMB4GCSqGSIb3DQEJARYRYWlhbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAK10</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。 |

|                | コマンドまたはアクション                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 目的                                                                                                                                                                             |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <pre> MRiWEAYDVQQIEw1LYXJuYXRha2ExEjAQBGNVBACTCUJhbmdbG9yZTEOMAwGA1UE ChMFQ2l2Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFwYXJuYSBD QTAEFw0wNTA1MDMYmJQ2MzdaFw0wNzA1MDMYmJUIMTdaIGQMSAwHgYJKoZIhvcN AQkBFhFhbWFuZGt1QGNpc2NvLmNvbTElMAkGA1UEBhMCSU4xEjAQBGNVBAGTCUth cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVdaXNjbzETMBEG A1UECzMkbnV0c3RvcnFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypywuoSNZXOMperXXI OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxxvYKvysCAwEAAsOBvzCBvDALBgNVHQ8E BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs L0FwYXJuYXUyMENBLmNybdAwOC6gLIYqZmlsZTovL1xc3N1LTA4XEN1cnRFbnJv bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB BQUAA0EAHv6UQ+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]: yes </pre> | <p>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。</p> <p>(注) 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。</p> |
| ス<br>テッ<br>プ 3 | <p><b>exit</b></p> <p>例 :</p> <pre>switch(config)# exit switch#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 設定モードを終了します。                                                                                                                                                                   |
| ス<br>テッ<br>プ 4 | <p><b>show crypto ca trustpoints</b></p> <p>例 :</p> <pre>switch# show crypto ca trustpoints</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | (任意)<br>トラストポイント CA の情報を表示します。                                                                                                                                                 |
| ス<br>テッ<br>プ 5 | <p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch# copy running-config startup-config</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | (任意)<br>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。                                                                                                                              |

## 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間で取り消され、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。

### はじめる前に

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。

### 手順

|        | コマンドまたはアクション                                                                                                                | 目的                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>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 | <b>crypto ca trustpointname</b><br><br>例：<br>switch(config)# crypto ca<br>trustpoint admin-ca<br>switch(config-trustpoint)# | 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 | <b>revocation-check {crl [none]   none}</b><br><br>例：<br>switch(config-trustpoint)#<br>revocation-check none                | 証明書取消確認方法を設定します。デフォルト方式は <b>crl</b> です。<br><br>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。 |
| ステップ 4 | <b>exit</b><br><br>例：<br>switch(config-trustpoint)# exit<br>switch(config)#                                                 | 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 | <b>show crypto ca trustpoints</b><br><br>例：<br>switch(config)# show crypto ca<br>trustpoints                                | (任意)<br>トラストポイント CA の情報を表示します。                                                               |

|        | コマンドまたはアクション                                                                                                         | 目的                                                |
|--------|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| ステップ 6 | <b>copy running-config startup-config</b><br><br>例：<br><pre>switch(config)# copy running-config startup-config</pre> | (任意)<br>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。 |

## 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。

### はじめる前に

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。

### 手順

|        | コマンドまたはアクション                                                                                                                     | 目的                         |
|--------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br><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 | <b>crypto ca enroll name</b><br><br>例：<br><pre>switch(config)# crypto ca enroll admin-ca Create the certificate request ..</pre> | 認証した CA に対する証明書要求を作成します。   |

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 目的                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
|        | <pre>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... -----BEGIN CERTIFICATE REQUEST----- MIIBqzCCARQCAQAwHDEaMBGGA1UEAxMRVnVnYXNjby5jb20wgZ8wDQYJ KoZlIhvcNAQEEDBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8r141KY 0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVksCzXv8S VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCScqGSIB3DQEJ DjEpMCCcwJQYDVROAQH/BBswGYIRVnVnYXNjby5jb22HBKwWH6IwDQYJ KoZlIhvcNAQEEDBQADgYEAKT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt PftRncWUE/pw6HayfQ12T3ecgNwel2d15133YBF2bktExiI6U188nTOjglXMjja8 8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0= -----END CERTIFICATE REQUEST-----</pre> | <p>(注) 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。</p> |
| ステップ 3 | <p><b>exit</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# exit switch(config)#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>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。</p>                                                           |
| ステップ 4 | <p><b>show crypto ca certificates</b></p> <p>例 :</p> <pre>switch(config)# show crypto ca certificates</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p>(任意)<br/>CA 証明書を表示します。</p>                                                                  |
| ステップ 5 | <p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>(任意)<br/>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。</p>                                      |

## 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。

### はじめる前に

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。

### 手順

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 目的                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <p><b>configure terminal</b></p> <p>例 :</p> <pre>switch# configure terminal switch(config)#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>グローバル コンフィギュレーションモードを開始します。</p>                                                                              |
| ステップ 2 | <p><b>crypto ca importnamecertificate</b></p> <p>例 :</p> <pre>switch(config)# crypto ca import admin-ca certificate input (cut &amp; paste) certificate in PEM format: -----BEGIN CERTIFICATE----- MIIEADCCA6qgAwIBAgIKCj00oQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G CSqGSIB3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD VQQIEW1LYXJuYXRha2ExEjAQBGNVBAcTCUJhbmhhdG9yZTEOMAwGA1UEChMFQ2l3 Y28xEzARBGNVBAsTCm5ldHN0b3JhZ2UxZjAQBGNVBAMTUCFwYXJuYySDQTAeFw0w NTEeXMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLzE2 Y2l3Y28uY29tMIGfMA0GCsqGSIB3DQEBQUAA4GNADCBiQKBgcQC/GNVAcDjQu41C dQ1WkjKjSICdpLfK5eJSmNCqujGpzcKsZPFxjF2UoiyeCYE8ylncWyw5E08rJ47 glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb x7RifdV06uFqFZEgS17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw GYIRVmVnYXMTMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBByEFKLi+2sspWEfgrR bhWmlVyo9jngMIHMBGNVHSMEgcQwgcGAFCco8kaDG6wJTEVNjskYUBoLFmxxoYGW pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWVufzGt1QGnPC2NvLmNvbTElMAkGA1UE BhMCSU4xEjAQBGNVBAgTCUthcm5hdGFryTESMBAGA1UEBxmJQmFuZ2Fsb3JlMQ4w DAYDVQQKEwVdaXNjbyETMBEGA1UECxMKbmV0c3RvcnFnZTESMBAGA1UEAxMjQXBh cm5hIENBghAFYnkjrLQZLE9JEiWMrR16MGsGA1UdHwRkMG1wLqAsoCqGKgH0dHA6 Ly9zc2UtMDgvQ2VydEVucm9sb3c9BcGFybmElMjBDQ55jcmwwMKAuoCyGKmZpbGU6 Ly9zcXhNHzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDQyZDZlZ2FzLzE2 AQEefjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3N1LTA4L0N1cnRfbnJvbGwvc3N1 LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xccc3N1LTA4 XEN1cnRfbnJvbGwvc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF AANBADbGBGsbE7GNLh9xeOTWBNbm24U69ZSuDDcOcuZUUTgrpnTqVpPyejtsyflw E36cIZu4WsExREqxbTk8ycx7V5o= -----END CERTIFICATE-----</pre> | <p>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。</p> <p>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。</p> |
| ステップ 3 | <p><b>exit</b></p> <p>例 :</p> <pre>switch(config)# exit switch#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <p>設定モードを終了します。</p>                                                                                             |



|        | コマンドまたはアクション                                                                                                 | 目的                                                |
|--------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| ステップ 4 | <b>show crypto ca certificates</b><br><br>例：<br><pre>switch# show crypto ca certificates</pre>               | (任意)<br>CA 証明書を表示します。                             |
| ステップ 5 | <b>copy running-config startup-config</b><br><br>例：<br><pre>switch# copy running-config startup-config</pre> | (任意)<br>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。



(注) 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。

## 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。



(注) エクスポートの URL を指定するときに使用できるのは、`bootflash:filename` という形式だけです。

### はじめる前に

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。

### 手順

|        | コマンドまたはアクション                                                                                                                                                                  | 目的                                                                                                                                                                                                                                                                                              |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br><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 | <b>crypto ca exportname pkcs12</b><br><b>bootflash:filenamepassword</b><br><br>例：<br><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 | <b>exit</b><br><br>例：<br><pre>switch(config)# exit switch#</pre>                                                                                                              | 設定モードを終了します。                                                                                                                                                                                                                                                                                    |
| ステップ 4 | <b>copy</b><br><b>booflash:filenamescheme://server/</b><br><b>[url/]filename</b><br><br>例：<br><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。<br><br><i>scheme</i> 引数として、 <b>tftp:</b> 、 <b>ftp:</b> 、 <b>scp:</b> 、または <b>sftp:</b> を指定できます。 <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。<br><br><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。 |

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

## PKCS 12 形式でのアイデンティティ情報のインポート

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。



(注) インポートの 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。

### はじめる前に

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。

### 手順

|        | コマンドまたはアクション                                                                                                                                                             | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b><code>copyscheme://server/[url]/filenamebootflash:filename</code></b><br><br>例 :<br><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。<br><br><b><code>scheme</code></b> 引数として、 <b><code>tftp:</code></b> 、 <b><code>ftp:</code></b> 、 <b><code>scp:</code></b> 、または <b><code>sftp:</code></b> を指定できます。<br><b><code>server</code></b> 引数は、リモートサーバのアドレスまたは名前であり、 <b><code>url</code></b> 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。<br><br><b><code>server</code></b> 、 <b><code>url</code></b> 、および <b><code>filename</code></b> 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 | <b><code>configure terminal</code></b><br><br>例 :<br><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 | <b><code>crypto ca importnamepkcs12 bootflash:filename</code></b><br><br>例 :<br><pre>switch(config)# crypto ca import 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 証明書をインポートします。                                                                                                                                                                                                                                                                                                                                                                                |

|        | コマンドまたはアクション                                                                                       | 目的                                                |
|--------|----------------------------------------------------------------------------------------------------|---------------------------------------------------|
| ステップ 4 | <b>exit</b><br><br>例 :<br>switch(config)# exit<br>switch#                                          | 設定モードを終了します。                                      |
| ステップ 5 | <b>show crypto ca certificates</b><br><br>例 :<br>switch# show crypto ca certificates               | (任意)<br>CA 証明書を表示します。                             |
| ステップ 6 | <b>copy running-config startup-config</b><br><br>例 :<br>switch# copy running-config startup-config | (任意)<br>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。

### はじめる前に

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。

### 手順

|        | コマンドまたはアクション                                                                                                                       | 目的                                                                                                                                                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>copyscheme:[//server/[url/]]filenamebootflash:filename</b><br><br>例 :<br>switch# copy tftp:adminca.crl<br>bootflash:adminca.crl | リモートサーバから CRL をダウンロードします。<br><br><i>scheme</i> 引数として、 <b>tftp:</b> 、 <b>ftp:</b> 、 <b>scp:</b> 、または <b>sftp:</b> を指定できます。 <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。<br><br><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。 |

|        | コマンドまたはアクション                                                                                                                            | 目的                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| ステップ 2 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>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 3 | <b>crypto ca crl requestnamebootflash:filename</b><br><br>例：<br>switch(config)# crypto ca crl request admin-ca<br>bootflash:adminca.crl | 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 | <b>exit</b><br><br>例：<br>switch(config)# exit<br>switch#                                                                                | 設定モードを終了します。                                      |
| ステップ 5 | <b>show crypto ca crlname</b><br><br>例：<br>switch# show crypto ca crl admin-ca                                                          | (任意)<br>CA の CRL 情報を表示します。                        |
| ステップ 6 | <b>copy running-config startup-config</b><br><br>例：<br>switch# copy running-config startup-config                                       | (任意)<br>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。

### 手順

|        | コマンドまたはアクション                                                                         | 目的                         |
|--------|--------------------------------------------------------------------------------------|----------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>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 | <b>crypto ca trustpointname</b><br><br>例：<br>switch(config)# crypto ca<br>trustpoint admin-ca<br>switch(config-trustpoint)# | 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 | <b>delete ca-certificate</b><br><br>例：<br>switch(config-trustpoint)#<br>delete ca-certificate                               | 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 | <b>delete certificate [force]</b><br><br>例：<br>switch(config-trustpoint)#<br>delete certificate                             | アイデンティティ証明書を削除します。<br><br>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、 <b>force</b> 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 | <b>exit</b><br><br>例：<br>switch(config-trustpoint)# exit<br>switch(config)#                                                 | 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 | <b>show crypto ca certificates [name]</b><br><br>例：<br>switch(config)# show crypto ca<br>certificates admin-ca              | (任意)<br>CA の証明書情報を表示します。                                                                                                                                                                                                            |
| ステップ 7 | <b>copy running-config startup-config</b><br><br>例：<br>switch(config)# copy<br>running-config startup-config                | (任意)<br>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。



- (注) 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。

## 手順

|        | コマンドまたはアクション                                                                                         | 目的                                                |
|--------|------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>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 | <b>crypto key zeroize rsalabel</b><br><br>例：<br>switch(config)# crypto key zeroize<br>rsa MyKey      | RSA キー ペアを削除します。                                  |
| ステップ 3 | <b>exit</b><br><br>例：<br>switch(config)# exit<br>switch#                                             | 設定モードを終了します。                                      |
| ステップ 4 | <b>show crypto key mypubkey rsa</b><br><br>例：<br>switch# show crypto key mypubkey rsa                | (任意)<br>RSA キー ペアの設定を表示します。                       |
| ステップ 5 | <b>copy running-config startup-config</b><br><br>例：<br>switch# copy running-config<br>startup-config | (任意)<br>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。 |

## 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                                        |
|-------------------------------------|-------------------------------------------|
| <b>show crypto key mypubkey rsa</b> | 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。 |

| コマンド                               | 目的                            |
|------------------------------------|-------------------------------|
| <b>show crypto ca certificates</b> | 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。 |
| <b>show crypto ca crl</b>          | CA の CRL についての情報を表示します。       |
| <b>show crypto ca trustpoints</b>  | 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。



(注) 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。

### 手順

- 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:
revokation methods:  crl
```


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
revokation methods:  crl
```

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-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRI1jK0ZeJANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYWlhbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1O
MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBGNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ21zY28xEzARBGNVBAstCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFwYXJuYSBD
QTAEfw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWVufuZGt1QGNpc2NvLmNvbTELMaKGA1UEBhMCSU4xEjAQBGNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVdaXNjbzETMBEG
A1UECzMkbnV0c3RvcnFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMperXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCACyWdWYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBmNybDAwoC6gLIYqZmlsZTovL1xccc3N1LTA4XEN1cnRFbnJv
bGx0cXQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBggjcvAQQDAgEAMA0GCSqGSIb3DQEB
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-----
MIIBQzCCARQCAQAwHDEaMBGGA1UEAxMRVnVnYXNjby5jaXNjby5jb20wgZ8wDQYJ
KoZlIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVA5MqNIgJ2kt8r141KY
0JC6ManNy4qxk8VEMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NjJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVKSzXv8S
VqyH0vEvAgMBAAGgTzAVBqkqhkiG9w0BCQcxCBMGBmJ2MTIzMDYGCsGSIb3DQEJ
DjEpMCcwJQYDVRORAQH/BBswGYIRVnVnYXNjby5jaXNjby5jb22HBKwWH6IwDQYJ
KoZlIhvcNAQEBBQADgYEAKT60KER6Qo8nj0sDXZVHsfJZh6K6JtDz3Gkd99G1FWgt
PftRncWUE/pw6HayfQ12T3ecgNwel2d15133YBF2bktExiI6U188nTojglXMjja8
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-----
MIIEADCCA6qgAwIBAgIKCj0OoQAAAAAADANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAKlOMRIwEAYD
VQOIEWlLYXJuYXRha2ExEjAQBGNVBACTCUJhbmdbbG9yZTEOMAwGA1UEChMFQ21z
Y28xEzARBGNVBAsTCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFWYXJuYSBDQTAeFw0w
NTEyMTIwMzAyNDhBaFw0wNjE5MTIwMzEyNDhBaMBwGjAYBgNVBAMTEVZlZ2FzLzE2
Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkKjKjSICdpLfK5eJSmNCQujGpzcKsZPFXjF2UoiyeCYE8y1ncWYw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMcNIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCA8wJQYDVRORAQH/BBsw
GYIRVnVnYXNjby5jb22HBKwWH6IwHQYDVROBBYEFKLi+2sspWEfgrR
bhWmlVyo9jngMIHMBGNVHSMGegcQwgGAFCCo8kaDG6wjTEVNjSkYUBoLFmxxoYGW
pIGTMIQMSAwHgYJKoZlIhvcNAQkBFhFhbWwFuZGt1QGNpc2NvLmNvbTELMkGA1UE
BHMCSU4xEjAQBGNVBAGTCUthcm5hdGFyYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVdaXNjby5jaXNjby5jb20wDQYJc3R5bGUwDQYJc3R5bGUwDQYJc3R5
cm5hIENBghAFYFNKJrLQZ1E9JEiWMrR16MGsGA1UdHwRkMGiWlqAsocCqGKG0dHA6
Ly9zc2UtdMDgV2VydEVucm9sb3B3B3B3B3B3B3B3B3B3B3B3B3B3B3B3B3B3B3B3B3
Ly9zcXhNzZS0wOFxZXJ0RW5yb2xsXEFwYXJuYXNjby5jaXNjby5jb20wDQYJc3R5
bGUwDQYJc3R5bGUwDQYJc3R5bGUwDQYJc3R5bGUwDQYJc3R5bGUwDQYJc3R5bGUw
LTA4X0FwYXJuYXNjby5jaXNjby5jb20wDQYJc3R5bGUwDQYJc3R5bGUwDQYJc3R5
bGUwDQYJc3R5bGUwDQYJc3R5bGUwDQYJc3R5bGUwDQYJc3R5bGUwDQYJc3R5bGUw
XENLcnRfbnJvbG9uZ2FzLzE2Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAAANB
ADBGBGsb3R5bGUwDQYJc3R5bGUwDQYJc3R5bGUwDQYJc3R5bGUwDQYJc3R5bGUw
-----
```

```
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。

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。

手順

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

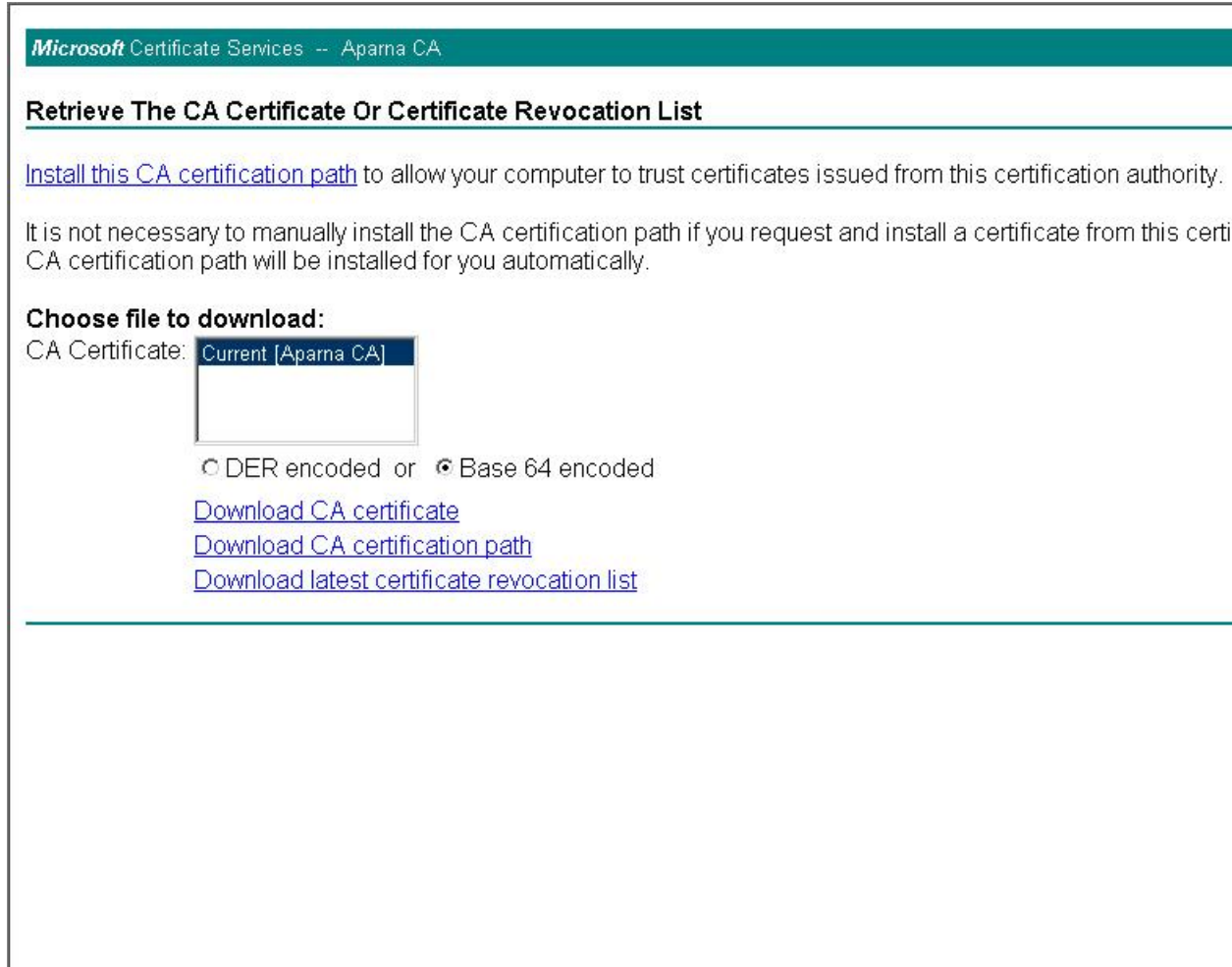
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail 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 -- 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 certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority. The CA certification path will be installed for you automatically.

Choose file to download:

CA Certificate:

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。

The screenshot shows a web browser window with the title "Microsoft Certificate Services -- Apama CA". The main heading is "Retrieve The CA Certificate Or Certificate Revocation List". Below this, there is a link: "Install this CA certification path to allow your computer to trust certificates issued from this certification authority." A paragraph follows: "It is not necessary to manually install the CA. A CA certification path will be installed for you." Under the heading "Choose file to download:", there is a dropdown menu for "CA Certificate:" with "Current [Apama CA]" selected. Below the dropdown are radio buttons for "DER encoded" and "Base64 encoded". There are three links: "Download CA certificate", "Download CA certification path", and "Download latest certificate revocation list". Overlaid on the right side of the browser window is a "File Download" dialog box. The dialog box contains a warning icon and text: "Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file." It lists: "File name: certnew.cer", "File type: Security Certificate", and "From: 10.76.45.108". A warning icon and text state: "This type of file could harm your computer if it contains malicious code." Below this is the question: "Would you like to open the file or save it to your computer?" and four buttons: "Open", "Save", "Cancel", and "More Info". At the bottom of the dialog box is a checked checkbox: "Always ask before opening this type of file".

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。

Microsoft Certificate Services -- Aparna CA

Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow...

It is not necessary to manually install the...
CA certification path will be installed for...

Choose file to download:
CA Certificate: **Current [Aparna CA]**

DER encoded or...

[Download CA certifica...](#)
[Download CA certifica...](#)
[Download latest certifi...](#)

Certificate

General Details Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	0560 D289 ACB4 1994 4F49 1...
Signature algorithm	sha1RSA
Issuer	Aparna CA, netstorage, Cisco...
Valid from	04 Mei 2005 4:16:37
Valid to	04 Mei 2007 4:25:17
Subject	Aparna CA, netstorage, Cisco...
Public key	RSA (512 Bits)

Edit Properties... Copy to File...

OK

- 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。

Microsoft Certificate Services -- Aparna CA

Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow...
 It is not necessary to manually install the...
 CA certification path will be installed for...

Choose file to download:
 CA Certificate: **Current [Aparna CA]**

DER encoded or...
[Download CA certifica](#)
[Download CA certifica](#)
[Download latest certifi](#)

Certificate

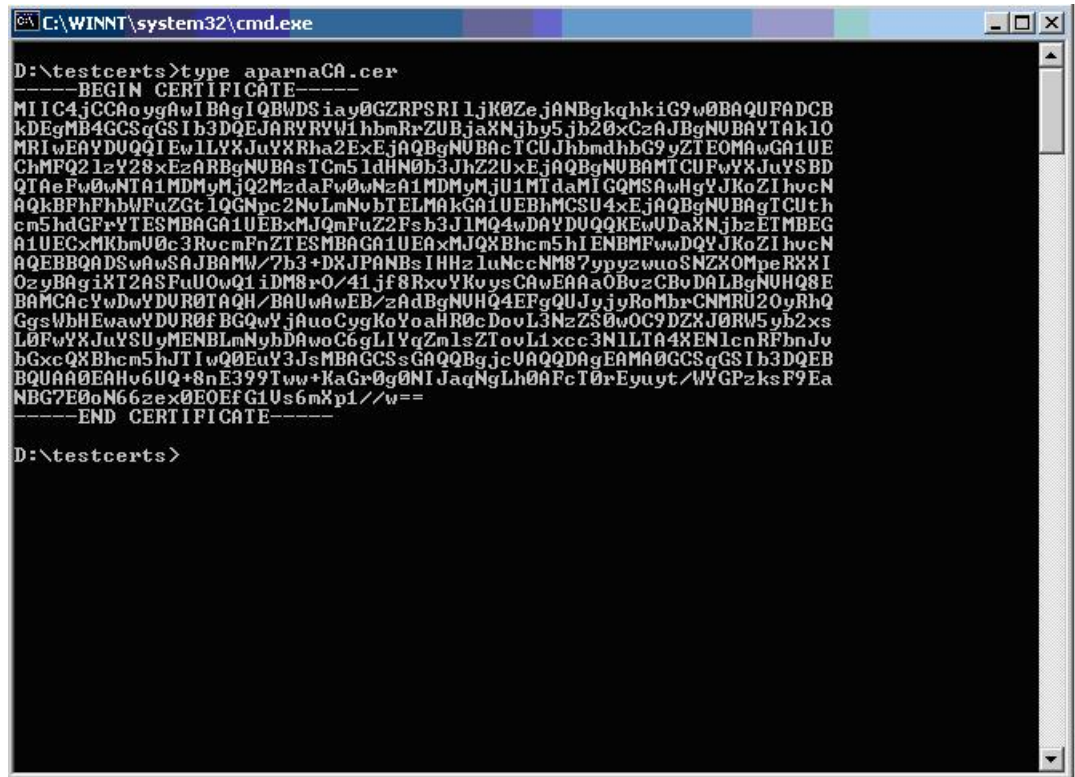
General Details Certification Path

Show: <All>

Field	Certificate Export Wizard
<input type="checkbox"/> Version	Export File Format Certificates can be exported in a variety of file formats. Select the format you want to use: <input type="radio"/> DER encoded binary X.509 (.CER) <input checked="" type="radio"/> Base-64 encoded X.509 (.CER) <input type="radio"/> Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) <input type="checkbox"/> Include all certificates in the certification path if possible <input type="radio"/> Personal Information Exchange - PKCS #12 (.PFX) <input type="checkbox"/> Include all certificates in the certification path if possible <input type="checkbox"/> Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above) <input type="checkbox"/> Delete the private key if the export is successful
<input type="checkbox"/> Serial number	
<input type="checkbox"/> Signature alg	
<input type="checkbox"/> Issuer	
<input type="checkbox"/> Valid from	
<input type="checkbox"/> Valid to	
<input type="checkbox"/> Subject	
<input type="checkbox"/> Public key	

< Back Next >

- 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
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjb3Y5b20xCzAJBgNVBAYTAk10
MRIwEAYDUQIIEwILYXJlYXRha2ExEjAQBgNVBACICUJhbmdhbG9yZTEOMAwwGA1UE
ChMPQ2l2Y28xEzARBgNVBAStCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFWYXJlYXN0
QTAcFw0wNTA1MDMzMzdaFw0wNTA1MDMzMzU1MTdaMIQMSAwHgYJKoZIhvcNAQk
BFhFhbWwFuZGt1QGNpc2NvLmNvbTElMAkGA1UEBhMCSU4xEjAQBgNVBAGTCUth
cm5hdGFrYXN0ESMBAGA1UEBjxMjQmFuZ2Fsb3JlMQ4wDAYDUQKewUDaXNjbzETMBEG
A1UECxMKbmU0c3RvcnFnZTESMBAGA1UEAxMJQXhBhcm5hIENBMFwwDQYJKoZIhvcNAQ
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHZluNcNMs7yppzwoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxyYKvysCAwEAaQ0BuzCBvDALBgNUHQ8E
BAMCAcYwDwYDUROTAQH/BAUwAwEB/zAdBgNUHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDUROfBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJlYXN0yMENBLmNybDAwoC6gLIYgZmlsZTovL1xc3N1LTA4XENlcnRFbnJv
bGxcQXhBhcm5hJTl1wQ0EuY3JsMBAAGCSsGAQQBgjcUAQQDAQEAMAA0GCSqGSIb3DQEB
BQUAAQEAHv6UQ+8nE399Tww+KaGr0g0NIJaNgLh0AFcT0rEyuYt/WVGPzksF9Ea
NBG7E0nN66zEx0E0EfG1Us6mXp1/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。

手順

- ステップ 1** Microsoft Certificate Services の Web インターフェイスから、[Request a certificate] をクリックし、[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 secure program. Once you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail 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** [Advanced request] をクリックし、[Next] をクリックします。

Microsoft Certificate Services -- Aparna 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** [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、[Next] をクリックします。

Microsoft Certificate Services -- Aparna CA

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that 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 using a base64 encoded certificate request file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

ステップ 4 [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、[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 generated by an external server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
VqyHOvEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMG
DjEpMCcwJQYDVORORAQH/BBswGYIRVmVnYXMtMS5j
KoZlIhvcNAQEEBQADgYEAkT6OKER6Qo8nj0sDXZVH
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 -- Aparna CA

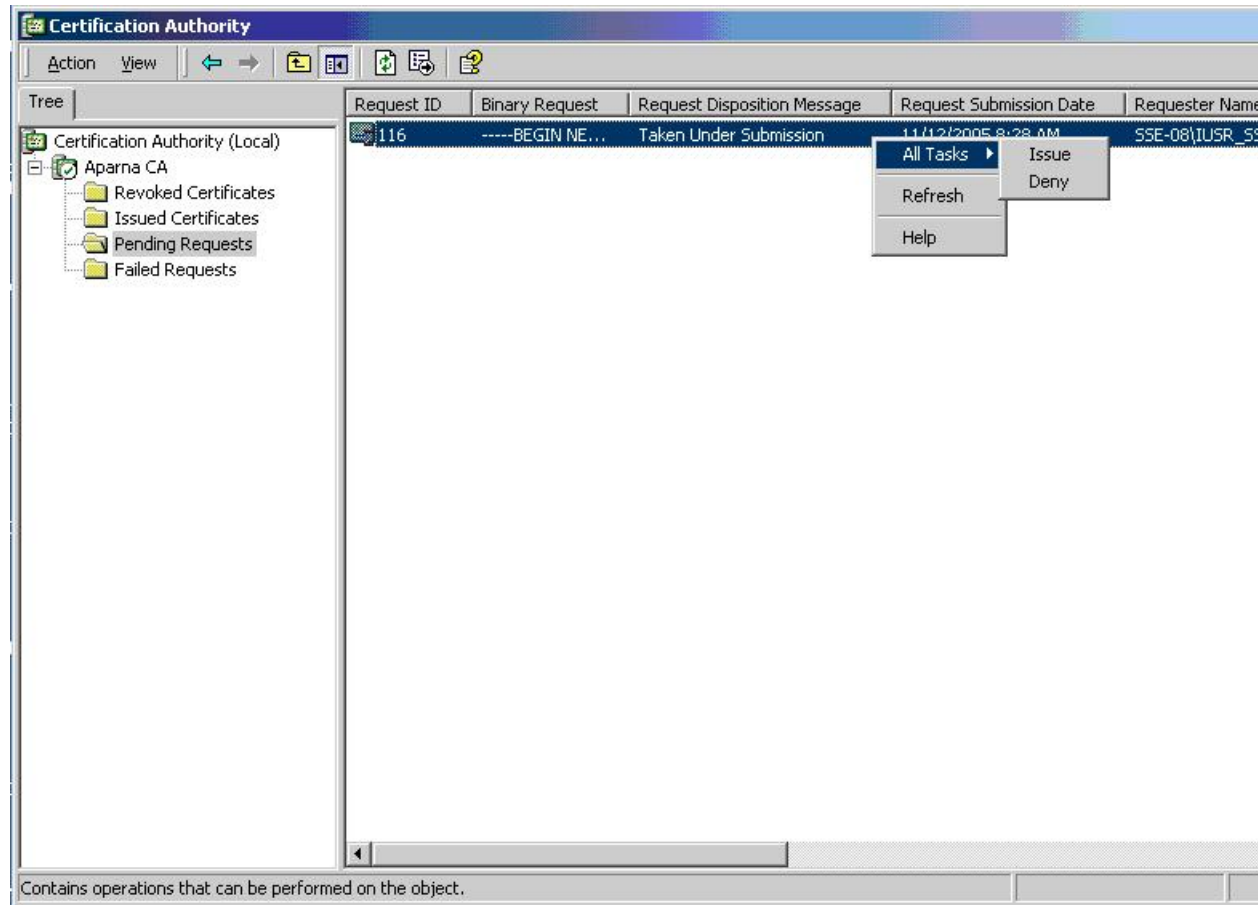
Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you r

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、[Check on a pending certificate] をクリックし、[Next] をクリックします。

Microsoft Certificate Services -- Aparna CA

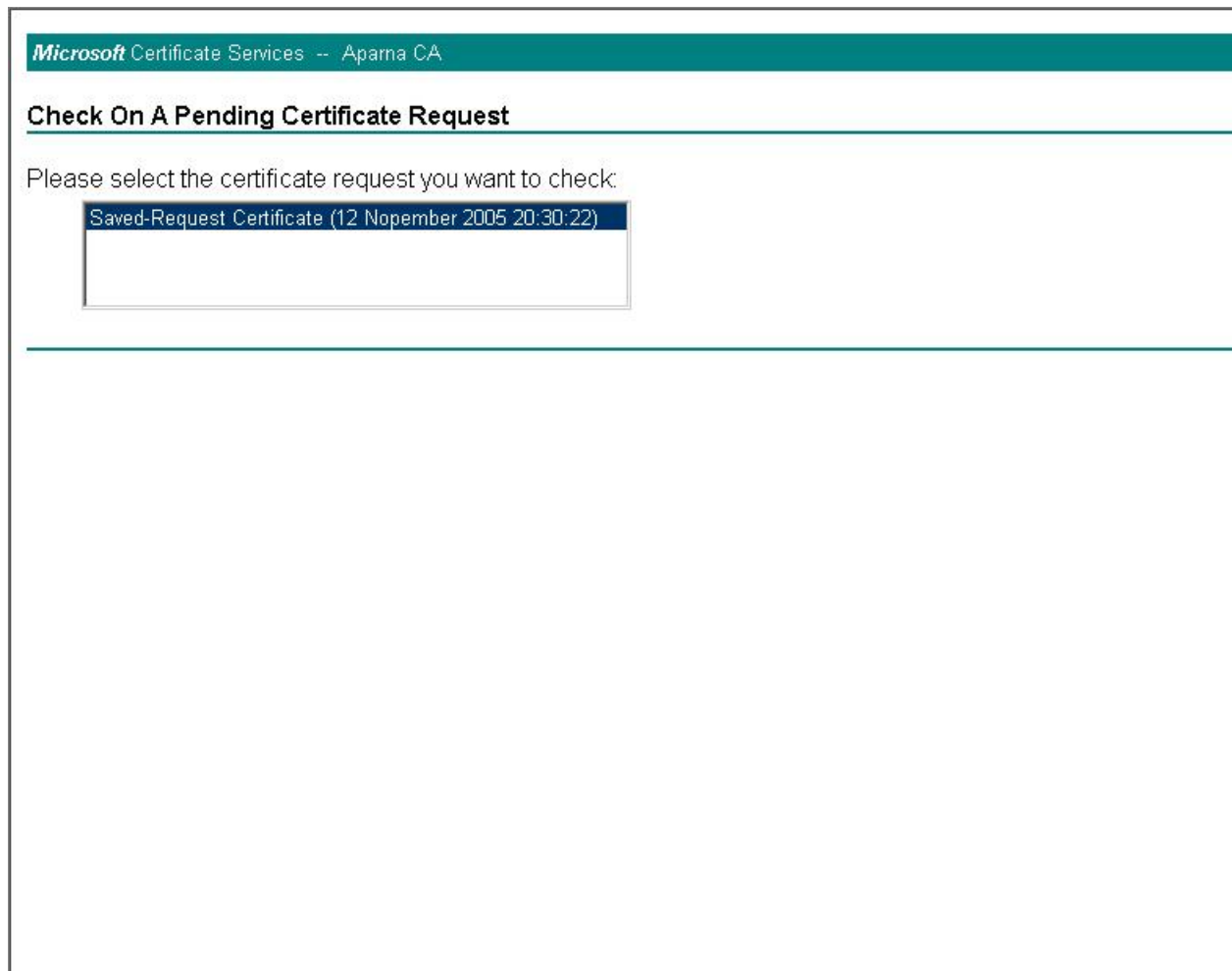
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail depending upon the type of certificate you request.

Select a task:

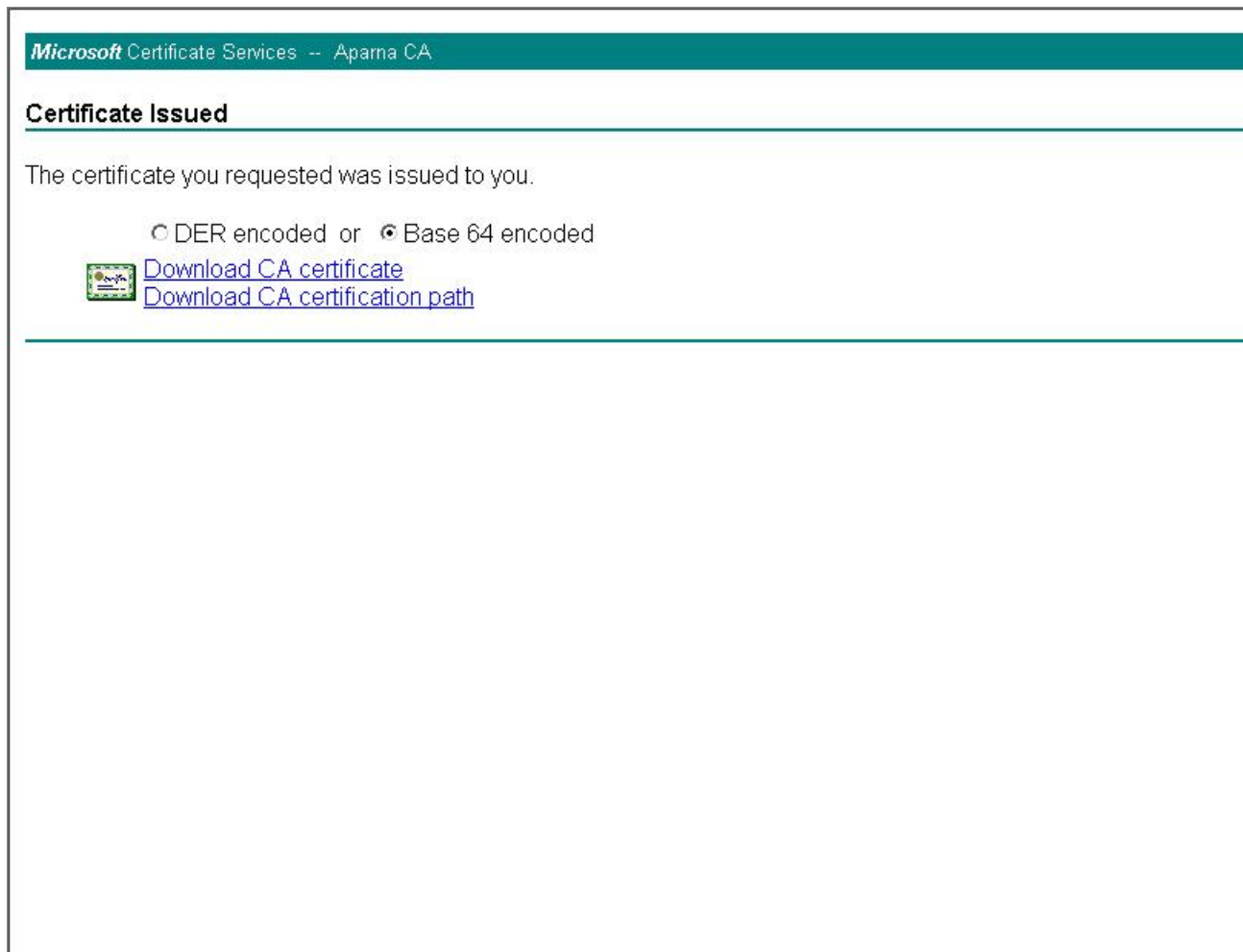
- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

ステップ 8 チェックする証明書要求を選択して、[Next] をクリックします。

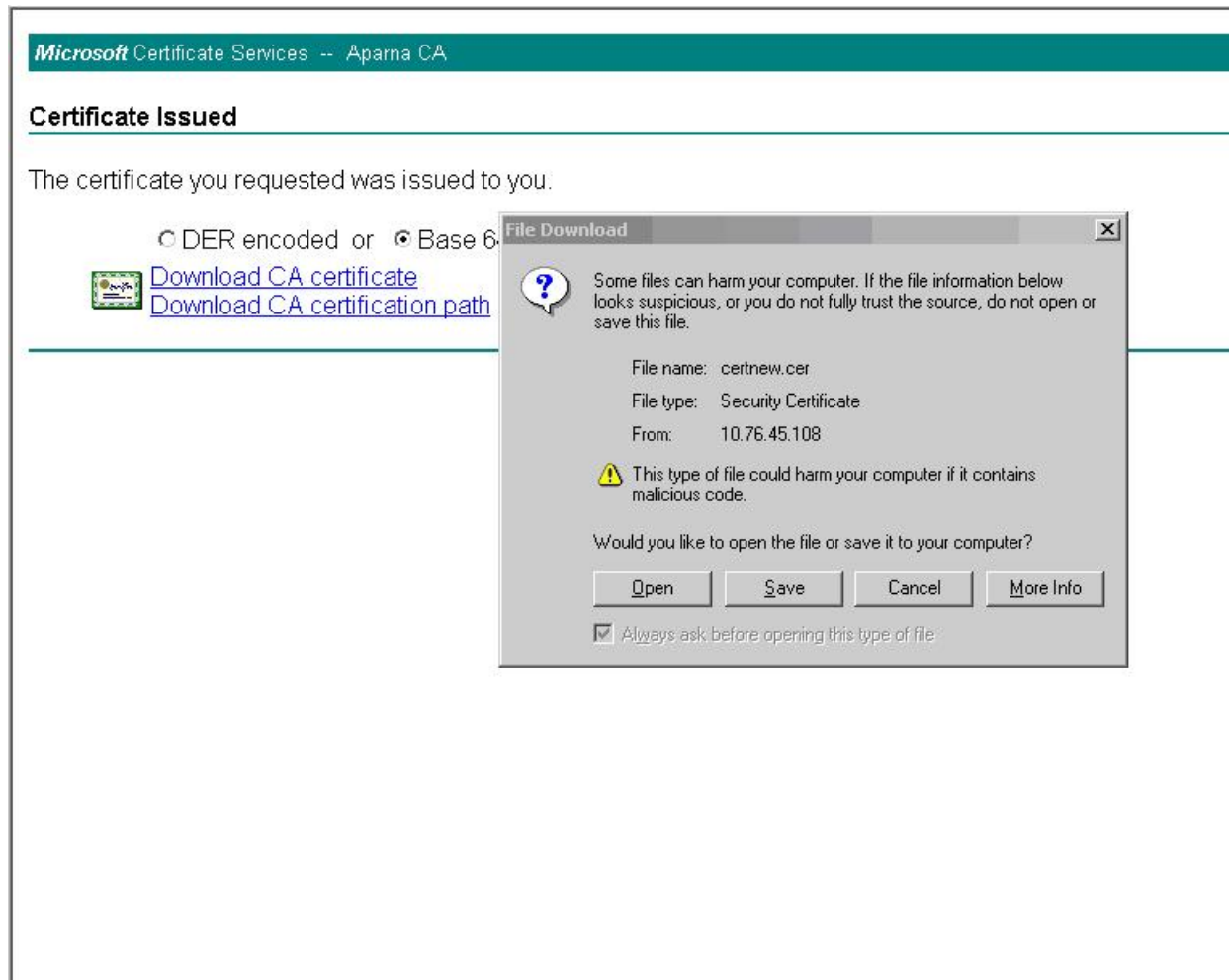


The screenshot shows a web browser window with the title "Microsoft Certificate Services -- Aparna CA". The main heading is "Check On A Pending Certificate Request". Below the heading, the text reads "Please select the certificate request you want to check:". A single list item is displayed in a scrollable box: "Saved-Request Certificate (12 Nopember 2005 20:30:22)".

ステップ 9 [Base 64 encoded] をクリックして、[Download CA certificate] をクリックします。

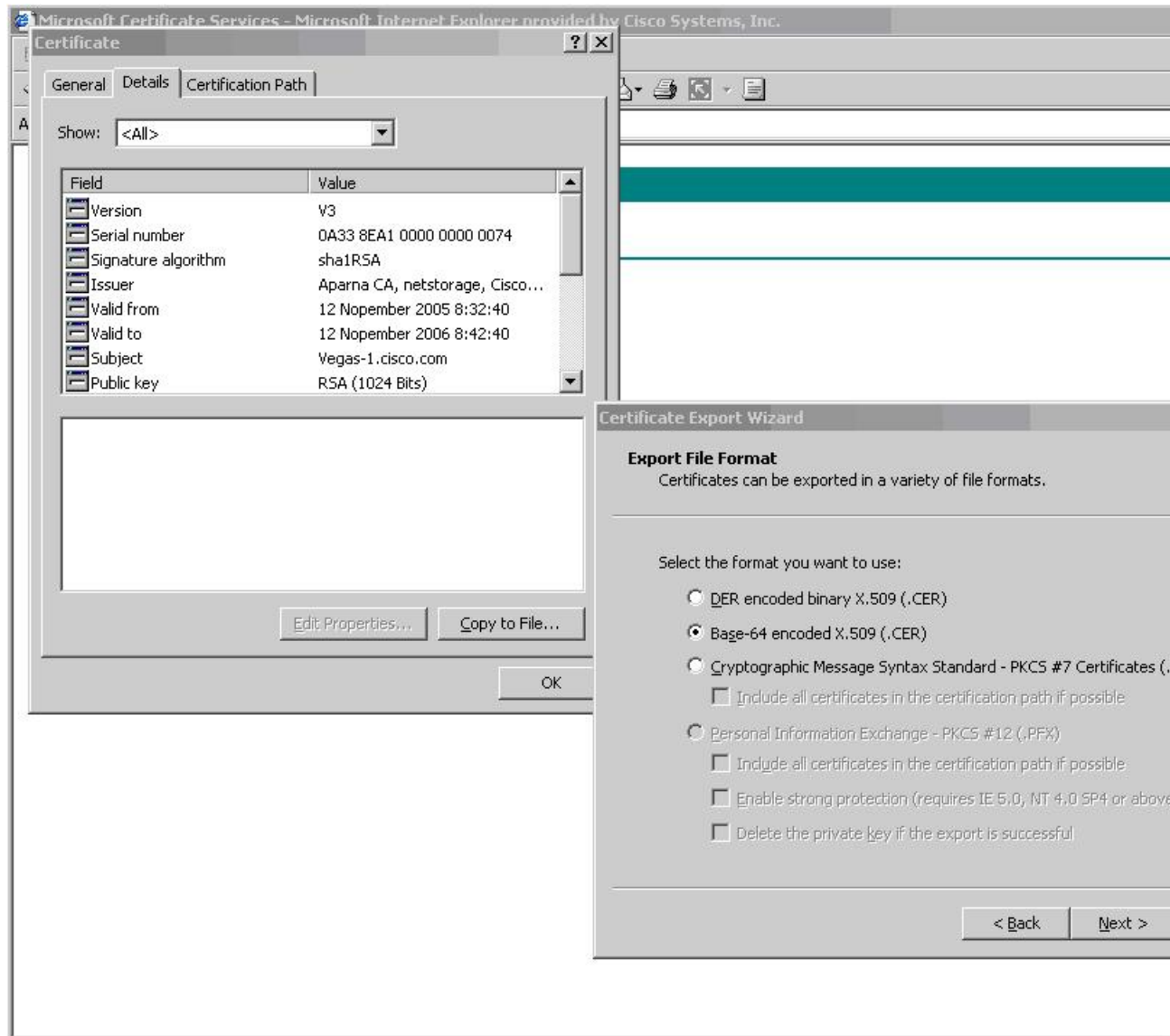


ステップ 10 [File Download] ダイアログボックスで、[Open] をクリックします。

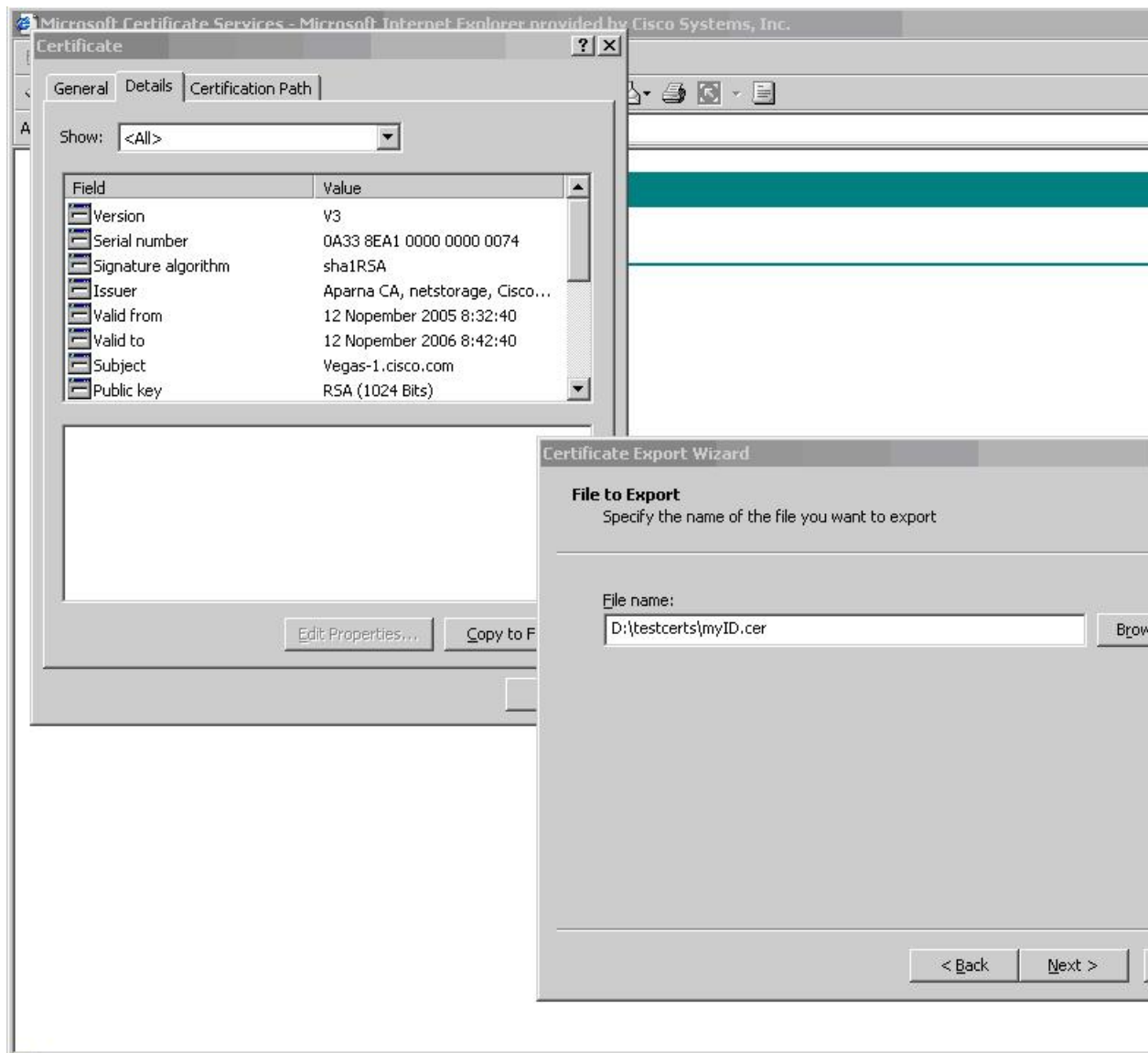


ステップ 11 [Certificate] ボックスで、[Details] タブをクリックし、[Copy to File...] をクリックします。[Certificate Export Wizard] ダイアログボックスで、[Base-64 encoded X.509 (.CER)] をクリックし、[Next] をク

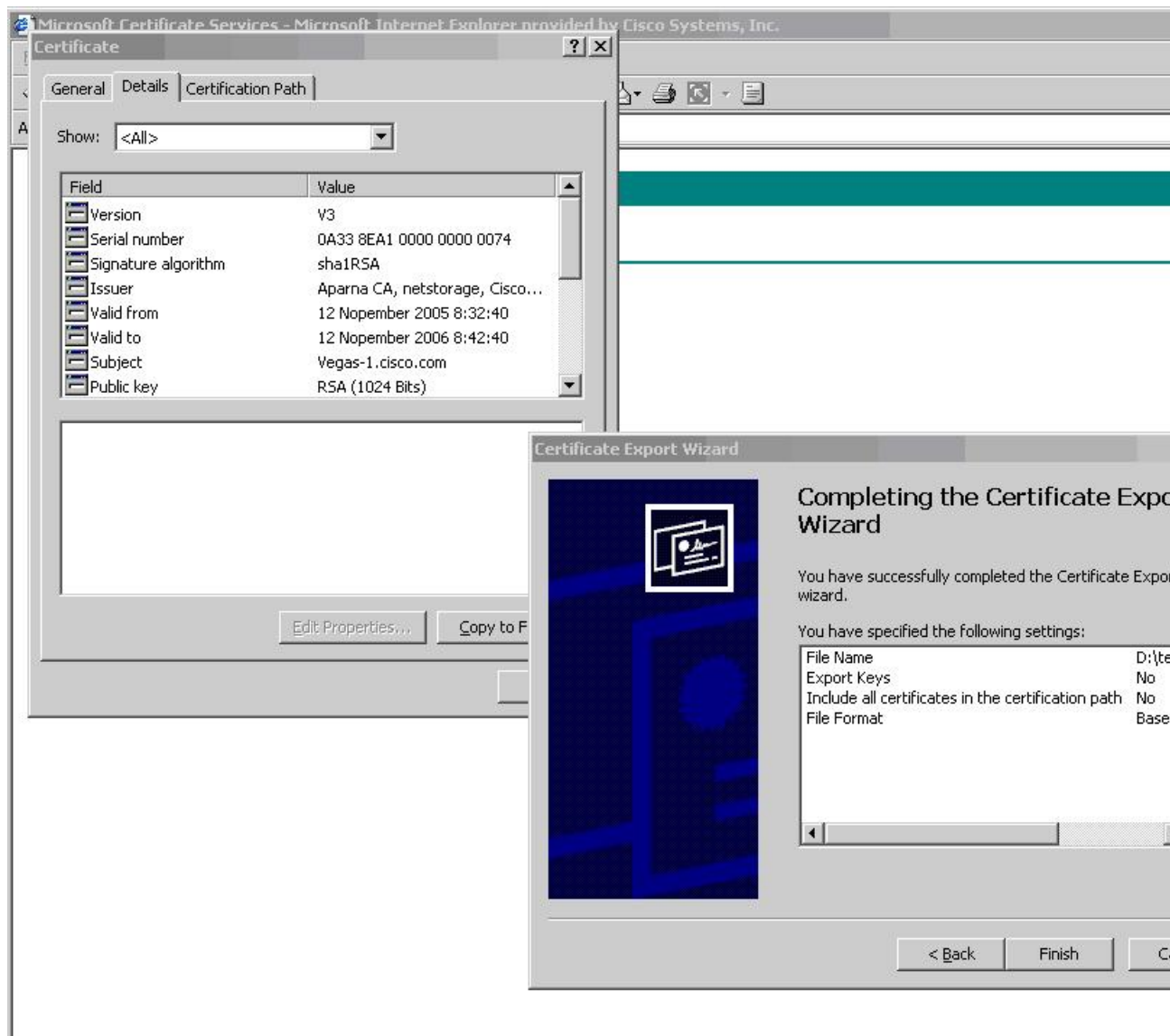
リックします。



ステップ 12 [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 13 [Finish] をクリックします。



ステップ 14 Microsoft Windows の type コマンドを入力して、アイデンティティ証明書を Base-64 でエンコードされた形式で表示します。

```

C:\WINNT\system32\cmd.exe
D:\testcerts>type myID.cer
-----BEGIN CERTIFICATE-----
MIIEADCA6ggAwwIBAgIKCjOoQAAAAAAAAADANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmrRZUBjaXNjb3Y5b20xCzAJBgNVBAYTAk1OMRIwEAYD
UQQIEwllYXJlYXRha2ExEjAQBgNVBAcTCUJhbmRhbG9yZTEOMAwGA1UEChMPQ21z
Y28xEzARBgNVBAstCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJlYXNDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNTExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEUZZZ2FzLTUu
Y21zY28uY29tMIIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNUACdJQu41C
dQ1WkJKjsICdPlfK5eJSmNCQujGpzcukS2PPXjF2UoiyeCYE8y1ncW9w5E08rJ47
g1xr42/sI9IRIh/8udu/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdU06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDUR0RAQH/BBsw
GYIRUmunYXNtMS5jaXNjb3Y5b20HBKwWH6IwHQYDUR0BBYEFKCLi+2sspWEfgrR
bhWm1Uyo9jngMIHMBgNUHSMGgcQwgcGAFCCo8kaDG6wjTEUNjskYUBoLFmxxoYGW
pIGTMIQMSAwHgYJKoZlIhucNAQkBFhFhbWVuZGt1QGnyc2NvLmNubTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFyYTESMBAQA1UEBxMJQmFuZ2Fs3J1Mq4w
DAYDUQkEwUDaXNjb3Y5b20HBGGA1UECXMkbnU0c3RvcnFnZTESMBAQA1UEAxMjQkX
cm5h1ENBghAFYnKJrLQZLE9JEiWMrR16MGsGA1UdHwRkMG1wLGAsoCqGKgh0dHA6
Ly9zc2UtdG9vQ2UyYdEUCm9sbc9BcGFybmE1MjB0S5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxZxJ0RW5yb2xsXEFwYXJlYXUyMENBLmNybDcBbigYIKwYBBQUH
AQEEFjb8MDsGCCsGAQUFBzACHi9odHRwOi8vc3NLLTA4L0N1cnRFbnJubGwvc3N1
LTA4X0FwYXJlYXUyMENBLmNydDA9BggrBgEFBQcwA0YXZm1sZTovL1xc3N1LTA4
XEN1cnRFbnJubGwvc3N1LTA4X0FwYXJlYXUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBA DbGCSbe7GNLh9xeOTWBNbm24U69ZS uDDcOcUZUUTgrpnTqUpPyejtsyflw
E36cIzu4WsExREqxhtk8ycx7U5o=
-----END CERTIFICATE-----

D:\testcerts>

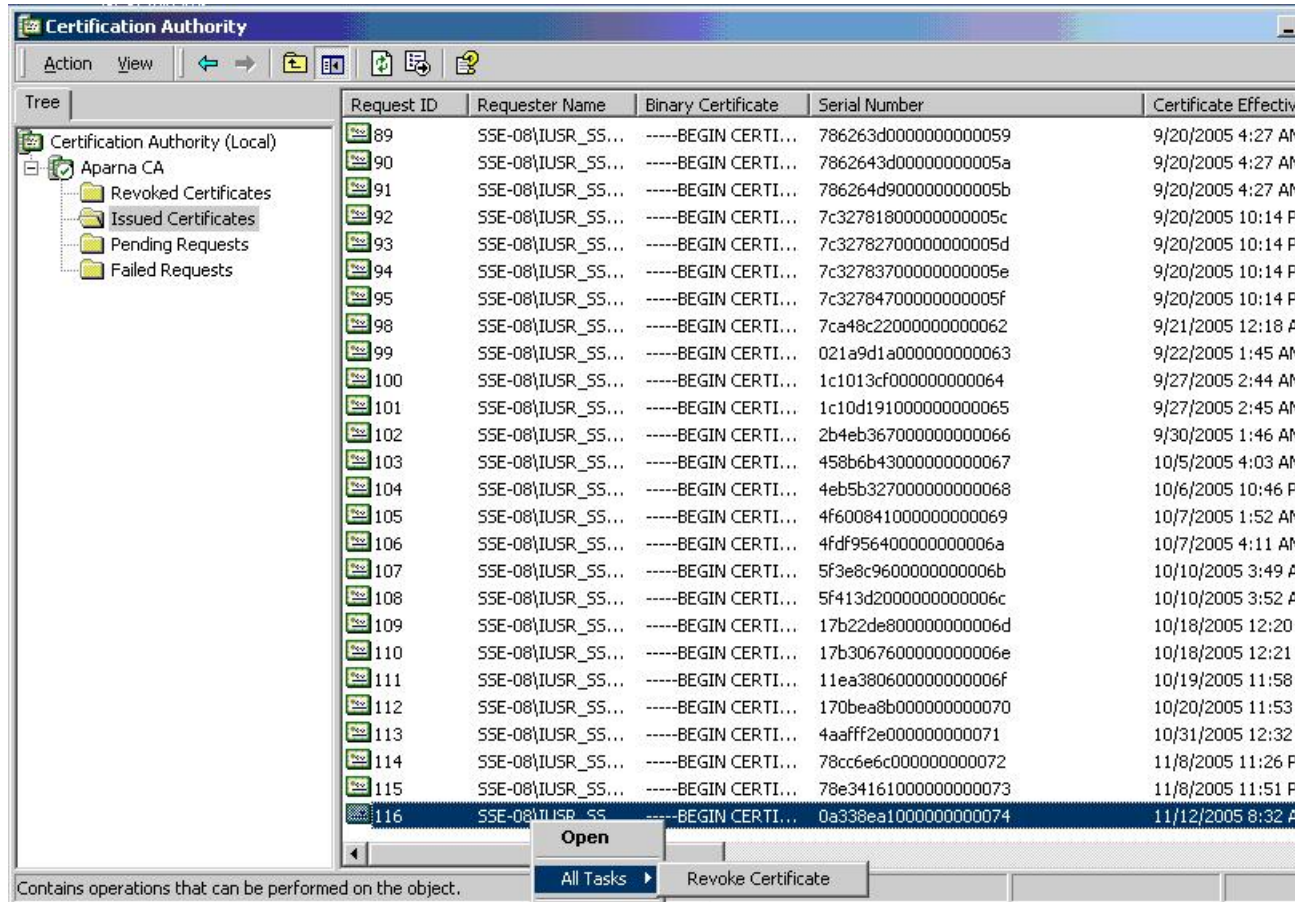
```

証明書の取り消し

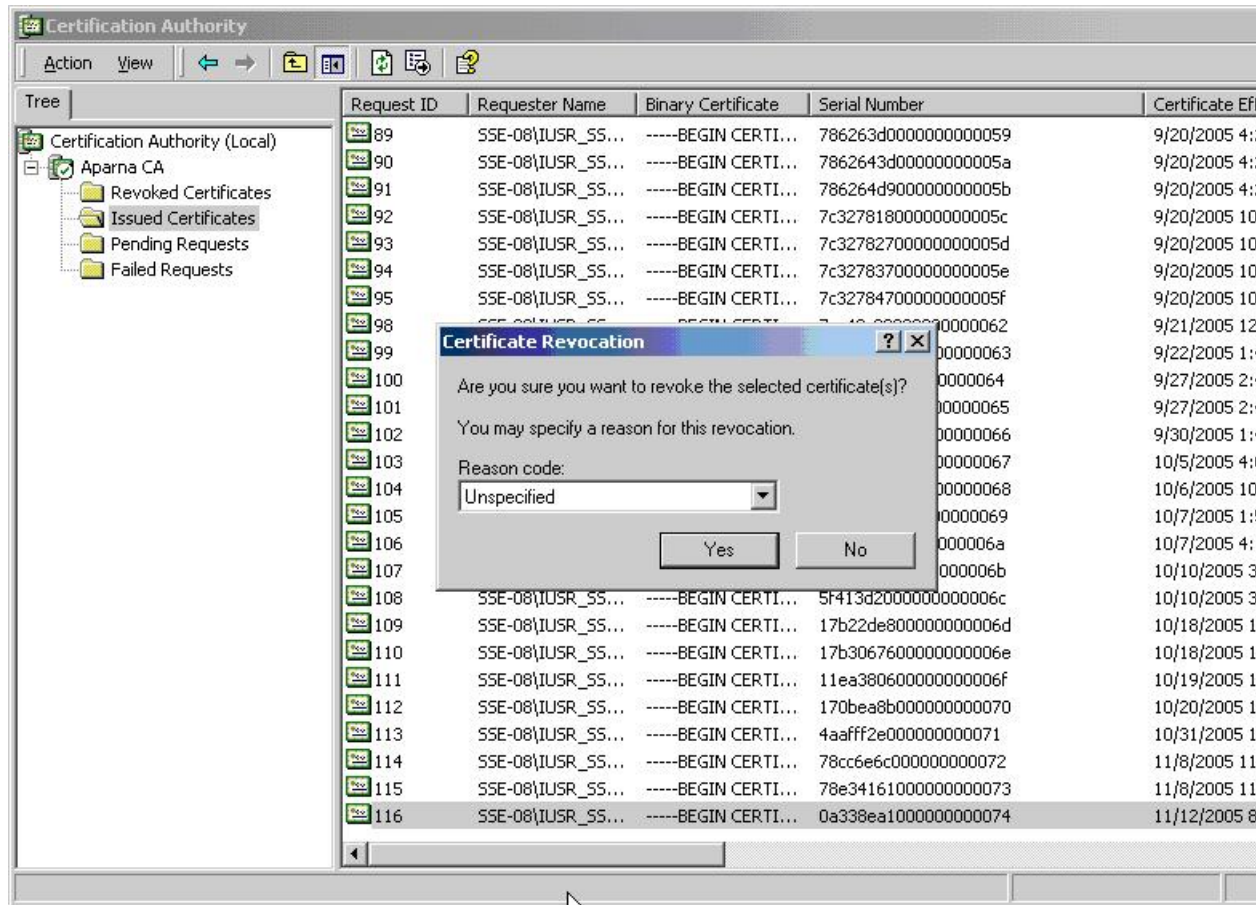
Microsoft CA 管理者プログラムを使用して証明書を取り消す手順は、次のとおりです。

手順

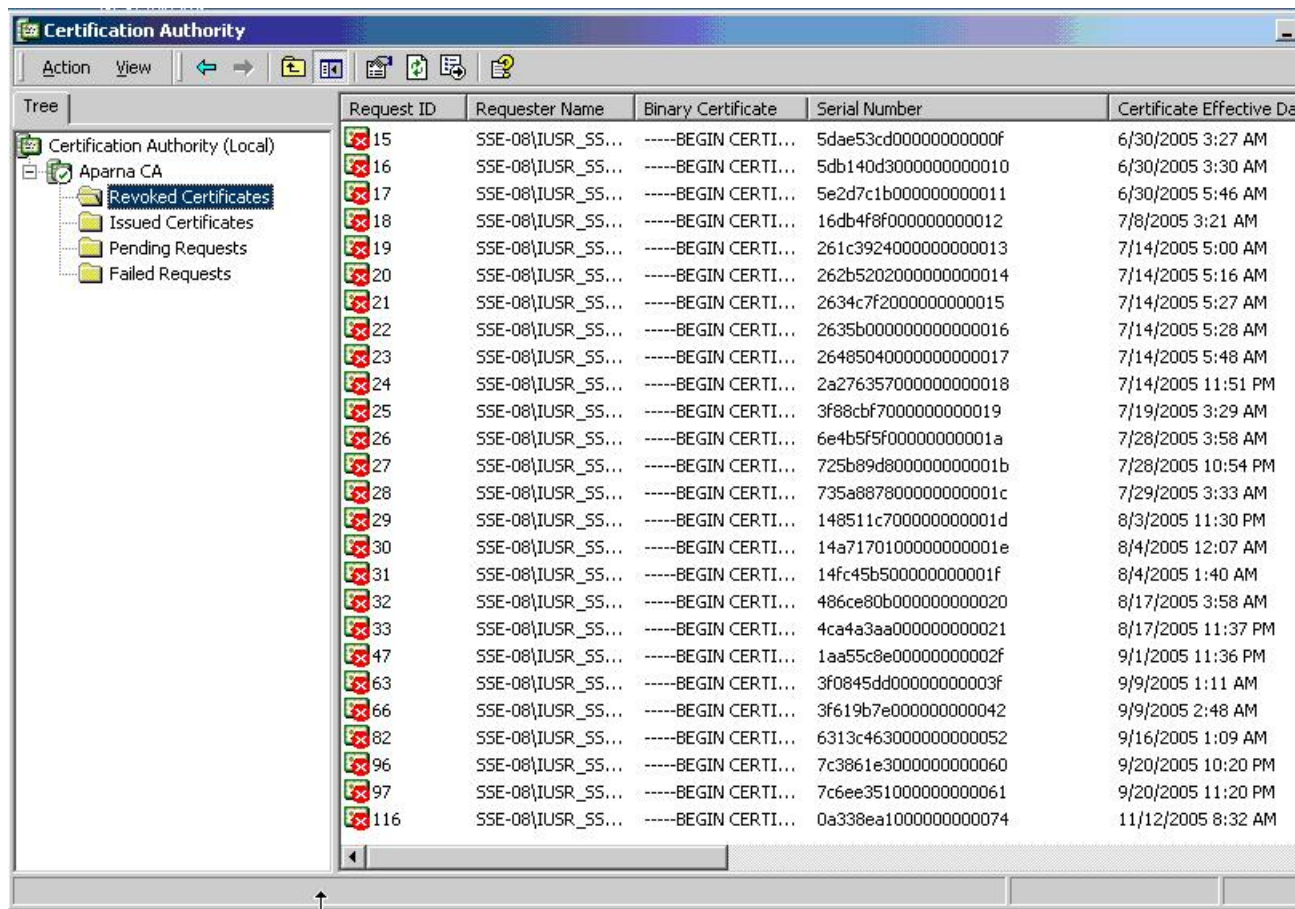
- ステップ 1** [Certification Authority] ツリーから、[Issued Certificates] フォルダをクリックします。リストから、取り消す証明書を右クリックします。
- ステップ 2** [All Tasks] > [Revoke Certificate] の順に選択します。



- 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。

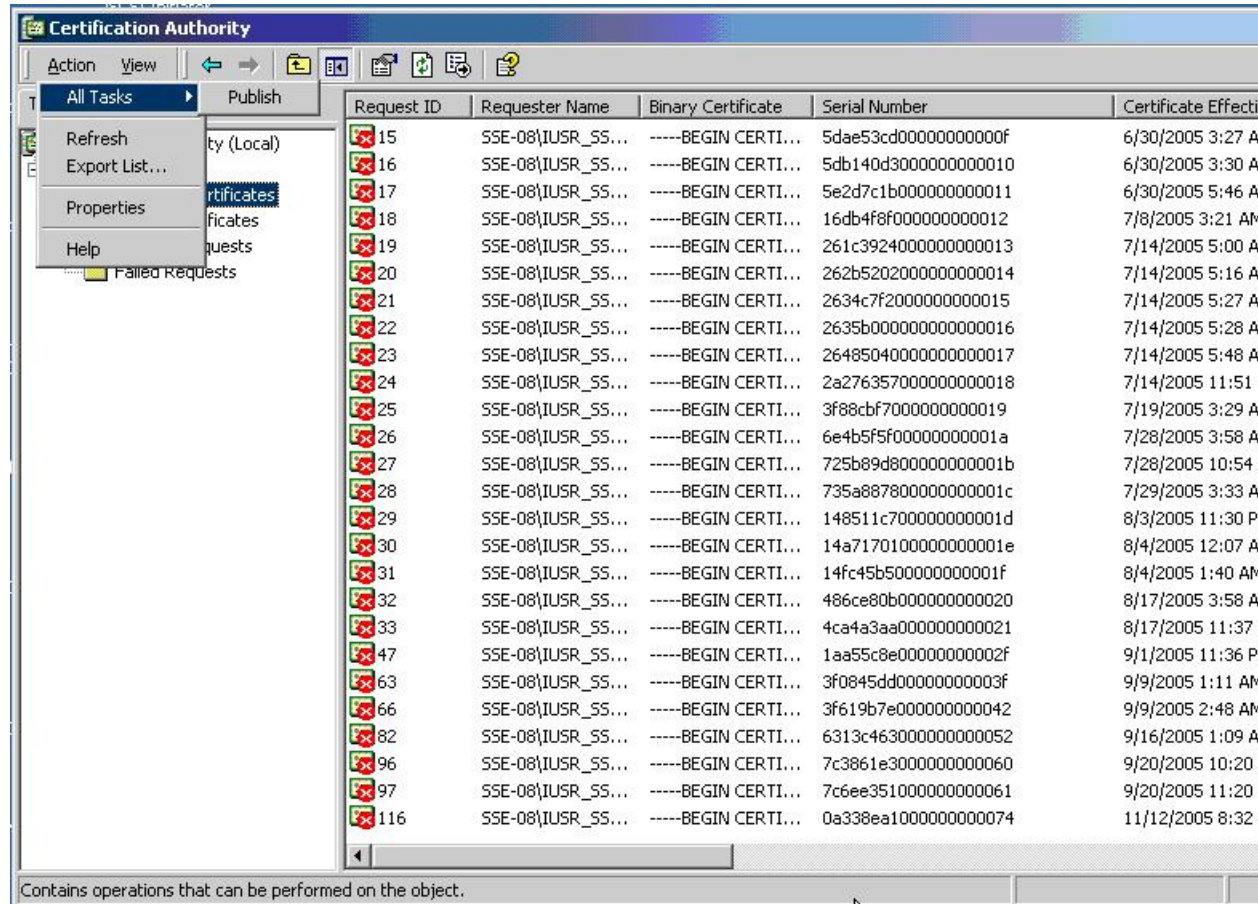


CRL の作成と公開

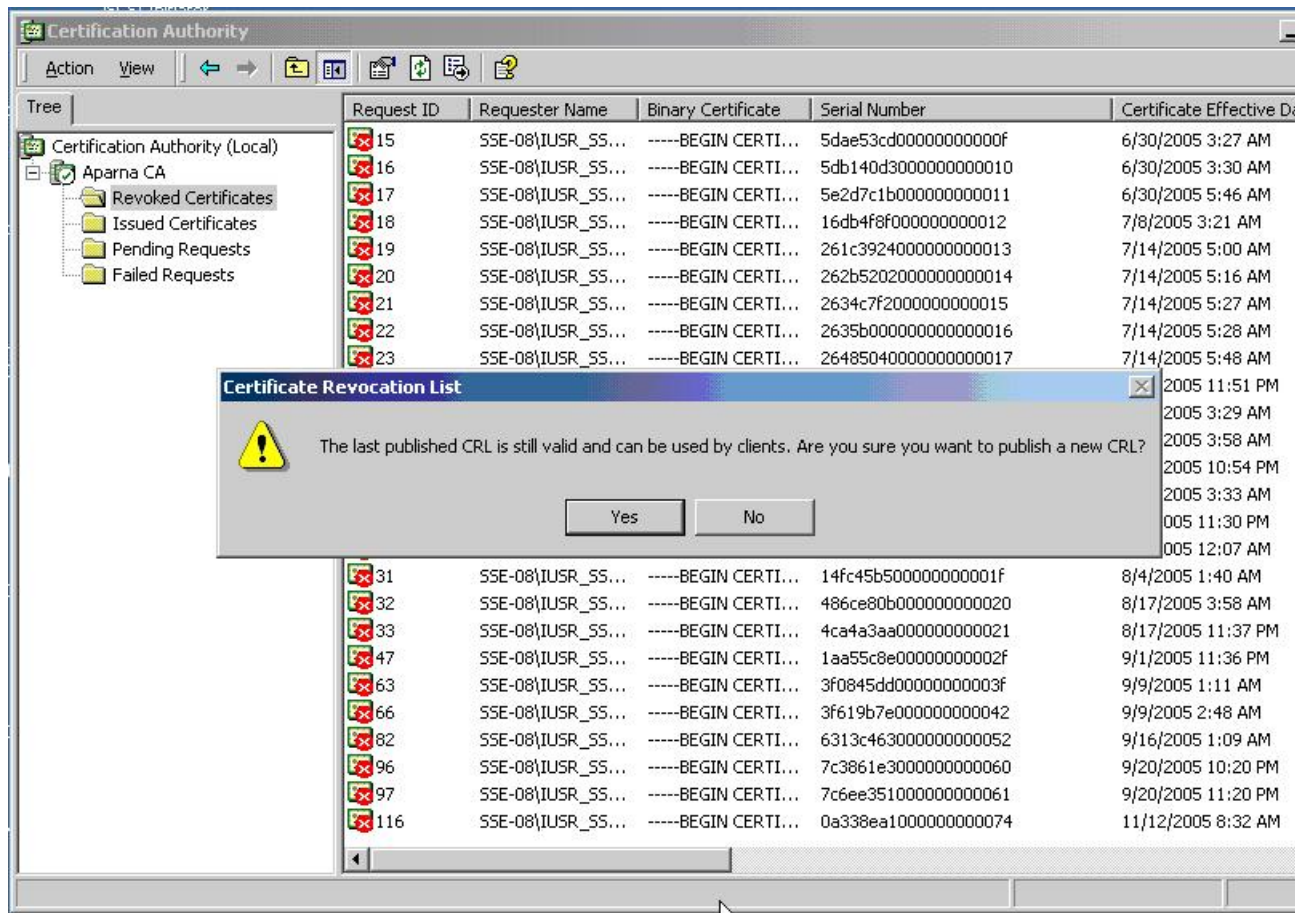
Microsoft CA 管理者プログラムを使用して CRL を作成および公開する手順は、次のとおりです。

手順

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。

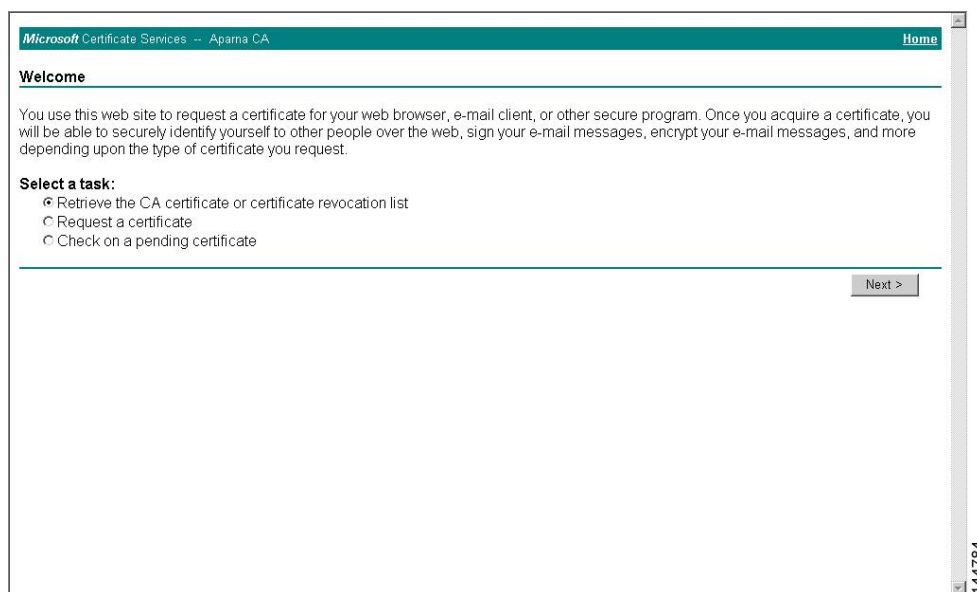


CRL のダウンロード

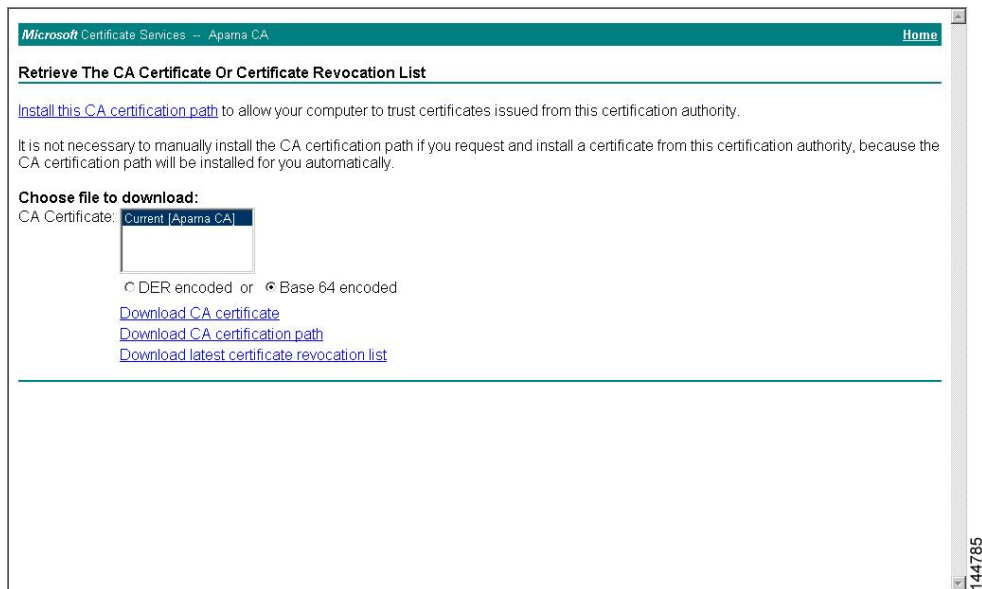
Microsoft 社の CA の Web サイトから CRL をダウンロードする手順は、次のとおりです。

手順

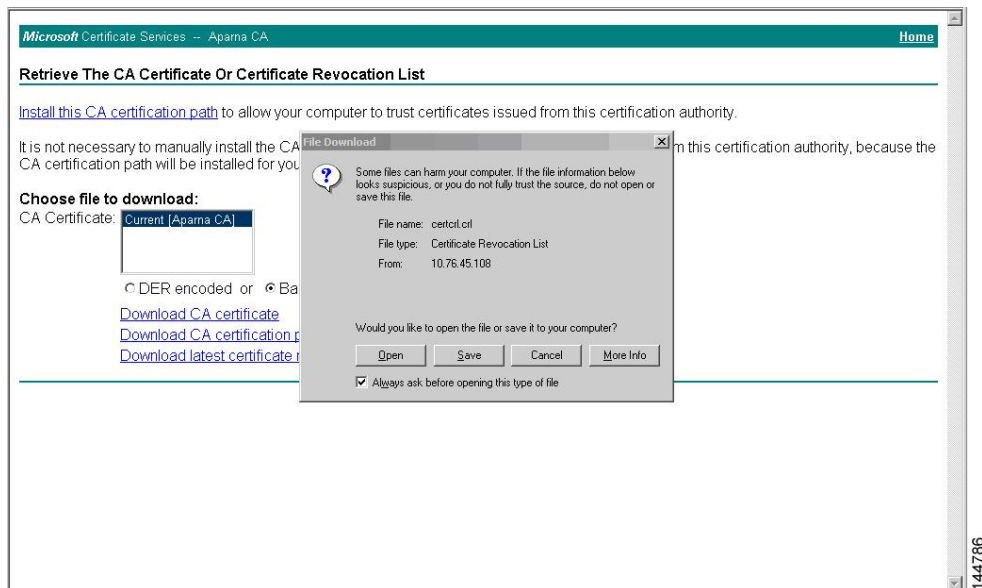
- ステップ 1** Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation list] をクリックし、[Next] をクリックします。



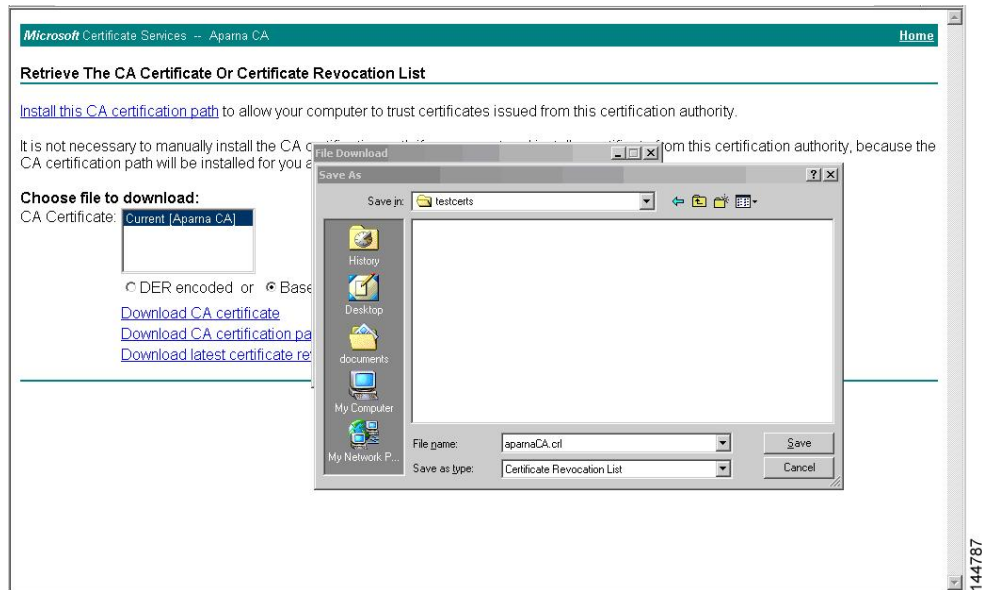
ステップ 2 [Download latest certificate revocation list] をクリックします。



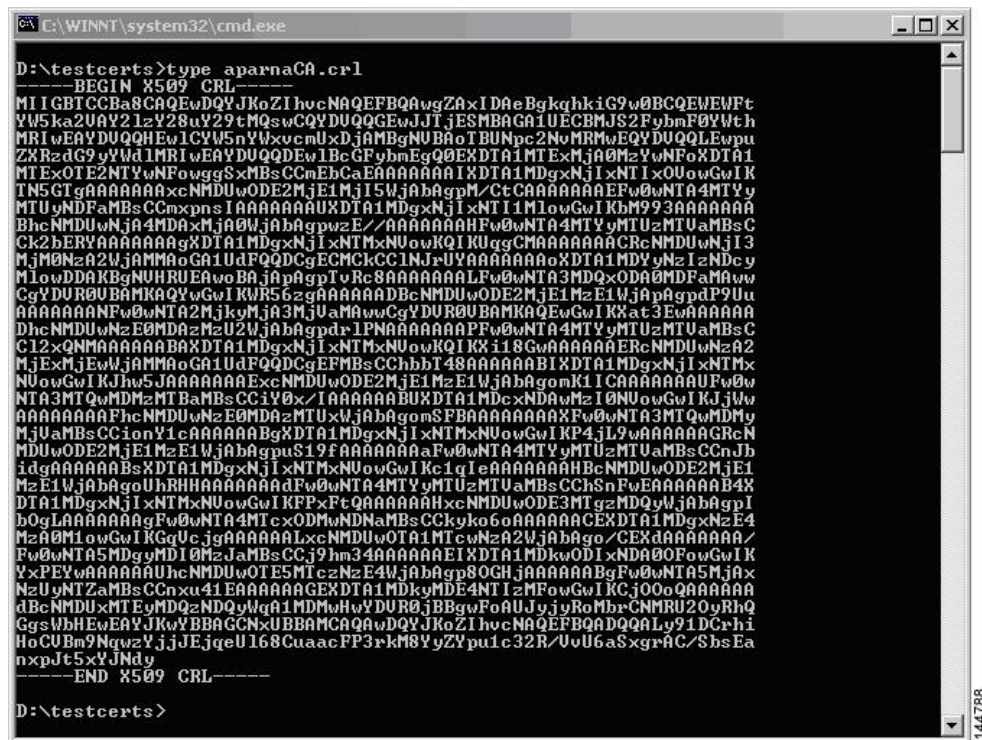
ステップ 3 [File Download] ダイアログボックスで、[Save] をクリックします。



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。



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。

手順

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: 611B09A1000000000002
    Revocation Date: Aug 16 21:52:19 2005 GMT
  Serial Number: 4CDE464E000000000003
    Revocation Date: Aug 16 21:52:29 2005 GMT
  Serial Number: 4CFC2B42000000000004
    Revocation Date: Aug 16 21:52:41 2005 GMT
  Serial Number: 6C699EC2000000000005
    Revocation Date: Aug 16 21:52:52 2005 GMT
  Serial Number: 6CCF7DDC000000000006
    Revocation Date: Jun 8 00:12:04 2005 GMT
  Serial Number: 70CC4FFF000000000007
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 4D9B1116000000000008
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 52A80230000000000009
    Revocation Date: Jun 27 23:47:06 2005 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      CA Compromise
  Serial Number: 5349AD4600000000000A
    Revocation Date: Jun 27 23:47:22 2005 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
```



```
CA Compromise
Serial Number: 53BD173C000000000000B
  Revocation Date: Jul  4 18:04:01 2005 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      Certificate Hold
Serial Number: 591E7ACE000000000000C
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 5D3FD52E000000000000D
  Revocation Date: Jun 29 22:07:25 2005 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      Key Compromise
Serial Number: 5DAB7713000000000000E
  Revocation Date: Jul 14 00:33:56 2005 GMT
Serial Number: 5DAE53CD000000000000F
  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: 1AA55C8E00000000002F
Revocation Date: Sep  5 17:07:06 2005 GMT
Serial Number: 3F0845DD00000000003F
Revocation Date: Sep  8 20:24:32 2005 GMT
Serial Number: 3F619B7E000000000042
Revocation Date: Sep  8 21:40:48 2005 GMT
Serial Number: 6313C463000000000052
Revocation Date: Sep 19 17:37:18 2005 GMT
Serial Number: 7C3861E3000000000060
Revocation Date: Sep 20 17:52:56 2005 GMT
Serial Number: 7C6EE351000000000061
Revocation Date: Sep 20 18:52:30 2005 GMT
Serial Number: 0A338EA1000000000074  <-- 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
```

(注) 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 0A338EA1000000000074) が最後に表示されています。



第 8 章

アクセスコントロールリストの設定

この章の内容は、次のとおりです。

- [ACL の概要, 135 ページ](#)
- [IP ACL の設定, 145 ページ](#)
- [ACL ロギングの設定, 154 ページ](#)
- [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, 157 ページ](#)
- [VLAN ACL の概要, 159 ページ](#)
- [VACL の設定, 160 ページ](#)
- [VACL の設定例, 163 ページ](#)
- [LOU しきい値の設定, 163 ページ](#)
- [ACL TCAM リージョンサイズの設定, 164 ページ](#)
- [仮想端末回線の ACL の設定, 167 ページ](#)

ACL の概要

アクセスコントロールリスト (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。スイッチは、あるパケットに対してある ACL を適用するかどうかを判断するとき、そのパケットを ACL 内のすべてのルールの条件に対してテストします。一致する条件が最初に見つかった時点で、パケットを許可するか拒否するかが決まります。一致する条件が見つからないと、スイッチは適用可能なデフォルトのルールを適用します。許可されたパケットについては処理が続き、拒否されたパケットはドロップされます。

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ハイパーテキストトランスファプロトコル (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。

IP ACL のタイプと適用

Cisco Nexus デバイスは、セキュリティトラフィックフィルタリング用に、IPv4 をサポートしています。スイッチでは、次の表に示すように、ポートの ACL、VLAN ACL、およびルータの ACL として、IP アクセスコントロールリスト (ACL) を使用できます。

表 10: セキュリティ ACL の適用

アプリケーション	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	<p>ACL は、次のいずれかに適用した場合、ポート ACL と見なされます。</p> <ul style="list-style-type: none"> イーサネット インターフェイス イーサネットポートチャネルインターフェイス <p>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。</p>	<p>IPv4 ACL</p> <p>IPv6 ACL</p>
ルータ ACL	<ul style="list-style-type: none"> VLAN インターフェイス (注) 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。 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ネルインターフェイス レイヤ 3 イーサネットポートチャネルサブインターフェイス トンネル 管理インターフェイス 	<p>IPv4 ACL</p> <p>IPv6 ACL</p>

アプリケーション	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
VLAN ACL (VACL)	アクセス マップを使用して ACL をアクションにアソシエートし、そのアクセス マップを VLAN に適用する場合、その ACL は VACL と見なされます。	IPv4 ACL
VTY ACL	VTY	IPv4 ACL IPv6 ACL

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 出力ルータ ACL
- 5 出力 VACL

ルール

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。スイッチは、許可ルールに指定された基準に一致するトラフィックを許可し、拒否ルールに指定された基準に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。

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。

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 ACL では、ICMP を名前で指定できます。

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。

暗黙のルール

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スイッチがトラフィックに適用するルールです。

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
```

この暗黙のルールによって、どの条件にも一致しない IP トラフィックは拒否されます。

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
```

```
permit icmp any any nd-na
permit icmp any any nd-ns
permit icmp any any router-advertisement
permit icmp any any router-solicitation
```

ICMPv6 のネイバー探索メッセージを拒否するルールを持つ IPv6 ACL を設定した場合を除き、最初の 4 つのルールによって、デバイスはネイバー探索アドバタイズメントメッセージと請求メッセージを許可するようになります。5 つめのルールにより、デバイスは不一致の IPv6 トラフィックを拒否します。



(注) IPv6 の ACL に **deny ipv6 any any** というルールを明示的に設定すると、暗黙の permit ルールでトラフィックをまったく許可できなくなります。**deny ipv6 any any** というルールを明示的に設定するものの、ICMPv6 ネイバー探索メッセージは許可したい場合は、5 つの暗黙のルールをすべて明示的に設定します。

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。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

シーケンス番号

Cisco Nexus デバイスはルールのシーケンス番号をサポートします。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規のルールを追加する：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。
- ルールを削除する：シーケンス番号を使用しない場合は、ルールを削除するのに、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
```
- ルールを移動する：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、デバイスでは、ACL 内ルールのシーケンス番号を再割り当てすることができます。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、それらのルールの上に 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 Nexus デバイスは、演算子とオペランドの組み合わせを論理演算ユニット (LOU) というレジスタ内に格納し、IP ACL で指定された TCP および UDP ポート上で演算 (より大きい、より小さい、等しくない、包含範囲) を行います。



(注) range 演算子は境界値も含みます。

これらの LOU は、これらの演算を行うために必要な Ternary Content Addressable Memory (TCAM) エントリ数を最小限に抑えます。最大で2つの LOU を、インターフェイスの各機能で使用できます。たとえば入力 RACL で2つの LOU を使用し、QoS 機能で2つの LOU を使用できます。ACL 機能で2つより多くの算術演算が必要な場合、最初の2つの演算が LOU を使用し、残りのアクセスコントロールエントリ (ACE) は展開されます。

デバイスが演算子とオペランドの組み合わせを LOU に格納するかどうかの判断基準を次に示します。

- 演算子またはオペランドが、他のルールで使用されている演算子とオペランドの組み合わせと異なる場合、この組み合わせは LOU に格納されません。

たとえば、演算子とオペランドの組み合わせ「gt 10」と「gt 11」は、別々に LOU の半分に格納されます。「gt 10」と「lt 10」も別々に格納されます。

- 演算子とオペランドの組み合わせがルール内の送信元ポートと宛先ポートのうちどちらに適用されるかは、LOU の使用方法に影響を与えます。同じ組み合わせの一方が送信元ポートに、他方が宛先ポートに別々に適用される場合は、2つの同じ組み合わせが別々に格納されます。

たとえば、あるルールによって、演算子とオペランドの組み合わせ「gt 10」が送信元ポートに、別のルールによって同じ組み合わせ「gt 10」が宛先ポートに適用される場合、両方の組み合わせが LOU の半分に格納され、結果として1つの LOU 全体が使用されることとなります。このため、「gt 10」を使用するルールが追加されても、これ以上 LOU は使用されません。

Cisco NX-OS Release 6.0(2)U5(1) では、**hardware profile tcam lou-thresholdvalue** コマンドを使用することにより、LOU しきい値を設定できます。展開された ACE の数がこのしきい値を超えると、デバイスはそれらを LOU レジスタに保存しません。それ以外の場合は、これらの ACE が TCAM エントリとして保存されます。



(注) TCAM または 24 の LOU レジスタがいっぱいになると、展開された ACE は保存されません。

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。

IPv4 TCAM はシングル幅です。一方、IPv6 TCAM はダブル幅です。たとえば、256 エントリの IPv6 TCAM を作成するには、IPv4 TCAM を 256 X 2、または 512 エントリに減らす必要があります。

IPv6 ポート ACL、VLAN ACL、ルータ ACL を作成して、QoS の IPv6 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。これらの新しい IPv6 TCAM をイネーブルにするには、既存の TCAM を削除するか、サイズを減らす必要があります。

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。

- デフォルトの ACL TCAM サイズに戻すには、**no hardware profile tcam region** コマンドを使用します。**write erase** コマンドを使用してからスイッチをリロードする必要はなくなりました。
- プラットフォームによっては、各 TCAM リージョンが異なる最小/最大/集約サイズ制限を持つ可能性があります。
- ARPACL TCAM のデフォルトサイズはゼロです。コントロールプレーンポリシング (CoPP) ポリシーで ARP ACL を使用する前に、この TCAM のサイズをゼロ以外のサイズに設定する必要があります。
- また、VACL および出力 VLAN ACL (E-VACL) を同じ値に設定する必要があります。
- IPv4 と IPv6 の両方のアドレスは、ダブル幅の TCAM 内であっても共存できません。
- 全体の TCAM の深さは、入力の場合は 2000、出力の場合は 1000 です。これは、256 のエントリ ブロックに切り分けることができます。
- TCAM の切り分け後には、スイッチをリロードする必要があります。
- すべての既存の TCAM のサイズを 0 に設定することはできません。
- デフォルトでは、すべての IPv6 TCAM はディセーブルです (TCAM サイズは 0 に設定されます)。

表 11: ACL リージョンによる TCAM サイズ

TCAM ACL リージョン	デフォルトサイズ	最小サイズ	インクリメンタルサイズ	最大サイズ
SUP (入力)	128 X 2	128 X 2	該当なし	128 X 2
SPAN (入力)	128	128	該当なし	128
ARPACL (入力)	0	0	128	128

TCAM ACL リージョン	デフォルトサイズ	最小サイズ	インクリメンタルサイズ	最大サイズ
PACL (入力)	384	ARPAcl (ディセーブル) = 128 ARPAcl (イネーブル) = 256	256	1664 (連結)
VACL (入力)	512	0	256	
RACL (入力)	512	256	256	
QOS (入力)	256	256	256	
PACL_IPV6 (入力)	0	0	256 X 2	
VACL_IPV6 (入力)	0	0	256 X 2	
RACL_IPV6 (入力)	0	0	256 X 2	
QOS_IPV6 (入力)	0	0	256 X 2	
E-VACL (出力)	512	0	256	1024 (連結)
E-RACL (出力)	512	0	256	
E-VACL_IPV6 (出力)	0	0	256 X 2	
E-RACL_IPV6 (出力)	0	0	256 X 2	
QOSLBL (前ルックアップ)	256	256	256	256
SUP_IPV6 (前ルックアップ)	128 X 2	256 X 2	該当なし	256 X 2

ACL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	ACLを使用するためにライセンスは必要ありません。

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。

VACLの前提条件は次のとおりです。

- VACLに使用するIP 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。

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。

- Release 7.0(3)I2(1)以降、送信元MACまたはDMACによってACEを作成できません。送信元MACおよびDMACオプションはオープンフローに固有です。7.0(3)I2(1)よりも前のリリースでは、オープンフローとタップアグリゲーションの両方がACLMGRプロセスによって処理されるために、これらのオプションがサポートされていました。7.0(3)I2(1)以降では、オープンフローはPOLICY_MGRプロセスによって処理され、タップアグリゲーションはACLMGRプロセスによって処理されます。この機能拡張のために、オープンフロー固有のオプションは、タップアグリゲーションに関して使用できません。タップアグリゲーションに関してこれらのオプションをサポートするための要件は存在しません。
- タップアグリゲーションポリシーではset-vlanオプションを設定できません。The set-vlanおよびstrip-vlanオプションはオープンフローに固有です。Release 7.0(3)I2(1)では、オープンフローとタップアグリゲーションは2つの異なるプロセスによって処理されます。このために、オープンフロー固有のオプションは、タップアグリゲーションに関して使用できません。
- HTTPメソッドとの一致に関する機能拡張として、パケットでTCPオプションのヘッダーの長さを指定するために、ACEシンタックスにtcp-option-lengthオプションが追加されました。ACEで最大4つのtcp-option-length (0のTCPオプション長を含む)を設定できます。

tcp-option-length オプションを設定しない場合、TCP オプション長は0と見なされます。これは、TCP オプションヘッダーのないパケットだけがこのACEと一致することを意味します。この機能により、HTTP メソッドが、可変長 TCP オプションヘッダーを持つパケットとも一致可能になるため、柔軟性が向上します。

- 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。
- 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。
- 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（追加された 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）
- 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。
- すべての着信および発信トラフィックに **match-local-traffic** オプションを使用するには、まずソフトウェアで ACL をイネーブルにする必要があります。

VACL には、次の設定があります。

- 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ます。
- DHCP スヌーピング機能がイネーブルのときには、ACL の統計情報はサポートされません。
- VLAN ACL として適用される IPv4 ACL に、TCP/UDP ポート番号の論理演算子を使用する 1 つまたは複数の ACE が含まれている場合、ポート番号は入力方向で一致しますが、出力方向では無視されます。
- 1 つの VLAN アクセス マップでは、1 つの IP ACL だけを照合できます。
- 1 つの IP ACL に、複数の許可/拒否 ACE を設定することができます。
- 1 つの VLAN に適用できるアクセス マップは 1 つだけです。

L3 ポート チャネルでは出力 RAACL を設定できません。

デフォルトの ACL 設定

次の表は、IP ACL パラメータのデフォルト設定をリスト表示しています。

表 12: IP ACL のデフォルトパラメータ

パラメータ	デフォルト
IP ACL	デフォルトの 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。

次の表に、VACL パラメータのデフォルト設定を示します。

表 13: VACL のデフォルトパラメータ

パラメータ	デフォルト
VACL	デフォルトの 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。

ACL ロギング

Cisco Nexus デバイスでは ACL ロギングがサポートされます。これを使用すると、特定のアクセスコントロールリスト (ACL) にヒットするフローをモニタできます。ACL エントリに関してこの機能をイネーブルにするには、オプションの **log** キーワードを使って特定の ACE を設定します。

オプションの **log** キーワードを使って ACE を設定すると、ACE エントリの許可条件または拒否条件と一致する各フローの統計情報がソフトウェアのログに記録されます。

IP ACL の設定

IP ACL の作成

スイッチに IPv4 または IPv6 の ACL を作成し、それにルールを追加することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# ipaccess-listname	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	switch(config-acl)# [<i>sequence-number</i>] { permit deny } <i>protocolsourcedestination</i>	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。 <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。詳細については、特定の Cisco Nexus デバイスの『 <i>Command Reference</i> 』を参照してください。
ステップ 4	switch(config-acl)# statistics	(任意) ACL のルールと一致するパケットのグローバル統計をスイッチが維持するように設定します。
ステップ 5	switch# show {ip ipv6} access-listsname	(任意) IP ACL の設定を表示します。
ステップ 6	switch# copy running-config startup-config	(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。

次に、IPv4 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics
```

次に、IPv6 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list acl-01-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
```

IP ACL の変更

既存の IPv4 または IPv6 ACL のルールを追加および削除できます。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。

手順

	コマンドまたはアクション	目的
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)# { ip ipv6 } access-listname	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	switch(config)# ip access-listname	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 4	switch(config-acl)# [<i>sequence-number</i>] { permit deny } <i>protocolsourcedestination</i>	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。詳細については、Cisco Nexus デバイスの『 <i>Command Reference</i> 』を参照してください。
ステップ 5	switch(config-acl)# no { <i>sequence-number</i> { permit deny } <i>protocolsourcedestination</i> }	(任意) 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。詳細については、Cisco Nexus デバイスの『 <i>Command Reference</i> 』を参照してください。
ステップ 6	switch(config-acl)# [no] statistics	(任意) ACL のルールと一致するパケットのグローバル統計をスイッチが維持するように設定します。 no オプションを指定すると、ACL のグローバルな統計情報がスイッチ内に維持されなくなります。
ステップ 7	switch# show ip access-listsname	(任意) IP ACL の設定を表示します。
ステップ 8	switch# copy running-config startup-config	(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。

IP ACL の削除

スイッチから IP ACL を削除できます。

スイッチから IP ACL を削除する前に、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てください。削除できるのは、現在適用されている ACL だけです。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。スイッチは、削除対象の ACL が空であると見なします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル 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 ipv6} access-listname	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	switch(config)# no ip access-listname	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 4	switch# show running-config	(任意) ACL の設定を表示します。削除された IP ACL は表示されないはずで。
ステップ 5	switch# copy running-config startup-config	(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。

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。

手順

	コマンドまたはアクション	目的
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。

	コマンドまたはアクション	目的
ステップ 2	<code>switch(config)# resequenceip access-listname starting-sequence-number increment</code>	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	<code>switch# show {ip ipv6} access-listsname</code>	(任意) IP ACL の設定を表示します。
ステップ 4	<code>switch# copy running-config startup-config</code>	(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。

mgmt0 への IP-ACL の適用

管理インターフェイス (mgmt0) に IPv4 ACL または IPv6 ACL を適用できます。

はじめる前に

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。

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	interfacemgmtport 例： <code>switch(config)# interface mgmt0</code> <code>switch(config-if)#</code>	管理インターフェイスのコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	ip access-group <i>access-list</i> {in out} 例： switch(config-if)#ip access-group acl-120 out	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 4	show running-config aclmgr 例： switch(config-if)# show running-config aclmgr	(任意) ACL の設定を表示します。
ステップ 5	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(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。

関連項目

- IP ACL の作成

ポート ACL としての IP ACL の適用

IPv4 ACL は、物理イーサネットインターフェイスまたはポートチャン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。



(注) 一部の設定パラメータは、ポートチャンネルに適用されていると、メンバポートの設定に反映されません。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# interface { ethernet [<i>chassis</i>]/ <i>slot</i> / <i>port</i> port-channel <i>channel-number</i> }	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	switch(config-if)# ip port access-group <i>access-list</i> in	IPv4 ACL を、インターフェイスまたはポートチャンネルに適用します。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

	コマンドまたはアクション	目的
		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	switch# show running-config	(任意) ACL の設定を表示します。
ステップ 5	switch# copy running-config startup-config	(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。

ルータ ACL としての IP ACL の適用

IPv4 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 チャンネル インターフェイスおよびサブインターフェイス
- VLAN インターフェイス
- トンネル
- 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。



(注) 論理演算ユニット (LOU) は、Out 方向に適用されたルータ ACL には使用できません。IPv4 ACL が Out 方向のルータ ACL として適用される場合、TCP/UDP ポート番号の論理演算子を持つアクセスコントロールエントリ (ACE) は複数の ACE に内部的に拡張され、In 方向に適用された同じ ACL と比較すると、より多くの TCAM エントリが必要になることがあります。

はじめる前に

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。

手順

	コマンドまたはアクション	目的
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。

	コマンドまたはアクション	目的
ステップ 2	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> • switch(config)# interfaceethernetslot/port[.number] • switch(config)# interfaceport-channelchannel-number[.number] • switch(config)# interfacetunneltunnel-number • switch(config)# interfacevlanvlan-ID • switch(config)# interfacemgmtport 	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。 <ul style="list-style-type: none"> • switch(config-if)# ipaccess-group access-list {in out} • switch(config-if)# ipv6 traffic-filter access-list {in out} 	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 4	switch(config-if)# show running-config aclmgr	(任意) ACL の設定を表示します。
ステップ 5	switch(config-if)# copy running-config startup-config	(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。

IP ACL の設定の確認

IP 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。

コマンドまたはアクション	目的
switch# show running-config	ACL が適用されたインターフェイスの設定を表 示します。
switch# show running-config interface	ACL が適用されたインターフェイスの設定を表 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 Cisco Nexus デバイスのコマンド
リファレンスを参照してください。

IP ACL の統計情報のモニタリングとクリア

IP ACL に関する統計情報（各ルールに一致したパケットの数など）を表示するには、**show ip access-lists** または **show ipv6 access-list** コマンドを使用します。このコマンドの出力フィールドの詳細については、Cisco Nexus デバイスの『*Command Reference*』を参照してください。



(注) MAC アクセス リストは、非 IPv4 および非 IPv6 トラフィックだけに適用可能です。

- **switch# show {ip | ipv6} access-listsname**
IP ACL の設定を表示します。IP ACL に **statistics** コマンドが指定されている場合は、**show ip access-lists** および **show ipv6 access-list** コマンドの出力に、各ルールに一致したパケットの数が表示されます。
- **switch#show ip access-listsname**
IP ACL の設定を表示します。IP ACL に **statistics** コマンドが指定されている場合は、**show ip access-lists** コマンドの出力に、各ルールに一致したパケットの数が表示されます。
- **switch# clear {ip | ipv6} access-list counters [access-list-name]**
すべての IP ACL、または特定の IP ACL の統計情報を消去します。
- **switch# clear ip access-list counters [access-list-name]**
すべての IP ACL、または特定の IP ACL の統計情報を消去します。

RACL 整合性チェッカーのトリガー

手動で RACL 整合性チェッカーをトリガーして、モジュールの入力 RACL および出力 RACL のハードウェアとソフトウェアの設定を比較し、結果を表示することができます。手動で RACL 整合性チェッカーをトリガーして結果を表示するには、任意のモードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	show consistency-checker racl moduleslot	指定されたモジュールの RACL 整合性チェックを開始し、結果を表示します。

次に、RACL 整合性チェックをトリガーし、結果を表示する例を示します。

```
switch# show consistency-checker racl module 1
Validates RACL on up interfaces:
Consistency Check: FAILED

Found consistencies for following Interfaces:
Ethernet1/9 (in)
Ethernet1/9 (out)
Ethernet1/17 (in)
Ethernet1/17 (out)
```

```
Found inconsistencies for following Interfaces and EID:
Ethernet1/3 (in)
Ethernet1/3 (out)
```

ACL ロギングの設定

ACL ロギング キャッシュの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# 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)# logging ip access-list cache entriesnum_entries	ソフトウェア内にキャッシュする最大ログエントリ数を設定します。エントリ数の範囲は 0 ~ 1000000 です。デフォルト値は 8000 エントリです。
ステップ 3	switch(config)# logging ip access-list cache intervalseconds	ログの更新間隔を秒数で設定します。この期間にわたってエントリが非アクティブの場合、キャッシュから削除されます。指定できる範囲は 5 ~ 86400 秒です。デフォルト値は 300 秒です。
ステップ 4	switch(config)# logging ip access-list cache thresholdnum_packets	エントリがログに記録されるまでに一致するパケット数を設定します。範囲は 0 ~ 1000000 パケットです。デフォルト値は 0 パケットです。つまり、パケットの一致数によってロギングがトリガーされることはありません。
ステップ 5	switch(config)# copy running-config startup-config	(任意) 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。

次に、ログ エントリの最大数を 5000、間隔を 120 秒、およびしきい値を 500000 に設定する例を示します。

```
switch# configure terminal
switch(config)# logging ip access-list cache entries 5000
switch(config)# logging ip access-list cache interval 120
switch(config)# logging ip access-list cache threshold 500000
switch(config)# copy running-config startup-config
```

インターフェイスへの ACL ロギングの適用

ACL ロギングは、イーサネットインターフェイスおよびポートチャンネルに対して適用できます。

はじめる前に

- ACL を作成します。
- ロギング用に設定された少なくとも 1 つのアクセス コントロール エントリ (ACE) からなる IP アクセス リストを作成します。
- ACL ロギング キャッシュを設定します。
- ACL ログの一致レベルを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# interface ethernet slot/port	イーサネット インターフェイスを指定します。
ステップ 3	switch(config-if)# ip access-group name in	指定したインターフェイスに、ログとともに ACL をアタッチします。ACL ロギングは、ACL がハードウェア上のインターフェイスに適用されるとイネーブルになります。
ステップ 4	switch(config-if)# copy running-config startup-config	(任意) 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。

次に、すべての入力トラフィックに関して `acl1` で指定されたロギングにイーサネットインターフェイスを適用する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip access-group acl1 in
switch(config-if)# copy running-config startup-config
```

ACL ログの一致レベルの適用

手順

	コマンドまたはアクション	目的
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)# aclog match-log-levelnumber	ACL ログ (aclog) で記録されるエン트리と一致するようにログレベルを指定します。number は 0～7 までの値です。デフォルト値は 6 です。 (注) ACL ログ機能 (aclog) のログレベルとログファイルのログ重大度レベルが ACL ログ一致レベル設定以上である場合に、ログメッセージがログに記録されます。
ステップ 3	switch(config)# copy running-config startup-config	(任意) 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。

次に、ACL ログに記録されるエントリに関するログ一致レベルを適用する例を示します。

```
switch# configure terminal
switch(config)# aclog match-log-level 3
switch(config)# copy running-config startup-config
```

ログファイルのクリア

ログファイルおよび NVRAM 内のメッセージをクリアできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# clear logging ip access-list cache	アクセスコントロールリスト (ACL) キャッシュをクリアします。

ACL ロギング設定の確認

MAC ACL ロギング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
switch# show startup-config acllog	スタートアップコンフィギュレーション内のアクセスコントロールリスト (ACL) ログファイルを表示します。
switch# show running-config acllog	実行コンフィギュレーション内のアクセスコントロールリスト (ACL) ログファイルを表示します。
switch# show logging ip access-list cache	IP アクセスリスト キャッシュを表示します。
switch# show logging ip access-list cache detail	IP アクセスリスト キャッシュに関する詳細情報を表示します。
switch# show logging ip access-list status	IP アクセスリスト キャッシュのステータスを表示します。

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

Release 6.0(2)U5(1) 以降、HTTP メソッド オプションが ACL CLI に追加されています。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たサーバにリダイレクトできます。



(注) HTTP メソッドとの一致に関する機能拡張として、パケットで TCP オプションのヘッダーの長さを指定するために、ACE シンタックスに `tcp-option-length` オプションが追加されました。ACE で最大 4 つの `tcp-option-length` (0 の TCP オプション長を含む) を設定できます。 `tcp-option-length` オプションを設定しない場合、TCP オプション長は 0 と見なされます。これは、TCP オプションヘッダーのないパケットだけがこの ACE と一致することを意味します。この機能により、HTTP メソッドが、可変長 TCP オプションヘッダーを持つパケットとも一致可能になるため、柔軟性が向上します。

次の HTTP メソッドをリダイレクトできます。

- connect
- delete
- get
- head
- post
- put

- trace

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 CLI を設定します。

はじめる前に

- IP アクセス リストを作成します。
- CLI コマンドの **hardware profile tcam region ifacl 512 double-wide** を使用して、IFACL リージョンに関してダブル幅の 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、Trident2 ベースの Cisco Nexus 3000 シリーズ スイッチでのみ適用されます。この設定を有効にするには、スイッチをリロードします。
- CLI コマンドの **hardware profile tap-aggregation** を使用して、別のインターフェイスにパケットをリダイレクトするタップアグリゲーション機能を有効にします。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	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)# ipaccess-listname	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。name 引数は 64 文字以内で指定します。
ステップ 3	switch(config-acl)# permitprotocolsource any http-method ? 例： switch(config-acl)# permit tcp 1.1.1.1/32 any http-method ? connect Match http packets with CONNECT method [0x434f4e4e] delete Match http packets with DELETE method [0x44454c45] get Match http packets with GET method [0x47455420] head Match http packets with HEAD method [0x48454144] post Match http packets with POST method [0x504f5354] put Match http packets with PUT method [0x50555420] trace Match http packets with TRACE method [0x54524143]	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 CLI を設定します。
ステップ 4	switch# showipaccess-listsname	(任意) IP ACL 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 5	switch# showruninterface <x/y>	(任意) インターフェイスの設定を表示します。

次の例では、イーサネットインターフェイス 1/33 が HTTP トラフィックを受信しています。イーサネットインターフェイス 1/34 は出力インターフェイスです。出力インターフェイスで **tap-aggregation** モードを有効にします。トラフィックと一致する ACL を作成します。イーサネットインターフェイス 1/34 への ACL に一致するリダイレクト HTTP get メソッドを設定します。HTTP トラフィックが受信されるポートに ACL を適用します。イーサネット 1/33 で ACL にヒットするすべての HTTP get トラフィックが、宛先インターフェイス（イーサネット 1/34 など）にリダイレクトされます。同じ手順を、上記の他のメソッドに使用できます。

トラブルシューティング情報—ACL にヒットしない場合やパケットがリダイレクトされない場合は、ダブル幅の TCAM が有効になっていることを確認します。タップアグリゲーションが有効になっていることを確認します。送信元ポートと宛先ポートの両方が同じ VLAN の STP フォワーディングステートになっていることを確認します。ACL が TCAM で **sh platform afm info attachment interface <interface>** コマンドを使用してプログラムされていることを確認します。HTTP リダイレクト機能は、レイヤ 3 ポートでは動作しません。



(注) Release 7.0(3)I2(1) 以降では、インターフェイスでの ACL ポリシーのチェックに CLI コマンドの **show hardware access-list interface <>** を使用します。

```
switch# configure terminal
switch(config)# interface Ethernet 1/33

L3-QI2-CR-one(config)# interface Ethernet 1/34
L3-QI2-CR-one(config-if)# mode tap-aggregation
switch(config)# ip access-list http-redirect-acl
switch(config-acl)# 10 permit tcp 10.1.1.1/32 10.2.2.2/32 http-method get redirect e1/34
switch(config-acl)# 10 permit tcp any any http-method get tcp-option-length 8 redirect e1/34
switch(config-acl)# 20 permit tcp any any http-method post redirect e1/34
switch(config-acl)# statistics per-entry

switch(config)# interface Ethernet 1/33
switch(config-if)# ip port access-group http-redirect-acl in

switch(config)# show ip access-lists
switch(config)# show run int 1/34
switch(config)# show hardware access-list interface 1/34
```

VLAN ACL の概要

VLAN ACL (VACL) は、IP ACL の適用例の 1 つです。VACL を設定して、VLAN 内でブリッジされてい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のフィルタリングだけに使用します。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。

VACL とアクセス マップ

VACL では、アクセス マップを使用して、IP ACL をアクションとリンクさせます。スイッチは、VACL で許可されているパケットに対して、設定済みのアクションを実行します。

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。

- フォワード：スイッチ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。
- ドロップ：トラフィックをドロップします。

統計情報

Cisco Nexus デバイスは、VACL 内の各ルールについて、グローバルな統計情報を保持できます。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) Cisco Nexus デバイスは、インターフェイス単位の VACL 統計情報はサポートしていません。

設定する各 VLAN アクセス マップごとに、VACL の統計情報をスイッチ内に保持するかどうかを指定できます。これにより、VACL によってフィルタリングされたトラフィックをモニタリングするため、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を行うために、VACL 統計情報の収集のオン/オフを必要に応じて切り替えることができます。

VACL の設定

VACL の作成または変更

VACL を作成または変更できます。VACL の作成には、IP ACL を、一致したトラフィックに適用するアクションとアソシエートさせるアクセス マップの作成が含まれます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル 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)# vlan access-map map-name	指定したアクセス マップのアクセス マップ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-access-map)# match addressip-access-list	マップの IPv4 および IPV6 ACL を指定します。
ステップ 4	switch(config-access-map)# action {drop forward}	スイッチが、ACL に一致したトラフィックに適用するアクションを指定します。
ステップ 5	switch(config-access-map)# [no] statistics	(任意) VACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。 no オプションを指定すると、VACL のグローバルな統計情報がスイッチ内に保持されなくなります。
ステップ 6	switch(config-access-map)# show running-config	(任意) ACL の設定を表示します。
ステップ 7	switch(config-access-map)# copy running-config startup-config	(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。

VACL 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。

VACL が VLAN に適用されているかどうかを確認してください。削除できるのは、現在適用されている VACL だけです。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。スイッチは、削除対象の VACL が空であると見なします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル 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 vlan access-map <i>map-name</i>	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。
ステップ 3	switch(config)# show running-config	(任意) ACL の設定を表示します。
ステップ 4	switch(config)# copy running-config startup-config	(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。

VACL の VLAN への適用

VACL を VLAN 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	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] vlan filter <i>map-name</i> vlan-list <i>list</i>	指定したリストによって、VACL を VLAN に適用します。 no オプションを使用すると、VACL の適用が解除されます。 vlan-list コマンドで指定できる VLAN は最大 32 個ですが、複数の vlan-list コマンドを設定すると、32 個を超える VLAN を指定できます。
ステップ 3	switch(config)# show running-config	(任意) ACL の設定を表示します。
ステップ 4	switch(config)# copy running-config startup-config	(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。

VACL の設定の確認

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。

コマンドまたはアクション	目的
switch# show running-config aclmgr	VACL 関連の設定を含む、ACL の設定を表示します。
switch# show vlan filter	VLAN に適用されている VACL の情報を表示します。
switch# 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 統計情報の表示と消去

VACL 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。

- **switch# show vlan access-list**
VACL の設定を表示します。VLAN アクセスマップに **statistics** コマンドが指定されている場合は、**show vlan access-list** コマンドの出力に、各ルールに一致したパケットの数が表示されます。
- **switch# clear vlan access-list counters**
すべての VACL、または特定の VACL の統計情報を消去します。

VACL の設定例

次に、**acl-ip-01** という名前の IP ACL によって許可されたトラフィックを転送するように VACL を設定し、その VACL を VLAN 50 ~ 82 に適用する例を示します。

```
switch# configure terminal
switch(config)# vlan access-map acl-ip-map
switch(config-access-map)# match ip address acl-ip-01
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan filter acl-ip-map vlan-list 50-82
```

LOU しきい値の設定

LOU しきい値を設定できます。展開された ACE の数がこのしきい値を超えると、デバイスはそれらを LOU レジスタに保存します。それ以外の場合は、これらの ACE が TCAM エントリとして保存されます。この設定は、次の ACL コンフィギュレーションについてのみ有効になります。

TCAM または LOU レジスタのすべての既存 ACL コンフィギュレーションは、この設定の影響を受けません。変更を有効にするには、**copyrs** コマンドを使用し、ボックスをリロードする必要があります。



(注) TCAM または 24 の LOU レジスタがいっぱいになると、展開された ACE は保存されません。

手順

	コマンドまたはアクション	目的
ステップ 1	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)# hardware profile tcam lou-thresholdvalue	LOU しきい値を設定します。また、新しいポリシーに関して、LOU 展開しきい値が有効になります。しきい値が既存のポリシーに対して有効になるように、設定を保存し、リロードすることをお勧めします。 しきい値の範囲は 1 ~ 100 です。デフォルトの LOU しきい値は 1 です。

次に、LOU しきい値を設定する例を示します。

```
switch# configure terminal
switch(config)# hardware profile tcam lou-threshold 20
switch(config)# copy running-config startup-config
switch(config)# reload
LOU expansion threshold changed to 20
```

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。

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 profile tcam region {arpacl {ipv6-e-racl e-racl}}	ACL TCAM リージョンサイズを変更します。

	コマンドまたはアクション	目的
	<pre> ifacl {ipv6-qos qos} qoslbl {ipv6-racl racl} vacl } tcam_size</pre>	<ul style="list-style-type: none"> • arpacl : アドレス解決プロトコル (ARP) の ACL (ARPA) TCAM リージョンサイズを設定します。 • e-racl : 出力ルータ ACL (ERACL) TCAM リージョンサイズを設定します。 • e-vacl : 出力の VLAN ACL (EVACL) TCAM リージョンサイズを設定します。 • ifacl : インターフェイス ACL (ifacl) TCAM リージョンサイズを設定します。エントリの最大数は 1500 です。 • qos : Quality of Service (QoS) TCAM リージョンサイズを設定します。 • qoslbl : QoS ラベル (qoslbl) TCAM リージョンサイズを設定します。 • racl : ルータの ACL (RA) TCAM リージョンサイズを設定します。 • vacl : VLAN ACL (VACL) TCAM リージョンサイズを設定します。 • tcam_size : TCAM サイズ。有効な範囲は 0 ~ 2,147,483,647 エントリです。 <p>(注) vacl および e-vacl TCAM リージョンを同じサイズに設定する必要があります。</p>
<p>ステップ 3</p>	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>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。</p>
<p>ステップ 4</p>	<p>switch(config)# show hardware profile tcam region</p> <p>例 :</p> <pre>switch(config)# show hardware profile tcam region</pre>	<p>スイッチの次のリロード時に適用される TCAM サイズを表示します。</p>
<p>ステップ 5</p>	<p>switch(config)# reload</p> <p>例 :</p> <pre>switch(config)# reload</pre>	<p>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。</p>

	コマンドまたはアクション	目的
		(注) copy running-config to startup-config を保存した後、次回のリロード時に新しいサイズ値が有効になります。

次に、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 profile 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、0 または 128 以外の値に ARP ACL TCAM 値を設定したときに表示されるエラーメッセージの例を示します。また、ARP ACL TCAM リージョンのサイズを変更する方法も示します。

```
switch(config)# hardware profile tcam region arpacl 200
ARPAcl size can be either 0 or 128
```

```
switch(config)# hardware profile tcam region arpacl 128
To start using ARPACL tcam, IFACL tcam size needs to be changed.
Changing IFACL tcam size to 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
```

次に、スイッチで TCAM VLAN ACL を設定する例を示します。

```
switch# configure sync
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-sync)# switch-profile s5010
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# hardware profile tcam region vacl 512
switch(config-sync-sp)# hardware profile tcam region e-vacl 512
switch(config-sync-sp)#
```

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 profile tcam region
  sup size = 16
  vacl size = 640
  ifacl size = 496
  qos size = 256
  rbacl size = 0
  span size = 0
  racl size = 1536
  e-racl size = 256
  e-vacl size = 640
  qoslbl size = 0
  arpacl size = 0
  ipv6-racl size = 0
  ipv6-e-racl size = 0
  ipv6-sup size = 0
  ipv6-qos size = 0
```

デフォルトの TCAM リージョンサイズに戻す

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	switch(config)# no hardware profile tcam region {arpacl e-racl} ifacl qos qoslbl racl } vacl } tcam_size	デフォルト ACL TCAM サイズに設定を戻します。
ステップ 3	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 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 4	switch(config)# reload	スイッチをリロードします。

次に、デフォルトの RA CL TCAM リージョンのサイズに戻す例を示します。

```
switch(config)# no hardware profile 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-configur startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

仮想端末回線の ACL の設定

仮想端末 (VTY) 回線とアクセスリストのアドレス間の IPv4 または IPv6 の着信接続と発信接続を制限するには、ラインコンフィギュレーションモードで **access-class** コマンドを使用します。アクセス制限を解除するには、このコマンドの **no** 形式を使用します。

VTY 回線で ACL を設定する場合には、次のガイドラインに従ってください。

- すべての VTY 回線にユーザが接続できるため、すべての VTY 回線に同じ制約を設定する必要があります。
- エントリ単位の統計情報は、VTY 回線の ACL ではサポートされません。

はじめる前に

適用する ACL が存在しており、この適用に対して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	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)# line vty 例： switch(config)# line vty switch(config-line)#	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 3	switch(config-line)# access-class access-list-number {in out} 例： switch(config-line)# access-class ozi2 in switch(config-line)# access-class ozi3 out switch(config)#	着信または発信アクセス制限を指定します。
ステップ 4	switch(config-line)# no access-class access-list-number {in out} 例： switch(config-line)# no access-class ozi2 in switch(config-line)# no access-class ozi3 out switch(config)#	(任意) 着信または発信アクセス制限を削除します。
ステップ 5	switch(config-line)# exit 例： switch(config-line)# exit switch#	ライン 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	switch# show running-config aclmgr 例： switch# show running-config aclmgr	(任意) スイッチの ACL の実行コンフィギュレーションを表示します。
ステップ 7	switch# copy running-config startup-config 例： switch# copy running-config startup-config	(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。

次に、VTY 回線の in 方向に `access-class ozi2` のコマンドを適用する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# line vty
switch(config-line)# access-class ozi2 in
switch(config-line)# exit
switch#
```

VTY 回線の ACL の確認

VTY 回線の ACL 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
<code>show running-config aclmgr</code>	スイッチで設定された ACL の実行コンフィギュレーションを表示します。
<code>show users</code>	接続されているユーザを表示します。
<code>show access-lists access-list-name</code>	エントリ単位の統計情報を表示します。

VTY 回線の ACL の設定例

次に、コンソール回線 (ttyS0) および VTY 回線 (pts/0 および pts/1) の接続ユーザの例を示します。

```
switch# show users
NAME      LINE      TIME          IDLE          PID COMMENT
admin     ttyS0     Aug 27 20:45  .            14425 *
admin     pts/0     Aug 27 20:06 00:46       14176 (172.18.217.82) session=ssh
admin     pts/1     Aug 27 20:52  .            14584 (10.55.144.118)
```

次に、172.18.217.82 を除き、すべての IPv4 ホストへの VTY 接続を許可する例と、10.55.144.118、172.18.217.79、172.18.217.82、172.18.217.92 を除き、すべての IPv4 ホストへの VTY 接続を拒否する例を示します。

```
switch# show running-config aclmgr
!Time: Fri Aug 27 22:01:09 2010
version 5.0(2)N1(1)
ip access-list ozi
 10 deny ip 172.18.217.82/32 any
 20 permit ip any any
ip access-list ozi2
 10 permit ip 10.55.144.118/32 any
 20 permit ip 172.18.217.79/32 any
 30 permit ip 172.18.217.82/32 any
 40 permit ip 172.18.217.92/32 any

line vty
 access-class ozi in
 access-class ozi2 out
```

次に、ACL のエントリ単位の統計情報をイネーブルにして、IP アクセスリストを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.
```

```
End with CNTL/Z.
switch(config)# ip access-list ozi2
switch(config-acl)# statistics per-entry
switch(config-acl)# deny tcp 172.18.217.83/32 any
switch(config-acl)# exit

switch(config)# ip access-list ozi
switch(config-acl)# statistics per-entry
switch(config-acl)# permit ip 172.18.217.20/24 any
switch(config-acl)# exit
switch#
```

次に、in および out 方向で VTY の ACL を適用する例を示します。

```
switch(config)# line vty
switch(config-line)# ip access-class ozi in
switch(config-line)# access-class ozi2 out
switch(config-line)# exit
switch#
```

次に、VTY 回線でアクセス制限を削除する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
switch(config)# line vty
switch(config-line)# no access-class ozi2 in
switch(config-line)# no ip access-class ozi2 in
switch(config-line)# exit
switch#
```



第 9 章

DHCP スヌーピングの設定

この章の内容は、次のとおりです。

- [DHCP スヌーピングの概要, 171 ページ](#)
- [DHCPv6 リレー エージェントの概要, 174 ページ](#)
- [DHCP スヌーピングのライセンス要件, 174 ページ](#)
- [DHCP スヌーピングの前提条件, 175 ページ](#)
- [DHCP スヌーピングの注意事項および制約事項, 175 ページ](#)
- [DHCP スヌーピングのデフォルト設定, 175 ページ](#)
- [DHCP スヌーピングの設定, 176 ページ](#)
- [DHCPv6 リレー エージェントの設定, 187 ページ](#)
- [DHCP スヌーピング設定の確認, 191 ページ](#)
- [DHCP バインディングの表示, 191 ページ](#)
- [DHCP スヌーピング バインディング データベースのクリア, 192 ページ](#)
- [DHCP リレー統計情報のクリア, 193 ページ](#)
- [DHCPv6 リレー統計情報のクリア, 193 ページ](#)
- [DHCP のモニタリング, 193 ページ](#)
- [DHCP スヌーピングの設定例, 194 ページ](#)

DHCP スヌーピングの概要

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、VLAN ベースごとにイネーブルに設定されます。デフォルトでは、すべての VLAN でこの機能は非アクティブです。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。

機能のイネーブル化とグローバルなイネーブル化

DHCP スヌーピングを設定するときは、DHCP スヌーピング機能のイネーブル化と DHCP スヌーピングのグローバルなイネーブル化の違いを理解することが重要です。

機能のイネーブル化

DHCP スヌーピング機能は、デフォルトではディセーブルです。DHCP スヌーピング機能がディセーブルになっていると、DHCP スヌーピングまたはこれに依存する機能を設定できません。DHCP スヌーピングおよびその依存機能を設定するコマンドは、DHCP スヌーピングがディセーブルになっているときは使用できません。

DHCP スヌーピング機能をイネーブルにすると、スイッチで DHCP スヌーピング バインディング データベースの構築と維持が開始されます。DHCP スヌーピング バインディング データベースに依存する機能は、その時点から使用できるようになり、設定も可能になります。

DHCP スヌーピング機能をイネーブルにしても、グローバルにイネーブルになるわけではありません。DHCP スヌーピングをグローバルにイネーブルにするには、個別に行う必要があります。

DHCP スヌーピング機能をディセーブルにすると、スイッチから DHCP スヌーピングの設定がすべて削除されます。DHCP スヌーピングをディセーブルにして設定を維持したい場合は、DHCP スヌーピング機能をディセーブルにするのではなく、DHCP スヌーピングをグローバルにディセーブル化します。

グローバルなイネーブル化

DHCP スヌーピングのイネーブル化の実行後、DHCP スヌーピングはデフォルトでグローバルにディセーブルになります。グローバルなイネーブル化は第 2 レベルのイネーブル化です。これにより、DHCP スヌーピング バインディング データベースのイネーブル化とは別に、スイッチがアクティブに DHCP スヌーピングを実行しているかどうかを個別に制御できます。

DHCP スヌーピングをグローバルにイネーブルにすると、DHCP スヌーピングがイネーブルになっている VLAN の信頼できない各インターフェイスについて、受信した DHCP メッセージの検証が開始され、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 スヌーピングをグローバルにディセーブルにすると、DHCP メッセージの検証と、信頼できないホストからの以降の要求の検証を停止します。DHCP スヌーピング バインディング データベースも削除されます。DHCP スヌーピングをグローバルにディセーブルにしても、DHCP スヌーピングの設定や、DHCP スヌーピング機能に依存するその他の機能の設定は削除されません。

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。信頼できないソースの場合、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スイッチです。これらのスイッチには、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スイッチやネットワーク外のスイッチ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スイッチは、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 Nexus 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が信頼されることを示します。

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スイッチ（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。



(注) DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。

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。



(注) 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。

スイッチが特定の 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、サーバからの DHCPACK メッセージをスイッチで受信すると、この機能により、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切れると、またはホストからの DHCPRELEASE メッセージをスイッチで受信すると、この機能により、データベース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。

`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。

DHCPv6 リレー エージェントの概要

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 VRF のクライアントに DHCPv6 サポートを提供できるため、VRF ごとに1つずつではなく、単一の IP アドレス プールを使用することで、IP アドレスを節約できます。

DHCP スヌーピングのライセンス要件

この機能には、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すべて Cisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

DHCP スヌーピングの前提条件

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 スヌーピングの注意事項および制約事項

DHCP スヌーピングを設定する場合は、次の注意事項および制約事項を考慮してください。

- 7.0(3)I2(1) より前のリリースでは、サポートされない DHCP スタティック バインディング設定は拒否され、エラーになっていましたが、Release 7.0(3)I2(1)以降、複数の IP およびポートにわたる スタティック DHCP バインディングで同じ MAC アドレスが許可されるようになりました。
- DHCP スヌーピング データベースには 2,000 のバインディングを格納できます。
- DHCP をグローバルにイネーブル化し、さらに少なくとも 1 つの VLAN で DHCP スヌーピングをイネーブルにするまで、DHCP スヌーピングはアクティブになりません。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレーエージェントとして機能するスイッチが設定され、イネーブルになっていることを確認してください。
- 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。
- DHCP スヌーピングおよび DHCP リレー機能は、同一の VLAN ポート上ではサポートされません。
- インターフェイスに DHCPv6 サーバアドレスを設定する場合、宛先インターフェイスはグローバル IPv6 アドレスと共に使用できません。
- DHCPv6 リレーの場合、インターフェイスに最大 32 の DHCPv6 サーバ IP アドレスを設定できます。

DHCP スヌーピングのデフォルト設定

次の表に、DHCP スヌーピング パラメータのデフォルト設定を示します。

表 14: DHCP スヌーピング パラメータのデフォルト値

パラメータ	デフォルト
DHCP スヌーピング機能	ディセーブル

パラメータ	デフォルト
DHCP スヌーピングのグローバルなイネーブル化	No
DHCP スヌーピング VLAN	なし
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 エージェントに対する VRF サポート	ディセーブル
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
DHCP リレー エージェント	ディセーブル
DHCPv6 リレー エージェント	ディセーブル
DHCPv6 relay option type cisco	ディセーブル

DHCP スヌーピングの設定

DHCP スヌーピングの最小設定

- 1 DHCP スヌーピング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	DHCP スヌーピング機能をイネーブルにします。	DHCP スヌーピング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。 詳細については、「 DHCP スヌーピング機能のイネーブル化またはディセーブル化 、(177 ページ)」を参照してください。
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。	詳細については、「 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 、(178 ページ)」を参照してください。

	コマンドまたはアクション	目的
ステップ 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。 詳細については、「 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 、(179 ページ)」を参照してください。
ステップ 4	DHCP サーバとスイッチが、信頼できるインターフェイスを使用し、接続されていることを確認します。	詳細については、「 インターフェイスの信頼状態の設定 、(181 ページ)」を参照してください。

DHCP スヌーピング機能のイネーブル化またはディセーブル化

スイッチの DHCP スヌーピング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 スヌーピングはディセーブルです。

はじめる前に

DHCP スヌーピング機能をディセーブルにすると、DHCP スヌーピングの設定がすべて消去されます。DHCP スヌーピングをオフにして DHCP スヌーピングの設定を維持したい場合は、DHCP をグローバルにディセーブル化します。

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] feature dhcp 例： switch(config)# feature dhcp	DHCP スヌーピング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 スヌーピング機能がディセーブルになり、DHCP スヌーピングの設定がすべて消去されます。
ステップ 3	showrunning-config dhcp 例： switch(config)# show running-config dhcp	(任意) DHCP スヌーピング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 4	copy running-config startup-config 例 : <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。

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

スイッチに対して 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。DHCP スヌーピングをグローバルにディセーブルにすると、DHCP スヌーピングの実行や はスイッチで停止されますが、DHCP スヌーピングの設定は維持されます。

はじめる前に

DHCP スヌーピング機能がイネーブルになっていることを確認します。デフォルトでは、DHCP スヌーピングはグローバルにディセーブルです。

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 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 snooping 例 : <pre>switch(config)# ip dhcp snooping</pre>	DHCP スヌーピング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 DHCP スヌーピングがディセーブルになります。
ステップ 3	showrunning-config dhcp 例 : <pre>switch(config)# show running-config dhcp</pre>	(任意) DHCP スヌーピングの設定を表示します。
ステップ 4	copy running-config startup-config 例 : <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。

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。

はじめる前に

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。

DHCP スヌーピングがイネーブルになっていることを確認してください。



- (注) 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。

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] ipdhcp snooping vlan vlan-list 例： 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。 no オプションを使用すると、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	showrunning-config dhcp 例： switch(config)# show running-config dhcp	(任意) DHCP スヌーピングの設定を表示します。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(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。

Option 82 データの挿入および削除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、デバイスは DHCP パケットに Option 82 情報を挿入しません。



(注) 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。

はじめる前に

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	config t 例： switch# config t 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 information option 例： switch(config)# ip dhcp snooping information option	DHCP パケットの Option 82 情報の挿入および削除をイネーブルにします。 no オプションを使用すると、Option 82 情報の挿入および削除がディセーブルになります。
ステップ 3	showrunning-config dhcp 例： switch(config)# show running-config dhcp	(任意) DHCP 設定を表示します。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(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。

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 スヌーピング機能では、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。

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 packet strict-validation 例： switch(config)# ip dhcp packet strict-validation	DHCP スヌーピング機能で、DHCP パケットの厳密な検証をイネーブルにします。 no オプションを使用すると、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	showrunning-config dhcp 例： switch(config)# show running-config dhcp	(任意) DHCP スヌーピングの設定を表示します。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(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。

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。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

はじめる前に

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 スヌーピングがイネーブルになっていることを確認してください。

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 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	次のいずれかのコマンドを入力します。 • interface ethernet port/slot • interface port-channel channel-number 例： switch(config)# interface ethernet 2/1 switch(config-if)#	<ul style="list-style-type: none"> • 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>port/slot</i> は、DHCP スヌーピングで <i>trusted</i> または <i>untrusted</i> 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>port/slot</i> は、DHCP スヌーピングで <i>trusted</i> または <i>untrusted</i> 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 例： switch(config-if)# ip dhcp snooping trust	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。 no オプションを使用すると、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	show running-config dhcp 例： switch(config-if)# show running-config dhcp	(任意) DHCP スヌーピングの設定を表示します。
ステップ 5	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(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。

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。

はじめる前に

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	config t 例： switch# config t 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 relay 例： switch(config)# ip dhcp relay	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、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	show ip dhcp relay 例： switch(config)# show ip dhcp relay	(任意) DHCP リレーの設定を表示します。
ステップ 4	showrunning-config dhcp 例： switch(config)# show running-config dhcp	(任意) DHCP 設定を表示します。
ステップ 5	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(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。

DHCP リレー エージェントに対する Option 82 のイネーブル化またはディセーブル化

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 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。

はじめる前に

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	[no] ip dhcp relay information option 例： switch(config)# 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イネーブルにします。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、この動作がディセーブルになります。
ステップ 3	[no] ip dhcp relay information sub-option circuit-id format-type string 例： switch(config)# ip dhcp relay information sub-option circuit-id format-type string	(任意) 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 Option 82 を設定します。
ステップ 4	show ip dhcp relay 例： switch(config)# show ip dhcp relay	(任意) DHCP リレーの設定を表示します。
ステップ 5	show running-config dhcp 例： switch(config)# show running-config dhcp	(任意) DHCP 設定を表示します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 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。

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。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCP 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 インスタンス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) 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。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： <pre>switch# config t 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。 <ul style="list-style-type: none"> • interfaceethernet<i>slot/port</i>[<i>.number</i>] • interfacevlan<i>vlan-id</i> • interfaceport-channel<i>channel-id</i>[<i>subchannel-id</i>] 例： <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	<ul style="list-style-type: none"> • 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。 • 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。

	コマンドまたはアクション	目的
ステップ 3	ip dhcp relay address <i>IP-address</i> 例： <pre>switch(config-if)# ip dhcp relay address 10.132.7.120</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	showip dhcp relay address 例： <pre>switch(config-if)# show ip dhcp relay address</pre>	(任意) 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	showrunning-config dhcp 例： <pre>switch(config-if)# show running-config dhcp</pre>	(任意) DHCP 設定を表示します。
ステップ 6	copy running-config startup-config 例： <pre>switch(config-if)# 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。

DHCP スタティック バインディングの作成

レイヤ 2 インターフェイスにスタティック DHCP ソース バインディングを作成できます。

はじめる前に

DHCP スヌーピング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： <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	ip source binding <i>IP-address MAC-address</i> vlan <i>vlan-id</i> { interface ethernet slot/port port-channel channel-no } 例 : <pre>switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3</pre>	レイヤ2イーサネットインターフェイスにスタティックな送信元アドレスをバインドします。
ステップ 3	show ip dhcp snooping binding 例 : <pre>switch(config)# ip dhcp snooping binding</pre>	(任意) DHCP スヌーピングのスタティックおよびダイナミックバインディングを示します。
ステップ 4	show ip dhcp snooping binding dynamic 例 : <pre>switch(config)# ip dhcp snooping binding dynamic</pre>	(任意) DHCP スヌーピングのダイナミックバインディングを示します。
ステップ 5	copy running-config startup-config 例 : <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。

次に、イーサネットインターフェイス 2/3 上に、VLAN 100 に関連付ける固定 IP ソース エントリを作成する例を示します。

```
switch# configure terminal
switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3
switch(config)#
```

DHCPv6 リレー エージェントの設定

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 エージェントはディセーブルにされます。

はじめる前に

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	[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。
ステップ 3	show ipv6 dhcp relay [interface interface] 例： switch(config)# show ipv6 dhcp relay	(任意) DHCPv6 リレーの設定を表示します。
ステップ 4	showrunning-config dhcp 例： switch(config)# show running-config dhcp	(任意) DHCP 設定を表示します。
ステップ 5	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(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。

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。

はじめる前に

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 エージェントがイネーブル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 option vpn 例： switch(config)# ipv6 dhcp relay option vpn	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： switch(config)# ipv6 dhcp relay option type cisco	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	show ipv6 dhcp relay [interface interface] 例： switch(config)# show ipv6 dhcp relay	(任意) DHCPv6 リレーの設定を表示します。
ステップ 5	showrunning-config dhcp 例： switch(config)# show running-config dhcp	(任意) DHCP 設定を表示します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(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。

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。

はじめる前に

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 エージェントがイネーブル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	show ipv6 dhcp relay [interface interface] 例： switch(config)# show ipv6 dhcp relay	(任意) DHCPv6 リレーの設定を表示します。
ステップ 4	showrunning-config dhcp 例： switch(config)# show running-config dhcp	(任意) 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	copy running-config startup-config 例： <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。

DHCP スヌーピング設定の確認

DHCP スヌーピング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。これらのコマンドの出力フィールドの詳細については、Cisco Nexus デバイスの『System Management Configuration Guide』を参照してください。

コマンド	目的
show running-config dhcp	DHCP スヌーピング設定を表示します。
show ip dhcp relay	DHCP リレーの設定を表示します。
show ipv6 dhcp relay [interfaceinterface]	DHCPv6 リレーのグローバルまたはインターフェイスレベルの設定を表示します。
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。

DHCP バインディングの表示

DHCP スタティックおよびダイナミック バインディング テーブルを表示するには、**show ip dhcp snooping binding** コマンドを使用します。DHCP ダイナミック バインディング テーブルを表示するには、**show ip dhcp snooping binding dynamic** を使用します。

このコマンドの出力フィールドの詳細については、Cisco Nexus デバイスの『System Management Configuration Guide』を参照してください。

次に、スタティック DHCP バインディングを作成してから、**show ip dhcp snooping binding** コマンドを使用してバインディングを確認する例を示します。

```
switch# configuration terminal
switch(config)# ip source binding 10.20.30.40 0000.1111.2222 vlan 400 interface port-channel
500
```

```
switch(config)# show ip dhcp snooping binding
MacAddress      IpAddress      LeaseSec      Type          VLAN  Interface
-----
00:00:11:11:22:22  10.20.30.40    infinite      static        400   port-channel500
```

DHCP スヌーピング バインディング データベースのクリア

DHCP スヌーピング バインディング データベースからエントリを削除できます。1つのエントリ、インターフェイスに関連するすべてのエントリ、データベース内のすべてのエントリなどを削除することが可能です。

はじめる前に

DHCP スヌーピングがイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	clear ip dhcp snooping binding 例： switch# clear ip dhcp snooping binding	(任意) 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。
ステップ 2	clear ip dhcp snooping binding interface ethernet slot/port[.subinterface-number] 例： switch# clear ip dhcp snooping binding interface ethernet 1/4	(任意) 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。
ステップ 3	clear ip dhcp snooping binding interface port-channel channel-number[.subchannel-number] 例： switch# clear ip dhcp snooping binding interface port-channel 72	(任意) 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。
ステップ 4	clear ip dhcp snooping binding vlan vlan-id mac mac-address ip ip-address interface {ethernet slot/port[.subinterface-number] port-channel channel-number[.subchannel-number]} 例： switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip	(任意) 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
	10.34.54.9 interface ethernet 2/11	
ステップ 5	show ip dhcp snooping binding 例： switch# show ip dhcp snooping binding	(任意) DHCP スヌーピング バインディング データベースを表示します。

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の DHCP リレーの統計情報をクリアするには、**clear ip dhcp relay statistics interface interface** コマンドを使用します。

clear ip dhcp relay statistics interface interface serverip ip-address [use-vrf vrf-name] コマンドを使用して、特定のインターフェイスのサーバレベルでの DHCP リレー統計情報をクリアします。

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の DHCPv6 リレーの統計情報をクリアするには、**clear ipv6 dhcp relay statistics interface interface** コマンドを使用します。

clear ipv6 dhcp relay statistics interface interface server-ip ip-address [use-vrf vrf-name] コマンドを使用して、特定のインターフェイスのサーバレベルでの DHCPv6 リレー統計情報をクリアします。

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。

show ip dhcp relay statistics [interface interface [serverip ip-address [use-vrf vrf-name]]] コマンドを使用して、グローバル、サーバ、またはインターフェイスレベルでの DHCP リレー統計情報をモニタします。

show ip dhcp snooping statistics vlan [vlan-id] interface [ethernet port-channel] [id] コマンド（オプション）を使用して、VLAN より下位のインターフェイス別のスヌーピング統計情報に関する正確な統計情報を確認します。

DHCP スヌーピングの設定例

次に、2つの VLAN 上で DHCP スヌーピングをイネーブルにして、Option 82 サポートをイネーブルにし、さらに DHCP サーバがイーサネット インターフェイス 2/5 に接続されているためにその 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例を示します。

```
feature dhcp
ip dhcp snooping
ip dhcp snooping info option

interface Ethernet 2/5
 ip dhcp snooping trust
ip dhcp snooping vlan 1
ip dhcp snooping vlan 50
```



第 10 章

ダイナミック ARP インспекションの設定

この章の内容は、次のとおりです。

- [DAI の概要, 195 ページ](#)
- [DAI のライセンス要件, 199 ページ](#)
- [DAI の前提条件, 199 ページ](#)
- [DAI の注意事項と制約事項, 200 ページ](#)
- [DAI のデフォルト設定, 201 ページ](#)
- [DAI の設定, 201 ページ](#)
- [DAI の設定の確認, 206 ページ](#)
- [DAI の統計情報のモニタリングとクリア, 207 ページ](#)
- [DAI の設定例, 207 ページ](#)

DAI の概要

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。

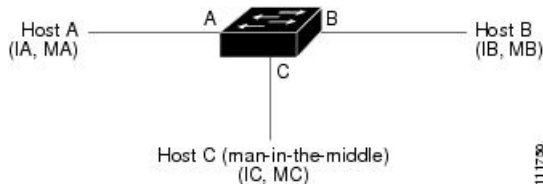
ARP スプーフィング攻撃

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。

次の図に、ARPキャッシュポイズニングの例を示します。

図4: ARPキャッシュポイズニング



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。カッコ内は、各ホストのIPおよびMACアドレスを示します。たとえば、ホストAはIPアドレスIA、およびMACアドレスMAを使用します。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。デバイスとホストBはこのARP要求を受信すると、IPアドレスIAおよびMACアドレスMAを持つホストのARPバインディングを、それぞれのARPキャッシュ内に書き込みます。たとえば、IPアドレスIAはMACアドレスMAにバインドされます。ホストBが応答すると、デバイスとホストAは、IPアドレスIBおよびMACアドレスMBを持つホストのバインディングを、それぞれのARPキャッシュ内に書き込みます。

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、デバイス、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とデバイスは、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とデバイスは、IB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。

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。このデータベースは、VLAN とデバイス上で DHCP スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。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。

信頼できない

ホストに接続されているインターフェイス

信頼できる

デバイスに接続されているインターフェイス

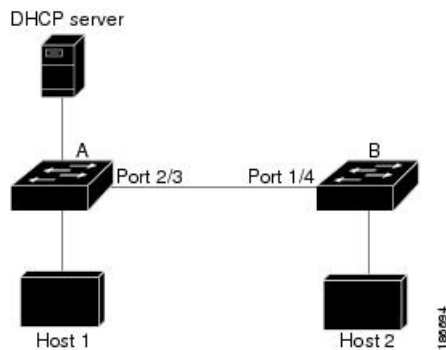
この設定では、デバイスからネットワークに送信される ARP パケットはすべて、セキュリティ検査をバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。

**注意**

信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

次の図では、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。

図 5: DAI をイネーブルにした VLAN での ARP パケット検証



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 が稼働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を検証するには、DAI が稼働しているデバイスに ARP ACL を設定します。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。



(注) 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。



(注) 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。

DAI のライセンス要件

次の表に、DAI 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	DAI 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すべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。

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。

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、またはこの機能がイネーブル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。
- 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。DAI が ARP パケットの有効性を判断するのにスタティック 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、DHCP スヌーピングの設定はイネーブルにするだけで済みます。DAI が ARP パケットの有効性を判断するのにダイナミック 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、DAI を設定した VLAN と同じ VLAN に DHCP スヌーピングを設定する必要があります。
- **feature dhcp** コマンドを使用して DHCP 機能をイネーブルにすると、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 機能がディセーブルになった設定から、DHCP 機能がイネーブル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 機能をイネーブル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、およびプライベート VLAN 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、DHCP スヌーピングがイネーブルになっていること、およびスタティック 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 スヌーピングがイネーブルになっていることを確認します。

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。

表 15: 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。
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 のイネーブル化とディセーブル化

VLAN に対して DAI をイネーブルまたはディセーブルにすることができます。デフォルトでは、DAI はすべての VLAN でディセーブルです。

はじめる前に

DAI をイネーブルにする場合は、次の点を確認してください。

- DHCP 機能がイネーブルになっていることを確認します。
- DAI をイネーブルにする VLAN が設定されている。

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/list 例： switch(config)# ip arp inspection vlan 13	VLAN の特定のリストに対して DAI をイネーブルにします。no オプションを使用すると、指定した VLAN の DAI がディセーブルになります。
ステップ 3	show ip arp inspection vlan/list 例： switch(config)# show ip arp inspection vlan 13	(任意) VLAN の特定リストの DAI ステータスを表示します。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(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。

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。

はじめる前に

DAI をイネーブルにする場合は、DHCP 機能がイネーブル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	interface <i>type</i> <i>number</i> / <i>slot</i> 例： switch(config)# interface ethernet 2/1 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	[no] ip arp inspection trust 例： switch(config-if)# ip arp inspection trust	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。
ステップ 4	show ip arp inspection interface <i>type</i> <i>number</i> / <i>slot</i> 例： switch(config-if)# show ip arp inspection interface ethernet 2/1	(任意) 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	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(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。

追加検証のイネーブル化またはディセーブル化

ARP パケットの追加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、ARP パケットの追加検証はイネーブルになりません。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 バインディング エントリと照合する送信元 IP アドレスのチェックは、イーサネット送信元 MAC アドレス (ARP 送信者の MAC アドレスではない) と ARP 送信者の 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、追加検証をイネーブル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。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。

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。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。

追加検証をイネーブルにする場合は、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** 検証をイネーブルにし、2つめの **ip arp inspection validate** コマンドで IP 検証をイネーブルにした場合は、2つめのコマンドを入力した時点で **src-mac** と **dst-mac** の検証がディセーブルになります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： 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 validate {[src-mac] [dst-mac] [ip]} 例： switch(config)# ip arp inspection validate src-mac dst-mac ip	追加の DAI 検証をイネーブルにします。あるいは、 no オプションを使用して、追加の DAI 検証をディセーブルにします。
ステップ 3	show running-config dhcp 例： switch(config)# show running-config dhcp	(任意) DAI の設定も含めて、DHCP スヌーピング設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	copy running-config startup-config 例 : <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。

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。

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 arp inspection log-buffer entriesnumber 例 : <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	show running-config dhcp 例 : <pre>switch(config)# show running-config dhcp</pre>	(任意) 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	copy running-config startup-config 例 : <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。

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。

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	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> • ip arp inspection vlan<i>vlan-list</i>loggingdhcp-bindings all • ip arp inspection vlan<i>vlan-list</i>loggingdhcp-bindings none • ip arp inspection vlan<i>vlan-list</i>loggingdhcp-bindings permit • no ip arp inspection vlan<i>vlan-list</i>loggingdhcp-bindings {all none permit} 例： <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。 no オプションを使用すると、DAI ログ フィルタリングが削除されます。 <ul style="list-style-type: none"> • DHCP バインディングに一致するすべてのパケットを記録します。 • DHCP バインディングに一致するパケットを記録しません。 • 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。 • DAI ログ フィルタリングを削除します。
ステップ 3	show running-config dhcp 例： <pre>switch(config)# show running-config dhcp</pre>	(任意) 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	copy running-config startup-config 例： <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。

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。

コマンド	目的
<code>show ip arp inspection interface ethernet</code>	信頼状態を表示します。
<code>show ip arp inspection vlan</code>	特定の VLAN の DAI 設定を表示します。
<code>show arp access-lists</code>	ARP ACL を表示します。
<code>show ip arp inspection log</code>	DAI のログ設定を表示します。

DAI の統計情報のモニタリングとクリア

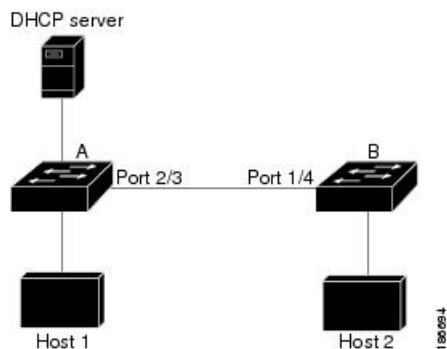
DAI の設定例

例 1 : 2 つのデバイスが DAI をサポートする場合

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。

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。

図 6 : DAI をサポートする 2 つのデバイス



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

例 1: 2つのデバイスが DAI をサポートする場合

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。

手順

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# config t
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 Jul 13 2008])
```

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
```

例 1: 2つのデバイスが DAI をサポートする場合

```

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。

手順

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# config t
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 Jun 13 2008])
    
```

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#
```



第 11 章

ユニキャスト RPF の設定

この章では、Cisco NX-OS デバイス上で出力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。

- [ユニキャスト RPF の概要, 213 ページ](#)
- [ユニキャスト RPF のライセンス要件, 215 ページ](#)
- [ユニキャスト RPF の注意事項と制約事項, 215 ページ](#)
- [ユニキャスト RPF のデフォルト設定, 216 ページ](#)
- [ユニキャスト RPF の設定, 217 ページ](#)
- [ユニキャスト RPF の設定例, 219 ページ](#)
- [ユニキャスト RPF の設定の確認, 219 ページ](#)

ユニキャスト RPF の概要

ユニキャスト RPF 機能では、変形または偽造（スプーフィング）された IPv4 ソースアドレスがネットワークに注入されて引き起こされる問題を、裏付けのない IPv4 パケットを廃棄することによって緩和します。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 をイネーブルにすると、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。



(注) 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、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。



(注) 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せん。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する必要があります（このプロセスは対照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。



注意 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。

手順

-
- ステップ 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。
- ステップ 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。
- ステップ 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。
- ステップ 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。
- ステップ 5** パケットを転送します。
-

グローバル統計情報

Cisco NX-OS デバイスがユニキャスト RPF チェックの失敗によりインターフェイスでパケットをドロップするたびに、その情報が転送エンジン (FE) 単位でデバイスにおいてグローバルにカウントされます。ドロップされたパケットのグローバル統計からは、ネットワーク上での攻撃の可能性に関する情報を得ることができませんが、攻撃の送信元となるインターフェイスは特定されません。ユニキャスト RPF チェックの失敗によりドロップされたパケットのインターフェイス単位の統計情報は利用できません。

ユニキャスト RPF のライセンス要件

製品	ライセンス要件
Cisco NX-OS	ユニキャスト RPF 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すべて Cisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

ユニキャスト RPF の注意事項と制約事項

ユニキャスト RPF の設定に関する注意事項と制約事項は次のとおりです。

- ユニキャスト RPF 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ユニキャスト RPF 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、集約デバイスでユニキャスト RPF 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 サーバにユニキャスト RPF 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全体でユニキャスト RPF を配布するエンティティが多いほど、インターネット コミュニティを通じた大規模なネットワークの中断が軽減される可能性が高くなり、攻撃の送信元をトレースできる可能性も高くなります。
- ユニキャスト RPF 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ユニキャスト RPF がネットワーク トラフィックを処理するように、ホーム ゲートウェイにユニキャスト RPF を設定する必要があります。
- ユニキャスト RPF 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。
- ネットワーク内部のインターフェイスにはユニキャスト RPF を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。ユニキャスト RPF 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。ストリクトユニキャスト RPF を設定しないでください。
- ユニキャスト RPF 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。



(注) 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。

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。

表 16: 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
Unicast RPF	ディセーブル

ユニキャスト RPF の設定

入力インターフェイスに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： 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 3	ip verify unicast source reachable-via {any [allow-default] rx} 例： switch(config-if)# ip verify unicast source reachable-via any	IPv4 用インターフェイスにユニキャスト RPF を設定します。 any キーワードはルーズ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

	コマンドまたはアクション	目的
		一致させることが可能になり、それを検証に使用できます。 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。
ステップ 4	ipv6 verify unicast source reachable-via {any [allow-default] rx} 例： Example: switch(config-if)# ipv6 verify unicast source reachable-via any	IPv6 用インターフェイスにユニキャスト RPF を設定します。 any キーワードはルーズ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になり、それを検証に使用できます。 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。
ステップ 5	exit 例： switch(config-cmap)# exit switch(config)#	クラスマップコンフィギュレーションモードを終了します。
ステップ 6	show ip interface ethernetslot/port 例： switch(config)# show ip interface ethernet 2/3	(任意) インターフェイスの IP 情報を表示します。
ステップ 7	show running-config interface ethernetslot/port 例： switch(config)# show running-config interface ethernet 2/3	(任意) 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 8	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(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。

ユニキャスト RPF の設定例

緩和モードの IPv4 パケット用ユニキャスト RPF の設定例を示します。

```
interface Ethernet2/3
 ip address 172.23.231.240/23
 ip verify unicast source reachable-via any
```

厳格モードの IPv4 パケット用ユニキャスト RPF の設定例を示します。

```
interface Ethernet2/2
 ip address 172.23.231.240/23
 ip verify unicast source reachable-via rx
```

緩和モードの IPv6 パケット用ユニキャスト RPF の設定例を示します。

```
interface Ethernet2/1
 ipv6 address 2001:0DB8:c18:1::3/64
 ipv6 verify unicast source reachable-via any
```

厳格モードの IPv6 パケット用ユニキャスト RPF の設定例を示します。

```
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、次のいずれかの作業を行います。

コマンド	目的
show running-config interface ethernetslot/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 startup-config interface ethernetslot/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。



第 12 章

コントロールプレーンポリシングの設定

この章の内容は、次のとおりです。

- [CoPP の概要, 222 ページ](#)
- [コントロールプレーン保護, 223 ページ](#)
- [CoPP ポリシー テンプレート, 225 ページ](#)
- [CoPP クラス マップ, 232 ページ](#)
- [1 秒間あたりのパケットのクレジット制限, 232 ページ](#)
- [CoPP と管理インターフェイス, 232 ページ](#)
- [CoPP のライセンス要件, 233 ページ](#)
- [CoPP の注意事項と制約事項, 233 ページ](#)
- [CoPP のアップグレードに関する注意事項, 234 ページ](#)
- [CoPP の設定, 235 ページ](#)
- [CoPP show コマンド, 239 ページ](#)
- [CoPP 設定ステータスの表示, 240 ページ](#)
- [CoPP のモニタリング, 240 ページ](#)
- [CoPP クラスに対するレート制限のディセーブル化と再イネーブル化, 241 ページ](#)
- [CoPP 統計情報のクリア, 243 ページ](#)
- [CoPP の設定例, 243 ページ](#)
- [CoPP の設定例, 245 ページ](#)
- [例：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, 248 ページ](#)
- [CoPP に関する追加情報, 248 ページ](#)

CoPP の概要

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 ポリシーのように見え、ルータまたはレイヤ 3 スイッチの任意の IP アドレスに宛てられた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拒絶 (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ます。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。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。

制御プレーン

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、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、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、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。またたとえば、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。

次に、DoS 攻撃の例を示します。

- 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



注意

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に、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。

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。ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) スヌーピングやダイナミック アドレス 解決 プロトコル (ARP) インスペクションなどの機能は、パケットをスーパーバイザ モジュールにリダイレクトします。

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すべて、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。

パケットの分類には、次のパラメータを使用できます。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート
- 宛先ポート
- レイヤ 4 プロトコル

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。

ポリシング レートは 1 秒間あたりのパケット (PPS) という形式で指定されます。分類されたそれぞれのフローは、PPS で表すポリシング レート制限を指定することによって個別にポリシング できます。

CoPP ポリシー テンプレート

Cisco NX-OS デバイスの初回起動時には、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 `copp-system-policy` が Cisco NX-OS ソフトウェアによって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、展開シナリオの CoPP ポリシー テンプレートを選択できます。

- **Default** : レイヤ2およびレイヤ3ポリシー。CPUにバインドされているスイッチドトラフィックとルーテッドトラフィックの間で適切なポリシング バランスを提供します。
- **Layer 2** : レイヤ2 ポリシー。CPU にバインドされているレイヤ2 トラフィック (たとえば BPDU) により多くのプリファレンスを与えます。
- **Layer 3** : レイヤ3 ポリシー。CPU にバインドされているレイヤ3 トラフィック (たとえば、BGP、RIP、OSPF など) により多くのプリファレンスを与えます。

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、Cisco NX-OS ソフトウェアにより **Default** ポリシングが適用されます。最初はこのデフォルト ポリシーを使用し、必要に応じて CoPP ポリシーを変更することを推奨します。

デフォルトの `copp-system-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。

`default`、`Layer 2` および `Layer 3` テンプレートを切り替えるには、`setup` コマンドを使って設定ユーティリティを再び入力することができます。

デフォルト CoPP ポリシー

このポリシーは、スイッチにデフォルトで適用されます。これには、ほとんどのネットワーク導入に適したポリサーレートを持つクラスが含まれています。このポリシーテンプレートを変更することはできませんが、デバイスの CoPP 設定を変更できます。セットアップユーティリティを実行してデフォルトの CoPP ポリシー プロファイルをセットアップすると、CoPP ポリシーに対して既に行われたすべての変更が削除されます。

このポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
```

```
    police pps 100
class copp-s-ttl1
    police pps 100
class copp-s-ip-options
    police pps 100
class copp-s-ip-nat
    police pps 100
class copp-s-ipmcmiss
    police pps 400
class copp-s-ipmc-g-hit
    police pps 400
class copp-s-ipmc-rpf-fail-g
    police pps 400
class copp-s-ipmc-rpf-fail-sg
    police pps 400
class copp-s-dhcpreq
    police pps 300
class copp-s-dhcpresp
    police pps 300
class copp-s-igmp
    police pps 400
class copp-s-routingProto2
    police pps 1300
class copp-s-eigrp
    police pps 200
class copp-s-pimreg
    police pps 200
class copp-s-pimautorp
    police pps 200
class copp-s-routingProto1
    police pps 1000
class copp-s-arp
    police pps 200
class copp-s-ntp
    police pps 1000
class copp-s-bpdu
    police pps 12000
class copp-s-cdp
    police pps 400
class copp-s-lacp
    police pps 400
class copp-s-lldp
    police pps 200
class copp-icmp
    police pps 200
class copp-telnet
    police pps 500
class copp-ssh
    police pps 500
class copp-snmp
    police pps 500
class copp-ntp
    police pps 100
class copp-tacacsradius
    police pps 400
class copp-stftp
    police pps 400
class copp-ftp
    police pps 100
class copp-http
    police pps 100
```

レイヤ 2 CoPP ポリシー

このポリシー テンプレートを変更することはできませんが、デバイスの CoPP 設定を変更できます。セットアップユーティリティを実行してレイヤ 2 CoPP ポリシー プロファイルをセットアップすると、CoPP ポリシー に対して行われたすべての変更が削除されます。

このポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
  class copp-s-ipmc-rpf-fail-g
    police pps 400
  class copp-s-ipmc-rpf-fail-sg
    police pps 400
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 1200
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 900
  class copp-s-arp
    police pps 200
  class copp-s-ntp
    police pps 100
  class copp-s-ptp
    police pps 1000
  class copp-s-bpdu
    police pps 12300
  class copp-s-cdp
    police pps 400
  class copp-s-lacp
    police pps 400
  class copp-s-lldp
    police pps 200
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
  class copp-ftp
    police pps 100
  class copp-http
```

```
police pps 100
```

レイヤ 3 CoPP ポリシー

このポリシー テンプレートを変更することはできませんが、デバイスの CoPP 設定を変更できます。セットアップユーティリティを実行してレイヤ 3 CoPP ポリシー プロファイルをセットアップすると、CoPP ポリシーに対して行われたすべての変更が削除されます。

このポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmis
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
  class copp-s-ipmc-rpf-fail-g
    police pps 400
  class copp-s-ipmc-rpf-fail-sg
    police pps 400
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 4000
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 4000
  class copp-s-arp
    police pps 200
  class copp-s-ntp
    police pps 1000
  class copp-s-bpdu
    police pps 6000
  class copp-s-cdp
    police pps 200
  class copp-s-lacp
    police pps 200
  class copp-s-lldp
    police pps 200
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
```



```
class copp-ssh
  police pps 500
class copp-snmp
  police pps 500
class copp-ntp
  police pps 100
class copp-tacacsradius
  police pps 400
class copp-stftp
  police pps 400
class copp-ftp
  police pps 100
class copp-http
  police pps 100
```

スタティック CoPP クラス

使用可能なスタティック CoPP クラスは次のとおりです。

• copp-s-default

パケットに関して `copy-to-CPU` が設定されており、パケットに関する他のより詳細な CoPP クラスで一致がない場合は、トラフィックの `Catch-all CoPP` クラスです。

```
class-map copp-s-default (match-any)
  police pps 400
    OutPackets 0
    DropPackets 0
```

• copp-s-l2switched

パケットに関して CPU ポートが選択されているときに他の明示的な CoPP クラスで一致がない場合は、レイヤ 2 トラフィックの `Catch-all CoPP` クラスです。

```
class-map copp-s-l2switched (match-any)
  police pps 200
    OutPackets 0
    DropPackets 0
```

• copp-s-l3destmiss

ハードウェア レイヤ 3 転送テーブルにルックアップのミスがあるレイヤ 3 トラフィックです。

```
class-map copp-s-l3destmiss (match-any)
  police pps 100
    OutPackets 0
    DropPackets 0
```

• copp-s-glean

IP アドレスに関する ARP 解決が提供されない直接接続サブネットの IP アドレスへのレイヤ 3 トラフィックで、ソフトウェアでの ARP 解決をトリガーするために使用されます。

```
class-map copp-s-glean (match-any)
  police pps 500
    OutPackets 0
    DropPackets 0
```

• copp-s-selfip

他のより詳細な CoPP クラスで一致がない場合は、ルータ インターフェイスのいずれかの IP アドレスに対して着信するパケットのデフォルトの CoPP クラスです。

```
class-map copp-s-selfip (match-any)
  police pps 500
```

```

    OutPackets    4
    DropPackets   0

```

• copp-s-l3mtufail

フラグメンテーションまたは ICMP メッセージの生成に関してソフトウェア処理を必要とする MTU チェック エラーがあるレイヤ 3 パケットです。

```

class-map copp-s-l3mtufail (match-any)
  police pps 100
    OutPackets    0
    DropPackets   0

```

• copp-s-ttl1

ルータのいずれかのインターフェイス IP アドレスに着信する、TTL=1 のレイヤ 3 パケットです。

```

class-map copp-s-ttl1 (match-any)
  police pps 100
    OutPackets    0
    DropPackets   0

```

• copp-s-ipmsmiss

マルチキャスト転送ルックアップに関するハードウェアレイヤ 3 転送テーブルにルックアップのミスがあるマルチキャスト パケットです。これらのデータ パケットは、マルチキャスト パケットのハードウェア転送に関するハードウェア転送テーブル エントリのインストーラをトリガーできます。

```

class-map copp-s-ipmcmis (match-any)
  police pps 400
    OutPackets    0
    DropPackets   0

```

• copp-s-l3slowpath

ソフトウェアで渡す必要のある他のパケットの例外ケースにヒットするレイヤ 3 パケットです (IP オプション パケットなど)。

```

class-map copp-s-l3slowpath (match-any)
  police pps 100
    OutPackets    0
    DropPackets   0

```

• copp-s-dhcpreq

DHCP 要求 パケットの CoPP クラスです。デフォルトでは、このクラスは、このクラスのパケットの CoPP レートをプログラムするためにのみ使用されます。「CPU へのコピー」は、DHCP スヌーピングまたはリレーが設定されるまで有効になりません。

```

class-map copp-s-dhcpreq (match-any)
  police pps 300
    OutPackets    0
    DropPackets   0

```

• copp-s-dai

ARP インスペクション代行受信パケットの CoPP クラスです。デフォルトでは、このクラスは、このクラスのパケットの CoPP レートをプログラムするためにのみ使用されます。「CPU へのコピー」は、IP ARP インスペクション機能が設定されるまで有効になりません。

```

class-map copp-s-dai (match-any)
  police pps 300
    OutPackets    0
    DropPackets   0

```

• copp-s-pimautorp

この CoPP クラスは、PIM auto-rp パケットを CPU (IP マルチキャスト グループ 224.0.1.39 および 224.0.1.40) にコピーするために使用されます。

```
class-map copp-s-pimautorp (match-any)
  police pps 200
    OutPackets    0
    DropPackets   0
```

• copp-s-arp

CPU にコピーされる ARP と ND の要求パケットおよび応答パケットの CoPP クラスです。

```
class-map copp-s-arp (match-any)
  police pps 200
    OutPackets    0
    DropPackets   0
```

• copp-s-ntp

Precision Time Protocol (PTP) パケットの CoPP クラスです。

```
class-map copp-s-ntp (match-any)
  police pps 1000
    OutPackets    0
    DropPackets   0
```

• copp-s-vxlan

この CoPP クラスは、NV オーバーレイ機能が設定されている場合およびリモートピア IP アドレス ラーニングのためにパケットが CPU にコピーされる場合に使用されます。

```
class-map copp-s-vxlan (match-any)
  police pps 1000
    OutPackets    0
    DropPackets   0
```

• copp-s-bfd

CPU にコピーされる Bidirectional Forwarding Detection (BFD) パケット (BFD プロトコル UDP ポートにより、ルータ インターフェイス IP アドレスに着信するパケット) の CoPP クラスです。

```
class-map copp-s-bfd (match-any)
  police pps 600
    OutPackets    0
    DropPackets   0
```

• copp-s-bpdu

CPU にコピーされる BPDU クラスのパケットの CoPP クラスです (STP、CDP、LLDP、LACP、UDLD パケットなど)。

```
class-map copp-s-bpdu (match-any)
  police pps 15000
    OutPackets    100738
    DropPackets   0
```

• copp-s-dpss

ポリシーが punt-to-CPU アクションによって設定される場合に、プログラム可能機能の onePK およびオープンフローに関して使用される CoPP クラスです (データパスサービスセット、オープンフロー punt-to-controller アクションなど)。

```
class-map copp-s-dpss (match-any)
  police pps 1000
```

```
OutPackets    0
DropPackets   0
```

• copp-s-mpls

MPLS ラベル除去アクションのためにタップアグリゲーション機能に関して使用されます。このクラスは、ラベル除去アクションのために、パケットを CPU にコピーして MPLS ラベル情報およびプログラムをラーニングするために使用されます。

```
class-map copp-s-mpls (match-any)
  police pps 100
    OutPackets    0
    DropPackets   0
```

CoPP クラス マップ

ポリシー内のクラスには、次の 2 つのタイプがあります。

- **スタティック**：これらのクラスは、各ポリシーテンプレートの一部であり、ポリシーまたは CoPP 設定から削除できません。スタティック クラスには、通常、デバイスの操作上重要と考えられ、ポリシーに必要なトラフィックが含まれます。
- **ダイナミック**：これらのクラスはポリシーから、作成、追加、または削除できます。ダイナミック クラスを使用して、要件に固有の CPU 行きトラフィック（ユニキャスト）用クラス/ポリシングを作成できます。



(注) copp-s-x という名前のクラスはスタティック クラスです。

ACL は、スタティックとダイナミックの両方のクラスに関連付けることができます。

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。

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。

CoPP のライセンス要件

この機能には、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すべて Cisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

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。

- 7.0(3)I2(1) よりも前のリリースでは、`copp-s-igmp` 用のポートで PIM が有効になっていない場合でも、常に、レイヤ 3 ポートで PIM-IGMP class-id が設定されていました。そのため、PIM が有効になっていない場合でも、IGMP パケットが CPU に着信していました。7.0(3)I2(1) 以降では、PIM が有効になっている場合にのみ、ポートで PIM_IGMP class-id が設定されます。PIM が有効になっていない場合はレイヤ 3 ポートで CPU に IGMP パケットをパントする必要がないため、`feature pim` を設定し、`copp-s-igmp` キューでパケットを取得するポートの PIM を有効にする必要があります。
- 導入のシナリオに応じてデフォルト、L2、または L3 ポリシーを選択し、観察された動作に基づいて、CoPP ポリシーを後で変更することを推奨します。
- `fast-reload` を実行した後、トラフィックが完全に収束してから、トラフィックにおいて +/- 2 ~ 5 % の不規則性が約 30 ~ 40 秒間発生する場合は、ARP パケットに関する CoPP 値を大きくします。
- 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に加えて、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。
- Release 6.0(2)U6(1) の場合、`write erase` コマンドとリロードにより、`copp-s-bfd` コマンドに関して、ポリシーの 1 秒間あたりのパケット (PPS) のデフォルト値が 900 に変更されます。
- 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。どちらの場合も、状況を分析して、別の CoPP ポリシーを使用するか、またはカスタマイズ済み CoPP ポリシーを変更する必要があるかどうかを評価します。
- 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 は入力だけでサポートされます。`service-policy output copp` は、コントロールプレーンインターフェイスには適用できません。
- 新しい CoPP ポリシーの作成はサポートされていません。
- `insert-before` オプションを使用して新しい CoPP クラス マップが CoPP ポリシー マップに挿入される場合、実行コンフィギュレーションにおけるクラスマップの順序は維持されます。ただし、`write erase` コマンドを実行し、スイッチをリロードすると、デフォルトの CoPP ポ

リシーが適用され、クラスマップがデフォルトの順序に並べ替えられます。ファイルを実行コンフィギュレーションにコピーすると、それが既存の CoPP ポリシーの変更操作となり、新しいクラスマップが最後に挿入されます。同様に、ファイルにおいてデフォルトクラスマップの順序変更がある場合、それは有効になりません。クラスマップの順序を保存するには、コンフィギュレーションをスタートアップにコピーして、リロードします。

- IPv6 と IPv4 の CoPP ACL エントリでは、別々の TCAM リージョンを使用します。IPv6 CoPP が動作するには、IPv6 ACL SUP TCAM リージョン (`ipv6-sup`) がゼロ以外のサイズに切り分けられている必要があります。詳細については、「[ACL TCAM リージョン, \(141 ページ\)](#)」および「[ACL TCAM リージョンサイズの設定, \(164 ページ\)](#)」のトピックを参照してください。
- CoPP には、すべての IPv4 CoPP ACL、IPv6 CoPP ACL および ARP ACL で最大 76 個のエントリを設定できます。システムは、72 個のスタティックエントリでプログラムされます (20 個の内部エントリ、43 個の IPv4 ACL エントリ、および 9 つの IPv6 ACL エントリ)。残りの 4 つのエントリを設定できます。さらにエントリを作成する必要がある場合は、未使用のスタティックな CoPP ACE を削除する必要があります。その後、追加エントリを作成します。
- Release 6.0(2)U5(1) 以降では、トンネルが設定されていない場合、Cisco Nexus 3000 シリーズスイッチは、すべてのパケットをドロップします。また、トンネルが設定されている場合でも、トンネルインターフェイスが設定されていないか、トンネルインターフェイスがシャットダウン状態のときは、パケットがドロップされます。

ポイントツーポイント トンネル (送信元と宛先) – Cisco Nexus 3000 シリーズスイッチは、**feature tunnel** コマンドが設定されており、着信パケットの外部送信元および宛先アドレスと一致するトンネル送信元および宛先アドレスによって設定されている使用可能なトンネルインターフェイスが存在する場合に、そのスイッチを宛先とするすべての IP-in-IP パケットのカプセル化を解除します。送信元および宛先パケットが一致しない場合またはインターフェイスがシャットダウン状態の場合は、パケットがドロップされます。

トンネルのカプセル化解除 (送信元のみ) – Cisco Nexus 3000 シリーズスイッチは、**feature tunnel** コマンドが設定されており、着信パケットの外部宛先アドレスと一致するトンネル送信元アドレスによって設定されている使用可能なトンネルインターフェイスが存在する場合に、そのスイッチを宛先とするすべての IP-in-IP パケットのカプセル化を解除します。送信元パケットが一致しない場合またはインターフェイスがシャットダウン状態の場合は、パケットがドロップされます。

CoPP のアップグレードに関する注意事項

CoPP には、アップグレードに関する次の注意事項があります。

- CoPP 機能をサポートしない Cisco NX-OS リリースから 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、スイッチの起動時にデフォルトポリシーを使って CoPP が自動的にイネーブルにされます。別のポリシー (デフォルト、13、12) をイネーブルにするには、アップグレード後にセットアップスクリプトを実行する必要があります。

CoPP 保護を設定しない場合、NX-OS デバイスは DoS 攻撃に対して脆弱な状態のままになります。

- 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追加クラスを含む 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実行する必要があります。
- セットアップスクリプトは、CPU に着信するさまざまなフローに対応するポリシーレートを変更するため、デバイスにトラフィックが発生する時間ではなく、スケジュールされたメンテナンス期間にセットアップスクリプトを実行することを推奨します。

CoPP の設定

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 permit および deny は、マッチング時には無視されます。

IPv4 または IPv6 パケットのポリシーを設定できます。

はじめる前に

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。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>configure terminal</p> <p>例 :</p> <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	<p>class-map type control-plane match-any class-map-name</p> <p>例 :</p> <pre>switch(config)# class-map type control-plane ClassMapA switch(config-cmap)#</pre>	<p>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。</p> <p>(注) 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。</p>

	コマンドまたはアクション	目的
ステップ 3	match access-group name <i>access-list-name</i> 例： <pre>switch(config-cmap)# match access-group name MyAccessList</pre>	(任意) IP ACL のマッチングを指定します。複数の IP ACL のマッチングを行う場合は、このステップを繰り返します。 (注) 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	exit 例： <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。
ステップ 5	show class-map type control-plane [class-map-name] 例： <pre>switch(config)# show class-map type control-plane</pre>	(任意) 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 6	copy running-config startup-config 例： <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。

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 マップにはポリシング 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、デフォルトの PPS をサポートします。

IPv4 または IPv6 パケットのポリシーを設定できます。

はじめる前に

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。

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	<p>policy-map type control-plane<i>policy-map-name</i></p> <p>例： <pre>switch(config)# policy-map type control-plane copp-system-policy switch(config-pmap)#</pre> </p>	<p>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大文字と小文字が区別されます。</p> <p>(注) ポリシーマップ名は変更できません。ポリシーマップの copp-system-policy 名のみを使用できます。単一の type control-plane ポリシーマップのみを設定できます。</p>
ステップ 3	<p>class {<i>class-map-name</i> [<i>insert-before</i><i>class-map-name2</i>] class}</p> <p>例： <pre>switch(config-pmap)# class ClassMapA switch(config-pmap-c)#</pre> </p>	<p>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。</p>
ステップ 4	<p>police [pps] {<i>pps-value</i>} [bc] <i>burst-size</i> [bytes kbytes mbytes ms packets us]</p> <p>例： <pre>switch(config-pmap-c)# police pps 100 bc 10</pre> </p>	<p>1秒間あたりのパケット (PPS) およびコミット済みバースト (BC) に関するレート制限を指定します。PPSの範囲は0～20,000です。デフォルト PPS は 0 です。BCの範囲は0～512000000です。デフォルト BC サイズの単位はバイトです。</p>
ステップ 5	<p>exit</p> <p>例： <pre>switch(config-pmap-c)# exit switch(config-pmap)#</pre> </p>	<p>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。</p>
ステップ 6	<p>exit</p> <p>例： <pre>switch(config-pmap)# exit switch(config)#</pre> </p>	<p>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。</p>
ステップ 7	<p>show policy-map type control-plane [expand] [<i>name</i><i>class-map-name</i>]</p> <p>例： <pre>switch(config)# show policy-map type control-plane</pre> </p>	<p>(任意) 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。</p>
ステップ 8	<p>copy running-config startup-config</p> <p>例： <pre>switch(config)# copy running-config startup-config</pre> </p>	<p>(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。</p>

コントロールプレーン サービス ポリシーの設定

はじめる前に

コントロールプレーン ポリシー マップを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： 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	control-plane 例： switch(config) # control-plane switch(config-cp)#	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 <i>policy-map-name</i> 例： switch(config-cp)# service-policy input copp-system-policy	入トラフィックのポリシー マップを指定します。
ステップ 4	exit 例： switch(config-cp)# exit switch(config)#	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。
ステップ 5	show running-config copp [all] 例： switch(config)# show running-config copp	(任意) CoPP 設定を表示します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 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。

CoPP show コマンド

CoPP の設定情報を表示するには、次の show コマンドのいずれかを入力します。

コマンド	目的
show ip access-lists [<i>acl-name</i>]	CoPP の ACL を含め、システム内で設定されているすべての IPv4 ACL を表示します。
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。
show ipv6 access-lists	CoPP IPv6 ACL を含め、デバイス上で設定されているすべての IPv6 ACL を表示します。
show arp access-lists	CoPP ARP ACL を含め、デバイス上で設定されているすべての ARP ACL を表示します。
show policy-map type control-plane [<i>expand</i>] [<i>name policy-map-name</i>]	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 PPS の値を表示します。
show running-config copp [<i>all</i>]	実行コンフィギュレーション内の CoPP 設定を表示します。
show running-config aclmgr [<i>all</i>]	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 startup-config copp [<i>all</i>]	スタートアップ 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
<code>show startup-config aclmgr [all]</code>	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

手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch# show copp status</code>	CoPP 機能の設定ステータスを表示します。

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 のモニタリング

手順

	コマンドまたはアクション	目的
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。

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-policy-default

class-map copp-system-class-igmp (match-any)
match protocol igmp
police cir 1024 kbps , bc 65535 bytes
conformed 0 bytes; action: transmit
violated 0 bytes;
class-map copp-system-class-pim-hello (match-any)
match protocol pim
police cir 1024 kbps , bc 4800000 bytes
conformed 0 bytes; action: transmit
violated 0 bytes;
....

switch# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy
class-map copp-s-selfIp (match-any)
  police pps 500
  OutPackets 268
  DropPackets 0
```

CoPPクラスに対するレート制限のディセーブル化と再イネーブル化

CoPP で制御される速度より速くデータを転送するには、CoPP クラスに対するデフォルトのレート制限をディセーブルにし、デバイスでの最大許容値にレートを設定します。パケットは最大限の速度で CPU に送信されるようになりますが、これらのパケットを処理するレートは CPU 能力に依存します。データ転送後に、CoPP クラスに対するレート制限を再びイネーブルにする必要があります。



重要 CoPP クラスに対するレート制限がディセーブルにされていると、CPU が大量のトラフィックを受けやすい状態になります。

はじめる前に

CPU が保護されていること、および過剰な外部トラフィックがデバイスインターフェイス、スーパバイザ モジュールおよび CPU に送信されていないことを確認してください。

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	copp rate-limit disable 例： <pre>switch(config)# copp rate-limit disable</pre>	CPU に送信されるデフォルトの 1 秒あたりのパケット数をディセーブルにし、各キューで最大限のレートで CPU にパケットを送信できるようにします。 重要 このコマンドを実行すると、CoPP レート制限がすべてのクラスに対してディセーブルにされたことを通知する警告メッセージが表示されます。したがって、CPU はトラフィック攻撃を受けやすくなります。できるだけ早く no copp rate-limit disable コマンドを実行してください。
ステップ 3	show policy-map interface control-plane 例： <pre>switch(config)# show policy-map interface control-plane</pre>	(任意) 適用された CoPP ポリシーに含まれ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。
ステップ 4	no copp rate-limit disable 例： <pre>switch(config)# no copp rate-limit disable</pre>	各キューで CPU に送信されるパケットのレート制限をデフォルト値にリセットします。
ステップ 5	exit 例： <pre>switch(config)# exit</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。

CoPP 統計情報のクリア

手順

	コマンドまたはアクション	目的
ステップ 1	switch# show policy-map interface control-plane	(任意) 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。

次に、インターフェース環境で、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

IP ACL の作成

```
ip access-list copp-sample-acl
permit udp any any eq 3333
permit udp any any eq 4444
```

次に、着信パケットに適合する使用可能なトンネルが存在しない場合にすべての IP-in-IP (プロトコル 4) パケットを即座にドロップするように CoPP ポリシーを変更する例を示します。次の例に示すように、デフォルトの `copp-s-selfip` ポリシーの前に `copp-s-ipinip` を作成します。

```
ip access-list copp-s-ipinip
10 permit 4 any any
class-map type control-plane match-any copp-s-ipinip
match access-group name copp-s-ipinip
policy-map type control-plane copp-system-policy
class copp-s-ipinip
police pps 0
class copp-s-selfip
police pps 500
class copp-s-default
police pps 400
```

関連する IP ACL を使用したサンプル CoPP クラスの作成

次に、CoPP の新規クラスおよび関連する ACL を作成する例を示します。

```
class-map type control-plane copp-sample-class
match access-group name copp-sample-acl
次に、CoPP ポリシーにクラスを追加する例を示します。
policy-map type control-plane copp-system-policy
Class copp-sample-class
Police pps 100
```

次に、既存のクラス（copp-s-bpdu）の PPS を変更する例を示します。

```
policy-map type control-plane copp-system-policy
  Class copp-s-bpdu
  Police pps <new_pps_value>
```

ダイナミック クラス（IPv6 ACL）の作成

次に、IPv6 ACL を作成する例を示します

```
ipv6 access-list copp-system-acl-eigrp6
10 permit 88 any ff02::a/128
```

既存または新規の CoPP のクラスと ACL を関連付ける

次に、ACL を既存または新規の CoPP クラスに関連付ける例を示します。

```
class-map type control-plane copp-s-eigrp
match access-grp name copp-system-acl-eigrp6
```

CoPP ポリシーにクラスを追加

次に、クラスがまだ追加されていない場合に、CoPP ポリシーにクラスを追加する例を示します。

```
policy-map type control-plane copp-system-policy
class copp-s-eigrp
police pps 100
```

ARP ACL ベースのダイナミック クラスの作成

ARP ACL では ARP TCAM を使用します。この TCAM のデフォルト サイズは 0 です。ARP ACL を CoPP で使用するには、その前に、この TCAM をゼロ以外のサイズに切り分ける必要があります。

```
hardware profile tcam region arpacl 128
copy running-config startup-config
reload
```

ARP ACL の作成

```
arp access-list copp-arp-acl
permit ip 20.1.1.1 255.255.255.0 mac any
```

ARP ACL をクラスに関連付けて、CoPP ポリシーにそのクラスを追加する手順は、IP ACL の場合の手順と同じです。

CoPP クラスの作成と ARP ACL の関連付け

```
class-map type control-plane copp-sample-class
match access-group name copp-arp-acl
```

CoPP ポリシーからのクラスの削除

```
policy-map type control-plane copp-system-policy
  no class-abc
```

システムからのクラスの削除

```
no class-map type control-plane copp-abc
```


insert-before オプションを使用して、パケットが複数のクラスと一致するかどうか、およびいずれか1つのクラスに優先度を割り当てる必要があるかどうかを確認

```
policy-map type control-plan copp-system-policy
class copp-ping insert-before copp-icmp
```

CoPP の設定例

次に、ACL、クラス、ポリシー、および個別のクラス ポリシングの CoPP の設定例を示します。

```
IP access list copp-system-acl-eigrp
  10 permit eigrp any 224.0.0.10/32
IP access list copp-system-acl-icmp
  10 permit icmp any any
IP access list copp-system-acl-igmp
  10 permit igmp any any
IP access list copp-system-acl-ntp
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
IP access list copp-system-acl-pimreg
  10 permit pim any any
IP access list copp-system-acl-ping
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
IP access list copp-system-acl-routingprotol
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
  30 permit udp any 224.0.0.0/24 eq rip
  40 permit tcp any gt 1024 any eq 639
  50 permit tcp any eq 639 any gt 1024
  70 permit ospf any any
  80 permit ospf any 224.0.0.5/32
  90 permit ospf any 224.0.0.6/32
IP access list copp-system-acl-routingproto2
  10 permit udp any 224.0.0.0/24 eq 1985
  20 permit 112 any 224.0.0.0/24
IP access list copp-system-acl-snmpp
  10 permit udp any any eq snmp
  20 permit udp any any eq snmptrap
IP access list copp-system-acl-ssh
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
IP access list copp-system-acl-stftp
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
  50 permit tcp any any eq 115
  60 permit tcp any eq 115 any
IP access list copp-system-acl-tacacsradius
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
  30 permit udp any any eq 1812
  40 permit udp any any eq 1813
  50 permit udp any any eq 1645
  60 permit udp any any eq 1646
  70 permit udp any eq 1812 any
  80 permit udp any eq 1813 any
  90 permit udp any eq 1645 any
  100 permit udp any eq 1646 any
IP access list copp-system-acl-telnet
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
IP access list copp-system-dhcp-relay
  10 permit udp any eq bootps any eq bootps
IP access list test
```

```

statistics per-entry
10 permit ip 1.2.3.4/32 5.6.7.8/32 [match=0]
20 permit udp 11.22.33.44/32 any [match=0]
30 deny udp 1.1.1.1/32 any [match=0]

IPv6 access list copp-system-acl-dhccp6
 10 permit udp any any eq 546
IPv6 access list copp-system-acl-dhcps6
 10 permit udp any ff02::1:2/128 eq 547
 20 permit udp any ff05::1:3/128 eq 547
IPv6 access list copp-system-acl-eigrp6
 10 permit 88 any ff02::a/128
IPv6 access list copp-system-acl-v6routingProto2
 10 permit udp any ff02::66/128 eq 2029
 20 permit udp any ff02::fb/128 eq 5353
IPv6 access list copp-system-acl-v6routingproto1
 10 permit 89 any ff02::5/128
 20 permit 89 any ff02::6/128
 30 permit udp any ff02::9/128 eq 521

class-map type control-plane match-any copp-icmp
 match access-group name copp-system-acl-icmp
class-map type control-plane match-any copp-ntp
 match access-group name copp-system-acl-ntp
class-map type control-plane match-any copp-s-arp
class-map type control-plane match-any copp-s-bfd
class-map type control-plane match-any copp-s-bpdu
class-map type control-plane match-any copp-s-dai
class-map type control-plane match-any copp-s-default
class-map type control-plane match-any copp-s-dhccpreq
 match access-group name copp-system-acl-dhcps6
class-map type control-plane match-any copp-s-dhccpresp
 match access-group name copp-system-acl-dhccp6
 match access-group name copp-system-dhcp-relay
class-map type control-plane match-any copp-s-eigrp
 match access-group name copp-system-acl-eigrp
 match access-group name copp-system-acl-eigrp6
class-map type control-plane match-any copp-s-glean
class-map type control-plane match-any copp-s-igmp
 match access-group name copp-system-acl-igmp
class-map type control-plane match-any copp-s-ipmcmis
class-map type control-plane match-any copp-s-l2switched
class-map type control-plane match-any copp-s-l3destmiss
class-map type control-plane match-any copp-s-l3mtufail
class-map type control-plane match-any copp-s-l3slowpath
class-map type control-plane match-any copp-s-pimautorp
class-map type control-plane match-any copp-s-pimreg
 match access-group name copp-system-acl-pimreg
class-map type control-plane match-any copp-s-ping
 match access-group name copp-system-acl-ping
class-map type control-plane match-any copp-s-ntp
class-map type control-plane match-any copp-s-routingProto1
 match access-group name copp-system-acl-routingproto1
 match access-group name copp-system-acl-v6routingproto1
class-map type control-plane match-any copp-s-routingProto2
 match access-group name copp-system-acl-routingproto2
class-map type control-plane match-any copp-s-selfIp
class-map type control-plane match-any copp-s-ttl1
class-map type control-plane match-any copp-s-v6routingProto2
 match access-group name copp-system-acl-v6routingProto2
class-map type control-plane match-any copp-s-nmp
 match access-group name copp-system-acl-nmp
class-map type control-plane match-any copp-s-sh
 match access-group name copp-system-acl-sh
class-map type control-plane match-any copp-s-tftp
 match access-group name copp-system-acl-tftp
class-map type control-plane match-any copp-tacacsradius
 match access-group name copp-system-acl-tacacsradius
class-map type control-plane match-any copp-telnet
 match access-group name copp-system-acl-telnet
policy-map type control-plane copp-system-policy
 class copp-s-selfIp
  police pps 500

```

```
class copp-s-default
  police pps 400
class copp-s-l2switched
  police pps 200
class copp-s-ping
  police pps 100
class copp-s-l3destmiss
  police pps 100
class copp-s-glean
  police pps 500
class copp-s-l3mtufail
  police pps 100
class copp-s-ttl1
  police pps 100
class copp-s-ipmcmis
  police pps 400
class copp-s-l3slowpath
  police pps 100
class copp-s-dhcpreq
  police pps 300
class copp-s-dhcpresp
  police pps 300
class copp-s-dai
  police pps 300
class copp-s-igmp
  police pps 400
class copp-s-routingProto2
  police pps 1300
class copp-s-v6routingProto2
  police pps 1300
class copp-s-eigrp
  police pps 200
class copp-s-pimreg
  police pps 200
class copp-s-pimautorp
  police pps 200
class copp-s-routingProto1
  police pps 1000
class copp-s-arp
  police pps 200
class copp-s-ntp
  police pps 1000
class copp-s-bfd
  police pps 350
class copp-s-bpdu
  police pps 12000
class copp-icmp
  police pps 200
class copp-telnet
  police pps 500
class copp-ssh
  police pps 500
class copp-snmp
  police pps 500
class copp-ntp
  police pps 100
class copp-tacacsradius
  police pps 400
class copp-stftp
  police pps 400
control-plane
  service-policy input copp-system-policy
```

例：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、デフォルト CoPP ポリシーを変更または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

  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 : switch

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

  Configure the default gateway for mgmt? (yes/no) [y]: n

  Enable the telnet service? (yes/no) [n]: y

  Enable the ssh service? (yes/no) [y]: n

  Configure the ntp server? (yes/no) [n]: n

  Configure CoPP System Policy Profile ( default / 12 / 13 ) [default]: 12

The following configuration will be applied:
  switchname switch
  telnet server enable
  no ssh server enable
  policy-map type control-plane copp-system-policy ( 12 )

Would you like to edit the configuration? (yes/no) [n]: n

Use this configuration and save it? (yes/no) [y]: y

[#####] 100%
```

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 Licensing Guide』
コマンドリファレンス	

