Cisco Nexus 3548 スイッチ NX-OS リリース 10.3(x)セキュリティ構成ガイド

初版：2022 年 8 月 19 日

最終更新：2023 年 1 月 9 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。

目 次

はじめに

ここでは、次の内容について説明します。

対象読者

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

表記法

コマンドの説明には、次のような表記法が使用されます。

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

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

例では、次の表記法を使用しています。

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

Cisco Nexus 3000 シリーズ スイッチの関連資料

Cisco Nexus 3000 シリーズ スイッチ全体のマニュアル セットは、次の URL にあります。

https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html

マニュアルに関するフィードバック

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

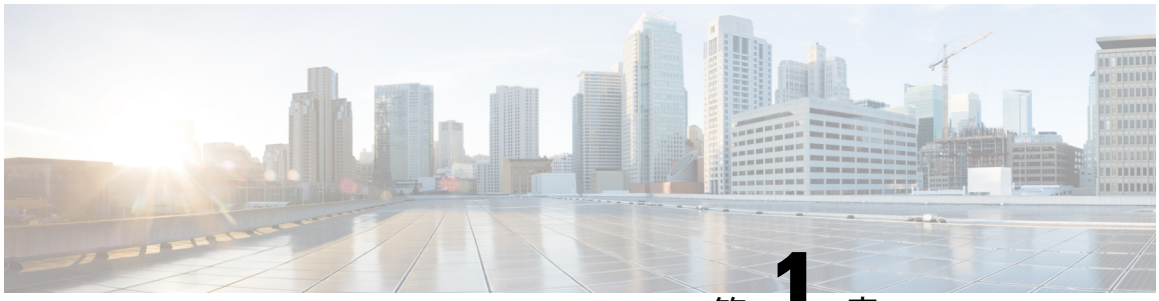
通信、サービス、およびその他の情報

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

Cisco バグ検索ツール

Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

通信、サービス、およびその他の情報



第 1 章

新規および変更情報

この章では、*[Cisco Nexus 3548* スイッチ *NX-OS* セキュリティ ガイド（*Cisco Nexus 3548 Switch NX-OS Security Guide*）*]*に記載されている、新機能および変更された機能に関するリリース固有の情報について説明します。

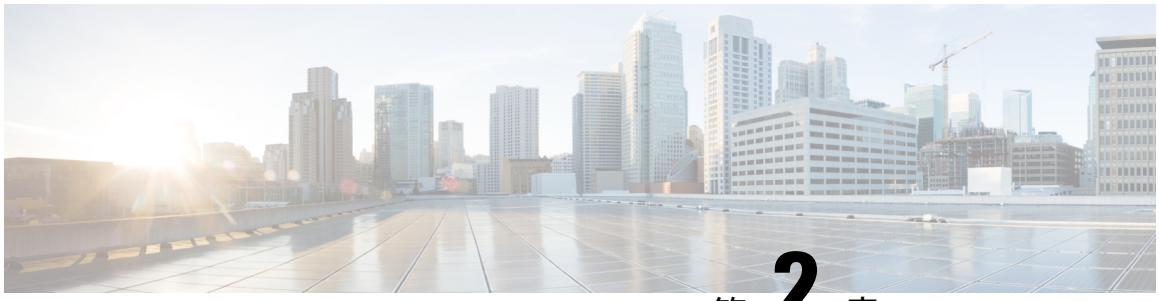
新規および変更情報

次の表では、このコンフィギュレーション ガイドでの重要な変更点の概要を示します。この表は、このマニュアルに加えられた変更や特定のリリースの新しい機能をすべて網羅するものではありません。

表 *1 : NX-OS* リリース *10.3(x)* の新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
NA	このリリースで追加された新機能はありません。	10.3(1)F	該当なし

新規および変更情報



第 2 章

概要

この章は、次の項で構成されています。

ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

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

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

認証

ログイン/パスワードダイアログ、チャレンジ/レスポンス、メッセージングサポート、および暗号化（選択したセキュリティプロトコルに基づく）などによるユーザの識別方法を提供します。認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。AAA 認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種インターフェイスに適用します。

許可

ワン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ァイル、ユーザ グループ サポート、およびIP、IPX、ARA、Telnet のサポートなど、リモートアクセスの制御方法を提供します。

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

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

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

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+ デー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。

SSH および Telnet

セキュア シェル（SSH）サーバーを使用すると、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

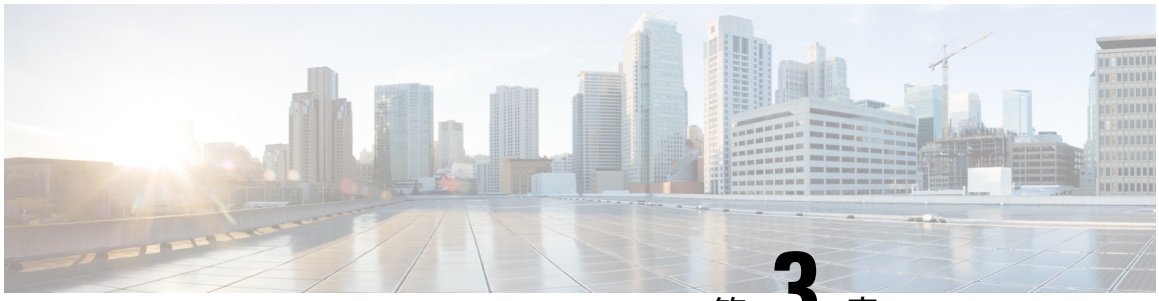
ます。Cisco NX-OS ソフトウェアの SSH サーバーは、市販の一般的な SSH クライアントと相互運用ができます。

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。

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。



第 3 章

認証、許可、アカウンティングの設定

この章は、次の項で構成されています。

AAA の概要

AAA セキュリティ サービス

認証、許可、アカウンティング（AAA）機能では、Cisco Nexus デバイスを管理するユーザーの 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。

ユーザーが入力したユーザー 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 サーバー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 サーバー間の通信は、事前共有秘密キーによって保護されます。すべての AAA サーバ用または特定の AAA サーバ専用に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：ユーザーを識別します。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 サーバー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 サーバーは、適切なユーザー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、ユーザー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ギング、および AAA サーバーへの情報の送信の方式を提供します。

Note Cisco NX-OS ソフトウェアは、認証、許可、アカウン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ー パスワード リストを簡単に管理できます。
- AAA サーバー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ー属性は管理が簡単です。

AAA サーバグループ

認証、許可、アカウンティングのためのリモート AAA サーバは、サーバ グループを使用して指定できます。サーバー 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 サーバーです。リモート AAA サーバーが応答しなかった場合、サーバー グループは、フェールオーバー サーバーを提供します。グループ内の最初のリモート サーバーが応答しなかった場合、いずれかのサーバーが応答を送信するまで、グループ内の次のリモート サーバーで試行

が行われます。サーバー グループ内のすべての AAA サーバーが応答しなかった場合、そのサーバー 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、複数のサーバー 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ーからエラーを受信すると、次のサーバー グループのサーバーが試行されます。

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
- ユーザー管理セッション アカウンティング

次の表に、AAA サービス設定オプションの CLI コマンドを示します。

***Table 2: 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**
ユーザー セッション アカウンティング	**aaa accounting default**

AAA サービスには、次の認証方式を指定できます。

- RADIUS サーバー グループ：RADIUS サーバーのグローバル プールを認証に使用します。
- 特定のサーバー グループ：指定した RADIUS または TACACS+ サーバー グループを認証に使用します。
- ローカル：ユーザー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：ユーザー名だけを使用します。

Note 方式がすべて RADIUS サーバーになっており、特定のサーバー 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 サーバーのグローバル プールから、設定された順序で RADIUS サーバーを選択します。このグローバル プールからのサーバーは、Cisco Nexus デバイス上の RADIUS サーバー グループ内で選択的に設定できるサーバーです。

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。

Table 3: 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
ユーザー ログイン認証	サーバ グループ、ローカル、なし
ユーザー管理セッション アカウンティング	サーバ グループ、ローカル

Note コンソール ログイン認証、ユーザー ログイン認証、およびユーザー管理セッション 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。

ユーザー ログインの認証および許可プロセス

ユーザー 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。
- サーバー グループ認証方式を使用して AAA サーバー 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 サーバーに認証要求を送信し、次のように処理されます。

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

  サーバー グループのすべての AAA サーバーが応答しなかった場合、その次のサーバー グループのサーバーが試行されます。

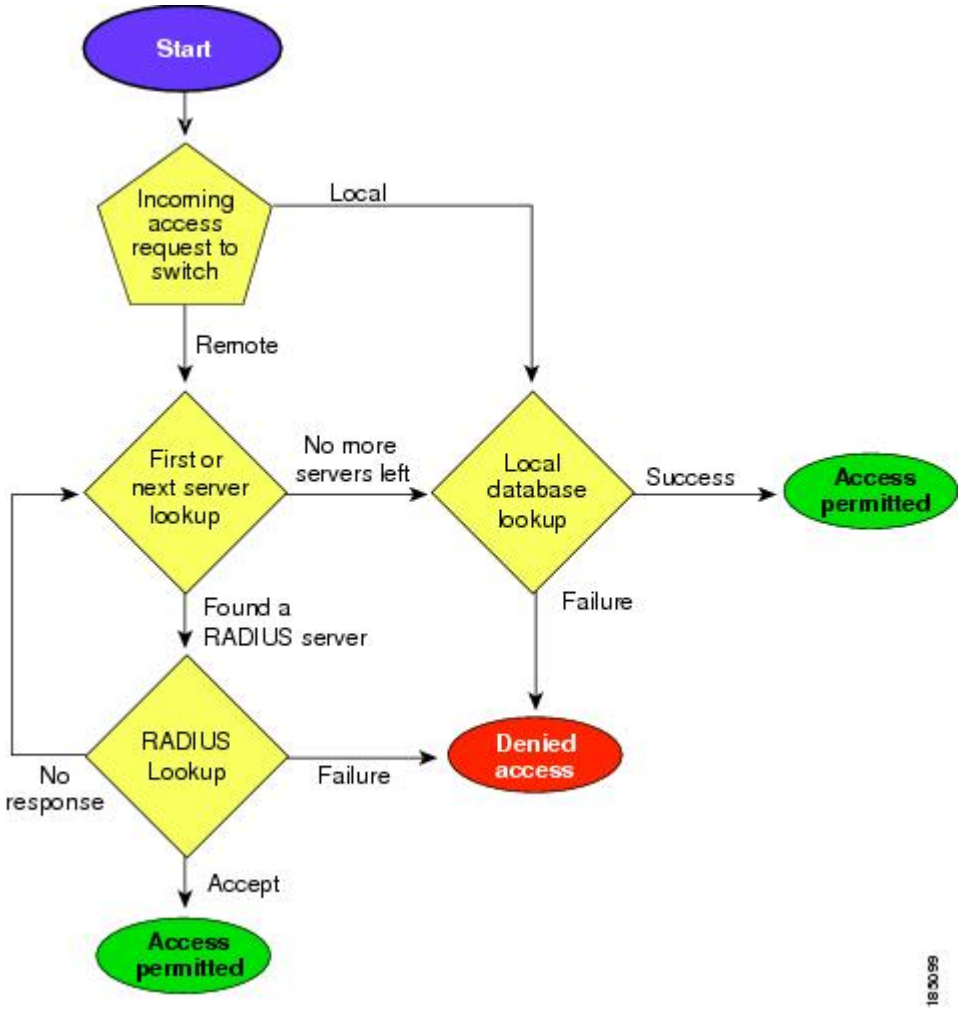
  設定されているすべての認証方式が失敗した場合、ローカル データベースを使用して認証が実行されます。
- Cisco Nexus デバイスがリモート AAA サーバーで正常に認証できた場合は、次の条件が適用されます。

  AAA サーバー 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ー ロールが認証応答とともにダウンロードされます。

  AAA サーバー 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ー ロールを取得するために、もう 1 つの要求が同じサーバーに送信されます。
- ユーザー名とパスワードがローカルで正常に認証された場合は、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。

Figure 1: ユーザー ログインの認証および許可のフロー



この図に示されている「残りのサーバーなし」とは、現在のサーバー グループ内のいずれのサーバー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 サーバーまたは TACACS+ サーバーが、IP で到達可能であること。
- Cisco Nexus デバイスが AAA サーバー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 サーバー上で設定されている。

- リモート サーバーが 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

そのユーザー名が 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ー名はサポートされません。AAA サーバーに数字だけのユーザー名が存在し、ログイン時にその名前を入力した場合でも、ユーザーは 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ー名でユーザー 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 サーバーまたは TACACS+ サーバー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
- ユーザー名だけ **none**

デフォルトの方式は、ローカルです。

Note 事前に設定されている一連の RADIUS サーバーに関しては、**aaa authentication** コマンドの **group radius** 形式および **group** *server-name* 形式を使用します。ホスト サーバーを設定するには、radius server-host コマンドを使用します。サーバー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+ サーバー グループを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 2	switch(config)# **aaa authentication login console** { **group** *group-list* [**none**] | **local** | **none**}	コンソールのログイン認証方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius** RADIUS サーバーのグローバル プールを使用して認証を行います。 • *named-group* を指定すると、TACACS+ サーバーまたは RADIUS サーバーの名前付きサブセットが認証に使用されます。 **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、ユーザー名だけが使用されます。 デフォルトのコンソール ログイン方式は、 **local** です。これは認証方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られなかった場合に使用されます。
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	(Optional) switch# **show aaa authentication**	コンソール ログイン認証方式の設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

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+サーバー グループを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login default** { **group** *group-list* [**none**] | **local** | **none**}	デフォルト認証方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius** RADIUS サーバーのグローバル プールを使用して認証を行います。 • *named-group* を指定すると、TACACS+ サーバーまたは RADIUS サーバーの名前付きサブセットが認証に使用されます。 **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、ユーザー名だけが使用されます。 デフォルトのログイン方式は **local** です。この方式は、方式が一切設定されていない場合、または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。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	(Optional) switch# **show aaa authentication**	デフォルトのログイン認証方式の設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

ログイン認証失敗メッセージの有効化

ユーザーがログインして、リモート AAA サーバーが応答しなかった場合は、ローカル ユーザー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た場合は、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.
```

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login error-enable**	ログイン認証失敗メッセージを有効にします。デフォルトでは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	(Optional) switch# **show aaa authentication**	ログイン失敗メッセージの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

AAA コマンド許可の設定

TACACS+ サーバーの許可方式が設定されている場合は、ユーザーが TACACS+ サーバー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+ サーバー 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 セッションでの許可は、Cisco Nexus 5000 プラットフォームではサポートされていません。Cisco Nexus 5500 プラットフォーム、リリース 6.x 以降ではサポートされています。

始める前に

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**} {{[**group** *group-name*] | [**local**]} | {[**group** *group-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。

例

次に、TACACS+ サーバー 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+ サーバー 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+ サーバー 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。

- サーバーが到達可能である場合、コマンドはサーバー応答に基づいて許可され、または許可されません。
- サーバーに到達する際にエラーが生じた場合、コマンドはユーザーのローカル 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+ サーバー 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。

- サーバーが到達可能である場合、コマンドはサーバー応答に基づいて許可され、または許可されません。
- サーバー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 ハンドシェーク認証プロトコル（MSCHAP）は、マイクロソフト版の CHAP です。リモート認証サーバー（RADIUS または TACACS+）を通じて、Cisco Nexus デバイスへのユーザー 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 サーバー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 サーバーを設定する必要があります。

次の表に、MSCHAP に必要な RADIUS VSA を示します。

Table 4: 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 サーバーから MSCHAP ユーザー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 ユーザー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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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	(Optional) switch# **show aaa authentication login mschap**	MS-CHAP 設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

デフォルトの AAA アカウンティング方式の設定

Cisco Nexus デバイスは、アカウンティングに TACACS+ 方式と RADIUS 方式をサポートします。スイッチは、ユーザー アクティビティをアカウンティング レコードの形で TACACS+ セキュリティ サーバーまたは RADIUS セキュリティ サーバーに報告します。各アカウンティング レコードに、アカウンティング属性値（AV）のペアが入っており、それが AAA サーバーに格納されます。

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

特定のアカウンティング方式を定義するデフォルト方式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 サーバー グループ：RADIUS サーバーのグローバル プールをアカウンティングに使用します。
- 特定のサーバー グループ：指定した RADIUS または TACACS+ サーバー グループをアカウンティングに使用します。
- ローカル：ユーザー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ティングに使用します。

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

Before you begin

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

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa accounting default** { **group** *group-list* | **local**}	デフォルトのアカウンティ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ー グループ名を指定できます。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius** RADIUS サーバーのグローバル プールを使用してアカウンティングを行います。 • *named-group* を指定すると、TACACS+ サーバーまたは RADIUS サーバーの名前付きサブセットがアカウンティングに使用されます。 **local** 方式はローカル データベースを使用してアカウンティングを行います。 デフォルトの方式は **local** です。サーバー 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ー グループから応答がないときに、このデフォルトの方式が使用されます。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	(Optional) switch# **show aaa accounting**	デフォルトの AAA アカウンティング方式の設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

No Service Password-Recovery について

No Service Password-Recovery 機能により、コンソールへのアクセスを持つ誰もがルータおよびルータのネットワークにアクセスする機能を与えられることになります。No Service Password-Recovery 機能を使用すると、『Cisco Nexus 9000 Series NX-OS Troubleshooting Guide』に記載されている標準的な手順でパスワードを回復できなくなります。

No Service Password-Recovery のイネーブル化

No Service Password-Recovery 機能が有効になっている場合、ネットワーク権限を持つ管理者以外は管理者パスワードを変更できません。

始める前に

no service password-recovery コマンドを開始する場合、シスコでは、デバイスから離れた場所にシステム コンフィギュレーション ファイルのコピーを保存することを推奨しています。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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 service password-recovery**
	例：
	`switch(config)# no service password-recovery`
	`WARNING: Executing this command will disable the password recovery mechanism. Do not execute this command without another plan for password recovery. Are you sure you want to continue? (y/n) : [y] y`
	`switch(config)# copy run start`
	`[########################################] 100%`
	`Copy complete, now saving to disk (please wait)...`
	`Copy complete.`
		パスワード回復メカニズムを無効にします。

ステップ 3	（任意） **copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 4	**Reload**	

	コマンドまたはアクション	目的

	例：
	`switch(config)# Reload`
	`This command will reboot the system. (y/n)?  [n] y`
	`2018 Jun 26 16:23:19 BAR %$ VDC-1 %$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface`
	
	`CISCO SWITCH Ver 8.34`
	
	`CISCO SWITCH Ver 8.34`
	`Manual system restart from Command Line Interface`
	`writing reset reason 9,`
	`..`
	`..`
	
	`switch(boot)# config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`switch(boot)(config)# admin-password Abcd!123$`
	`ERROR: service password-recovery disabled. Cannot change password!`
	`switch(boot)(config)#`	

ステップ 5	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 6	（任意） **show user-account** 例： `switch# show user-account`	ロール設定を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

AAA サーバーの VSA の使用

VSA

ベンダー固有属性（VSA）を使用して、AAA サーバー上でのCisco Nexus デバイスのユーザー 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 サーバーを使用する場合は、認証結果とともに許可情報などのユーザー属性を返すよう、RADIUS プロトコルが RADIUS サーバーに指示します。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：ユーザー 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：ユーザー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 サーバー上でのスイッチのユーザー ロールと SNMPv3 パラメータの指定

AAA サーバーで VSA cisco-av-pair を使用して、次の形式で、Cisco Nexus デバイスのユーザー 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ー ロールは、network-operator です。

Note Cisco Unified Wireless Network TACACS+ 設定と、ユーザー 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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show accounting log** [*size*] [**start-time** *year month day hh* **:** *mm* **:** *ss*]	アカウンティング ログを表示します。このコマンド出力には、デフォルトで最大 250,000 バイトのアカウンティング ログが表示されます。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	(Optional) switch# **clear accounting log**	アカウンティング 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。

コマンド	目的
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。

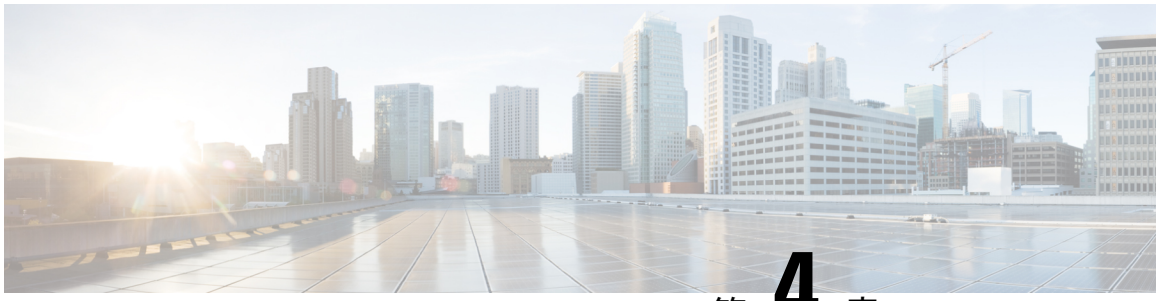
```
switch(config)# aaa authentication login default group radius
switch(config)# aaa authentication login console group radius
switch(config)# aaa accounting default group radius
```

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。

Table 5: 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	ローカル
デフォルト認証方式	ローカル
ログイン認証失敗メッセージ	ディセーブル
MSCHAP 認証	ディセーブル
デフォルト アカウンティング方式	ローカル
アカウンティング ログの表示サイズ	250 KB



第 4 章

802.1X の設定

この章では、Cisco NX-OS デバイス上で IEEE 802.1X ポートベースの認証を構成する手順について説明します。また、次のセクションを含みます：

802.1X について

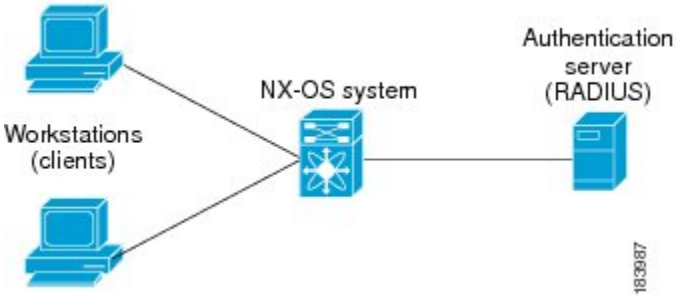
802.1X では、クライアント サーバ ベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、Cisco NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

デバイスのロール

802.1X ポート ベースの認証では、ネットワーク上のデバイスにそれぞれ特定のロールがあります。

図 *2 : 802.1X* デバイスのロール



特定のロールは次のとおりです。

[サプリカント（Suppliccant）]

LAN および Cisco NX-OS デバイス サービスへのアクセスを要求し、Cisco NX-OS デバイスからの要求に応答するクライアント デバイスです。ワークステーションでは、Microsoft Windows XP が動作するデバイスで提供されるような、802.1X 準拠のクライアント ソフトウェアが稼働している必要があります。

[認証サーバ（Authentication server）]

サプリカントの実際の認証を行います。認証サーバはサプリカントの識別情報を確認し、LAN および Cisco NX-OS デバイスのサービスへのアクセスをサプリカントに許可すべきかどうかを Cisco NX-OS デバイスに通知します。Cisco NX-OS デバイスはプロキシとして動作するので、認証サービスはサプリカントに対しては透過的に行われます。認証サーバとして、拡張認証プロトコル（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティ デバイスだけがサポートされています。この認証サーバは、Cisco Secure Access Control Server バージョン 3.0 で使用可能です。RADIUS はサプリカント サーバ モデルを使用し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。

[オーセンティケータ（Authenticator）]

サプリカントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。オーセンティケータは、サプリカントと認証サーバとの仲介デバイス（プロキシ）として動作し、サプリカントから識別情報を要求し、得られた識別情報を認証サーバに確認し、サプリカントに応答をリレーします。オーセンティケータには、EAP フレームのカプセル化/カプセル化解除、および認証サーバとの対話を処理する、RADIUS クライアントが含まれています。

オーセンティケータが EAPOL フレームを受信して認証サーバにリレーする際は、イーサネット ヘッダーを取り除き、残りの EAP フレームを RADIUS 形式にカプセル化します。このカプセル化のプロセスでは EAP フレームの変更または確認が行われないため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートする必要があります。オーセンティケータは認証サーバからフレームを受信すると、サーバのフレーム ヘッダーを削除し、残りの EAP フレームをイーサネット用にカプセル化してサプリカントに送信します。

Cisco NX-OS デバイスがなれるのは、802.1X オーセンティケータだけです。

認証の開始およびメッセージ交換

オーセンティケータ（Cisco NX-OS デバイス）とサプリカント（クライアント）のどちらも認証を開始できます。ポート上で認証をイネーブルにした場合、オーセンティケータはポートのリンク ステートがダウンからアップに移行した時点で、認証を開始する必要があります。続いて、オーセンティケータは EAP-Request/Identity フレームをサプリカントに送信して識別情報を要求します（通常、オーセンティケータは 1 つまたは複数の識別情報の要求のあとに、最初の Identity/Request フレームを送信します）。サプリカントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

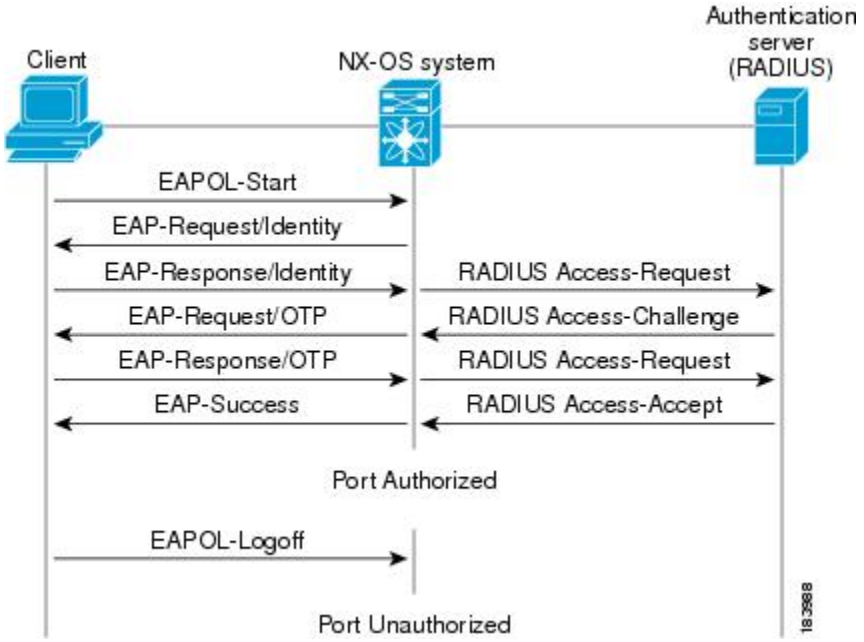
サプリカントがブートアップ時にオーセンティケータから EAP-Request/Identity フレームを受信しなかった場合、サプリカントは EAPOL 開始フレームを送信することにより認証を開始することができます。この開始フレームにより、オーセンティケータはサプリカントの識別情報を要求します。

ネットワーク アクセス デバイスで 802.1X がイネーブルになっていない場合、またはサポートされていない場合、Cisco NX-OS デバイスはサプリカントからの EAPOL フレームをすべてドロップします。サプリカントが、認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、サプリカントはポートが許可ステートにあるものとしてデータを送信します。ポートが許可ステートになっている場合は、サプリカントの認証が成功したことを意味します。

サプリカントが自己の識別情報を提示すると、オーセンティケータは仲介装置としてのロールを開始し、認証が成功または失敗するまで、サプリカントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、オーセンティケータのポートは許可ステートになります。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。

図 *3:* メッセージ交換



ユーザのシークレットパスフレーズは、認証時やパスフレーズの変更時などにネットワークを通過することはありません。

インターフェイスのオーセンティケータ PAE ステータス

インターフェイスで 802.1X をイネーブルにすると、Cisco NX-OS ソフトウェアにより、オーセンティケータ Port Access Entity（PAE）インスタンスが作成されます。オーセンティケータ PAE は、インターフェイスでの認証をサポートするプロトコル エンティティです。インターフェイスで 802.1X をディセーブルにしても、オーセンティケータ PAE インスタンスは自動的にクリアされません。必要に応じ、オーセンティケータ PAE をインターフェイスから明示的に削除し、再度適用することができます。

許可ステートおよび無許可ステートのポート

サプリカントのネットワークへのアクセスが許可されるかどうかは、オーセンティケータのポート ステートで決まります。ポートは、無許可ステートで開始します。このステートにあるポートは、802.1X プロトコル パケットを除いたすべての入トラフィックおよび出トラフィックを禁止します。サプリカントの認証に成功すると、ポートは許可ステートに移行し、サプリカントのすべてのトラフィック送受信を通常どおりに許可します。

802.1X 認証をサポートしていないクライアントが無許可ステートの 802.1X ポートに接続した場合、オーセンティケータはクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x 対応のクライアントが、802.1x プロトコルの稼働していないポートに接続すると、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

ポートには次の許可ステートがあります。

Force authorized
802.1X ポートベースの認証をディセーブルにし、認証情報の交換を必要としないで許可ステートに移行します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。この許可ステートはデフォルトです。

Force unauthorized
ポートが無許可ステートのままになり、クライアントからの認証の試みをすべて無視します。オーセンティケータは、インターフェイスを経由してクライアントに認証サービスを提供することができません。

Auto
802.1X ポートベースの認証をイネーブルにします。ポートは無許可ステートで開始し、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに移行したとき、またはサプリカントから EAPOL 開始フレームを受信したときに、認証プロセスが開始します。オーセンティケータは、クライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。オーセンティケータはサプリカントの MAC アドレスを使用して、ネットワーク アクセスを試みる各サプリカントを一意に識別します。

サプリカントの認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたサプリカントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできます。認証サーバに到達できない場合、オーセンティケータは要求を再送信できます。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、サプリカントのネットワーク アクセスは認可されません。

サプリカントはログオフするとき、EAPOL ログオフ メッセージを送信します。このメッセージによって、オーセンティケータのポートは無許可ステートに移行します。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL ログオフ フレームを受信した場合、ポートは無許可ステートに戻ります。

MAC 認証バイパス

MAC 認証バイパス機能を使用して、サプリカントの MAC アドレスに基づいてサプリカントを認証するように、Cisco NX-OS デバイスを設定できます。たとえば、プリンタなどのデバイスに接続されている 802.1X 機能を設定したインターフェイスで、この機能をイネーブルにすることができます。

サプリカントからの EAPOL 応答を待機している間に 802.1X 認証がタイムアウトした場合は、MAC 認証バイパスを使用して Cisco NX-OS デバイスはクライアントの許可を試みます。

インターフェイスで MAC 認証バイパス機能をイネーブルにすると、Cisco NX-OS デバイスは MAC アドレスをサプリカント ID として使用します。認証サーバには、ネットワーク アクセ

スが許可されたサプリカントの MAC アドレスのデータベースがあります。Cisco NX-OS デバイスは、インターフェイスでクライアントを検出した後、クライアントからのイーサネット パケットを待ちます。Cisco NX-OS デバイスは、MAC アドレスに基づいてユーザ名とパスワードを含んだRADIUSアクセス/要求フレームを認証サーバに送信します。許可に成功した場合、Cisco NX-OS デバイスはクライアントにネットワークへのアクセスを許可します。

リンクのライフタイム中に EAPOL パケットがインターフェイスで検出される場合、このインターフェイスに接続されているデバイスが 802.1X 対応サプリカントであることを Cisco NX-OS デバイスが判別し、（MAC 認証バイパスではなく）802.1X 認証を使用してインターフェイスを許可します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

Cisco NX-OS デバイスがすでに MAC 認証バイパスを使用してインターフェイスを許可していて、802.1X サプリカントを検出した場合、Cisco NX-OS デバイスはインターフェイスに接続されているクライアントを無許可にしません。再認証を実行する際に、Cisco NX-OS デバイスは 802.1X 認証を優先再認証プロセスとして使用します。

MAC 認証バイパスで許可されたクライアントを再認証することができます。再認証プロセスは、802.1X で認証されたクライアントと同様です。再認証中に、ポートは前に割り当てられた VLAN に残ります。再認証に成功した場合、スイッチはポートを同じ VLAN 内に保持します。

再認証が Session-Timeout RADIUS 属性（Attribute [27]）と Termination-Action RADIUS 属性（Attribute [29]）に基づいていて、Termination-Action RADIUS 属性（Attribute [29]）アクションが初期化の場合、（属性値は DEFAULT）、MAC 認証バイパス セッションが終了して、再認証中に接続が失われます。MAC 認証バイパスがイネーブルで 802.1X 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再許可を開始します。これらの AV ペアの詳細については、RFC 3580「IEEE 802.1X リモート認証ダイヤル イン ユーザ サービス（RADIUS）使用ガイドライン」を参照してください。

MAC 認証バイパスは、次の機能と相互作用します。

802.1X 認証：802.1X 認証がポートでイネーブルの場合にだけ、MAC 認証バイパスをイネーブルにできます。

ポート セキュリティ：この機能は、Nexus 3548 プラットフォーム スイッチではサポートされていません。

Network Admission Control（NAC）レイヤ 2 IP 検証：例外リスト内のホストを含む 802.1X ポートが MAC 認証バイパスで認証されたあとに、この機能が有効になります。

MAC-Based Authentication（MAB）に基づくダイナミック VLAN 割り当て

Cisco Nexus 3548 シリーズ スイッチはダイナミック VLAN 割り当てをサポートします。802.1X 認証またはMABが完了した後。ポートを起動する前に、認証の結果としてピア/ホストを特定のVLANに配置できるようにすることができます（許可の一部として）。RADIUS サーバは、一般的に Access-Accept 内にトンネル属性を含めることによって目的の VLAN を示します。VLAN をポートにバインドするこの手順は、ダイナミック VLAN 割り当てを構成します。

RADIUS からの VLAN 割り当て

dot1x または MAB によって認証が完了すると、RADIUS サーバからの応答にダイナミック VLAN 情報を含むことができるようになり、これをポートに割り当てることができます。この情報は、トンネル属性の形式の受け入れアクセス メッセージの RADIUS サーバからの応答に存在します。VLAN 割り当てのために、次のトンネル属性が送信されます。

Tunnel-type=VLAN(13)

Tunnel-Medium-Type=802

Tunnel-Private-Group-ID=VLANID

アクセス VLAN の設定のために、3 つのパラメータをすべて受け取る必要があります。

シングル ホストおよびマルチ ホストのサポート

802.1X 機能では、1 つのポートのトラフィックを 1 台のエンドポイント装置に限定することも（シングル ホスト モード）、1 つのポートのトラフィックを複数のエンドポイント装置に許可することも（マルチ ホスト モード）できます。

シングル ホスト モードでは、802.1X ポートで 1 台のエンドポイント装置のみからのトラフィックが許可されます。エンドポイント装置が認証されると、Cisco NX-OS デバイスはポートを許可ステートにします。エンドポイント装置がログオフすると、Cisco NX-OS デバイスはポートを無許可ステートに戻します。802.1X のセキュリティ違反とは、認証に成功して許可された単一の MAC アドレスとは異なる MAC アドレスをソースとするフレームが検出された場合をいいます。このような場合、このセキュリティ アソシエーション（SA）違反（他の MAC アドレスからの EAPOL フレーム）が検出されたインターフェイスはディセーブルにされます。シングル ホスト モードは、ホストツースイッチ型トポロジで 1 台のホストが Cisco NX-OS デバイスのレイヤ 2 ポート（イーサネット アクセス ポート）またはレイヤ 3 ポート（ルーテッド ポート）に接続されている場合にだけ適用できます。

マルチ ホスト モードに設定されている 802.1X ポートで、認証が必要になるのは最初のホストだけです。最初のホストの許可に成功すると、ポートは許可ステートに移行します。ポートが許可ステートになると、後続のホストがネットワーク アクセスの許可を受ける必要はありません。再認証に失敗したり、または EAPOL ログオフ メッセージを受信して、ポートが無許可ステートになった場合には、接続しているすべてのクライアントはネットワーク アクセスを拒否されます。マルチ ホスト モードでは、SA 違反の発生時にインターフェイスをシャットダウンする機能がディセーブルになります。マルチ ホスト モードは、スイッチツースイッチ型トポロジおよびホストツースイッチ型トポロジの両方に適用できます。

サポートされるトポロジ

802.1X ポートベースの認証は、ポイントツーポイント トポロジをサポートします。

この設定では、802.1X 対応のオーセンティケータ（Cisco NX-OS デバイス）ポートにサプリカント（クライアント）を 1 台だけ接続することができます。オーセンティケータは、ポートのリンク ステートがアップ ステートに移行したときにサプリカントを検出します。サプリカン

トがログオフしたとき、または別のサプリカントに代わったときには、オーセンティケータはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

802.1X 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。

表 *6:* ライセンス要件

製品	ライセンス要件
Cisco NX-OS	802.1X に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。

802.1x の注意事項と制約事項

802.1X ポートベースの認証には、次の設定に関する注意事項と制約事項があります。

- 802.1X ポートでマルチ認証モードが有効になります。VLAN の割り当ては、最初の認証済みホストに対し行われます。ユーザ クレデンシャルに基づいてその後に許可されたデータ ホストは、正しく認証されたと見なされます。ただし、まだ VLAN が割り当てられていないか、ポートで最初に正しく認証されたホストと一致する VLAN 割り当てがなされていることを条件とします。これにより、ポートで正常に認証されたすべてのホストは、確実に同じ VLAN メンバになります。VLAN 割り当ての柔軟性は、最初に認証されたホストだけで生じます。
- Cisco Nexus シリーズ スイッチは、以下のものについては、802.1X をサポートしていません。
  - 40G インターフェイス
  - トランジット トポロジの設定
  - VPC ポート
  - PVLAN ポート
  - L3（ルーテッド）ポート
  - ポート セキュリティ
  - CTS および MACsec が有効になっているポート。
  - Dot1x と LACP ポートチャネル
  - VPC ポートおよびサポートされていないすべての機能では、802.1X は無効になります

- Cisco NX-OS ソフトウェアが 802.1X 認証をサポートするのは、物理ポート上だけです。
- Cisco NX-OS ソフトウェアは、ポート チャネルまたはサブインターフェイスでは 802.1X 認証をサポートしません。
- Cisco NX-OS ソフトウェアは、ポート チャネルのメンバ ポートでは 802.1X 認証をサポートしますが、ポート チャネル自体ではサポートしません。
- メンバーが 802.1X 用に設定されている場合、Cisco NX-OS ソフトウェアは、ポート チャネル メンバーでのシングルホスト モードの設定をサポートしません。メンバ ポートではマルチ ホスト モードだけがサポートされます。
- 802.1X 設定を含むメンバ ポートと含まないメンバ ポートはポート チャネルで共存できます。ただし、チャネリングと 802.1X が連携して動作するためには、すべてのメンバ ポートで 802.1X 設定を同一にする必要があります。
- 802.1X 認証を有効にした場合、サプリカントが認証されてから、イーサネット インターフェイス上のレイヤ 2 またはレイヤ 3 のすべての機能が有効になります。
- 802.1X 対応ポートでは、認証が成功した後にのみ STP BPDU が許可されます。STP の競合を回避するために、STP エッジポートでのみ 802.1X 機能をイネーブルにすることを推奨します。
- Cisco NX-OS ソフトウェアが 802.1X 認証をサポートするのは、ポート チャネル、トランク、またはアクセス ポート内のイーサネット インターフェイス上だけです。
- Cisco NX-OSソフトウェアは、CTS または MACsec 機能については動作しません。グローバルな「mac-learn disable」と dot1x 機能は相互に排他的であり、同時に設定することはできません。
- Dot1x は IPソースガードおよび URPF 機能とは相互に排他的であり、同時に設定することはできません。Cisco Nexus シリーズ スイッチを Cisco NX-OS リリース9.3（3）にアップグレードする場合は、これらの機能のいずれかを無効にする必要があります。
- Cisco NX-OS ソフトウェアは、ポート チャネル内のトランク インターフェイスまたはメンバ インターフェイス上ではシングル ホスト モードをサポートしません。
- Cisco NX-OS ソフトウェアは、ポート チャネル上では MAC アドレス認証バイパス機能をサポートしません。ポートチャネルでサポートされるモードは、マルチホストモードだけです。
- Cisco NX-OS ソフトウェアは、vPC ポートでの Dot1X および MCT をサポートしません。
- スイッチのリロード中、Dot1x は RADIUS アカウンティングの停止を生成しません。
- Cisco NX-OS ソフトウェアは、次の 802.1X プロトコル拡張機能をサポートしません。
  - 論理 VLAN 名から ID への 1 対多のマッピング
  - Web 許可
  - ダイナミック ドメイン ブリッジ割り当て

- IP テレフォニー

- 非アクティブなセッションの再認証を防ぐには、authentication timer inactivity コマンドを使用して、非アクティブタイマーを、authentication timer reauthenticateコマンドで設定された再認証間隔よりも短い間隔に設定します。
- インターフェイスで dot1x が有効になっている異なる VLAN で、同じ MAC が学習されると、セキュリティ違反が発生します。
- DME 対応プラットフォームで dot1x を有効にした状態で MAC の学習を無効に設定しても、エラー メッセージは表示されません。
- VLAN がインターフェイスで設定されていなくても、タグ付き EAPOL フレームは処理され、クライアントのインターフェイスで認証は成功します。
- 孤立ポートで学習されたセキュアな MAC は、vPCピアで同期されません。

802.1x のデフォルト設定

表 *7: 802.1x* のデフォルト パラメータ

パラメータ	デフォルト
802.1X 機能	ディセーブル
AAA 802.1X 認証方式	設定なし
インターフェイス単位の 802.1x プロトコル イネーブル ステート	ディセーブル（force-authorized） ポートはサプリカントとの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。
定期的な再認証	ディセーブル
再認証の間隔（秒）	3,600 秒
待機タイムアウト時間	60 秒（Cisco NX-OS デバイスがサプリカントとの認証情報の交換に失敗した後、待機状態を続ける秒数）
再送信タイムアウト時間	30 秒（Cisco NX-OS デバイスが EAP-Request/Identity フレームに対するサプリカントからの応答を待ち、要求を再送信するまでの秒数）

パラメータ	デフォルト
最大再送信回数	2 回（Cisco NX-OS デバイスが認証プロセスを再開するまでに、EAP-Request/Identity フレームを送信する回数）
ホスト モード	シングル ホスト
サプリカント タイムアウト時間	30 秒（認証サーバからサプリカントに要求をリレーする場合、要求をサプリカントに再送信する前に応答のためにCisco NX-OS デバイスが待つ時間）
認証サーバ タイムアウト時間	30 秒（応答をサプリカントから認証サーバにリレーする場合、サーバーに応答を再送信する前にCisco NX-OS デバイスが返信のために待つ時間）

802.1X の設定

802.1X の設定プロセス

ここでは、802.1X を設定するプロセスについて説明します。

手順

ステップ 1 802.1X 機能をイネーブルにします。
ステップ 2 リモート RADIUS サーバへの接続を設定します。
ステップ 3 イーサネット インターフェイスで 802.1X 機能をイネーブルにします。

802.1X を有効化

サプリカント デバイスを認証する前に、Cisco NX-OS デバイス上で 802.1X 機能をイネーブルにする必要があります。

手順

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

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	
ステップ 2	**feature dot1x** 例： `switch(config)# feature dot1x`	802.1X 機能をイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x** 例： `switch# show dot1x`	802.1X機能のステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

802.1X の AAA 認証方式の設定

802.1X 認証にリモート RADIUS サーバを使用できます。RADIUS サーバおよび RADIUS サーバ グループを設定し、デフォルト AAA 認証方式を指定したあとに、Cisco NX-OS デバイスは 802.1X 認証を実行します。

始める前に

リモート RADIUS サーバ グループの名前またはアドレスを取得します。

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 authentication dot1x default group** 例： `switch(config)# aaa authentication dot1x default group rad2`	802.1X 認証に使用する RADIUS サーバ グループを指定します。 group-list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
		• radius：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：認証に RADIUS サーバのグローバル プールを使用します。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show radius-server** 例： `switch# show radius-server`	RADIUS サーバの設定を表示します。
ステップ 5	**show radius-server group** 例： `switch# show radius-server group rad2`	RADIUS サーバ グループの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

インターフェイスでの 802.1X 認証の制御

インターフェイス上で実行される 802.1X 認証を制御できます。インターフェイスの 802.1X 認証ステートは、次のとおりです。

自動（Auto）
インターフェイス上で、802.1X 認証を有効にします。

強制認証
インターフェイス上の 802.1X 認証を無効にし、認証を行わずにインターフェイス上のすべてのトラフィックを許可します。このステートがデフォルトです。

Force-unauthorized
インターフェイス上のすべてのトラフィックを禁止します。

始める前に

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x port-control** {**auto** | **force-authorized** | **force-unauthorised**} 例： `switch(config-if)# dot1x port-control auto`	インターフェイスの 802.1X 認証ステートを変更します。デフォルトの設定は force-authorized です。

ステップ 4	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

インターフェイスでのオーセンティケータ PAE の作成または削除

インターフェイスで 802.1X オーセンティケータ Port Access Entity（PAE）インスタンスを作成または削除できます。

（注） デフォルトでは、インターフェイスで 802.1X をイネーブルにしたときに、Cisco NX-OS ソフトウェアによってインターフェイスでオーセンティケータ PAE インスタンスが作成されます。

始める前に

802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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	**show dot1x interface ethernet** *slot* | *port* 例： `switch# show dot1x interface ethernet 2/1`	インターフェイス上の 802.1X の設定を表示します。

ステップ 3	**interface ethernet** *slot* | *port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	[**no**] **dot1x pae authenticator** 例： `switch(config-if)# dot1x pae authenticator`	インターフェイスでオーセンティケータ PAE インスタンスを作成します。インターフェイスから PAE インスタンスを削除するには、**no** 形式を使用します。 （注） インターフェイスでオーセンティケータ PAE インスタンスを作成します。インターフェイスから PAE インスタンスを削除するには、**no** 形式を使用します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

インターフェイスの定期再認証のイネーブル化

インターフェイスの 802.1X 定期再認証をイネーブルにし、再認証を実行する頻度を指定します。期間を指定しないで再認証をイネーブルにした場合、再認証を行う間隔はグローバル値にデフォルト設定されます。

（注） 再認証プロセス中、すでに認証されているサプリカントのステータスは影響を受けません。

始める前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	dot1x re-authentication 例： `switch(config-if)# dot1x re-authentication`	インターフェイスに接続されているサプリカントの定期再認証をイネーブルにします。デフォルトでは、定期再認証はディセーブルです。
ステップ 4	**dot1x timeout re-authperiod** 例： `switch(config-if)# dot1x timeout re-authperiod 3300`	再認証の間隔（秒）を設定します。デフォルトは 3600 秒です。値の範囲は 1 ～ 65535 です。 （注） インターフェイス上の定期再認証をイネーブルにする場合だけ、このコマンドは Cisco NX-OS デバイスの動作に影響します。

ステップ 5	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 6	**show dot1x all** 例： `switch# show dot1x all`	802.1X 機能のすべてのステータスおよび設定情報を表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

手動によるサプリカントの再認証

Cisco NX-OS デバイス全体のサプリカントまたはインターフェイスのサプリカントを手動で再認証できます。

（注） 再認証プロセス中、すでに認証されているサプリカントのステータスは影響を受けません。

始める前に

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**dot1x re-authenticate** [**interface** *slot* | **port**] 例： `switch# dot1x re-authenticate interface 2/1`	Cisco NX-OS デバイスまたはインターフェイス上のサプリカントを再認証します。

インターフェイスの 802.1X 認証タイマーの変更

Cisco NX-OS デバイスのインターフェイス上で変更できる 802.1X 認証タイマーは、次のとおりです。

待機時間タイマー
Cisco NX-OS デバイスがサプリカントを認証できない場合、スイッチは所定の時間アイドル状態になり、その後再試行します。待機時間タイマーの値でアイドルの時間が決まります。認証が失敗する原因には、サプリカントが無効なパスワードを提供した場合があります。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。デフォルトは、グローバル待機時間タイマーの値です。範囲は 1 ～ 65535 秒です。

レート制限タイマー
レート制限時間中、サプリカントから過剰に送信されている EAPOL-Start パケットを抑制します。オーセンティケータはレート制限時間中、認証に成功したサプリカントからの EAPOL-Start パケットを無視します。デフォルト値は 0 秒で、オーセンティケータはすべての EAPOL-Start パケットを処理します。範囲は 1 ～ 65535 秒です。

レイヤ 4 パケットに対するスイッチと認証サーバ間の再送信タイマー
認証サーバは、レイヤ4パケットを受信するたびにスイッチに通知します。スイッチがパケット送信後に通知を受信できない場合、Cisco NX-OS デバイスは所定の時間だけ待機した後、パケットを再送信します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

EAP 応答フレームに対するスイッチとサプリカント間の再送信タイマー
サプリカントは、Cisco NX-OS デバイスの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。Cisco NX-OS デバイスがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機した後、フレームを再送信します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。
EAP 要求フレームに対するスイッチとサプリカント間の再送信タイマー

（注） このデフォルト値は、リンクの信頼性が低下した場合や、特定のサプリカントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う場合にだけ変更します。

始める前に

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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	**configure interface ethernet 2/1**
	例：
	`switch# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x timeout quiet-period** *seconds* 例： `switch(config-if)# dot1x timeout quiet-period 25`	オーセンティケータが EAP-Request/Identity フレームに対するサプリカントからの応答を待ち、要求を再送信するまでの時間を秒数で設定します。デフォルトはすべてのインターフェイスに設定されるグローバル秒数です。範囲は 1 ～ 65535 秒です。
ステップ 4	**dot1x timeout ratelimit-period** *seconds* 例： `switch(config-if)# dot1x timeout ratelimit-period 10`	認証に成功したサプリカントからの EAPOL-Start パケットを無視する時間を秒数で設定します。デフォルト値は 0 秒です。範囲は 1 ～ 65535 秒です。

	コマンドまたはアクション	目的
ステップ 5	**dot1x timeout server-timeout** *seconds* 例： `switch(config-if)# dot1x timeout server-timeout 60`	Cisco NX-OS デバイスが認証サーバにパケットを送信する前に待機する時間を秒数で設定します。デフォルトは30秒です。範囲は 1 ～ 65535 秒です。
ステップ 6	**dot1x timeout supp-timeout** *seconds* 例： `switch(config-if)# dot1x timeout supp-timeout 20`	Cisco NX-OS デバイスが EAP 要求フレームを再送信する前に、サプリカントがEAP要求フレームに応答してくるのを待機する時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。
ステップ 7	**dot1x timeout tx-period** *seconds* 例： `switch(config-if)# dot1x timeout tx-period 40`	サプリカントからEAP要求フレームを受信した通知が送信されない場合に、EAP 要求フレームを再送信する間隔を秒数で設定します。デフォルトはすべてのインターフェイスに設定されるグローバル秒数です。範囲は 1 ～ 65535 秒です。
ステップ 8	**dot1x timeout inactivity-period** *seconds* 例： `switch(config-if)# dot1x timeout inactivity-period 1800`	スイッチが非アクティブ状態を維持できる秒数を設定します。最小推奨値は 1800 秒です。

ステップ 9	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 10	**show dot1x all** 例： `switch# show dot1x all`	802.1X の設定を表示します。
ステップ 11	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

MAC 認証バイパスのイネーブル化

サプリカントの接続されていないインターフェイス上で、MAC 認証バイパスをイネーブルにすることができます。

始める前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x mac-auth-bypass** [**eap**] 例： `switch(config-if)# dot1x mac-auth-bypass`	MAC 認証バイパスをイネーブルにします。デフォルトはバイパスのディセーブルです。**eap** キーワードを使用して、許可に EAP を使用するように Cisco NX-OS デバイスを構成します。

ステップ 4	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

シングル ホスト モードまたはマルチ ホスト モードのイネーブル化

インターフェイス上でシングル ホスト モードまたはマルチ ホスト モードをイネーブルにすることができます。

始める前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル 構成 モードを開始します。

ステップ 2	**interface ethernet** *slot* | *port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x host-mode** { **multi-host** | **single-host**} 例： `switch(config-if)# dot1x host-mode multi-host`	ホスト モードを設定します。デフォルトは、single-host です。 （注） 指定したインターフェイスで dot1x port-control インターフェイス コンフィギュレーション コマンドが auto に設定されていることを確認してください。
ステップ 4	**dot1x host-mode multi-auth** 例： `switch(config-if)# dot1x host-mode multi-auth`	複数認証モードを設定します。ポートは、EAP または MAB のいずれか、または両方の組み合わせが正常に認証された場合にのみ許可されます。認証に失敗すると、ネットワーク アクセスが制限されます。

ステップ 5	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

802.1X 機能のディセーブル化

Cisco NX-OS デバイス上の 802.1X 機能をディセーブルにできます。

802.1X をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。Cisco NX-OS ソフトウェアは、802.1X を再度イネーブルにして設定を回復する場合に使用できる自動チェッ

クポイントを作成します。詳細については、ご使用のプラットフォームの『*Cisco NX-OS* システム管理設定ガイド』を参照してください。

始める前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**no feature dot1x** 例： `no feature dot1x`	802.1X 機能をディセーブルにします。 （注） 802.1X 機能をディセーブルにすると、802.1X のすべての設定が削除されます。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

802.1X インターフェイス設定のデフォルト値へのリセット

インターフェイスの 802.1X 設定をデフォルト値にリセットすることができます。

始める前に

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet** *slots port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x default** 例： `switch(config-if)# dot1x default`	インターフェイスの 802.1X 設定をデフォルト値に戻します。

ステップ 4	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

インターフェイスでのオーセンティケータとサプリカント間のフレームの最大数の設定

セッションがタイムアウトするまでに、Cisco NX-OS デバイスがインターフェイス上でサプリカントに認証要求を再送信する最大回数を設定できます。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

始める前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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** *slots* | *port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x max-req** *count* 例： `switch(config-if)# dot1x max-req 3`	最大認証要求リトライ回数を変更します。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

	コマンドまたはアクション	目的
		（注） 指定したインターフェイスで dot1x port-control インターフェイス コンフィギュレーション コマンドが auto に設定されていることを確認してください。

ステップ 4	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

インターフェイスでの再認証最大リトライ回数の設定

セッションがタイムアウトするまでに、Cisco NX-OS デバイスがインターフェイス上でサプリカントに再認証要求を再送信する最大回数を設定できます。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

始める前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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** *slots* | *port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x max-reauth-req** *retry-count* 例： `switch(config-if)# dot1x max-reauth-req 3`	最大再認証要求リトライ回数を変更します。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

802.1X 構成の確認

802.1X 情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show dot1x	802.1X 機能のステータスを表示します。
show dot1x all [**details** | **statistics** | **summary**]	802.1X機能のすべてのステータスおよび設定情報を表示します。
show dot1x interface ethernet *slot/port* [**details** | **statistics** | **summary**]	イーサネットインターフェイスの802.1X機能のステータスおよび設定情報を表示します。
show running-config dot1x [**all**]	実行コンフィギュレーション内の 802.1X 機能の設定を表示します。
show startup-config dot1x	スタートアップ コンフィギュレーション内の 802.1X 機能の設定を表示します。

これらのコマンドの出力フィールドの詳細については、ご使用のプラットフォームの『*Cisco NX-OS* セキュリティ コマンド リファレンス』を参照してください。

802.1X のモニタリング

Cisco NX-OS デバイスが保持している 802.1X のアクティビティに関する統計情報を表示できます。

始める前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**show dot1x** {**all** | **interface ethernet** *slot* | *port*} **statistics** 例： `switch# show dot1x all statistics`	802.1X 統計情報を表示します。

802.1X の設定例

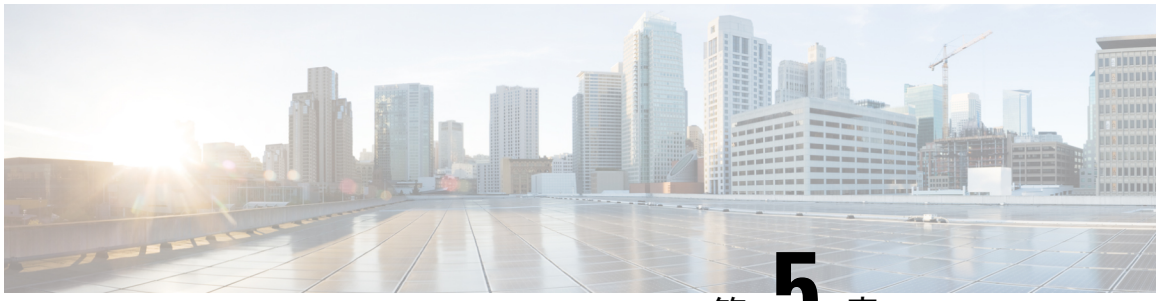
次に、アクセス ポートに 802.1X を設定する例を示します。

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae-authenticator
dot1x port-control auto
```

次に、トランク ポートに 802.1X を設定する例を示します。

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae-authenticator
dot1x port-control auto
dot1x host-mode multi-host
```

（注） 802.1X 認証が必要なすべてのインターフェイスに対して、**dot1x pae authenticator** コマンドおよび **dot1x port-control auto** コマンドを繰り返してください。



第 5 章

RADIUS の設定

この章は、次の項で構成されています。

RADIUS の設定

RADIUS の概要

Remote Access Dial-In User Service（RADIUS）分散クライアント/サーバー 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、すべてのユーザー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 サーバーに認証要求およびアカウンティング要求を送信します。

RADIUS ネットワーク環境

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

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

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク。

  たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバ ベースのセキュリティ データベースを使用できます。

- すでに RADIUS を使用中のネットワーク。

  RADIUS を使用したCisco 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 サーバーに移行するときの最初の手順になります。

- リソース アカウンティングが必要なネットワーク。

RADIUS アカウンティングは、RADIUS 認証または RADIUS 認可とは個別に使用できます。RADIUSアカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネットサービスプロバイダー（ISP）は、RADIUSアクセスコントロールおよびアカウンティング用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。

- 認証プロファイルをサポートするネットワーク。

  ネットワークでRADIUSサーバを使用すると、AAA認証を設定し、ユーザごとのプロファイルをセットアップできます。ユーザー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

ユーザー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：ユーザーが認証されたことを表します。
   - REJECT：ユーザーは認証されず、ユーザー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サーバーによってチャレンジが発行されます。チャレンジは、ユーザーから追加データを収集します。
   - CHANGE PASSWORD：RADIUS サーバーからユーザー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。

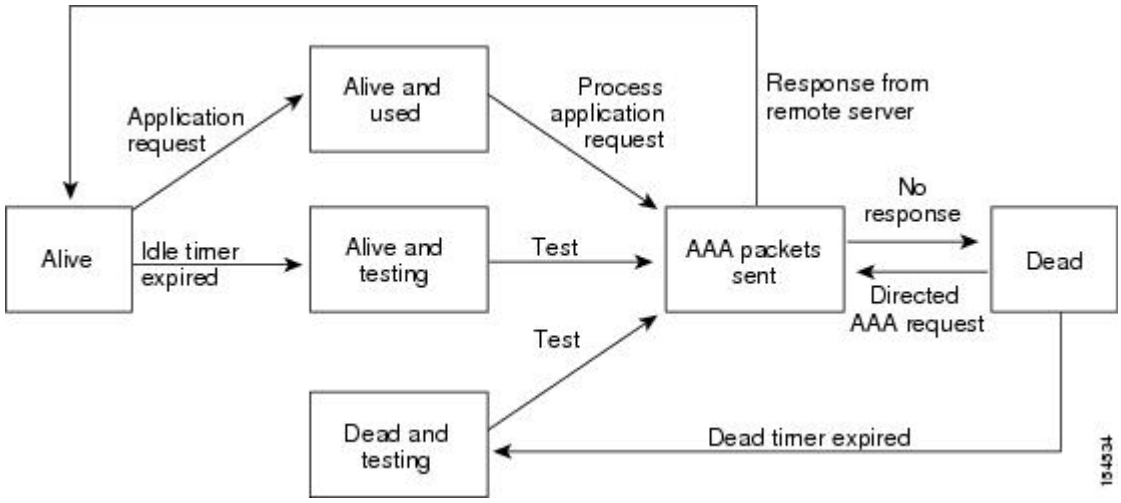
- ユーザがアクセス可能なサービス（Telnet、rlogin、またはローカルエリアトランスポート（LAT）接続、ポイントツーポイントプロトコル（PPP）、シリアルラインインターネットプロトコル（SLIP）、EXEC サービスなど）
- ホストまたはクライアントの IPv4 アドレス、アクセス リスト、ユーザー タイムアウトなどの接続パラメータ

RADIUS サーバのモニタリング

応答を返さない RADIUS サーバーがあると、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 サーバーをモニタリングし、RADIUS サーバーが応答を返す（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 サーバーをデッド（dead）状態としてマークし、デッド RADIUS サーバーには AAA 要求を送信しません。また、定期的にデッド RADIUS サーバーをモニタリングし、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 サーバーが稼働状態であることを確認してから、実際の AAA 要求がサーバーに送信されます。RADIUS サーバー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 サーバーの状態を示します。

***Figure 4: RADIUS* サーバーの状態**



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

ベンダー固有属性

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバーと RADIUS サーバー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 サーバーを使用する場合は、認証結果とともに許可情報などのユーザー属性を返すよう、RADIUS プロトコルが RADIUS サーバーに指示します。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：ユーザー 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：ユーザー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 サーバーの IPv4 アドレスまたはホスト名を取得すること。
- RADIUS サーバーから事前共有キーを取得すること。
- Cisco Nexus デバイスが、AAA サーバーの 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。

- Cisco Nexus デバイスに設定できる RADIUS サーバーの最大数は 64 です。
- ASCII（PAP）認証は RADIUS サーバーではサポートされていません。

RADIUS サーバの設定

ここでは、RADIUS サーバーの設定方法について説明します。

Procedure

ステップ 1 Cisco Nexus デバイスと RADIUS サーバーとの接続を確立します。

ステップ 2 RADIUS サーバー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 サーバーの指定を許可
- 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 サーバー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 サーバーについて、IPv4 アドレスまたはホスト名を設定する必要があります。すべての RADIUS サーバー ホストは、デフォルトの RADIUS サーバー グループに追加されます。最大 64 の RADIUS サーバーを設定できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *host-name*}	RADIUS サーバーの IPv4 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。
ステップ 4	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。
ステップ 5	(Optional) switch# **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。

Example

次に、RADIUS サーバーとしてホスト 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ーについて、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 サーバー ホスト間の共有秘密テキスト ストリングです。

Before you begin

リモートの RADIUS サーバーの事前共有キー値を取得していること。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server key** [**0** | **7**] *key-value*	すべての RADIUS サーバー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	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。 **Note** 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。

	Command or Action	Purpose
ステップ 5	(Optional) switch# **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。

Example

次に、デバイスで使用するすべてのサーバーについて、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 サーバー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 サーバー ホスト間の共有秘密テキスト ストリングです。

Before you begin

リモートの RADIUS サーバーの事前共有キー値を取得していること。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value*	特定の RADIUS サーバー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。 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	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。

	Command or Action	Purpose
		Note 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	(Optional) switch# **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。

Example

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch (config)# **aaa group server radius** *group-name*	RADIUS サーバー グループを作成し、そのグループの RADIUS サーバー グループ コンフィギュレーション サブモードを開始します。 *group-name* 引数は、最大 127 文字の英数字のストリングで、大文字小文字が区別されます。
ステップ 3	switch (config-radius)# **server** {*ipv4-address* | *server-name*}	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。

	Command or Action	Purpose
		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	(Optional) switch (config-radius)# **deadtime** *minutes*	モニタリング デッド タイムを設定します。デフォルト値は 0 分です。指定できる範囲は 1 ～ 1440 です。 **Note** RADIUS サーバ グループのデッド タイム間隔が 0 より大きい場合は、この値がグローバルなデッド タイム値より優先されます。
ステップ 5	(Optional) switch(config-radius)# **source-interface** *interface*	特定の RADIUS サーバー 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。 **Note** 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	switch(config-radius)# **exit**	設定モードを終了します。
ステップ 7	(Optional) switch(config)# **show radius-server group** [*group-name*]	RADIUS サーバー グループの設定を表示します。
ステップ 8	(Optional) switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

Example

次に、RADIUS サーバー 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
```

What to do next

AAA サービスに RADIUS サーバー 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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip radius source-interface** *interface*	このデバイスで設定されているすべての RADIUS サーバー 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	(Optional) switch# **show radius-server**	RADIUS サーバーの設定情報を表示します。
ステップ 5	(Optional) switch# **copy running-config startup config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、RADIUS サーバー 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 サーバーを指定することをユーザーに許可できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server directed-request**	ログイン時にユーザーが認証要求の送信先となる RADIUS サーバー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	(Optional) switch# **show radius-server directed-request**	directed request の設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、ネットワークにログインしたときに、ユーザーが RADIUS サーバー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 サーバー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 サーバーへの送信を 1 回だけ再試行します。このリトライの回数は、サーバーごとに最大 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 サーバーからの応答を待機する時間を決定します。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 2	switch(config)# **radius-server retransmit** *count*	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 timeout** *seconds*	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	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。
ステップ 6	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、RADIUS サーバーで、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 サーバーへの送信を 1 回だけ再試行します。このリトライの回数は、サーバーごとに最大 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 サーバー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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **retransmit** *count*	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。

	Command or Action	Purpose
		Note 特定の RADIUS サーバに指定した再送信回数は、すべての RADIUS サーバに指定した再送信回数より優先されます。
ステップ 3	switch(config)#**radius-server host** {*ipv4-address* | *host-name*} **timeout** *seconds*	特定のサーバの送信タイムアウト間隔を指定します。デフォルトはグローバル値です。 **Note** 特定の RADIUS サーバに指定したタイムアウト間隔は、すべての RADIUS 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	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	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。
ステップ 6	(Optional) switch# **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。

Example

次に、RADIUS ホスト サーバー 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 サーバのアカウンティングおよび認証属性の設定

RADIUS サーバをアカウンティング専用、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 サーバはアカウンティングと認証の両方に使用されます。RADIUS のアカウンティ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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	(Optional) switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **acct-port** *udp-port*	RADIUS アカウンティ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	(Optional) switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **accounting**	特定の RADIUS サーバーをアカウンティング用にのみ使用することを指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	(Optional) switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **auth-port** *udp-port*	RADIUS 認証メッセージ用の UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。 範囲は 0 ～ 65535 です。
ステップ 5	(Optional) switch(config)# **radius-server host** {*ipv4-address* |*host-name*} **authentication**	特定の RADIUS サーバーを認証用にのみ使用することを指定します。デフォルトでは、アカウンティ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	(Optional) switch(config)# **show radius-server**	RADIUS サーバー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。

Example

次に、RADIUS サーバーのアカウンティ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 サーバーの定期的モニタリングの設定

RADIUSサーバーの可用性をモニタリングできます。パラメータとして、サーバーに使用するユーザー名とパスワード、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サーバー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、サーバーを定期的にテストできます。

Note セキュリティ上の理由から、RADIUS データベース内の既存のユーザー名と同じテスト ユーザー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 サーバー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 サーバーの定期的なモニタリングを実行しません。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **test** { **idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}	サーバー 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ー名は 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。 **Note** RADIUS サーバー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 deadtime** *minutes*	スイッチが、前回応答しなかった RADIUSサーバー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。

	Command or Action	Purpose
ステップ 5	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。
ステップ 6	(Optional) switch# **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。

Example

次に、ユーザー名（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 サーバー 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 サーバーのデッド 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 サーバーをデッド状態であると宣言した後、そのサーバー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。

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

Procedure

	Command or Action	Purpose
ステップ 1	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。

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

Example

次に、RADIUS サーバーに 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

Procedure

	Command or Action	Purpose
ステップ 1	switch# **test aaa server radius** {*ipv4-address* | *server-name*} [**vrf** *vrf-name*] *username password* **test aaa server radius** {*ipv4-address* | *server-name*} [**vrf** *vrf-name*] *username password*	RADIUS サーバーにテスト 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 サーバー 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。

Example

次に、可用性を確認するために、RADIUS サーバーとサーバー 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 サーバー統計情報の表示

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show radius-server statistics** {*hostname* | *ipv4-address*}	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 サーバーのアクティビティに関する統計情報を表示します。

始める前に

Cisco NX-OS デバイスに RADIUS サーバーを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） switch# **show radius-server statistics** {*hostname* | *ipv4-address*}	Cisco NX-OS デバイスでの RADIUS サーバー統計情報を表示します。
ステップ 2	switch# **clear radius-server statistics** {*hostname* | *ipv4-address*}	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。

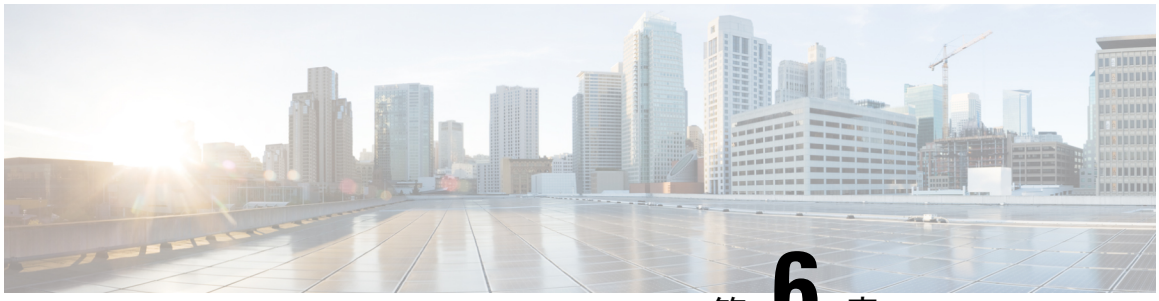
```
switch# configure terminal
switch(config)# radius-server key 7 "ToIkLhPpG"
switch(config)# radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# exit
switch(config-radius)#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

Table 8: デフォルトの *RADIUS* パラメータ

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



第 6 章

TACACS+ の設定

この章は、次の項で構成されています。

TACACS+ の設定について

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ー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+ サーバーへのアクセス権を持ち、このサーバーを設定する必要があります。

TACACS+ では、認証、許可、アカウンティングの各ファシリティを個別に提供します。TACACS+を使用すると、単一のアクセス コントロール サーバー（TACACS+ デーモン）で、各サービス（認証、許可、アカウンティング）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、そのサーバー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/サーバー プロトコルでは、トランスポート要件を満たすため TCP（TCP ポート 49）を使用します。Cisco 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+ を使用したユーザー ログイン

ユーザーが 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、ユーザー名とパスワードを取得します。

Note TACACS+ では、デーモンがユーザーを認証するために十分な情報を得られるまで、デーモンとユーザーとの自由な対話を許可します。この動作では通常、ユーザー名とパスワードの入力が要求されますが、ユーザーの母親の旧姓など、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：ユーザーの認証に成功したので、サービスを開始します。Cisco Nexus デバイスがユーザーの許可を要求している場合は、許可が開始されます。
   - REJECT：ユーザーの認証に失敗しました。TACACS+ デーモンは、ユーザー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、スイッチは代わりのユーザー認証方式の使用を試します。

   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。ユーザーは 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
- 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、ユーザー タイムアウトなどの接続パラメータ

デフォルトの TACACS+ サーバー暗号化タイプと事前共有キー

TACACS+ サーバー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+ サーバー 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+ サーバー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+ サーバーの設定時に **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+ サーバのコマンド許可サポート

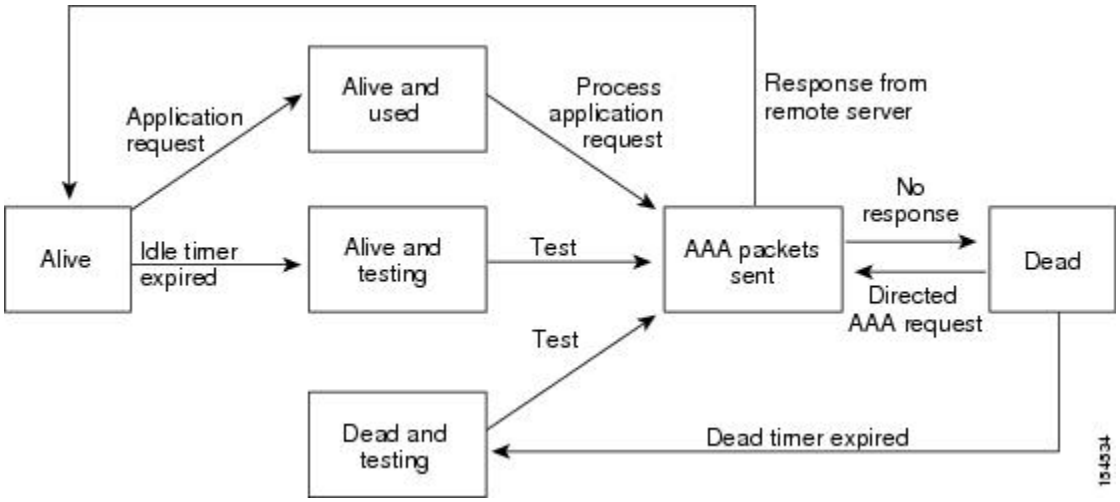
デフォルトでは、認証されたユーザーがコマンドライン インターフェイス（CLI）でコマンドを入力したときに、Cisco NX-OS ソフトウェアのローカル データベースに対してコマンド許可が行われます。また、TACACS+ を使用して、認証されたユーザに対して許可されたコマンドを確認することもできます。

TACACS+ サーバのモニタリング

応答を返さない TACACS+ サーバーがあると、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+ サーバーをモニタリングし、TACACS+ サーバーが応答を返す（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+ サーバーをデッド（dead）としてマークし、デッド TACACS+ サーバーには 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+ サーバーをモニタリングし、それらのサーバー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+ サーバーが稼働状態であることを確認してから、実際の AAA 要求がサーバーに送信されます。TACACS+ サーバーの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco 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+ サーバーの状態を示します。

Figure 5: TACACS+ サーバーの状態



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

TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバーの IPv4 アドレスまたはホスト名を取得すること。
- TACACS+ サーバー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 サーバーの 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 デバイスに設定できる TACACS+ サーバーの最大数は 64 です。
- TACACS+サーバホストを構成し、実際にホストを使用するようにAAA構成を行った後、次のエラー メッセージが散発的に表示されることがあります：

  `[%TACACS-3-TACACS_ERROR_MESSAGE: すべてのサーバーが応答に失敗しました（%TACACS-3-TACACS_ERROR_MESSAGE: All servers failed to respond）]`

  この問題の既知されていて、回避策はありません。リモート認証が TACACS サーバ接続の問題なしに正しく機能する場合は、メッセージを無視して構成を続行できます。

TACACS+ の設定

TACACS+ サーバの設定プロセス

ここでは、TACACS+ サーバーを設定する方法について説明します。

Procedure

ステップ 1 TACACS+ をイネーブルにします。

ステップ 2 TACACS+ サーバーとCisco Nexus デバイスとの接続を確立します。

ステップ 3 TACACS+ サーバー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+ サーバーのサブセットを使用して TACACS+ サーバー 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+ サーバーの指定を許可
- 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+ サーバー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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。
ステップ 4	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

TACACS+ サーバ ホストの設定

リモートの TACACS+ サーバーにアクセスするには、Cisco Nexus デバイス上に、TACACS+ サーバーのIPv4アドレスまたはホスト名を設定する必要があります。すべてのTACACS+サーバーホストは、デフォルトのTACACS+サーバーグループに追加されます。最大64のTACACS+サーバーを設定できます。

設定済みのTACACS+サーバー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+サーバー 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）が該当サーバーで使用されます。

TACACS+ サーバー 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 の TACACS+ サーバーの IPv4 アドレスまたはホスト名を取得します。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*}	TACACS+ サーバーの IPv4 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。
ステップ 4	(Optional) switch# **show tacacs-server**	TACACS+ サーバーの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

サーバー グループから TACACS+ サーバー 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ーについて、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+ サーバー 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+ サーバーの事前共有キー値を取得していること。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**tacacs-server key** [**0** | **6** | **7**] *key-value*	すべての TACACS+ サーバ用の TACACS+ キーを指定します。*key-value* がクリアテキスト形式（**0**）か、タイプ 6 暗号化形式（**6**）か、タイプ 7 暗号化形式（**7**）かを指定できます。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	(Optional) switch# **show tacacs-server**	TACACS+ サーバーの設定を表示します。 **Note** 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	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

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+ サーバーの事前共有キーの設定

TACACS+ サーバー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+ サーバー ホスト間の共有秘密テキスト ストリングです。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value*	特定の TACACS+ サーバー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。 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	(Optional) switch# **show tacacs-server**	TACACS+ サーバーの設定を表示します。 **Note** 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	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

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。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa group server tacacs+** *group-name*	TACACS+ サーバー グループを作成し、そのグループのTACACS+ サーバー 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-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value*	特定の TACACS+ サーバー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。 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 4	(Optional) switch(config-tacacs+)# **deadtime** *minutes*	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。 **Note** TACACS+ サーバー 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 5	(Optional) switch(config-tacacs+)# **source-interface** *interface*	特定の TACACS+ サーバー 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。

	Command or Action	Purpose
		Note 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 6	switch(config-tacacs+)# **exit**	コンフィギュレーション モードを終了します。
ステップ 7	(Optional) switch(config)# **show tacacs-server groups**	TACACS+ サーバー グループの設定を表示します。
ステップ 8	(Optional) switch(config)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、TACACS+ サーバー 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。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip tacacs source-interface** *interface* **Example:**	このデバイスで設定されているすべてのTACACS+サーバー 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

	Command or Action	Purpose
	`switch(config)# ip tacacs source-interface mgmt 0`	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**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	TACACS+サーバの設定情報を表示します。
ステップ 5	(Optional) **copy running-config startup config** **Example:** `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

ログイン時の TACACS+ サーバーの指定

認証要求の送信先 TACACS+ サーバーをユーザー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、ユーザーは *username@hostname* としてログインできます。ここで、*hostname* は設定済みの RADIUS サーバーの名前です。

Note ユーザー指定のログインは、Telnet セッションでのみサポートされます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server directed-request**	ログイン時にユーザーが認証要求の送信先となる TACACS+ サーバー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	(Optional) switch# **show tacacs-server directed-request**	TACACS+ の directed request の設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

TACACS+ サーバでの AAA 許可の設定

TACACS+ サーバのデフォルトの AAA 許可方式を設定できます。

Before you begin

TACACS+ をイネーブルにします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa authorization ssh-certificate default** { **group** *group-list* [**none**] | **local** | **none**}
	Example:
	`switch(config)# aaa authorization ssh-certificate`
	`default group TACACSServer1 TACACSServer2`
		TACACS+ サーバのデフォルトの AAA 許可方式を設定します。
		ssh-certificate キーワードは、証明書認証を使用した TACACS+ 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。
		group-list 引数には、TACACS+ サーバ グループの名前をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。**local** 方式では、ローカル データベースを認証に使用します。**none** 方式では、AAA 認証が使用されないように指定します。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	(Optional) **show aaa authorization** [**all**] **Example:** `switch# show aaa authorization`	AAA 許可設定を表示します。**all** キーワードを指定すると、デフォルト値が表示されます。

	Command or Action	Purpose
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

TACACS+ サーバでのコマンド許可の設定

TACACS+サーバでコマンド許可を設定できます。コマンド許可では、デフォルトロールを含むユーザのロールベース許可コントロール（RBAC）がディセーブルになります。

Before you begin

TACACS+ を有効にします。

AAA コマンドの許可を設定する前に TACACS ホストおよびサーバー グループを設定してください。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa authorization** {**commands** | **config-commands**} **default** [**group** *group-list* [**local**] | **local**]
	Example:
	`switch(config)# aaa authorization commands`
	`default group TacGroup`
		すべてのロールに関するデフォルトのコマンド許可方式を設定します。
		commands キーワードを使用するとすべての EXEC コマンドの許可ソースを設定でき、**config-commands** キーワードを使用するとすべてのコンフィギュレーション コマンドの許可ソースを設定できます。すべてのコマンドのデフォルト許可は、ユーザーに割り当てたロールに関する許可されたコマンドのリストであるローカル許可です。
		group-list 引数には、TACACS+ サーバー グループの名前をスペースで区切ったリストを指定します。このグループに属するサーバーに対して、コマンドの許可のためのアクセスが行われます。**local** 方式では、許可にローカル ロールベース データベースが使用されます。

	Command or Action	Purpose
		local 方式は、設定されたすべてのサーバ グループから応答が得られなかった場合に、**local** をフォールバック方式として設定しているときにだけ使用されます。 デフォルトの方式は **local** です。 TACACS+ サーバ グループの方式のあとにフォールバック方式を設定していないと、すべてのサーバ グループから応答が得られなかった場合は許可に失敗します。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	(Optional) **show aaa authorization** [**all**] **Example:** `switch(config)# show aaa authorization`	AAA 許可設定を表示します。**all** キーワードを指定すると、デフォルト値が表示されます。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

TACACS+ サーバでのコマンド許可のテスト

TACACS+ サーバで、ユーザに対するコマンド許可をテストできます。

Note 許可用の正しいコマンドを送信しないと、結果の信頼性が低くなります。

Before you begin

TACACS+ をイネーブルにします。

TACACS+ サーバにコマンド許可が設定されていることを確認します。

Procedure

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

コマンド許可検証のイネーブル化とディセーブル化

デフォルトのユーザ セッションまたは別のユーザ名に対して、コマンドライン インターフェイス（CLI）でコマンド許可検証をイネーブルにしたり、ディセーブルにしたりできます。

（注） 許可検証をイネーブルにした場合は、コマンドは実行されません。

手順

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

TACACS+ サーバでの許可に使用する特権レベルのサポートの設定

TACACS+ サーバでの許可に使用する特権レベルのサポートを設定できます。

許可の決定に特権レベルを使用する Cisco IOS デバイスとは異なり、Cisco NX-OS デバイスでは、ロールベース アクセス コントロール（RBAC）を使用します。両方のタイプのデバイスを同じ TACACS+ サーバーで管理できるようにするには、TACACS+ サーバーで設定した特権レベルを、Cisco NX-OS デバイスで設定したユーザー ロールにマッピングします。

TACACS+サーバでのユーザの認証時には、特権レベルが取得され、それを使用して「priv-*n*」という形式（*n*が特権レベル）のローカルユーザロール名が生成されます。このローカルロールの権限がユーザに割り当てられます。特権レベルは16あり、対応するユーザ ロールに直接マッピングされます。次の表に、各特権レベルに対応するユーザ ロール権限を示します。

特権レベル	ユーザ ロール権限
15	network-admin 権限
13 ～ 1	• スタンドアロン ロール権限（**feature privilege** コマンドがディセーブルの場合） • ロールの累積権限からなる特権レベル0と同じ権限（**feature privilege** コマンドが有効の場合）
0	**show** コマンドや **exec** コマンド（**ping**、**trace**、**ssh** など）を実行するための権限

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **feature privilege** **Example:** `switch(config)# feature privilege`	ロールの累積権限を有効または無効にします。**enable** コマンドは、この機能を有効にした場合しか表示されません。デフォルトは無効です。
ステップ 3	[**no**] **enable secret** [**0** | **5**] *password* [**priv-lvl** *priv-lvl* | **all**] **Example:** `switch(config)# enable secret 5 def456 priv-lvl 15`	特定の特権レベルのシークレット パスワードを有効または無効にします。特権レベルが上がるたびに、正しいパスワードを入力するようにユーザに要求します。デフォルトは無効です。 パスワードの形式としてクリア テキストを指定する場合は**0**を入力し、暗号化された形式を指定する場合は**5**を入力します。*password* 引数に指定できる文字数は、最大64文字です。*priv-lvl* 引数は、1 ～ 15です。

	Command or Action	Purpose
		Note シークレット パスワードを有効にするには、**feature privilege** コマンドを入力してロールの累積権限を有効にする必要があります。
ステップ 4	[**no**] **username** *username* **priv-lvl** *n* **Example:** `switch(config)# username user2 priv-lvl 15`	ユーザの許可に対する特権レベルの使用を有効または無効にします。デフォルトは無効です。 **priv-lvl** キーワードはユーザに割り当てる特権レベルを指定します。デフォルトの特権レベルはありません。特権レベル 0 ～ 15（priv-lvl 0 ～ priv-lvl 15）は、ユーザ ロール priv-0 ～ priv-15 にマッピングされます。
ステップ 5	(Optional) **show privilege** **Example:** `switch(config)# show privilege`	ユーザ名、現在の特権レベル、および累積権限のサポートのステータスを表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ステップ 7	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 8	**enable** *level* **Example:** `switch# enable 15`	上位の特権レベルへのユーザの昇格を有効にします。このコマンドの実行時にはシークレット パスワードが要求されます。*level* 引数はユーザのアクセスを許可する特権レベルを指定します。指定できるレベルは 15 だけです。

権限ロールのユーザ コマンドの許可または拒否

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

権限ロールのルールを変更する場合は、次の注意事項に従う必要があります。

- priv-14 ロールと priv-15 ロールは変更できません。

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

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **role name priv-***n*
	Example:
	`switch(config)# role name priv-5`
	`switch(config-role)#`
		権限ロールをイネーブルまたはディセーブルにして、ロール コンフィギュレーション モードを開始します。*n* 引数には、特権レベルを 0 ～ 13 の数値で指定します。

ステップ 3	**rule** *number* {**deny** | **permit**} **command** *command-string* **Example:** `switch(config-role)# rule 2 permit command pwd`	権限ロールのユーザ コマンド ルールを設定します。これらのルールで、ユーザによる特定のコマンドの実行を許可または拒否します。ロールごとに最大256のルールを設定できます。ルール番号によって、ルールが適用される順序が決まります。ルールは降順で適用されます。たとえば、1 つのロールが 3 つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。 *command-string* 引数には、空白スペースを含めることができます。 **Note** 256 個の規則に対してこのコマンドを繰り返します。

ステップ 4	**exit**
	Example:
	`switch(config-role)# exit`
	`switch(config)#`
		ロール コンフィギュレーション モードを終了します。

ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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+ サーバー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+ サーバーからの応答を待つ時間を指定します。これを過ぎるとタイムアウト エラーになります。

Procedure

	Command or Action	Purpose
ステップ 1	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 timeout** *seconds*	TACACS+ サーバー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	(Optional) switch# **show tacacs-server**	TACACS+ サーバーの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

サーバー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+ サーバー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+ サーバーからの応答を待機する時間を決定します。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **timeout** *seconds*	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 **Note** 特定の TACACS+ サーバに指定したタイムアウト間隔は、すべての TACACS+ サーバに指定したタイムアウト間隔より優先されます。

	Command or Action	Purpose
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	(Optional) switch# **show tacacs-server**	TACACS+ サーバーの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

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+ サーバー用に別の 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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **port** *tcp-port*	TACACS+アカウンティング メッセージ用の UDP ポートを指定します。デフォルトの TCP ポートは 49 です。有効な範囲は 1 ～ 65535 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	(Optional) switch# **show tacacs-server**	TACACS+ サーバーの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

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+ サーバーの定期的モニタリングの設定

TACACS+ サーバーの可用性をモニタリングできます。パラメータとして、サーバーに使用するユーザー名とパスワード、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+ サーバー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、サーバー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。

Note ネットワークのセキュリティ保護のため、TACACS+データベース内の既存のユーザー名と同じユーザー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+サーバー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。

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

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **test** { **idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}	サーバー 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ー名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 **Note** TACACS+ サーバー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)# **tacacs-server dead-time** *minutes*	Cisco Nexus デバイスが、前回応答しなかった TACACS+ サーバー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 4	switch(config)# **exit**	設定モードを終了します。

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

Example

次に、TACACS+ サーバー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+ サーバーのデッド 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+ サーバーをデッド状態であると宣言した後、そのサーバーがアライブ状態に戻ったかどうかを判断するためにテストパケットを送信するまでの間隔を指定します。

Note デッドタイム間隔が 0 分の場合、TACACS+ サーバーは、応答を返さない場合でも、デット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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server deadtime** *minutes*	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	(Optional) switch# **show tacacs-server**	TACACS+ サーバーの設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

TACACS+ サーバまたはサーバ グループの手動モニタリング

Procedure

	Command or Action	Purpose
ステップ 1	switch# **test aaa server tacacs+** {*ipv4-address* | *host-name*} [**vrf** *vrf-name*] *username password*	TACACS+ サーバーにテスト 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*	TACACS+ サーバー 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。

Example

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。

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

Procedure

	Command or Action	Purpose
ステップ 1	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	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show tacacs-server statistics** {*hostname* | *ipv4-address*}	TACACS+ 統計情報を表示します。

Example

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show tacacs+** {**status** | **pending** | **pending-diff**}	Cisco Fabric Services の TACACS+ 設定の配布状況と他の詳細事項を表示します。
ステップ 2	switch# **show running-config tacacs** [**all**]	実行コンフィギュレーションの TACACS+ 設定を表示します。
ステップ 3	switch# **show startup-config tacacs**	スタートアップ コンフィギュレーションの TACACS+ 設定を表示します。
ステップ 4	switch# **show tacacs-serve** [*host-name* | *ipv4-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての TACACS+ サーバー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 "ShMoMhTl"
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+ サーバーの事前共有キーを設定して、サーバーグループ TacServer1 を認証するためにリモート AAA サーバーを指定する例を示します。

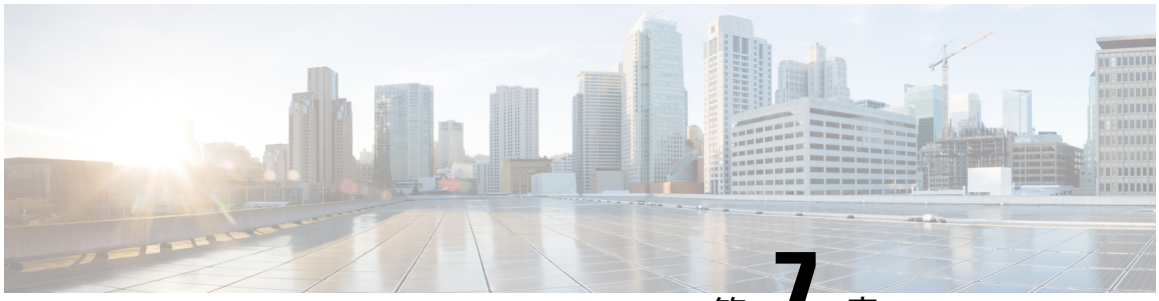
```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ikvhw10"
switch(config)# tacacs-server host 1.1.1.1
switch(config)# tacacs-server host 1.1.1.2

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。

Table 9: 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
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	テスト



第 7 章

SSH および Telnet の設定

この章は、次の項で構成されています。

SSH および Telnet の設定

SSH および Telnet の概要

SSH サーバー

セキュア シェル（SSH）プロトコル サーバー機能を使用すると、SSH クライアントは Cisco Nexus デバイスとの間で、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 Nexus デバイス スイッチの SSH サーバーは、無償あるいは商用の SSH クライアントと連係して動作します。

SSH がサポートするユーザー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ー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 サーバー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 サーバー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ー 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 Algrorithm（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）

⚠

Caution SSH キーをすべて削除すると、SSH サービスを開始できません。

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ーが別サイトのログイン サーバーとの 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 サーバー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 パスワードレス ファイル コピーを目的として AAA プロトコル（RADIUS や TACACS+ など）を介してリモート認証されたユーザ アカウントにインポートされた SSH 公開キーと秘密キーは、同じ名前のローカル ユーザ アカウントでない限り、Nexus デバイスがリロードされると保持されません。リモート ユーザ アカウントは、SSH キーがインポートされる前にデバイスで設定されます。

SSH の設定

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]}	SSH サーバー キーを生成します。 *bits* 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	(Optional) switch# **show ssh key**	SSH サーバー キーを表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、SSH サーバー 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

ユーザー アカウント用に SSH 形式で SSH 公開キーを指定できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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	(Optional) switch# **show user-account**	ユーザー アカウントの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

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+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

Note 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

ユーザー アカウント用に IETF SECSH 形式で SSH 公開キーを指定できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **copy** *server-file* **bootflash:** *filename*	サーバーから 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）サーバーを利用できます。
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	(Optional) switch# **show user-account**	ユーザー アカウントの設定を表示します。
ステップ 6	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

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

ユーザー 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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **copy** *server-file* **bootflash:** *filename*	サーバーから 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。

	Command or Action	Purpose
		FTP、SCP、SFTP、または TFTP サーバーを利用できます。
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	(Optional) switch# **show user-account**	ユーザー アカウントの設定を表示します。
ステップ 4	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

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
```

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **ssh** {*hostname* | *username@hostname*} [**vrf** *vrf-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 *hostname* 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 を使用してサーバーからファイルをダウンロードする場合は、サーバーと信頼性のある SSH 関係を確立します。

Procedure

	Command or Action	Purpose
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 サーバーは、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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **[no] feature ssh**	SSH サーバーをイネーブル/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	(Optional) switch# **show ssh server**	SSH サーバーの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

SSH サーバ キーの削除

SSH サーバーをディセーブルにした後、SSH サーバー キーを削除できます。

Note SSHを再度イネーブルにするには、まず、SSHサーバーキーを生成する必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature ssh**	SSHサーバー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。 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	(Optional) switch# **show ssh key**	SSH サーバーの設定を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show users**	ユーザーセッション情報を表示します。
ステップ 2	switch# **clear line** *vty-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。

Procedure

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
```

Note SSHサーバー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 サーバー 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
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/
cTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4ZXIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5/
```

```
Ninn0Mc=

bitcount:1024
fingerprint:
4b:4d: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
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
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 サーバのイネーブル化

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

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **[no] feature telnet**	Telnet サーバーをイネーブル/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 サーバーの再イネーブル化

Cisco Nexus デバイスの Telnet サーバー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。

Procedure

	Command or Action	Purpose
ステップ 1	switch(config)# **[no] feature telnet**	Telnet サーバーを再度イネーブルにします。

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ー名も取得します。
- Cisco Nexus デバイス上で Telnet サーバーをイネーブルにします。
- リモート デバイス上で Telnet サーバーをイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **telnet** *hostname*	リモート デバイスとの Telnet セッションを作成します。引数 *hostname* には、IPv4 アドレスまたはデバイス名を指定します。

Example

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show users**	ユーザーセッション情報を表示します。
ステップ 2	switch# **clear line** *vty-line*	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。

Procedure

- switch# **show ssh key** [**dsa** | **rsa**]

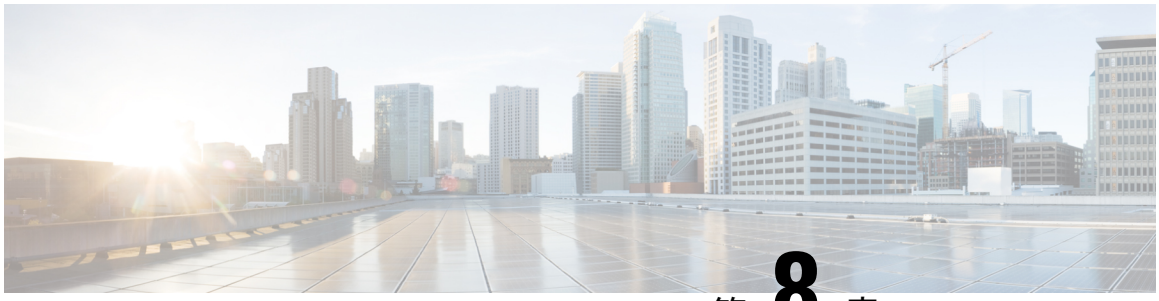
コマンドまたはアクション	目的
switch# **show running-config security**[**all**]	実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。**all** キーワードを指定すると、SSH およびユーザー アカウントのデフォルト値が表示されます。
switch# **show ssh server**	SSH サーバーの設定を表示します。
switch# **show user-account**	ユーザー アカウント情報を表示します。

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。

Table 10: 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	有効（Enabled）



第 8 章

アクセス コントロール リストの設定

この章は、次の項で構成されています。

ACL について

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行され、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 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。

Table 11: セキュリティ *ACL* の適用

適用	サポートするインターフェイス	サポートする **ACL** のタイプ
ポート ACL	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。 • 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 ポート ACL をトランク ポートに適用すると、その ACL は、当該トランク ポート上のすべての VLAN 上のトラフィックをフィルタリングします。	IPv4 ACL
ルータ ACL	• VLAN インターフェイス **Note** VLANインターフェイスを設定するには、先に VLAN インターフェイスをグローバルにイネーブルにする必要があります。 • 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	IPv4 ACL
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

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

ACL によるネットワーク トラフィックのフィルタリング方法を設定する際に、何を作成、変更、削除するかを決めるのがルールです。ルールは実行コンフィギュレーション内に表示されます。ACL をインターフェイスに適用するか、またはインターフェイスにすでに適用されている ACL 内のルールを変更すると、スーパーバイザ モジュールは実行コンフィギュレーション内のルールから ACL のエントリを作成し、それらの ACL エントリを適用可能な I/O モジュールに送信します。ACL の設定によっては、ルールよりも ACL エントリの方が数が多くなることがあります。特に、ルールを設定するときにオブジェクト グループを使用してポリシーベース ACL を実装する場合などです。

ルールは ACL で作成できます。ルールは、**permit** または **deny** コマンドを使用してアクセス リスト コンフィギュレーション モードで作成できます。これにより、デバイスは許可ルール内の基準と一致するトラフィックを許可し、拒否ルール内の基準と一致するトラフィックをブロックします。ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

ここでは、ルールを設定する際に使用できるオプションをいくつか紹介します。

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 ACL および MAC 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。

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

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。

- 既存のルールの間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、それらのルールの間に1つ以上のルールを挿入する必要があるときに便利です。

論理演算子と論理演算ユニット

TCP および UDP トラフィックの IP ACL ルールでは、論理演算子を使用して、ポート番号に基づきトラフィックをフィルタリングできます。

Cisco 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。

Note 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 に格納されます。

  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になります。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。

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。

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。
- Cisco Nexus デバイスによっては、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。
- 全体の TCAM の深さは、出力と入力の場合は 4000 エントリで共有されています。これは、16 のエントリ ブロックに切り分けることができます。
- TCAM は、ACL 機能ごとに 256 の統計エントリをサポートします。
- 各方向に 32 の 64 の ACL L4OP がサポートされます。
- 各方向のラベルごとに 2 つの L4OP がサポートされます。各ラベルは、同じ ACL の複数のインターフェイスで共有できます。
- 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 *12 : 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
SUP（入力）	112	48	16

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
PACL（入力）	400	0	16
VACL（入力）、VACL（出力）	640（入力）、640（出力）	0（入力）、0（出力）	16
RACL（入力）	1536	0	16
QOS（入力）、QOS（出力）	192（入力）、64（出力）	16（入力）、64（出力）	16
E-VACL（出力）	640	0	16
E-RACL（出力）	256	0	16
NAT	256	0	16

ACL のライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

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。

- ACL の設定には Session Manager を使用することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。

- 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）
- 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。
- 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。
- ワープ モードでの出力 RACL および VACL はサポートされていないため、適用しないでください。
- 出力 ACL は、マルチキャスト トラフィックには適用できません。
- マルチキャスト トラフィックでは SVI での入力 RACL がサポートされていますが、トラフィックに必ず送信先または送信元となるマルチキャスト グループを定義する ACL に **log** キーワードが含まれている場合は、SVI での入力 RACL の適用はサポートされません。
- SVI のマルチキャスト トラフィックの入力 RACL ACE を照合するには、ACE にマルチキャスト DIP の照合を含める必要があります。また、これらの ACE をインストールする前に、**RACL - ハードウェア プロファイル tcam mcast racl-bridge を使用してブリッジング** コマンドを有効にする必要があります。
- PACL はワープ モードでは適用できません。
- SVI とレイヤ 3 インターフェイスの同じ入力 RACL では TCAM リソースを共有できないため、それぞれが個別に TCAM リソースを使用します。ただし、ACL 統計情報リソースは共有されます。アップグレード前に RACL TCAM をほとんど使い切っている場合、アップグレード後に RACL アプリケーションで障害が発生する可能性があります。その場合は、RACL TCAM を切り分けることができます。
- ARP ACL は Nexus 3500 プラットフォームではサポートされません。
- 物理または論理レイヤ 3 インターフェイスに適用される入力 RACL がサポートされています。入力 RACL をレイヤ 3 SVI に適用するには、ハードウェア プロファイル *tcam mcast racl-bridge* 構成を、マルチキャスト トラフィックを一致させるための回避策として使用できます。
- Cisco NX-OS リリース 7.0(3)I7(6) 以前から、Cisco NX-OS リリース 9.3(1) から 9.3(2) 以降にアップグレードし、デフォルトの lou しきい値構成を使用すると lou しきい値が 1 に設定されます。

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。

Table 13: 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。
オブジェクト グループ	デフォルトではオブジェクト グループは存在しません。

次の表に、VACL パラメータのデフォルト設定を示します。

Table 14: 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。

IP ACL の設定

IP ACL の作成

スイッチに IPv4 ACL を作成し、その ACL にルールを追加できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **ip access-list** *name*	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)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*	IP ACL 内にルールを作成します。多数のルールを作成できます。 *sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、特定の Cisco Nexus デバイスの

	コマンドまたはアクション	目的
		『*Command Reference*』を参照してください。
ステップ 4	（任意） switch(config-acl)# **statistics**	ACL 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。
ステップ 5	（任意） switch# **show ip access-lists** *name*	IP ACL の設定を表示します。
ステップ 6	（任意） switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

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
```

IP ACL の変更

既存の IPv4 ACL に対してルールの追加または削除を行うことができます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

Procedure

	Command or Action	Purpose
ステップ 1	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 access-list** *name*	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-list** *name*	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)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*	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

	Command or Action	Purpose
		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。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。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。
ステップ 5	(Optional) switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}	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『*Command Reference*』を参照してください。
ステップ 6	(Optional) switch(config-acl)# [**no**] **statistics**	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保持されなくなります。
ステップ 7	(Optional) switch# **show ip access-lists** *name*	IP ACL の設定を表示します。
ステップ 8	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

Related Topics

IP ACL 内のシーケンス番号の変更 （120 ページ）

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no ip access-list** *name*	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-list** *name*	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	(Optional) switch# **show running-config**	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す。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **resequence ip access-list** *name starting-sequence-number increment*	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。*starting-sequence-number* 引数と *increment* 引数は、1 ～ 4294967295 の整数で指定します。
ステップ 3	(Optional) switch# **show ip access-lists** *name*	IP ACL の設定を表示します。
ステップ 4	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

mgmt0 への IP-ACL の適用

IPv4 ACL は、管理インターフェイス（mgmt0）に適用できます。

始める前に

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：
	`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 mgmt** *port*
	例：
	`switch(config)# interface mgmt0`
	`switch(config-if)#`
		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。

ステップ 3	**ip access-group** *access-list* {**in** | **out**} 例： `switch(config-if)#ip access-group acl-120 out`	IPv4 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	（任意） **show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	ACL の設定を表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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 PortChannel に適用できます。これらのインターフェイス タイプに適用された ACL は、ポート ACL と見なされます。

Note 一部の設定パラメータは、ポート チャネルに適用されていると、メンバー ポートの設定に反映されません。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel** *channel-number*}	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** *access-list* **in**	IPv4 ACL を、インターフェイスまたはポート チャネルに適用します。ポート ACL では、インバウンド フィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。
ステップ 4	(Optional) switch# **show running-config**	ACL の設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

ルータ ACL としての IP ACL の適用

IPv4 ACL は、次のタイプのインターフェイスに適用できます。

- 物理層 3 インターフェイスおよびサブインターフェイス
- レイヤ 3 イーサネット ポート チャネル インターフェイス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。

Note 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制御エントリ（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。

Before you begin

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	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	次のいずれかのコマンドを入力します。 • switch(config)# **interface ethernet** *slot*/*port*[**.** *number*] • switch(config)# **interface port-channel** *channel-number*[**.** *number*] • switch(config)# **interface tunnel** *tunnel-number* • switch(config)# **interface vlan** *vlan-ID* • switch(config)# **interface mgmt** *port*	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	switch(config-if)# **ip access-group** *access-list* {**in** | **out**}	IPv4 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	(Optional) switch(config-if)# **show running-config aclmgr**	ACL の設定を表示します。
ステップ 5	(Optional) switch(config-if)# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

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。

Procedure

- switch# **show running-config**

  ACL の設定（IP ACL の設定と IP ACL が適用されるインターフェイス）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。

Example

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『*Command Reference*』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** 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。

Note MAC アクセス リストは、非 IPv4 トラフィックだけに適用可能です。

Procedure

- switch# **show ip access-lists** *name*

  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# **show ip access-lists** *name*

  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 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。

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

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。

Note 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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **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。

	Command or Action	Purpose
ステップ 3	switch(config-access-map)# **match ip address** *ip-access-list*	マップの IPv4 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	(Optional) switch(config-access-map)# [**no**] **statistics**	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	(Optional) switch(config-access-map)# **show running-config**	ACL の設定を表示します。
ステップ 7	(Optional) switch(config-access-map)# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no vlan access-map** *map-name*	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	(Optional) switch(config)# **show running-config**	ACL の設定を表示します。
ステップ 4	(Optional) switch(config)# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

VACL の VLAN への適用

VACL を VLAN に適用できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **vlan filter** *map-name* **vlan-list** *list*	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	(Optional) switch(config)# **show running-config**	ACL の設定を表示します。
ステップ 4	(Optional) switch(config)# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

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。

Procedure

- 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。

Procedure

- 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
```

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** | **e-racl**} | **ifacl** | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** } *tcam_size*	ACL TCAM リージョン サイズを変更します。 • **arpacl**：アドレス解決プロトコル（ARP）の ACL（ARPACL）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。

	コマンドまたはアクション	目的
		• **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。 • **nat**：NAT TCAM リージョンのサイズを設定します。 • **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（RACL）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。 （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。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 4	switch(config)# **show hardware profile tcam region** 例： `switch(config)# show hardware profile tcam region`	スイッチの次回のリロード時に適用される TCAM サイズを表示します。
ステップ 5	switch(config)# **reload** 例： `switch(config)# reload`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
		（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。

例

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、スイッチで TCAM VLAN ACL 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)# hardware profile tcam region vacl 512
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

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
```

この例では、特定のリージョンの TCAM の使用率を判断する方法を示しています。この例には 5 つの RACL エントリがあります。

```
switch(config)# show system internal aclqos platform mtc info tcam 0 region racl
         racl TCAM configuration for asic id 0:
[        sup tcam]: range     0 -   47
[       vacl tcam]: range   512 - 1087
[      ifacl tcam]: range   112 -  511
[        qos tcam]: range  3712 - 3903
[      rbacl tcam]: range     0 -    0
[       span tcam]: range     0 -    0
```

```
[       racl tcam]: range  1984 - 3455 *
[     e-racl tcam]: range  3456 - 3711
[     e-vacl tcam]: range  1088 - 1727
[     qoslbl tcam]: range     0 -    0
[       ipsg tcam]: range     0 -    0
[     arpacl tcam]: range     0 -    0
[  ipv6-racl tcam]: range     0 -    0
[ipv6-e-racl tcam]: range     0 -    0
[   ipv6-sup tcam]: range     0 -    0
[   ipv6-qos tcam]: range     0 -    0
[        nat tcam]: range  1728 - 1983
[      e-qos tcam]: range  3904 - 3967
[        pbr tcam]: range     0 -    0
[   ipv6-pbr tcam]: range     0 -    0
[       copp tcam]: range    48 -  111

    TCAM [racl tcam]: [v:1, size:1472, start:1984 end:3455]
    In use tcam entries: 5
        3451-3455
    Link Local Entries:
    nat size =  256
```

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** | **nat** | **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	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 4	switch(config)# **reload**	スイッチをリロードします。

例

次に、デフォルトの RACL 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 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 回線にユーザーが接続できるため、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。

始める前に

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	（任意） switch(config-line)# **no access-class access-list-number {in | out}** **例：** `switch(config-line)# no access-class ozi2 in`	着信または発信アクセス制限を削除します。

	コマンドまたはアクション	目的
	`switch(config-line)# no access-class ozi3 out` `switch(config)#`	

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	（任意） switch# **show running-config aclmgr** 例： `switch# show running-config aclmgr`	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	（任意） switch# **copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

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
show running-config aclmgr	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。
show users	接続されているユーザーを表示します。
show access-lists *access-list-name*	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）の接続ユーザーの例を示します。

```
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#
```

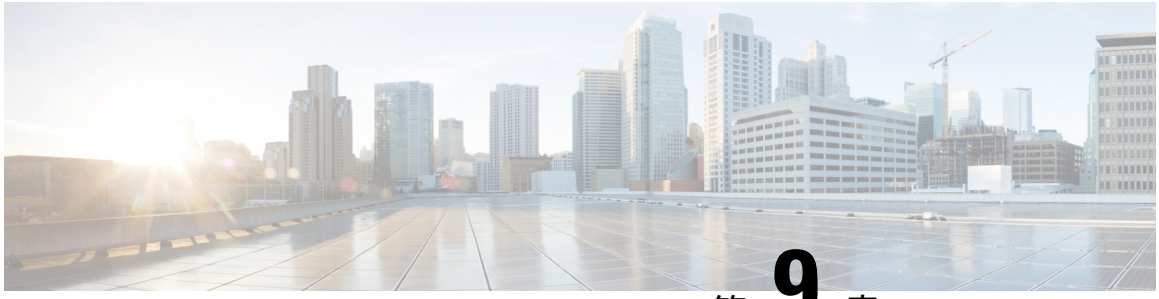
次に、in および out 方向で VTY の ACL を適用する例を示します。

```
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

この章は、次の項で構成されています。

DHCP スヌーピングについて

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

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

DHCP スヌーピングは、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、およびサーバーが含まれます。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。ユーザー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。

Note 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 サーバー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。

Note DHCP スヌーピング バインディング データベースは DHCP スヌーピング バインディング テーブルとも呼ばれます。

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、サーバーからの 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。

DHCP リレー エージェントについて

DHCP リレー エージェント

DHCP リレーエージェントを実行するようにデバイスを設定できます。DHCP リレーエージェントは、クライアントとサーバの間で DHCP パケットを転送します。これは、クライアントとサーバが同じ物理サブネット上にない場合に便利な機能です。リレー エージェントは DHCP メッセージを受信すると、新規の DHCP メッセージを生成して別のインターフェイスに送信します。リレーエージェントはゲートウェイアドレスを設定し（DHCP パケットの giaddr フィールド）、パケットにリレー エージェント情報のオプション（Option 82）を追加して（設定されている場合）、DHCP サーバに転送します。サーバからの応答は、Option 82 を削除してからクライアントに転送されます。

Option 82 をイネーブルにすると、デバイスはデフォルトでバイナリの ifindex 形式を使用します。必要に応じて Option 82 設定を変更して、代わりに符号化ストリング形式を使用できます。

Note デバイスは、Option 82 情報がすでに含まれている DHCP 要求を中継するときには、Option 82 情報を変更せずに元のままの状態で要求と一緒に転送します。

DHCP リレー エージェントに対する VRF サポート

DHCP ブロードキャスト メッセージを Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスのクライアントから別の VRF の DHCP サーバに転送するように、DHCP リレー エージェントを設定できます。単一の DHCP サーバを使用して複数の VRF のクライアントの DHCP をサポートできるため、IP アドレス プールを VRF ごとではなく 1 つにまとめることにより、IP アドレスを節約できます。

DHCP リレー エージェントに対する VRF サポートをイネーブルにするには、DHCP リレー エージェントに対する Option 82 をイネーブルにする必要があります。

DHCP リレー アドレスと VRF 情報を構成したインターフェイスに DHCP 要求が着信した場合、DHCP サーバーのアドレスが、別の VRF のメンバーであるインターフェイスのネットワークに属するものであれば、デバイスは要求に Option 82 情報を挿入し、それをサーバーの VRF の DHCP サーバーに転送します。Option 82 情報は次のとおりです。

VPN 識別子

DHCP 要求を受信するインターフェイスが属する VRF の名前。

リンクの選択

DHCP 要求を受信するインターフェイスのサブネット アドレス。

サーバ識別子オーバーライド

DHCP 要求を受信するインターフェイスの IP アドレス。

（注） DHCP サーバは、VPN 識別子、リンクの選択、サーバ識別子オーバーライドの各オプションをサポートする必要があります。

デバイスは DHCP 応答メッセージを受信すると、Option 82 情報を取り除き、クライアントの VRF の DHCP クライアントに応答を転送します。

DHCP リレー バインディング データベース

リレー バインディングは、リレー エージェントのアドレスおよびサブネットに、DHCP または BOOTP クライアントを関連付けるエントリです。各リレー バインディングは、クライアントの MAC アドレス、アクティブなリレー エージェント アドレス、アクティブなリレー エージェントアドレスマスク、クライアントが接続されている論理および物理インターフェイス、giaddr リトライ回数、および合計リトライ回数を格納します。giaddr リトライ回数は、リレーエージェントアドレスに送信される要求パケットの数です。合計リトライ回数は、リレーエージェントによって送信される要求パケットの合計数です。1 つのリレーバインディングエントリが、各 DHCP または BOOTP クライアントに対して維持されます。

Note DHCP スマート リレーをグローバルにイネーブルにするか、または任意のスイッチのインターフェイス レベルでイネーブルにする場合、すべてのスイッチのリレー バインディングは vPC ピアと同期する必要があります。

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。

- 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サーバーや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 サーバーと 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。

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。

***Table 15: 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
DHCP スヌーピングのグローバルなイネーブル化	なし
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
DHCP リレー エージェント	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

Procedure

	Command or Action	Purpose
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。

	Command or Action	Purpose
		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, on page 143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化します。	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, on page 144を参照してください。
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, on page 145を参照してください。
ステップ 4	DHCP サーバーとスイッチが、信頼できるインターフェイスを使用して接続されていることを確認します。	詳細については、インターフェイスの信頼状態の設定, on page 149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。

Before you begin

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] feature dhcp** **Example:** `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

	Command or Action	Purpose
		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	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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 DHCP メッセージのリレー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。

Before you begin

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip dhcp snooping** **Example:** `switch(config)# ip dhcp snooping`	DHCP スヌーピングをグローバルにイネーブル化します。**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	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。

	Command or Action	Purpose
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

Before you begin

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。

Note DHCP スヌーピングを使用して設定を行っている VLAN で VACL が設定されている場合、その VACL で DHCP サーバーと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip dhcp snooping vlan** *vlan-list* **Example:** `switch(config)# ip dhcp snooping vlan 100,200,250-252`	*vlan-list* 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	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。

	Command or Action	Purpose
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

Option 82 データの挿入および削除の有効化または無効化

DHCP リレー エージェントを使用せずに転送された DHCP パケットへの Option 82 情報の挿入および削除を有効または無効にできます。デフォルトでは、デバイスは DHCP パケットに Option 82 情報を挿入しません。

Note Option 82 に対する DHCP リレー エージェントのサポートは、個別に設定されます。

Before you begin

DHCP 機能がイネーブルになっていることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`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** **Example:** `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	(Optional) [**no**] **ip dhcp snooping sub-option circuit-id format-type string format** **Example:** `switch(config)# ip dhcp snooping sub-option circuit-id format-type string format`	入力 ifindex 名、ホスト名、またはホスト名と ifindex 名の組み合わせをエンコードした文字列形式を使用するには、オプション 82 を設定します（ホスト名を使用する場合は「%h」、ifindex を使用する場合は「%p」、ホスト名と ifindex 名を両方使用する場合は「%h」と「%p」の組み合わせを指定します）。

	Command or Action	Purpose
ステップ 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	DHCP 設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

Option 82 ユーザー定義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

サーバーに転送された DHCP パケットへの Option 82 ユーザー定義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設定できます。この設定は、ポートごとに適用され、エンコード文字列形式の入力 ifindex 名を使用する Option82 グローバル コンフィギュレーションよりも優先されます。SVI 上で DHCP リレーを設定すると、入力物理 *ifindex* に基づくユーザー定義文字列が、リレー対象の DHCP パケットに付加されます。

デフォルト状態のデバイスは、DHCP パケットに Option 82 情報を挿入しません。

Note ユーザー定義の Option 82 設定は、DHCP リレーと DHCP スヌーピングの両方に適用されます。

Before you begin

DHCP 機能がイネーブルになっていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	**config t**	グローバル コ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**	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。

	Command or Action	Purpose
ステップ 3	**interface ethernet** *slot/port*	インターフェイス コンフィギュレーション モードを開始します。slot/port は、Option 82 文字列を設定するレイヤ 2 イーサネット入力インターフェイスです。
ステップ 4	**ip dhcp option82 suboption circuit-id** *user-defined-circuit-id* **Example:** switch(config-if)# ip dhcp option82 suboption circuit-id po5-option82-string	ユーザーが定義した Option82 文字列をポート チャネル 5 で入力します。「po5-option82-string」という文字列が、ポート チャネル 5 で入力中の DHCP パケットに付加されます。イーサネット インターフェイスでも同じように設定されます。
ステップ 5	(Optional) **show ip dhcp option82 suboption info interface po5**	DHCP Option 82 の情報と統計情報を表示します。
ステップ 6	(Optional) **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip dhcp packet strict-validation** **Example:** `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	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。

	Command or Action	Purpose
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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

Before you begin

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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interface ethernet** *port*/*slot*
	• **interface port-channel** *channel-number*
	Example:
	`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。 *port*/*slot* は、DHCP スヌーピングで trusted または untrusted に設定するレイヤ2イーサネットインターフェイスです。
		• インターフェイス コンフィギュレーション モードを開始します。 *port*/*slot* は、DHCP スヌーピングで trusted または untrusted に設定するレイヤ 2 ポートチャネル インターフェイスです。

ステップ 3	[**no**] **ip dhcp snooping trust** **Example:**	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

	Command or Action	Purpose
	`switch(config-if)# ip dhcp snooping trust`	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	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	DHCP スヌーピングの設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

DHCP リレー エージェントのイネーブル化またはディセーブル化

DHCP リレー エージェントをイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP リレー エージェントはイネーブルです。

Before you begin

DHCP 機能がイネーブルになっていることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`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** **Example:** `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	(Optional) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	DHCP リレーの設定を表示します。
ステップ 4	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	DHCP 設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

DHCP リレー エージェントに対する Option 82 の有効化または無効化

デバイスに対し、リレー エージェントによって転送された DHCP パケットへの Option 82 情報の挿入と削除を有効または無効にできます。

デフォルトでは、DHCP リレー エージェントは DHCP パケットに Option 82 情報を挿入しません。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip dhcp relay** **Example:** `switch(config)# ip dhcp relay`	DHCP リレー機能をイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 3	[**no**] **ip dhcp relay information option** **Example:** `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有効にします。Option 82 情報は、デフォルトでバイナリ ifIndex 形式です。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 4	(Optional) **show ip dhcp relay** **Example:** `switch(config)# show ip dhcp relay`	DHCP リレーの設定を表示します。
ステップ 5	(Optional) **show running-config dhcp** **Example:** `switch(config)# show running-config dhcp`	DHCP 設定を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

DHCP リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化

ある VRF のインターフェイスで受信した DHCP 要求を、別の VRF インスタンスの DHCP サーバーにリレーできるよう、デバイスを設定することができます。

始める前に

DHCP リレー エージェントの Option 82 をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**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 information option vpn** 例： `switch(config)# ip dhcp relay information option vpn`	DHCP リレーエージェントに対して VRF サポートをイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 3	[**no**] **ip dhcp relay sub-option type cisco** 例： `switch(config)# ip dhcp relay sub-option type cisco`	リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID リレー エージェント Option 82 サブオプションを設定する場合は、DHCP をイネーブルにして、シスコ独自の番号である 150、152、および 151 を使用します。**no** オプションを使用すると、DHCP では、リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID サブオプションに対して、RFC 番号 5、11、151 が使用されるようになります。
ステップ 4	（任意） **show ip dhcp relay** 例：	DHCP リレーの設定を表示します。

	コマンドまたはアクション	目的
	`switch(config)# show ip dhcp relay`	
ステップ 5	（任意） **show running-config dhcp** 例： `switch(config)# show running-config dhcp`	DHCP 設定を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

レイヤ 3 インターフェイスの DHCP リレー エージェントに対するサブネット ブロードキャスト サポートのイネーブル化またはディセーブル化

クライアントからのサブネットのブロードキャスト IP アドレスに DHCP パケットのリレーをサポートするように、デバイスを設定できます。この機能がイネーブルの場合、VLAN ACL（VACL）は、IP ブロードキャスト パケット、すべてのサブネット ブロードキャスト（プライマリ サブネット ブロードキャストおよびセカンダリ サブネット ブロードキャスト）パケットを許容します。

始める前に

DHCP 機能がイネーブルになっていることを確認します。

DHCP リレー エージェントがイネーブルであることを確認します。

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	**interface** *interface slot/port*
	例：
	`switch(config)# interface ethernet 2/2`
	`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。*slot/port* は、DHCP リレー エージェントに対するサブネット ブロードキャスト サポートをイネーブルまたはディセーブルにするインターフェイスです。

	コマンドまたはアクション	目的
ステップ 3	**[no] ip dhcp relay subnet-broadcast** 例： `switch(config-if)# ip dhcp relay subnet-broadcast`	DHCP リレー エージェントに対するサブネット ブロードキャスト 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 4	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 6	（任意） **show ip dhcp relay** 例： `switch# show ip dhcp relay`	DHCP リレーの設定を表示します。
ステップ 7	（任意） **show running-config dhcp** 例： `switch# show running-config dhcp`	DHCP 設定を表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

Before you begin

DHCP 機能が有効になっていることを確認します。

DHCP サーバが正しく設定されていることを確認します。

インターフェイスに設定する、各 DHCP サーバの IP アドレスを決定します。

DHCP サーバー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。

Note DHCP サーバ アドレスを設定しているインターフェイスで入力ルータ ACL が設定されている場合、そのルータ ACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`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	次のいずれかのオプションを使用します。
	• **interface ethernet** *slot*/*port*[**.** *number*]
	• **interface vlan** *vlan-id*
	• **interface port-channel** *channel-id*[*.subchannel-id*]
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		• インターフェイス コンフィギュレーション モードを開始します。*slot*/*port* は、DHCP サーバー 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、*number* 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。*vlan-id* は、DHCP サーバー 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。*channel-id* は、DHCP サーバー 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、*subchannel-id* 引数を使用してサブチャネル ID を指定します。

ステップ 3	**ip dhcp relay address** *IP-address* [**use-vrf** *vrf-name*] **Example:** `switch(config-if)# ip dhcp relay address 10.132.7.120 use-vrf red`	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。

	Command or Action	Purpose
		複数の IP アドレスを設定するには、アドレスごとに **ip dhcp relay address** コマンドを使用します。
ステップ 4	(Optional) **show ip dhcp relay address** **Example:** `switch(config-if)# show ip dhcp relay address`	設定済みのすべての DHCP サーバー アドレスを表示します。
ステップ 5	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	DHCP 設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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。

始める前に

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：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ip source binding** *IP-address MAC-address* **vlan** *vlan-id* { **interface ethernet** *slot/port* | **port-channel** *channel-no*} 例： `switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3`	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。

	コマンドまたはアクション	目的
ステップ 3	（任意） **show ip dhcp snooping binding** 例： `switch(config)# ip dhcp snooping binding`	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	（任意） **show ip dhcp snooping binding dynamic** 例： `switch(config)# ip dhcp snooping binding dynamic`	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	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

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)#
```

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 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。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	(Optional) **clear ip dhcp snooping binding** **Example:** `switch# clear ip dhcp snooping binding`	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	(Optional) **clear ip dhcp snooping binding interface ethernet** *slot*/*port*[.*subinterface-number*] **Example:** `switch# clear ip dhcp snooping binding interface ethernet 1/4`	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。

	Command or Action	Purpose
ステップ 3	(Optional) **clear ip dhcp snooping binding interface port-channel** *channel-number*[*.subchannel-number*] **Example:** `switch# clear ip dhcp snooping binding interface port-channel 72`	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	(Optional) **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*] } **Example:** `switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface ethernet 2/11`	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。
ステップ 5	(Optional) **show ip dhcp snooping binding** **Example:** `switch# show ip dhcp snooping binding`	DHCP スヌーピング バインディング データベースを表示します。

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ー レベルでの DHCP 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ーするには、show ip dhcp snooping statistics コマンドを使用します。

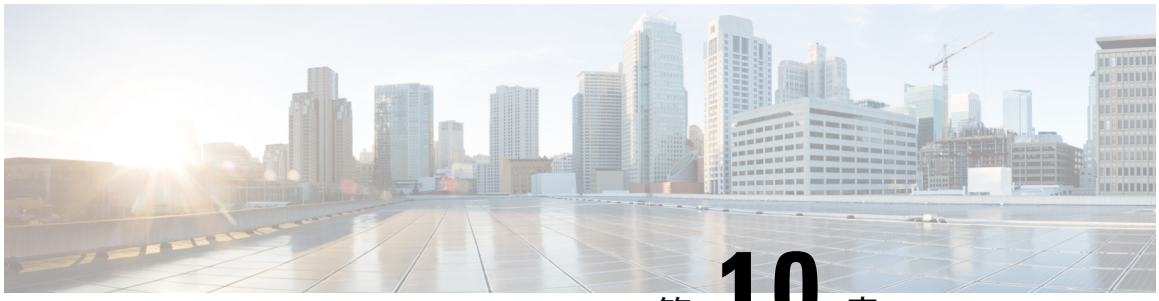
show ip dhcp relay statistics [**interface** *interface* [**serverip** *ip-address* [**use-vrf** *vrf-name*]]] コマンドを使用して、グローバル、サーバー、またはインターフェイス レベルでの DHCP リレー統計情報をモニターします。

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 サーバーがイーサネット 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

MAC ACL の設定

この章では、Cisco NX-OS デバイスの MAC アクセス コントロール リスト（ACL）を設定する手順について説明します。

MAC ACL の概要

MAC ACL は、パケットのレイヤ 2 ヘッダーを使用してトラフィックをフィルタリングする ACL です。バーチャライゼーションのサポートなど、MAC ACL の基本的な機能の多くは IP ACL と共通です。

MAC パケット分類

MAC パケット分類により、レイヤ 2 インターフェイス上の MAC ACL を、IP トラフィックなどインターフェイスに入るすべてのトラフィックに適用するか、非 IP トラフィックだけに適用するかを制御できます。

MAC パケット分類は、HSRP、VRRP、OSPF などのレイヤ 3 コントロール プレーン プロトコルでは機能しません。VLAN で MAC パケット分類を有効にすると、これらのプロトコルで基本的な機能が壊れます。

MAC パケット分類の状態	インターフェイスでの効果
イネーブル	• インターフェイス上の MAC ACL は、IP トラフィックなどインターフェイスに入るすべてのトラフィックに適用されます。 • IP ポート ACL をインターフェイスで適用できますが、トラフィックのフィルタリングは行われません。
ディセーブル	• インターフェイス上の MAC ACL は、インターフェイスに入る非 IP トラフィックだけに適用されます。 • インターフェイスで IP ポート ACL を適用することができます。これにより、トラフィックがフィルタリングされます。

MAC ACL のデフォルト設定

次の表に、MAC ACL パラメータのデフォルト設定を示します。

***Table 16: MAC ACL* のデフォルト パラメータ**

パラメータ	デフォルト
MAC ACL	デフォルトでは MAC ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。

MAC ACL の注意事項と制約事項

MAC ACL の設定に関する注意事項と制約事項は次のとおりです。

- MAC ACL は入トラフィックだけに適用されます。
- ハードウェアの制限により、MAC ACL は Cisco Nexus 3500 プラットフォーム スイッチの ARP パケットをフィルタ処理しません。

MAC ACL の設定

MAC ACL の作成

MAC ACL を作成し、これにルールを追加できます。

Procedure

	Command or Action	Purpose
ステップ 1	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)# **mac access-list** *name*	MAC ACL を作成して、ACL コンフィギュレーション モードを開始します。
ステップ 3	switch(config-mac-acl)# {**permit** | **deny**} *source destination protocol*	MAC ACL 内にルールを作成します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	(Optional) switch(config-mac-acl)# **statistics per-entry**	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。
ステップ 5	(Optional) switch(config-mac-acl)# **show mac access-lists** *name*	MAC ACL の設定を表示します。
ステップ 6	(Optional) switch(config-mac-acl)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、MAC ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01

MAC ACL acl-mac-01
        statistics per-entry
        10 permit 00c0.4f00.0000 0000.00ff.ffff any

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

MAC ACL の変更

MAC ACL をデバイスから削除できます。

Before you begin

MAC ACL が設定されているインターフェイスを探すには、**summary** キーワードを指定して **show mac access-lists** コマンドを使用します。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **mac access-list** *name*	名前で指定した ACL の ACL コンフィギュレーション モードを開始します。
ステップ 3	(Optional) switch(config-mac-acl)# [*sequence-number*] {**permit** | **deny**} *source destination protocol*	MAC ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	(Optional) switch(config-mac-acl)# **no** {*sequence-number* | {**permit** | **deny**} *source destination protocol*}	指定したルールを MAC ACL から削除します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 5	(Optional) switch(config-mac-acl)# [**no**] **statistics per-entry**	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 **no** オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 6	(Optional) switch(config-mac-acl)# **show mac access-lists** *name*	MAC ACL の設定を表示します。
ステップ 7	(Optional) switch(config-mac-acl)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、MAC ACL を変更する例を示します。

```
switch# configure terminal
switch(config)# mac access-list acl-mac-01
switch(config-mac-acl)# 100 permit 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# 80 permit 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# no 80
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01

MAC ACL acl-mac-01
        statistics per-entry
        10 permit 00c0.4f00.0000 0000.00ff.ffff any
        100 permit 00c0.4f00.0000 0000.00ff.ffff any

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

MAC ACL 内のシーケンス番号の変更

MAC ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。ACL にルールを挿入する必要がある場合で、シーケンス番号が不足しているときは、再割り当てすると便利です。

Procedure

	Command or Action	Purpose
ステップ 1	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)# **resequence mac access-list** *name starting-sequence-number increment*	ACL 内に記述されているルールにシーケンス番号を付けます。starting-sequence number に指定したシーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。
ステップ 3	(Optional) switch(config)# **show mac access-lists** *name*	MAC ACL の設定を表示します。
ステップ 4	(Optional) switch(config)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、MAC ACL のシーケンスを変更する例を示します。

```
switch# configure terminal
switch(config)# resequence mac access-list acl-mac-01 100 15
switch(config)# show mac access-lists acl-mac-01
```

```
MAC ACL acl-mac-01
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any
        115 permit 00c0.4f00.0000 0000.00ff.ffff any

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

MAC ACL の削除

MAC ACL をデバイスから削除できます。

Procedure

	Command or Action	Purpose
ステップ 1	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 mac access-list** *name*	名前で指定した MAC ACL を実行コンフィギュレーションから削除します。
ステップ 3	(Optional) switch(config)# **show mac access-lists** *name* **summary**	MAC ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	(Optional) switch(config)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、MAC ACL を削除する例を示します。

```
switch# configure terminal
switch(config)# show mac access-lists

MAC ACL acl-mac-01
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any
        115 permit 00c0.4f00.0000 0000.00ff.ffff any
MAC ACL acl-mac-02
        statistics per-entry
        10 permit 00a0.3f00.0000 0000.00dd.ffff any
MAC ACL acl-mac-03
        statistics per-entry
        10 permit 00b0.5f00.0000 0000.00aa.fbbf any

switch(config)# no mac access-list acl-mac-02
switch(config)# show mac access-lists acl-mac-02 summary
switch(config)# show mac access-lists

MAC ACL acl-mac-01
```

```
        statistics per-entry
        100 permit 00c0.4f00.0000 0000.00ff.ffff any
        115 permit 00c0.4f00.0000 0000.00ff.ffff any
MAC ACL acl-mac-03
        statistics per-entry
        10 permit 00b0.5f00.0000 0000.00aa.fbbf any

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

ポート ACL としての MAC ACL の適用

MAC ACL をポート ACL として、次のいずれかのインターフェイス タイプに適用できます。

- レイヤ 2 またはレイヤ 3 のイーサネット インターフェイス
- レイヤ 2 またはレイヤ 3 のポート チャネル インターフェイス

Before you begin

適用する ACL が存在し、必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	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	次のいずれかのコマンドを入力します。 • switch(config)# **interface ethernet** *slot*/*port* • switch(config)# **interface port-channel** *channel-number*	• レイヤ 2 またはレイヤ 3 のインターフェイス コンフィギュレーション モードを開始します。 • レイヤ 2 またはレイヤ 3 のポート チャネル インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **mac port access-group** *access-list*	MAC ACL をインターフェイスに適用します。
ステップ 4	(Optional) switch(config-if)# **show running-config aclmgr**	ACL の設定を表示します。
ステップ 5	(Optional) switch(config-if)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、イーサネット インターフェイスに MAC ACL をポート ACL として適用する方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# mac port access-group acl-mac-01
switch(config-if)# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Sat Jul 19 23:36:04 2014

version 6.0(2)A4(1)
mac access-list acl-mac-01
  statistics per-entry
  100 permit 00C0.4F00.0000 0000.00FF.FFFF any
  115 permit 00C0.4F00.0000 0000.00FF.FFFF any
mac access-list acl-mac-03
  statistics per-entry
  10 permit 00B0.5F00.0000 0000.00AA.FBBF any
ip access-list copp-system-acl-bfd
  10 permit udp any any eq 3784
ip access-list copp-system-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any

...

interface Ethernet1/3
  mac port access-group acl-mac-01

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

次の例は、ポートチャネル インターフェイスに MAC ACL をポート ACL として適用する方法を示しています。

```
switch# configure terminal
switch(config)# interface port-channel 5
switch(config-if)# mac port access-group acl-mac-01
switch(config-if)# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Sat Jul 19 23:37:04 2014

version 6.0(2)A4(1)
mac access-list acl-mac-01
  statistics per-entry
  100 permit 00C0.4F00.0000 0000.00FF.FFFF any
  115 permit 00C0.4F00.0000 0000.00FF.FFFF any
mac access-list acl-mac-03
  statistics per-entry
  10 permit 00B0.5F00.0000 0000.00AA.FBBF any
ip access-list copp-system-acl-bfd
  10 permit udp any any eq 3784
ip access-list copp-system-acl-eigrp
```

```
  10 permit eigrp any any
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any


...

interface port-channel5
  mac port access-group acl-mac-01

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

MAC パケット分類のイネーブル化または無効化

MAC パケット分類は、VLAN 単位でイネーブルまたはディセーブルに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	**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	**vlan** *vlan-number*
	例：
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		VLANインターフェイスを作成します。number の範囲は 1 ～ 4094 です。

ステップ 3	[**no**] **mac packet-classify**
	例：
	`switch(config-vlan)# mac packet-classify`
	`switch(config-vlan)#`
		vlan の MAC パケット分類を有効にします。**no** オプションを使用すると、vlan の MAC パケット分類がディセーブルになります。

ステップ 4	**exit**
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		vlan 構成を終了します。

ステップ 5	（任意） **show running-config vlan** *vlan-number*	実行設定を表示します。

例

次に、VLAN 単位で MAC パケット分類をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# vlan 50
switch(config-vlan)# mac packet-classify
switch(config-vlan)# exit
switch(config)# show running-config vlan 50

!Command: show running-config interface Vlan50
!Time: Wed Aug  6 20:39:03 2014

version 6.0(2)A4(1)

interface Vlan50
  mac packet-classify

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

MAC ACL の設定の確認

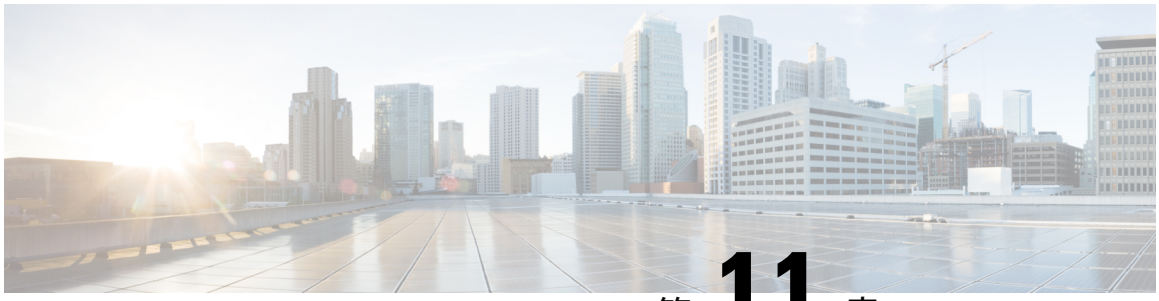
MAC ACL の設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。
show running-config aclmgr [**all**]	MAC ACL および MAC ACL が適用されるインターフェイスを含めて、ACL の設定を表示します。 **Note** **all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show startup-config aclmgr [**all**]	ACL のスタートアップ コンフィギュレーションを表示します。 **Note** **all** オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

MAC ACL 統計情報のクリア

clear mac access-list counters コマンドを使用して、MAC ACL 統計情報を消去できます。

コマンド	目的
clear mac access-list counters	すべての MAC ACL、または特定の MAC ACL の統計情報を消去します。



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。この章には次のセクションがあります。

ユニキャスト RPF の概要

ユニキャスト RPF 機能を使用すると、ネットワークに変形または偽造（スプーフィング）された IPv4 ソース アドレスが注入されて引き起こされる問題を、裏付けのない IPv4 パケットを廃棄する方法により緩和します。たとえば、Smurf や Tribal Flood Network（TFN）など、いくつかの一般的なサービス拒絶（DoS）攻撃では、偽造の送信元 IPv4 アドレスやすぐに変更される送信元 IPv4 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防ぎます。ユニキャスト RPF では、送信元アドレスが有効で IP ルーティング テーブルと一致するパケットだけを転送することにより、攻撃を回避します。

インターフェイス上でユニキャスト RPF を有効にすると、スイッチはそのインターフェイス上で受信されたすべての入力パケットを検証することにより、送信元アドレスと発信元インターフェイスがルーティング テーブル内に現れ、しかもパケット受信場所のインターフェイスと一致することを確認します。この送信元アドレス検査は転送情報ベース（FIB）に依存しています。

Note ユニキャスト RPF は入力機能であり、接続のアップストリーム エンドにあるスイッチの入力インターフェイスにのみ適用されます。

ユニキャスト RPF は、FIB のリバース ルックアップを実行することにより、スイッチ インターフェイスでの受信パケットがそのパケットの送信元への最良リターン パス（リターン ルート）

で着信していることを確認します。パケットが最適なリバース パス ルートのいずれかから受信された場合、パケットは通常どおりに転送されます。パケットを受信したインターフェイス上にリバース パス ルートがない場合、攻撃者によって送信元アドレスが変更される可能性があります。ユニキャスト RPF がそのパケットのリバースパスを見つけられない場合は、パケットはドロップされます。

Note ユニキャスト RPF では、コストが等しいすべての「最良」リターン パスが有効と見なされます。つまり、複数のリターン パスが存在していても、各パスのルーティング コスト（ホップ カウントや重みなど）が他のパスと等しく、そのルートが FIB 内にある限り、ユニキャスト RPF は機能します。ユニキャスト RPF は、Enhanced Interior Gateway Routing Protocol（EIGRP）バリアントが使用されていて、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

ユニキャスト Reverse Path Forwarding（RPF）機能を使用すると、ネットワークに変形または偽造（スプーフィング）された IP ソース アドレスが注入されて引き起こされる問題を、裏付けのない IP ソース アドレスを廃棄する方法により緩和します。たとえば、Smurf や Tribal Flood Network（TFN）など、いくつかの一般的なサービス拒絶（DoS）攻撃では、偽造の送信元 IP アドレスやすぐに変更される送信元 IP 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防ぎます。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。

グローバル統計

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すが、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 の注意事項と制約事項

ユニキャスト RPF に関する注意事項と制約事項は次のとおりです。

- Cisco Nexus 3548 シリーズ スイッチの固有機能であるワープ モードで URPF を有効にすると、マルチキャスト エントリ数が半分になり、8 k から 4 k になります。同様に、ホスト エントリの数も、8 k の半分の 4 k になります。通常モードでは、サポートされる LPM エントリの数が半分に（24 k から 12 k に）なりますが、これは Cisco Nexus 3000 シリーズ スイッチの場合と同じです。

- 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 サーバーにユニキャスト 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多いからです。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。

ユニキャスト RPF のデフォルト設定

次の表に、ユニキャスト RPF パラメータのデフォルト設定を示します。

Table 17: ユニキャスト *RPF* パラメータのデフォルト設定

パラメータ	デフォルト
ユニキャスト RPF	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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`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**} **Example:**	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** キーワードは緩和モードのユニキャスト RPF を指定します。

	Command or Action	Purpose
	`switch(config-if)# ip verify unicast source reachable-via any`	**allow-default** キーワードを指定すると、送信元アドレスのルックアップでデフォルト ルートと一致させることが可能であり、これを検証に使用できます。 **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	**exit**
	Example:
	`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 5	(Optional) **show ip interface ethernet** *slot*/*port* **Example:** `switch(config)# show ip interface ethernet 2/3`	インターフェイスの IP 情報を表示します。
ステップ 6	(Optional) **show running-config interface ethernet** *slot*/*port* **Example:** `switch(config)# show running-config interface ethernet 2/3`	実行コンフィギュレーション内のインターフェイスの情報を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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
```

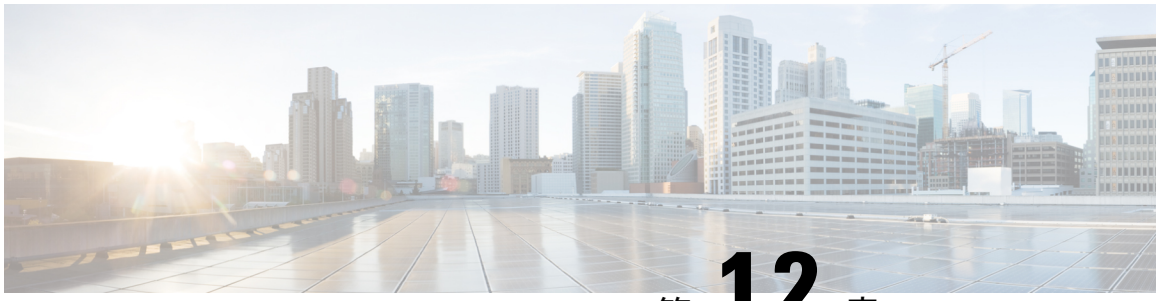
厳格モード（ストリクト モード）の IPv4 パケット用ユニキャスト RPF の設定例を示します。

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

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 ethernet *slot/port*	実行コンフィギュレーション内のインターフェイスの設定を表示します。
show running-config ip [**all**]	実行コンフィギュレーション内の IPv4 設定を表示します。
show startup-config interface ethernet *slot/port*	スタートアップ コンフィギュレーション内のインターフェイスの設定を表示します。
show startup-config ip	スタートアップ コンフィギュレーション内の IP 設定を表示します。



第 12 章

コントロール プレーン ポリシングの設定

この章は、次の内容で構成されています。

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妨害（DoS）攻撃です。

Cisco NX-OS デバイスは、DoS 攻撃がパフォーマンスに影響しないようにするために CoPP を提供します。このような攻撃は誤って、または悪意を持って実行される場合があり、通常は、スーパーバイザ モジュールまたは CPU 自体に宛てられた大量のトラフィックが含まれます。

スーパーバイザ モジュールは、管理対象のトラフィックを次の 3 つの機能コンポーネント（プレーン）に分類します。

データ プレーン
すべてのデータ トラフィックを処理します。NX-OS デバイスの基本的な機能は、インターフェイス間でパケットを転送することです。スイッチ自身に向けられたものでないパケットは、中継パケットと呼ばれます。データ プレーンで処理されるのはこれらのパケットです。

コントロール プレーン
ルーティング プロトコルのすべての制御トラフィックを処理します。ボーダー ゲートウェイ プロトコル（BGP）や Open Shortest Path First（OSPF）プロトコルなどのルーティング プロトコルは、デバイス間で制御パケットを送信します。これらのパケットはルータのアドレスを宛先とし、コントロール プレーン パケットと呼ばれます。

管理プレーン
コマンドライン インターフェイス（CLI）や簡易ネットワーク管理プロトコル（SNMP）など、NX-OS デバイスを管理する目的のコンポーネントを実行します。

スーパーバイザ モジュールには、管理プレーンとコントロール プレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。スーパーバイザ モジュールの動作が途絶したり、スーパーバイザ モジュールが攻撃されたりすると、重大なネットワークの停止につながります。たとえばスーパーバイザに過剰なトラフィックが加わると、スーパーバイザ モジュールが過負荷になり、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

Caution コントロール プレーンの保護策を講じることで、スーパーバイザ モジュールを偶発的な攻撃や悪意ある攻撃から確実に保護することが重要です。

コントロール プレーン保護

コントロール プレーンを保護するために、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、クラスマップとポリシーマップを使用してパケット分類とレート制御ポリシーを設定し、厳格さを強めることが考えられます。

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-ptp
    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-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-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 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-ptp
    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
```

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。

スイッチ宛ての Protocol-Independent Multicast（PIM）データ登録パケットと一致するように、新しい CoPP クラス「copp-s-pim-datareg」が追加されました。この CoPP クラスは、PIM データ登録パケットを 600 パケット/秒（pps）のポリサー レートで別個のキューに分類するために役立ちます。PIM プロトコルの 3 つの CoPP クラスを以下に示します。

- **copp-s-pimreg** - PIM hello や join-prune などの、マルチキャスト パケットである PIM プロトコル パケットに一致します。
- **copp-s-pimautorp** – PIM RP 選択プロトコル パケットに一致します。
- **copp-s-pim-datareg** - PIM データ登録パケットに一致します。

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。

- 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が変更されたら、CoPP を変更する必要があります。
- **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、ポリシングの 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 を継続的にモニター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応答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。
- アップグレードする際には、デフォルト LLDP CoPP 値が 500 pps 未満であるかどうか確認してください。500 pps 未満である場合は、次のコマンドを使用して、手動で 500 pps に変更してください。

```
switch(config)# policy-map type control-plane policy-map-name
switch(config-pmap)# class copp-s-lldp
switch(config-pmap-c)# police pps 500
```

- glean（キャッシュ モードのクラス デフォルトのクラス マップ）に関するハードウェア カウンタはありません。
- MTU 障害クラス マップに関するカウンタはありません。
- NAT に関するハードウェア カウンタはありません。
- IPMCMISS に関するハードウェア カウンタはありません。
- スタティック クラス マップには match ACL ステートメントを追加できません。
- トンネルが設定されていない場合、Cisco Nexus 3500 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 3500 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 3500 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。
- 前面パネル ポート経由で NXAPI を使用する場合は、パケットがドロップせず、出力が大きい CLI が予定時間内に戻るように、3000 PPS トラフィックを許可するように（http の）CoPP ポリシーを増やす必要があります。
- セットアップ スクリプトを実行すると、「*Enter to basic configuration (yes/no)?*」というプロンプトが表示されます。
  - *no* と応答すると、デフォルトの CoPP ポリシー テンプレートはシステムに適用されません。
  - *yes* と応答すると、稼働バージョンのデフォルトの CoPP ポリシー テンプレートがシステムに適用されます。この操作により、システム CoPP クラスに設定されているデフォルト以外のポリサー レートが上書きされます。

（注） スクリプトのセットアップ スクリプトの実行中に Ctrl+C を押すと、デフォルトの CoPP ポリシー テンプレートはシステムに適用されず、既存の CoPP ポリシーは変更されません

- セットアップ スクリプトを実行して基本設定を入力した後に Ctrl+C を押すと、残りのすべてのステップがスキップされ、「*Apply and save the config before exiting (yes/no)?*」というプロンプトが表示されます。
  - *no* と応答すると、デフォルトの CoPP ポリシーテンプレートはシステムに適用されません。
  - *yes* と応答すると、稼働バージョンのデフォルトの CoPP ポリシー テンプレートが適用されます。この操作により、システム CoPP クラスに設定されているデフォルト以外のポリサー レートが上書きされます。
- セットアップ スクリプトは、ユーザー定義の CoPP クラスを変更しません。
- セットアップ スクリプトが正常に実行され、その一環としてデフォルトの CoPP ポリシーテンプレートが適用されると、制御パケットが短時間ドロップされることがあります。この期間中に、コントロール プレーン プロトコルがフラップすることがあります。
- PPS のクレジットが使い果たされると、セットアップ スクリプトがデフォルトの CoPP ポリシーテンプレートの設定に失敗することがあります。これにより、PPS がゼロのシステム CoPP クラスが 1 つ以上生じることがあります。これにより、高い PPS 値を持つユーザー定義クラスがあるときに起こる可能性があります。デフォルトの CoPP ポリシーを適用するには、ユーザー定義の CoPP クラスの PPS 値を再設定して、セットアップ スクリプトを再度実行する必要があります。
- CDP（copp-s-cdp）、LLDP（copp-s-lldp）、LACP（copp-s-lacp）、BPDU（copp-s-bpdu）クラスのハードウェアおよびソフトウェア一致パケット カウンタが、Cisco Nexus 3548 プラットフォーム スイッチで集約されます。同様に、copp-s-dhcpreq および copp-s-dhcpresp クラスのハードウェアおよびソフトウェア一致パケット カウンタも集約されます。

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、l3、l2）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ング 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。
- Cisco NX-OS Release 6.0(2)A3(2) にアップグレードする際には、デフォルト LLDP CoPP 値が 500 pps 未満であるかどうか確認してください。500 より小さい場合は、次のコマンドを使用して、手動で 500 に変更してください。

```
switch(config)# policy-map type control-plane copp-system-policy
switch(config-pmap)# class copp-s-lldp
switch(config-pmap-c)# police pps 500
```

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。

始める前に

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	**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	**class-map type control-plane match-any** *class-map-name*
	例：
	`switch(config)# class-map type control-plane ClassMapA`
	`switch(config-cmap)#`
		コントロール プレーン クラス マップを指定し、クラス マップ コンフィギュレーション モードを開始します。デフォルトのクラス一致は match-any です。名前は最大 64 文字で、大文字と小文字は区別されます。
		（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。

	コマンドまたはアクション	目的
ステップ 3	（任意） **match access-group name** *access-list-name* 例： `switch(config-cmap)# match access-group name MyAccessList`	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：
	`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 5	（任意） **show class-map type control-plane** [*class-map-name*] 例： `switch(config)# show class-map type control-plane`	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	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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、そのクラスのデフォルトPPSは0になります。

IPv4 パケットのポリシーを設定できます。

始める前に

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：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**policy-map type control-plane** *policy-map-name*
	例：
	`switch(config)# policy-map type control-plane copp-system-policy`
	`switch(config-pmap)#`
		コントロール プレーン ポリシー マップを指定し、ポリシー マップ コンフィギュレーション モードを開始します。ポリシー マップ名は大文字と小文字が区別されます。
		（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。

ステップ 3	**class** {*class-map-name* | **class**}
	例：
	`switch(config-pmap)# class ClassMapA`
	`switch(config-pmap-c)#`
		コントロール プレーン クラス マップ名またはクラス デフォルトを指定し、コントロール プレーン クラス コンフィギュレーション モードを開始します。

ステップ 4	**police** [**pps**] {*pps-value*} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**] 例： `switch(config-pmap-c)# police pps 100 bc 10`	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。

ステップ 5	**exit**
	例：
	`switch(config-pmap-c)# exit`
	`switch(config-pmap)#`
		ポリシー マップ クラス コンフィギュレーション モードを終了します。

ステップ 6	**exit**
	例：
	`switch(config-pmap)# exit`
	`switch(config)#`
		ポリシー マップ コンフィギュレーション モードを終了します。

ステップ 7	（任意） **show policy-map type control-plane** [**expand**] [**name** *class-map-name*] 例： `switch(config)# show policy-map type control-plane`	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。

	コマンドまたはアクション	目的
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

コントロール プレーン サービス ポリシーの設定

始める前に

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	**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 4	（任意） **show running-config copp** [**all**] 例： `switch(config)# show running-config copp`	CoPP 設定を表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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 [*acl-name*]	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 [*class-map-name*]	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 policy-map type control-plane [**expand**] [**name** *policy-map-name*]	コントロール プレーン ポリシー マップと関連するクラスマップおよび PPS の値を表示します。
show running-config copp [**all**]	実行コンフィギュレーション内の CoPP 設定を表示します。
show running-config aclmgr [**all**]	実行コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。**all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show startup-config copp [**all**]	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
show startup-config aclmgr [**all**]	スタートアップ コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。**all** オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

CoPP 設定ステータスの表示

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show copp status**	CoPP 機能の設定ステータスを表示します。

Example

次に、CoPP 設定ステータスを表示する例を示します。

```
switch# show copp status
```

CoPP のモニタリング

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show policy-map interface control-plane**	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。

Example

次に、CoPP をモニタする例を示します。

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

service-policy  input: copp-system-policy

  class-map copp-s-default (match-any)
    police pps 400 , bc 0 packets
      HW Matched Packets    0
      SW Matched Packets   0
  class-map copp-s-ping (match-any)
    match access-group name copp-system-acl-ping
    police pps 100 , bc 0 packets
      HW Matched Packets    0
      SW Matched Packets   0
....
```

CoPP 統計情報のクリア

Procedure

	Command or Action	Purpose
ステップ 1	(Optional) switch# **show policy-map interface control-plane**	現在適用されている CoPP ポリシーおよびクラスごとの統計情報を表示します。
ステップ 2	switch# **clear copp statistics**	CoPP 統計情報をクリアします。

Example

次に、インターフェイス環境で、CoPP 統計情報をクリアする例を示します。

```
switch# show policy-map interface control-plane
switch# clear copp statistics
```

CoPP の設定例

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>
```

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
```

コントロール プレーン クラス マップの設定の表示

```
show class-map type control-plane copp-s-pim-datareg
class-map type control-plane match-any copp-s-pim-datareg
```

次の例は、copp-s-pim-datareg クラスのインターフェイス コントロール プレーン情報を示しています。

```
switch# sh policy-map interface control-plane class copp-s-pim-datareg

       Control Plane

  service-policy  input: copp-system-policy

    class-map copp-s-pim-datareg (match-any)
      police pps 600 , bc 0 packets
        HW Matched Packets    55753
        SW Matched Packets   33931

switch#
```

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 つのクラスにプライオリティ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-routingproto1
        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-snmp
        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]

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-dhcpreq
  match access-group name copp-system-acl-dhcps6
class-map type control-plane match-any copp-s-dhcpresp
  match access-group name copp-system-acl-dhcpc6
  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-ipmcmiss
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-ptp
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-snmp
  match access-group name copp-system-acl-snmp
class-map type control-plane match-any copp-ssh
  match access-group name copp-system-acl-ssh
class-map type control-plane match-any copp-stftp
  match access-group name copp-system-acl-stftp
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-ipmcmiss
    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-ptp
    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
```

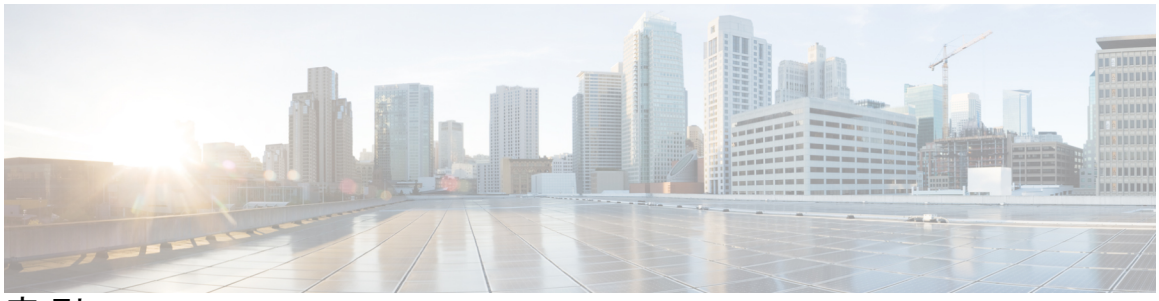
例：セットアップユーティリティによるデフォルトCoPPポリシーの変更または再適用

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 / l2 / l3 ) [default]: l2

The following configuration will be applied:
  switchname switch
  telnet server enable
  no ssh server enable
  policy-map type control-plane copp-system-policy ( l2 )

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

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

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

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



索 引

A

C

D

I

L

M

R

S

T

V

あ

か

き

く

け

こ

さ

し

せ

て

と

に

は

へ

ほ

も

ゆ

ら

り

る

れ

ろ

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。