Cisco Nexus 5000 シリーズ NX-OS セキュリティ コンフィギュレーション ガイド リリース 5.2(1)N1(1)

初版：2012 年 07 月 02 日

最終更新：2012 年 07 月 02 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/

Text Part Number: OL-26844-01-J

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。 マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。 説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2012 Cisco Systems, Inc. All rights reserved.

目 次

はじめに

ここでは、次の項について説明します。

対象読者

この出版物は Cisco Nexus シリーズ デバイスおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダの設定と保守を行う経験豊富な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]	角カッコで囲まれているものは、省略可能な要素（キーワードまたは引数）です。
[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。

表記法	説明
{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、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコ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。 角カッコ内の波カッコと縦棒は、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、screen フォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

関連資料

完全な Cisco NX-OS 5000 シリーズ マニュアル セットは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

コンフィギュレーション ガイド

これらのガイドは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html
このカテゴリのマニュアルは次のとおりです。

- 『*Adapter-FEX Configuration Guide*』
- 『*Cisco Fabric Manager Configuration Guide*』
- 『*Cisco Nexus 5000 Series NX-OS Software Configuration Guide*』
- 『*Configuration Limits for Cisco NX-OS*』
- 『*FabricPath Configuration Guide*』
- 『*Fibre Channel over Ethernet Configuration Guide*』
- 『*Layer 2 Switching Configuration Guide*』
- 『*Multicast Routing Configuration Guide*』
- 『*Operations Guide*』
- 『*SAN Switching Configuration Guide*』
- 『*Quality of Service Configuration Guide*』
- 『*Security Configuration Guide*』
- 『*System Management Configuration Guide*』
- 『*Unicast Routing Configuration Guide*』

メンテナンスおよび操作ガイド

さまざまな機能に対応する『Cisco Nexus 5000 Series NX-OS Operations Guide』は、http://www.cisco.com/en/US/products/ps9670/prod_maintenance_guides_list.html で入手できます。

インストレーション ガイドおよびアップグレード ガイド

これらのガイドは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_installation_guides_list.html

このカテゴリのマニュアルは次のとおりです。

- 『*FabricPath Command Reference*』
- 『*Software Upgrade and Downgrade Guides*』
- 『*Regulatory Compliance and Safety Information*』

ライセンス ガイド

『*License and Copyright Information for Cisco NX-OS Software*』は、http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html で入手できます。

コマンド リファレンス

これらのガイドは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html

このカテゴリのマニュアルは次のとおりです。

- 『*Command Reference Master Index*』
- 『*Fabric Extender Command Reference*』
- 『*FabricPath Command Reference*』
- 『*Fibre Channel Command Reference*』
- 『*Fundamentals Command Reference*』
- 『*Layer 2 Interfaces Command Reference*』
- 『*Multicast Routing Command Reference*』
- 『*QoS Command Reference*』
- 『*Security Command Reference*』
- 『*System Management Command Reference*』
- 『*TrustSec Command Reference*』
- 『*Unicast Routing Command Reference*』
- 『*vPC Command Reference*』

テクニカル リファレンス

『*Cisco Nexus 5000 and Cisco Nexus 2000 MIBs Reference*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mib/reference/NX5000_MIBRef.html で入手できます。

エラー メッセージおよびシステム メッセージ

『*Nexus 5000 Series NX-OS System Message Reference*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/system_messages/reference/sl_nxos_book.html で入手できます。

トラブルシューティング ガイド

『*Cisco Nexus 5000 Series Troubleshooting Guide*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/troubleshooting/guide/N5K_Troubleshooting_Guide.html で入手できます。

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。

マニュアルの入手方法およびテクニカル サポート

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

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

第 1 章

このリリースの新規および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。 この表は、実行コンフィギュレーション ガイドへのすべての変更や、またはこのリリースの新機能の詳細なリストを提供しません。

このリリースの新規および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。 この表は、実行コンフィギュレーション ガイドへのすべての変更や、またはこのリリースの新機能の詳細なリストを提供しません。

表 *1*：このリリースの新規および変更情報

機能	説明	参照先
CoPP 用の IPv6 のサポート	追加プロトコルに対する IPv6 サポート。	コントロール プレーン ポリシングの設定，（229 ページ）
RACL 用の IPv6 のサポート	RACL 用の新しい IPv6 のサポート	アクセス コントロール リストの設定，（125 ページ）

このリリースの新規および変更情報

第 2 章

概要

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

認証、許可、アカウンティング

Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）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 サーバでは、権限が定義された属性値（AV）のペアを、対象のユーザに関連付けることで、ユーザに対して特定の権限を認可します。 AAA 認可は、ユーザに認可されている操作を示す一連の属性を組み合わせて実行します。 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約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。

（注） 認証は AAA と別個に設定することができます。 ただし RADIUS または TACACS+ を使用する場合や、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。

関連トピック

RADIUS および TACACS+ セキュリティ プロトコル

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

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

RADIUS

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

TACACS+

ルータまたはネットワーク アクセス サーバにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。TACACS+ は AAA を使用して実装されます。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。 TACACS+ では、個別の、およびモジュールでの認証、許可、およびアカウンティング機能が提供されます。

関連トピック

SSH および Telnet

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

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

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

関連トピック

IP ACL

IP ACL は、トラフィックをパケットのレイヤ 3 ヘッダーの IPv4 情報に基づいてフィルタリングするために使用できるルールの順序セットです。 各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。 Cisco NX-OS ソフトウェアがパケットに IP ACL を適用することを判定するときは、すべてのルールの条件に照らしてパケットを調べます。 最初の一致によってパケットを許可するか拒否するか判定します。一致するものがない場合は、Cisco NX-OS ソフトウェアは適切なデフォルト ルールを適用します。 Cisco NX-OS ソフトウェアは、許可されたパケットの処理を継続し、拒否されたパケットをドロップします。

関連トピック

第 3 章

認証、許可、アカウンティングの設定

この章では、Cisco Nexus 5000 シリーズ スイッチに認証、許可、アカウンティング（AAA）を設定する方法を説明します。 次のような構成になっています。

AAA について

AAA セキュリティ サービス

認証、認可、アカウンティング（AAA）機能では、Cisco Nexus 5000 シリーズ スイッチを管理するユーザにつき、ID を確認し、アクセス権を付与し、アクションを追跡できます。 Cisco Nexus 5000 シリーズ スイッチは、Remote Access Dial-In User Service（RADIUS）または Terminal Access Controller Access Control device Plus（TACACS+）プロトコルをサポートします。

ユーザが入力したユーザ ID とパスワードに基づいて、スイッチは、ローカル データベースを使用してローカル認証/ローカル許可を実行するか、1 つまたは複数の AAA サーバを使用してリモート認証またはリモート許可を実行します。 スイッチと AAA サーバ間の通信は、事前共有秘密キーによって保護されます。 すべての AAA サーバ用または特定の AAA サーバ専用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 5000 シリーズ スイッチでの許可は、AAA サーバからダウンロードされる属性により実行されます。 RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。
- アカウンティング：課金、監査、レポートのための情報収集、ローカルでの情報のロギング、および AAA サーバへの情報の送信の方式を提供します。

（注） Cisco NX-OS ソフトウェアは、認証、許可、アカウン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
- スケーラビリティ
- 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対するユーザ パスワード リストを簡単に管理できます。
- AAA サーバはすでに企業内に幅広く導入されており、簡単に AAA サービスに使用できます。
- ファブリック内のすべてのスイッチのアカウンティング ログを一元管理できます。
- ファブリック内の各スイッチのユーザ属性は、スイッチ上のローカルデータベースを使用するよりも簡単に管理できます。

AAA サーバ グループ

認証、許可、アカウンティングのためのリモート AAA サーバは、サーバ グループを使用して指定できます。 サーバ グループとは、同じ AAA プロトコルを実装した一連のリモート AAA サーバです。 リモート AAA サーバが応答しなかった場合、サーバ グループは、フェールオーバー サーバを提供します。 グループ内の最初のリモート サーバが応答しなかった場合、いずれかのサーバが応答を送信するまで、グループ内の次のリモート サーバで試行が行われます。 サーバ グループ内のすべての AAA サーバが応答しなかった場合、そのサーバ グループ オプションは障害が発生しているものと見なされます。 必要に応じて、複数のサーバ グループを指定できます。 スイッチが最初のグループ内のサーバからエラーを受信すると、次のサーバ グループのサーバが試行されます。

AAA サーバ設定オプション

Cisco Nexus 5000 シリーズ スイッチでは、次のサービスごとに異なった AAA 設定を作成できます。

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

次の表に、AAA サービス設定オプションの CLI コマンドを示します。

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

（注） 方式がすべてRADIUSサーバになっており、特定のサーバ グループが指定されていない場合、Cisco Nexus 5000 シリーズ スイッチは、設定されている RADIUS サーバのグローバル プールから、設定の順序で、RADIUS サーバを選択します。 このグローバル プールのサーバは、Nexus 5000 シリーズ スイッチ上の RADIUS サーバ グループ内で選択的に設定可能なサーバです。

次の表に、AAA サービスに対して設定できる AAA 認証方式を示します。

表 *3*： *AAA* サービスのための *AAA* 認証方式

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

（注） コンソール ログイン認証、ユーザ ログイン認証、およびユーザ管理セッション アカウンティングでは、Cisco Nexus 5000 シリーズ スイッチは、各オプションを指定された順序で試行します。 その他の設定済みオプションが失敗した場合、ローカル オプションがデフォルト方式です。

ユーザ ログインの認証および許可プロセス

ユーザ ログインの認証および許可プロセスは、次のように実行されます。

- 目的の Cisco Nexus 5000 シリーズ スイッチにログインする際、Telnet、SSH、Fabric Manager または Device Manager、コンソール ログインのいずれかのオプションを使用できます。
- サーバ グループ認証方式を使用してAAAサーバ グループが設定してある場合は、Cisco Nexus 5000 シリーズ スイッチが、グループ内の最初の AAA サーバに認証要求を送信し、次のように処理されます。

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

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

  設定されている認証方式がすべて失敗した場合、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 5000 シリーズ スイッチがリモート AAA サーバでユーザの認証に成功した場合は、次の条件が適用されます。

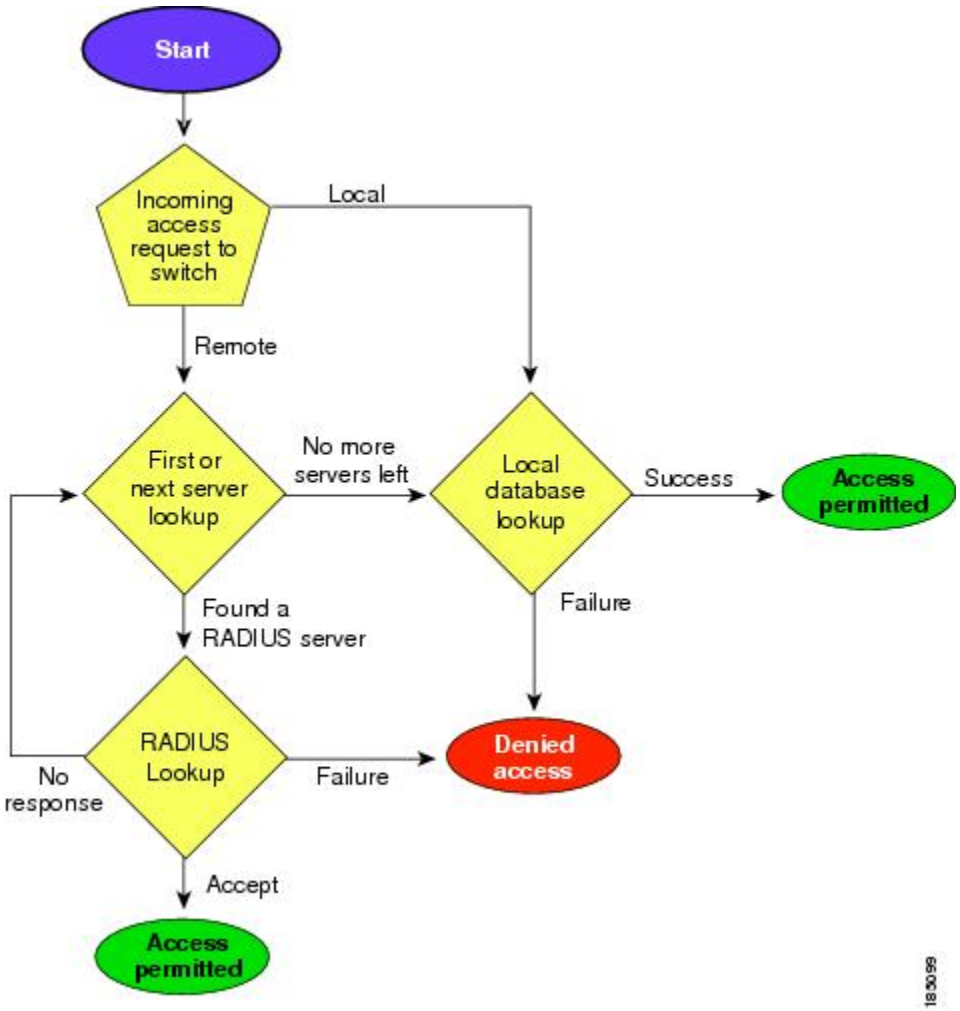
  AAA サーバ プロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザ ロールが認証応答とともにダウンロードされます。

  AAA サーバ プロトコルが TACACS+ の場合、シェルのカスタム属性として指定されているユーザ ロールを取得するために、もう 1 つの要求が同じサーバに送信されます。

- ユーザ名とパスワードがローカルで正常に認証された場合は、Cisco Nexus 5000 シリーズ スイッチにログインでき、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。

次の図には、認証および許可プロセスのフロー チャートを示します。

図 *1*：ユーザ ログインの認証および許可のフロー



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

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

リモート AAA の前提条件

リモート AAA サーバには、次の前提条件があります。

- 少なくとも 1 台の RADIUS サーバまたは TACACS+ サーバが、IP で到達可能であること。
- Cisco Nexus 5000 シリーズ スイッチが AAA サーバのクライアントとして設定されている。
- 事前に共有された秘密キーが Cisco Nexus 5000 シリーズ スイッチ上およびリモート AAA サーバ上で設定されている。
- リモート サーバが Cisco Nexus 5000 シリーズ スイッチからの AAA 要求に応答する。

AAA の注意事項と制約事項

Cisco Nexus 5000 シリーズ スイッチは、TACACS+ または RADIUS で作成されたか、ローカルに作成されたかに関係なく、すべて数字のユーザ名はサポートしません。 すべて数字のユーザ名が AAA サーバに存在し、ログイン時に入力された場合には、Cisco Nexus 5000 シリーズ スイッチはそのユーザをログインさせます。

注意 すべて数字のユーザ名でユーザ アカウントを作成しないでください。

AAA の設定

コンソール ログイン認証方式の設定

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS サーバまたは TACACS+ サーバの名前付きサブセット
- Cisco Nexus 5000 シリーズ スイッチ上のローカル データベース
- ユーザ名だけ（**none**）

デフォルトの方式は、local です。

（注） 事前に設定されている一連の RADIUL サーバには、**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 サーバを設定するには、**radius server-host** コマンドを使用します。 サーバの名前付きグループを作成するには、**aaa group server radius** コマンドを使用します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login console** {**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 サーバのグローバル プールが認証に使用されます。 • *named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが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。この方式は、方式が一切設定されていない場合、および設定済みのどの方式でも応答が得られなかった場合に使用されます。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa authentication**	（任意） コンソール ログイン認証方式の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、コンソール ログインの認証方式を設定する例を示します。

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

デフォルトのログイン認証方式の設定

デフォルトの方式は、local です。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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 サーバのグローバル プールが認証に使用されます。 • *named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが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、および設定済みのどの方式でも応答が得られなかった場合に使用されます。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa authentication**	（任意） デフォルトのログイン認証方式の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ログイン認証失敗メッセージのイネーブル化

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

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 モードを開始します。
ステップ 2	switch(config)# **aaa authentication login error-enable**	ログイン認証失敗メッセージをイネーブルにします。 デフォルトはディセーブルです。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa authentication**	（任意） ログイン失敗メッセージの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

AAA コマンド許可の設定

TACACS+ サーバの許可方式が設定されている場合、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 コマンドを含め、TACACS+ サーバで実行されるすべてのコマンドを許可できます。

許可方式には、次のものがあります。

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

デフォルトの方式は、Local です。

（注） コンソール セッション上の許可はありません。

はじめる前に

AAA コマンドの許可を設定する前に、TACACS+ をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**aaa authorization** {**commands** | **config-commands**} {**default**} {{[**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 コマンドを許可するには、**config-commands** キーワードを使用します。
		許可方式を指定するには、**group**、**local**、または **none** キーワードを使用します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MSCHAP 認証のイネーブル化

Microsoft Challenge Handshake Authentication Protocol（MSCHAP; 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）は、マイクロソフト版のCHAPです。リモート認証サーバ（RADIUSまたはTACACS+）を通じて、Cisco Nexus 5000 シリーズ スイッチへのユーザ ログインにMSCHAPを使用できます。

デフォルトでは、Cisco Nexus 5000 シリーズ スイッチはスイッチとリモート サーバの間でPassword Authentication Protocol（PAP; パスワード認証プロトコル）認証を使用します。 MSCHAP がイネーブルの場合は、MSCHAP VSA（Vendor-Specific Attribute; ベンダー固有属性）を認識するようにRADIUS サーバを設定する必要があります。

次の表に、MSCHAP に必要な RADIUS VSA を示します。

表 *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 サーバから MSCHAP ユーザに送信されるチャレンジを保持します。 これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。
211	11	MSCHAP-Response	チャレンジに対する応答として MSCHAP ユーザが入力した値を保持します。 Access-Request パケットでしか使用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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。 デフォルトはディセーブルです。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa authentication login mschap**	（任意） MS-CHAP 設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

VSA, （20 ページ）

AAA アカウンティングのデフォルト方式の設定

Cisco Nexus 5000 シリーズ スイッチは、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 サーバまたは RADIUS セキュリティ サーバに報告します。 各アカウンティング レコードに、アカウンティング属性値（AV）のペアが入っており、それが AAA サーバに格納されます。

AAA アカウンティングをアクティブにすると、Cisco Nexus 5000 シリーズ スイッチは、これらの属性をアカウンティング レコードとして報告します。そのアカウンティング レコードは、セキュリティ サーバ上のアカウンティング ログに格納されます。

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

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

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

はじめる前に

必要に応じて、AAA アカウン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 グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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 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。

	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 プールがアカウンティングに使用されます。 • *named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットがアカウンティングに使用されます。 **local** 方式では、アカウンティングにローカル データベースが使用されます。 デフォルトのアカウンティング方式は **local** です。サーバグループが設定されていないとき、または設定済みのすべてのサーバグループから応答がないときに、このデフォルトの方式が使用されます。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa accounting**	（任意） 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	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

AAA サーバの VSA の使用

VSA

ベンダー固有属性（VSA）を使用して、AAA サーバ上でのCisco Nexus 5000 シリーズのユーザ ロールおよび SNMPv3 パラメータを指定できます。

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）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。 VSA を使用するとベンダーは、一般的な用途には適合し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 5000 シリーズ スイッチでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。 この許可情報は、VSA で指定されます。

VSA の形式

次の VSA プロトコル オプションが、Cisco Nexus 5000 シリーズ スイッチでサポートされています。

- Shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されます。
- Accounting：accounting-request パケットで使用されます。 値にスペースが含まれている場合は、二重引用符で囲んでください。

次の属性が Cisco Nexus 5000 シリーズ スイッチでサポートされています。

- roles：ユーザに割り当てるすべてのロールをリストします。 値フィールドは、グループ名を空白で区切ったリストの入ったストリングです。
- accountinginfo：標準の RADIUS アカウンティング プロトコルで処理される属性に加えて、追加のアカウンティング情報が格納されます。 この属性が送信されるのは、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分内だけです。この属性は、アカウンティング プロトコル関連の PDU でしか使用できません。

AAA サーバ上でのスイッチのユーザ ロールと SNMPv3 パラメータの指定

AAA サーバで VSA cisco-av-pair を使用して、次の形式で、Cisco Nexus 5000 シリーズ スイッチのユーザ ロール マッピングを指定できます。

```
shell:roles="roleA roleB …"
```

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

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

次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

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

詳細については、『*Cisco Nexus 5000 Series NX-OS 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 5000 シリーズ スイッチは、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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show accounting log** [*size*] [**start-time** *year month day hh* **:** *mm* **:** *ss*]	アカウンティング 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	switch# **clear accounting log**	（任意） 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。

手順

	コマンドまたはアクション	目的
ステップ 1	**show aaa accounting**	AAA アカウンティングの設定を表示します。
ステップ 2	**show aaa authentication** [**login** {**error-enable** | **mschap**}]	AAA 認証情報を表示します。
ステップ 3	**show aaa authorization**	AAA 許可の情報を表示します。
ステップ 4	**show aaa groups**	AAA サーバ グループの設定を表示します。
ステップ 5	**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。

	コマンドまたはアクション	目的
ステップ 6	**show startup-config aaa**	スタートアップ コンフィギュレーションの AAA 設定を表示します。

AAA の設定例

次に、AAA を設定する例を示します。

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

デフォルトの AAA 設定

次の表に、AAA パラメータのデフォルト設定を示します。

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

第 4 章

RADIUS の設定

この章の内容は、次のとおりです。

RADIUS の設定

RADIUS について

Remote Access Dial-In User Service（RADIUS）分散クライアント/ サーバ システムを使用すると、不正アクセスからネットワークを保護できます。 シスコの実装では、RADIUS クライアントは Cisco Nexus 5000 シリーズ スイッチで稼働し、すべてのユーザ認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウン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 5000 シリーズ スイッチをネットワークに追加できます。 この作業は、AAA サーバに移行するときの最初の手順になります。

- リソース アカウンティングが必要なネットワーク。

RADIUS アカウンティングは、RADIUS 認証または RADIUS 許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。 ユーザごとのプロファイルにより、Nexus 5000 シリーズ スイッチは、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 アグリーメントを提供できます。

RADIUS の操作について

ユーザがログインを試行し、RADIUS を使用して Cisco Nexus 5000 シリーズ スイッチに対する認証を行う際には、次のプロセスが実行されます。

1. ユーザが、ユーザ名とパスワードの入力を求められ、入力します。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   - ACCEPT：ユーザが認証されたことを表します。
   - REJECT：ユーザは認証されず、ユーザ名とパスワードの再入力を求められるか、アクセスを拒否されます。
   - CHALLENGE：RADIUS サーバによってチャレンジが発行されます。 チャレンジは、ユーザから追加データを収集します。
   - CHANGE PASSWORD：RADIUS サーバからユーザに対して新しいパスワードの選択を求める要求が発行されます。

ACCEPT または REJECT 応答には、EXEC またはネットワーク認可に使用される追加データが含まれています。 RADIUS 許可を使用するには、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。

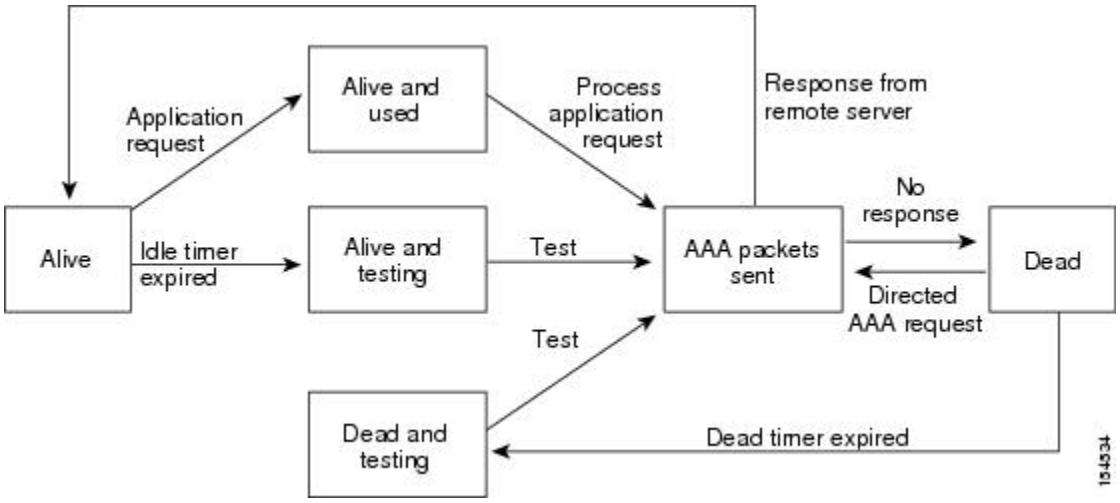
- ユーザがアクセス可能なサービス（Telnet、rlogin、または local-area transport（LAT; ローカル エリア トランスポート）接続、PPP（ポイントツーポイント プロトコル）、シリアルライン インターネット プロトコル（SLIP）、EXEC サービスなど）
- 接続パラメータ（ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセス リスト、ユーザ タイムアウト）

RADIUS サーバ モニタリング

応答を返さないRADIUSサーバがあると、AAA要求の処理に遅延が発生する可能性があります。AAA 要求の処理時間を節約するため、定期的にRADIUSサーバをモニタリングし、RADIUS サーバが応答を返す（アライブ）かどうかを調べるよう、スイッチを設定できます。 スイッチは、応答を返さないRADIUSサーバをデッド（dead）としてマークし、デッドRADIUSサーバにはAAA要求を送信しません。 また、定期的にデッドRADIUS サーバをモニタリングし、それらが応答を返したらアライブ状態に戻します。 このプロセスにより、RADIUS サーバが稼働状態であることを確認してから、実際の AAA 要求がサーバに送信されます。 RADIUS サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、スイッチによって、障害が発生したことを知らせるエラー メッセージが表示されます。

次の図には、さまざまな RADIUS サーバの状態を示します。

図 *2*： *RADIUS* サーバの状態



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

ベンダー固有属性

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間でのベンダー固有属性（VSA）の通信のための方式を規定する標準を作成しています。 IETF は、属性 26 を使用します。 VSA を使用するとベンダーは、一般的な用途には適合し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 5000 シリーズ スイッチでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。 この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションが、Cisco Nexus 5000 シリーズ スイッチでサポートされています。

- Shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されます。
- Accounting：accounting-request パケットで使用されます。 値にスペースが含まれている場合は、二重引用符で囲む必要があります。

Cisco Nexus 5000 シリーズ スイッチは、次の属性をサポートしています。

- roles：ユーザが属するすべてのロールの一覧です。 値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。
- 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 Protocol Data Unit（PDU; プロトコル データ ユニット）だけです。

RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IPv4 または IPv6 アドレスまたはホスト名を取得こと。
- RADIUS サーバから事前共有キーを取得すること。
- Cisco Nexus 5000 シリーズ スイッチが、AAA サーバの RADIUS クライアントとして設定されていること。

RADIUS の注意事項と制約事項

RADIUS 設定時の注意事項と制限事項は次のとおりです。

- Cisco Nexus 5000 シリーズ スイッチ上に設定できる RADIUS サーバの最大数は 64 です。

RADIUS サーバの設定

ここでは、RADIUS サーバの設定方法について説明します。

手順

ステップ 1 Cisco Nexus 5000 シリーズ スイッチと RADIUS サーバとの接続を確立します。

ステップ 2 RADIUS サーバの事前共有秘密キーを設定します。

ステップ 3 必要に応じて、AAA 認証方式用に、RADIUS サーバのサブセットを使用して RADIUS サーバ グループを設定します。

ステップ 4 必要に応じて、次のオプションのパラメータを設定します。

- デッドタイム間隔
- ログイン時に RADIUS サーバの指定を許可
- 送信リトライ回数とタイムアウト間隔
- アカウンティングおよび認証属性

ステップ 5 必要に応じて、定期的に RADIUS サーバをモニタリングするよう設定します。

RADIUS サーバ ホストの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*}	RADIUS サーバの IPv4 または IPv6 アドレス、またはホスト名を指定します。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	switch# **copy running-config startup-config**	（任意） 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、変更を永続的に保存します。

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

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

RADIUS のグローバルな事前共有キーの設定

Cisco Nexus 5000 シリーズ デバイスで使用するすべてのサーバについて、グローバル レベルで事前共有キーを設定できます。 事前共有キーとは、スイッチと RADIUS サーバ ホスト間の共有秘密テキスト ストリングです。

はじめる前に

リモートの RADIUS サーバの事前共有キー値を取得していること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server key** [**0** | **7**] *key-value*	すべての RADIUS サーバで使用する事前共有キーを指定します。 クリア テキスト形式（**0**）または暗号化形式（**7**）の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 文字の長さまで指定可能です。 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**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。

	コマンドまたはアクション	目的
		（注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、デバイスで使用するすべてのサーバについて、グローバル レベルで事前共有キーを設定する例を示します。

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

RADIUS サーバの事前共有キーの設定

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

はじめる前に

リモートの RADIUS サーバの事前共有キー値を取得していること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **7**] *key-value*	特定の RADIUS サーバの事前共有キーを指定します。クリア テキスト形式（**0**）または暗号化形式（**7**）の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 文字の長さまで指定可能です。 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。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。 （注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。 暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、RADIUS 事前共有キーを設定する例を示します。

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

RADIUS サーバ グループの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch (config)# **aaa group server radius** *group-name*	RADIUS サーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション サブモードを開始します。 *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* | *ipv6-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。

	コマンドまたはアクション	目的
		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	switch (config-radius)# **deadtime** *minutes*	（任意） モニタリング デッド タイムを設定します。 デフォルト値は 0 分です。 指定できる範囲は 1 ～ 1440 です。 （注） RADIUS サーバ グループのデッド タイム間隔が 0 より大きい場合は、この値がグローバルなデッド タイム値より優先されます。
ステップ 5	switch(config-radius)# **source-interface** *interface*	（任意） 特定の RADIUS サーバ グループに発信元インターフェイスを割り当てます。 サポートされているインターフェイスのタイプは管理および VLAN です。 （注） **source-interface** コマンドを使用して、**ip radius source-interface** コマンドによって割り当てられたグローバル ソース インターフェイスを上書きします。
ステップ 6	switch(config-radius)# **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	switch(config)# **show radius-server group** [*group-name*]	（任意） RADIUS サーバ グループの設定を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、RADIUS サーバ グループを設定する例を示します。

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

次の作業

AAA サービスに RADIUS サーバ グループを適用します。

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

RADIUS サーバ グループにアクセスする際に使用する、RADIUS サーバ グループ用のグローバル発信元インターフェイスを設定できます。 また、特定の RADIUS サーバ グループ用に異なる発信元インターフェイスを設定することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip radius source-interface** *interface*	このデバイスで設定されているすべての RADIUS サーバ グループ用のグローバル発信元インターフェイスを設定します。発信元インターフェイスは、管理または VLAN インターフェイスにすることができます。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定情報を表示します。
ステップ 5	switch# **copy running-config startup config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

ログイン時にユーザによる RADIUS サーバの指定を許可

ログイン時にユーザによる RADIUS サーバの指定を許可できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server directed-request**	ログイン時にユーザが認証要求の送信先となる RADIUS サーバを指定できるようにします。 デフォルトはディセーブルです。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show radius-server directed-request**	（任意） directed request の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定

すべての RADIUS サーバに対するグローバルな再送信リトライ回数とタイムアウト間隔を設定できます。 デフォルトでは、スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。 このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。タイムアウト間隔は、Cisco Nexus 5000 シリーズ スイッチがタイムアウト エラーを宣言する前に、RADIUS サーバからの応答を待機する時間を決定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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 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。

	コマンドまたはアクション	目的
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**	コンフィギュレーションモードを終了します。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-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。 （注） 特定の RADIUS サーバに指定した再送信回数は、すべての RADIUS サーバに指定した再送信回数より優先されます。
ステップ 3	switch(config)#**radius-server host** {*ipv4-address* | *ipv6-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。

	コマンドまたはアクション	目的
		（注） 特定の RADIUS サーバに指定した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**	コンフィギュレーション モードを終了します。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 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、変更を永続的に保存します。

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

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

RADIUS サーバのアカウン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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **acct-port** *udp-port*	（任意） 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。 指定できる範囲は 0 ～ 65535 です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting**	（任意） 特定の RADIUS サーバ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	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **auth-port** *udp-port*	（任意） RADIUS 認証メッセージ用の UDP ポートを指定します。 デフォルトの UDP ポートは 1812 です。 指定できる範囲は 0 ～ 65535 です。
ステップ 5	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication**	（任意） 特定の RADIUS サーバ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**	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	switch(config)# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、RADIUS サーバ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 サーバの定期的モニタリングの設定

RADIUS サーバの可用性をモニタリングできます。 パラメータとして、サーバに使用するユーザ名とパスワード、およびアイドル タイマーがあります。 アイドル タイマーには、RADIUS サーバがどのくらいの期間要求を受信しなかった場合にスイッチがテスト パケットを送信するかを指定します。 このオプションを設定することで、サーバを定期的にテストできます。

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

テストアイドル タイマーには、RADIUS サーバがどのくらいの期間要求を受信しなかった場合にスイッチがテスト パケットを送信するかを指定します。

デフォルトのアイドル タイマー値は 0 分です。 アイドル時間間隔が 0 分の場合、スイッチは RADIUS サーバの定期的なモニタリングを実行しません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}	サーバ モニタリング用のパラメータを指定します。 デフォルトのユーザ名は test、デフォルトのパスワードは test です。 デフォルトのアイドル タイマー値は 0 分です。 指定できる範囲は、0 ～ 1440 分です。 （注） RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	switch(config)# **radius-server deadtime** *minutes*	スイッチが、前回応答しなかった RADIUS サーバをチェックするまでの時間（分）を指定します。 デフォルト値は 0 分です。 指定できる範囲は 1 ～ 1440 分です。
ステップ 4	switch(config)# **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 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 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、変更を永続的に保存します。

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

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

デッド タイム間隔の設定

すべての RADIUS サーバのデッド タイム間隔を設定できます。 デッド タイム間隔には、Cisco Nexus 5000 シリーズ スイッチが RADIUS サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを判断するためにテスト パケットを送信するまでの間隔を指定します。 デフォルト値は 0 分です。

（注） デッド タイム間隔が 0 分の場合、RADIUS サーバは、応答を返さない場合でも、デッ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。

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**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

RADIUS サーバまたはサーバ グループの手動モニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **test aaa server radius** {*ipv4-address*| *ipv6-address* | *server-name*} [**vrf** *vrf-name*] *username password* **test aaa server radius** {*ipv4-address* | *ipv6-address* | *server-name*} [**vrf** *vrf-name*] *username password*	RADIUS サーバにテスト メッセージを送信して可用性を確認します。
ステップ 2	switch# **test aaa group** *group-name username password*	RADIUS サーバ グループにテスト メッセージを送信して可用性を確認します。

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

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

RADIUS 設定の確認

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show running-config radius** [**all**]	実行コンフィギュレーションの RADIUS 設定を表示します。
ステップ 2	switch# **show startup-config radius**	スタートアップ コンフィギュレーションの RADIUS 設定を表示します。
ステップ 3	switch# **show radius-server** [*server-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての RADIUS サーバのパラメータを表示します。

RADIUS サーバ統計情報の表示

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-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 サーバのアクティビティに関する統計情報を表示します。

はじめる前に

Cisco NX-OS デバイスに RADIUS サーバを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}	（任意） Cisco NX-OS デバイスでの RADIUS サーバ統計情報を表示します。
ステップ 2	switch# **clear radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-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。

表 *6*：デフォルトの *RADIUS* パラメータ

パラメータ	デフォルト
サーバの役割	認証とアカウンティング
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	test

第 5 章

TACACS+ の設定

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

- TACACS+ の設定について，45 ページ

TACACS+ の設定について

TACACS+ について

Terminal Access Controller Access Control System Plus（TACACS+）セキュリティ プロトコルは、Cisco Nexus 5000 シリーズ スイッチにアクセスしようとするユーザを集中的に検証します。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。 Cisco Nexus 5000 シリーズ スイッチに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ では、認証、許可、アカウンティングの各ファシリティを個別に提供します。 TACACS+ を使用すると、単一のアクセス コントロール サーバ（TACACS+ デーモン）で、各サービス（認証、許可、アカウンティング）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、そのサーバまたはネットワーク上で使用可能な他のサービスを利用できます。

TACACS+ クライアント/サーバ プロトコルでは、トランスポート要件を満たすため TCP（TCP ポート 49）を使用します。 Cisco Nexus 5000 シリーズ スイッチは、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 5000 シリーズ スイッチは、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する。
- 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する。 RADIUS プロトコルはパスワードだけを暗号化します。

TACACS+ を使用したユーザ ログイン

ユーザが TACACS+ を使用して、Cisco Nexus 5000 シリーズ スイッチに対し Password Authentication Protocol（PAP; パスワード認証プロトコル）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 5000 シリーズ スイッチが接続を確立すると、TACACS+ デーモンにアクセスして、ユーザ名とパスワードを取得します。

（注） TACACS+ では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。 この動作では通常、ユーザ名とパスワードの入力が要求されますが、ユーザの母親の旧姓など、その他の項目の入力が要求されることもあります。

2. Cisco Nexus 5000 シリーズ スイッチが、TACACS+ デーモンから次のいずれかの応答を受信します。
   - ACCEPT：ユーザの認証に成功したので、サービスを開始します。 Cisco Nexus 5000 シリーズ スイッチがユーザの許可を要求している場合は、許可が開始されます。
   - REJECT：ユーザの認証に失敗しました。 TACACS+ デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン シーケンスを再試行するよう要求します。
   - ERROR：認証中に、デーモン内、またはデーモンと Cisco Nexus 5000 シリーズ スイッチ間のネットワーク接続でエラーが発生しました。 Cisco Nexus 5000 シリーズ スイッチが ERROR 応答を受信した場合、スイッチは代わりのユーザ認証方式を試します。

   Cisco Nexus 5000 シリーズ スイッチで許可がイネーブルになっている場合は、この後、許可フェーズの処理が実行されます。 ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
3. TACACS+ 許可が必要な場合、Cisco Nexus 5000 シリーズ スイッチは、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。

サービスには次が含まれます。

- ◦ Telnet、rlogin、Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）、Serial Line Internet Protocol（SLIP;シリアル ライン インターネット プロトコル）、EXEC サービス
  - ◦ 接続パラメータ（ホストまたはクライアントの IP アドレス（IPv4 または IPv6）、アクセス リスト、ユーザ タイムアウト）

デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー

TACACS+ サーバに対してスイッチを認証するには、TACACS+ 事前共有キーを設定する必要があります。 事前共有キーは、Cisco Nexus 5000 シリーズ スイッチと TACACS+ サーバ ホストの間で共有される秘密テキスト 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 5000 シリーズ スイッチ上のすべての TACACS+サーバ設定で使用されるグローバルな事前共有秘密キーを設定できます。

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

TACACS+ サーバのコマンド許可サポート

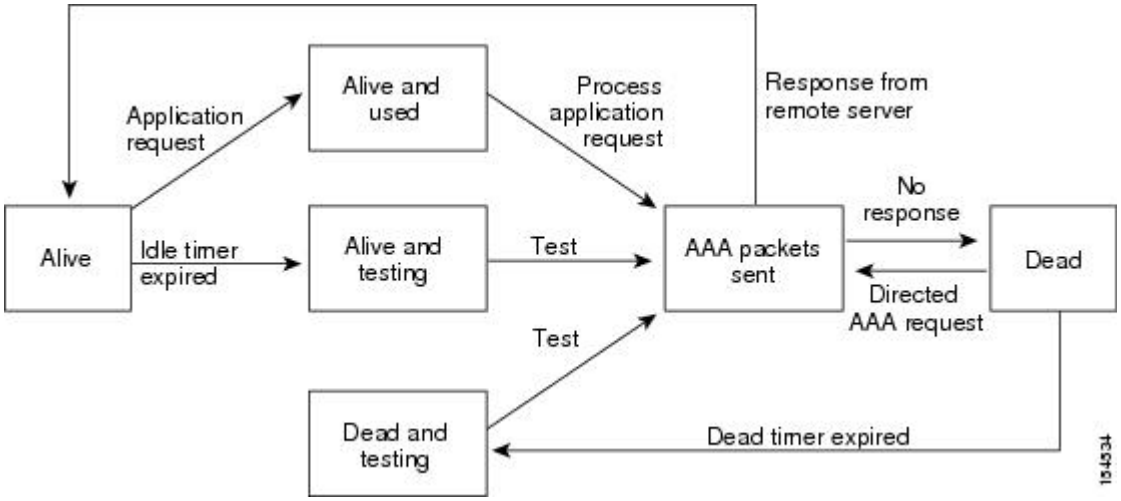
デフォルトでは、認証されたユーザがコマンドライン インターフェイス（CLI）でコマンドを入力したときに、Cisco NX-OS ソフトウェアのローカル データベースに対してコマンド許可が行われます。 また、TACACS+ を使用して、認証されたユーザに対して許可されたコマンドを確認することもできます。

TACACS+ サーバのモニタリング

応答を返さない TACACS+ サーバがあると、AAA 要求の処理に遅延が発生する可能性があります。 AAA 要求の処理時間を節約するため、Cisco Nexus 5000 シリーズ スイッチは定期的に TACACS+ サーバをモニタリングし、TACACS+ サーバが応答を返す（アライブ）かどうかを調べることができます。 Cisco Nexus 5000 シリーズ スイッチは、応答を返さない TACACS+ サーバをデッド（dead）としてマークし、デッド TACACS+ サーバには AAA 要求を送信しません。 またCisco Nexus 5000 シリーズ スイッチは、定期的にデッド TACACS+ サーバをモニタリングし、それらが応答を返したらアライブ状態に戻します。 このモニタリング プロセスでは、実際の AAA 要求がサーバに送信される前に、TACACS+ サーバが稼働状態であることを確認します。 TACACS+ サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco Nexus 5000 シリーズ スイッチによって、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。

次の図では、さまざまな TACACS+ サーバの状態を示します。

図 *3*： *TACACS+* サーバの状態



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

TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバの IPv4 または IPv6 アドレスまたはホスト名を取得すること。
- TACACS+ サーバから事前共有キーを取得していること。
- Cisco Nexus 5000 シリーズ スイッチが、AAA サーバの TACACS+ クライアントとして設定されていること。

TACACS+ の注意事項と制約事項

TACACS+ に関する注意事項と制約事項は次のとおりです。

- Cisco Nexus 5000 シリーズ スイッチ上に設定できる TACACS+ サーバの最大数は 64 です。

TACACS+ の設定

TACACS+ サーバの設定プロセス

ここでは、TACACS+ サーバを設定する方法について説明します。

手順

ステップ 1 TACACS+ をイネーブルにします。

ステップ 2 TACACS+ サーバと Cisco Nexus 5000 シリーズ スイッチとの接続を確立します。

ステップ 3 TACACS+ サーバの事前共有秘密キーを設定します。

ステップ 4 必要に応じて、AAA 認証方式用に、TACACS+ サーバのサブセットを使用して TACACS+ サーバグループを設定します。

ステップ 5 必要に応じて、次のオプションのパラメータを設定します。

- デッドタイム間隔
- ログイン時に TACACS+ サーバの指定を許可
- タイムアウト間隔
- TCP ポート

ステップ 6 必要に応じて、定期的に TACACS+ サーバをモニタリングするよう設定します。

TACACS+ のイネーブル化

デフォルトでは、Cisco Nexus 5000 シリーズ スイッチで TACACS+ 機能はディセーブルに設定されています。認証に関するコンフィギュレーション コマンドと検証コマンドを使用するために、TACACS+ 機能をイネーブルにするには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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**	コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバ ホストの設定

リモートの TACACS+ サーバにアクセスするには、Cisco Nexus 5000 シリーズ スイッチ上に、TACACS+ サーバの IP アドレス（IPv4 または IPv6）またはホスト名を設定する必要があります。すべての TACACS+ サーバ ホストは、デフォルトの TACACS+ サーバ グループに追加されます。最大 64 の TACACS+ サーバを設定できます。

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

TACACS+ サーバ ホストを設定する前に、次の点を確認してください。

- TACACS+ をイネーブルにします。
- リモート TACACS+ サーバの IP アドレス（IPv4 または IPv6）またはホスト名を取得していること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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* | *ipv6-address* | *host-name*}	TACACS+ サーバの IP アドレス（IPv4 または IPv6）、またはホスト名を指定します。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

サーバ グループから TACACS+ サーバ ホストを削除できます。

TACACS+ のグローバルな事前共有キーの設定

Cisco Nexus 5000 シリーズ スイッチで使用するすべてのサーバについて、グローバル レベルで事前共有キーを設定できます。 事前共有キーとは、Cisco Nexus 5000 シリーズ スイッチと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

事前共有キーを設定する前に、次の点を確認してください。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server key** [**0** | **7**] *key-value*	すべての TACACS+ サーバで使用する事前共有キーを指定します。 クリア テキスト形式（**0**）または暗号化形式（**7**）の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 文字の長さまで指定可能です。 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**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。 （注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。 暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、グローバルな事前共有キーを設定する例を示します。

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

関連トピック

TACACS+ のイネーブル化 , （49 ページ）

TACACS+ サーバの事前共有キーの設定

TACACS+ サーバの事前共有キーを設定できます。 事前共有キーとは、Cisco Nexus 5000 シリーズ スイッチと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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* | *ipv6-address* | *host-name*} **key** [**0** | **7**] *key-value*	特定の TACACS+ サーバの事前共有キーを指定します。 クリア テキスト形式（**0**）または暗号化形式（**7**）の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 文字の長さまで指定可能です。 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**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。 （注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ 事前共有キーを設定する例を示します。

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

TACACS+ サーバ グループの設定

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

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

はじめる前に

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用して、TACACS+ をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa group server tacacs+** *group-name*	TACACS+ サーバ グループを作成し、そのグループの TACACS+ サーバ グループ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-tacacs+)# **server** {*ipv4-address* | *ipv6-address* | *host-name*}	TACACS+ サーバを、TACACS+ サーバ グループのメンバーとして設定します。 指定した TACACS+ サーバが見つからない場合は、**tacacs-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	switch(config-tacacs+)# **deadtime** *minutes*	（任意） モニタリング デッド タイムを設定します。 デフォルト値は 0 分です。 指定できる範囲は 0 ～ 1440 です。 （注） TACACS+ サーバ グループのデッド タイム間隔が 0 より大きい場合は、その値がグローバルなデッド タイム値より優先されます。

	コマンドまたはアクション	目的
ステップ 5	switch(config-tacacs+)# **source-interface** *interface* 例： `switch(config-tacacs+)# source-interface mgmt 0`	（任意） 特定の TACACS+ サーバ グループに発信元インターフェイスを割り当てます。 サポートされているインターフェイスのタイプは管理および VLAN です。 （注） **source-interface** コマンドを使用して、**ip tacacs source-interface** コマンドによって割り当てられたグローバル ソース インターフェイスを上書きします。
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	switch(config)# **show tacacs-server groups**	（任意） TACACS+ サーバ グループの設定を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ サーバ グループを設定する例を示します。

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

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

TACACS+ サーバ グループにアクセスする際に使用する、TACACS+ サーバ グループ用のグローバル発信元インターフェイスを設定できます。 また、特定の TACACS+ サーバ グループ用に異なる発信元インターフェイスを設定することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 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	**ip tacacs source-interface** *interface* 例： `switch(config)# ip tacacs source-interface mgmt 0`	このデバイスで設定されているすべての TACACS+ サーバ グループ用のグローバル発信元インターフェイスを設定します。 発信元インターフェイスは、管理または VLAN インターフェイスにすることができます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定情報を表示します。
ステップ 5	**copy running-config startup config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ログイン時の TACACS+ サーバの指定

認証要求の送信先 TACACS+ サーバをユーザが指定できるようにスイッチを設定するには、directed-request オプションをイネーブルにします。 デフォルトでは、Cisco Nexus 5000 シリーズ スイッチは、デフォルトの AAA 認証方式に基づいて認証要求を転送します。 このオプションをイネーブルにすると、ユーザは *username@hostname* としてログインできます。ここで、*hostname* は設定済みの RADIUS サーバの名前です。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **tacacs-server directed-request**	ログイン時に、ユーザが認証要求の送信先となる TACACS+ サーバを指定できるようにします。 デフォルトはディセーブルです。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **exit**	コンフィギュレーションモードを終了します。
ステップ 4	switch# **show tacacs-server directed-request**	（任意） TACACS+ の directed request の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

はじめる前に

TACACS+ 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	**aaa authorization ssh-certificate default** {**group** *group-list* [**none**] | **local** | **none**} 例： `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。

	コマンドまたはアクション	目的

ステップ 3	**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 4	**show aaa authorization** [**all**] 例： `switch# show aaa authorization`	（任意） AAA 認可設定を表示します。 **all** キーワードは、デフォルト値を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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 Role-Based Authorization Control（RBAC; ロールベース許可コントロール）がディセーブルになります。

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

はじめる前に

TACACS+ をイネーブルにします。

AAA コマンドの認可を設定する前に TACACS ホストおよびサーバ グループを設定します。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
ステップ 2	**aaa authorization** {**commands** | **config-commands**} **default** [**group** *group-list* [**local**] | **local**] 例： `switch(config)# aaa authorization commands default group TacGroup`	すべてのロールに対するデフォルトのコマンド許可方式を設定します。 **commands** キーワードは、すべての EXEC コマンドの許可ソースを設定し、**config-commands** キーワードは、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します。 すべてのコマンドの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、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 データベースを使用します。 設定済みのすべてのサーバ グループで応答に失敗し、フォールバック方式として **local** を設定済みの場合、**local** 方式だけが使用されます。 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** 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 4	**show aaa authorization** [**all**] 例： `switch(config)# show aaa authorization`	（任意） AAA 認可設定を表示します。 **all** キーワードは、デフォルト値を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

（注） 許可の正しいコマンドを送信しないと、結果の信頼性が低くなります。

はじめる前に

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。

手順

	コマンドまたはアクション	目的
ステップ 1	**test aaa authorization command-type** {**commands** | **config-commands**} **user** *username* **command** *command-string* 例： `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。 （注） *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、Role-Based Access Control（RBAC; ロールベース アクセス コントロール）を使用します。 両方のタイプのデバイスを同じ TACACS+ サーバで管理できるようにするには、TACACS+ サーバ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 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
14	vdc-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** コマンドがイネーブルの場合）。
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。

（注） **feature privilege** コマンドをイネーブルにすると、権限ロールは低いレベルの権限ロールの権限を継承します。

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	[**no**] **feature privilege** 例： `switch(config)# feature privilege`	ロールの累積権限をイネーブルまたはディセーブルにします。 **enable** コマンドは、この機能をイネーブルにした場合しか表示されません。 デフォルトはディセーブルです。
ステップ 3	[**no**] **enable secret** [**0** | **5**] *password* [**priv-lvl** *priv-lvl* | **all**] 例： `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イネーブルまたはディセーブルにします。 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。 デフォルトはディセーブルです。 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。 （注） シークレット パスワードをイネーブルにするには、**feature privilege** コマンドを入力してロールの累積権限をイネーブルにする必要があります。
ステップ 4	[**no**] **username** *username* **priv-lvl** *n* 例： `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イネーブルまたはディセーブルにします。 デフォルトはディセーブルです。 **priv-lvl** キーワードはユーザに割り当てる権限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	**show privilege** 例： `switch(config)# show privilege`	（任意） 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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 7	**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。

	コマンドまたはアクション	目的
ステップ 8	**enable** *level* 例： `switch# enable 15`	上位の特権レベルへのユーザの昇格をイネーブルにします。 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**。

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**] **role name priv-***n*
	
	例：
	`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* 例： `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 つの規則を持っている場合、規則 3 が規則 2 よりも前に適用され、規則 2 は規則 1 よりも前に適用されます。

	コマンドまたはアクション	目的
		command-string 引数には、空白スペースを含めることができます。 （注） 256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**
	例：
	`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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

グローバルな TACACS+ タイムアウト間隔の設定

Cisco Nexus 5000 シリーズ スイッチがすべての TACACS+ サーバからの応答を待つグローバルなタイムアウト間隔を設定できます。これを過ぎるとタイムアウトエラーになります。タイムアウト間隔には、スイッチが TACACS+ サーバからの応答を待つ時間を指定します。これを過ぎるとタイムアウト エラーになります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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**	コンフィギュレーションモードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

サーバのタイムアウト間隔の設定

Cisco Nexus 5000 シリーズ スイッチが、タイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機するタイムアウト間隔を設定できます。 タイムアウト間隔は、スイッチがタイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機する時間を決定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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* | *ipv6-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。 （注） 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。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、TACACS+ サーバ用に別の TCP ポートを設定できます。 デフォルトでは、Cisco Nexus 5000 シリーズ スイッチは、すべての TACACS+ 要求にポート 49 を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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* | *ipv6-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。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、TCP ポートを設定する例を示します。

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

TACACS+ サーバの定期的モニタリングの設定

TACACS+ サーバの可用性をモニタリングできます。 パラメータとして、サーバに使用するユーザ名とパスワード、およびアイドル タイマーがあります。 アイドル タイマーには、TACACS+ サーバがどのくらいの期間要求を受信しなかった場合に、Cisco Nexus 5000 シリーズ スイッチがテスト パケットを送信するかを指定します。このオプションを設定して、サーバを定期的にテストしたり、1 回だけテストを実行できます。

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

テスト アイドル タイマーには、TACACS+ サーバがどのくらいの期間要求を受信しなかった場合に、Cisco Nexus 5000 シリーズ スイッチがテスト パケットを送信するかを指定します。

（注） デフォルトのアイドル タイマー値は 0 分です。 アイドル時間間隔が 0 分の場合、TACACS+ サーバの定期モニタリングは実行されません。

TACACS+ サーバの定期的なモニタリングを設定する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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* | *ipv6-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}	サーバ モニタリング用のパラメータを指定します。デフォルトのユーザ名はtest、デフォルトのパスワードは test です。 アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 （注） TACACS+ サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	switch(config)# **tacacs-server dead-time** *minutes*	Cisco Nexus 5000 シリーズ スイッチが、前回応答しなかったTACACS+サーバをチェックするまでの時間（分）を指定します。 デフォルト値は 0 分、指定できる範囲は 0 ～ 1440 分です。
ステップ 4	switch(config)# **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 5	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ サーバの定期的モニタリングを設定する例を示します。

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

デッド タイム間隔の設定

すべての TACACS+ サーバのデッド タイム間隔を設定できます。 デッド タイム間隔には、Cisco Nexus 5000 シリーズ スイッチが TACACS+ サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを判断するためにテスト パケットを送信するまでの間隔を指定します。

（注） デッドタイム間隔が 0 分の場合、TACACS+ サーバは、応答を返さない場合でも、デッ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。

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**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバまたはサーバ グループの手動モニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password*	TACACS+ サーバにテスト メッセージを送信して可用性を確認します。
ステップ 2	switch# **test aaa group** *group-name username password*	TACACS+ サーバ グループにテスト メッセージを送信して可用性を確認します。

次に、手動でテスト メッセージを送信する例を示します。

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

TACACS+ のディセーブル化

TACACS+ をディセーブルにできます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ 統計情報の表示

スイッチが TACACS+ のアクティビティについて保持している統計情報を表示する手順は、次のとおりです。

手順

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

このコマンドの出力フィールドの詳細については、Nexus スイッチのコマンド リファレンス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。

手順

	コマンドまたはアクション	目的
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* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての TACACS+ サーバのパラメータを表示します。

TACACS+ の設定例

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

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

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

TACACS+ のデフォルト設定

次の表に、TACACS+ パラメータのデフォルト設定を示します。

表 *7*：***TACACS+*** のデフォルト パラメータ

パラメータ	デフォルト
TACACS+	ディセーブル
デッドタイム間隔	0 分
タイムアウト間隔	5 秒
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	test

第 6 章

SSH および Telnet の設定

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

SSH および Telnet の設定

SSH および Telnet の概要

SSH サーバ

Secure Shell（SSH）サーバ機能を使用すると、SSH クライアントがCisco Nexus デバイスに対して、セキュアで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認証メカニズムには、RADIUS、TACACS+、およびローカルに格納されたユーザ名とパスワードを使用した認証があります。

SSH クライアント

SSH クライアント機能は、SSH プロトコルを介して実行されるアプリケーションで、認証と暗号化を行います。 SSH クライアントを使用すると、スイッチは、別のCisco Nexus デバイスまたはSSHサーバを稼働している他の任意のデバイスと、セキュアな暗号化された接続を確立できます。この接続は、暗号化されたアウトバウンド接続を実現します。 認証と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

Cisco Nexus デバイスの SSH クライアントは、無償あるいは商用の SSH サーバと連係して動作します。

SSH サーバ キー

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

- Rivest, Shamir, and Adelman（RSA）公開キー暗号化を使用した SSH バージョン 2
- Digital System 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）

注意 SSH キーをすべて削除すると、SSH サービスを開始できません。

Telnet サーバ

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。 Telnet を使用すると、あるサイトのユーザが別サイトのログイン サーバとの TCP 接続を確立して、システム間でキーストロークをやり取りできます。 Telnet は、リモート システムのアドレスとして、IP アドレスまたはドメイン名を受け取ります。

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

SSH の注意事項および制約事項

SSH には、次の注意事項および制約事項があります。

- Cisco Nexus 5000 シリーズ スイッチは、SSH バージョン 2（SSHv2）だけをサポートしています。

SSH の設定

SSH サーバ キーの生成

セキュリティ要件に基づいて SSH サーバ キーを生成できます。 デフォルトの SSH サーバ キーは、1024 ビットで生成される RSA キーです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]}	SSH サーバ キーを生成します。 *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	switch# **show ssh key**	（任意） SSH サーバ キーを表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、SSH サーバ キーを生成する例を示します。

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

ユーザ アカウント用 SSH 公開キーの指定

SSH 公開キーを設定すると、パスワードを要求されることなく、SSH クライアントを使用してログインできます。 SSH 公開キーは、次の 3 種類のいずれかの形式で指定できます。

- Open SSH 形式
- Internet Engineering Task Force（IETF）SECSH 形式

- Privacy Enhanced Mail（PEM）形式の公開キー証明書

Open SSH 形式による SSH 公開キーの指定

ユーザ アカウント用に SSH 形式で SSH 公開キーを指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **username** *username* **sshkey** *ssh-key*	SSH 形式で SSH 公開キーを設定します。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# **show user-account**	（任意） ユーザ アカウントの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、Open SSH 形式で SSH 公開キーを指定する例を示します。

```
switch# configure terminal
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

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

IETF SECSH 形式による SSH 公開キーの指定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **copy** *server-file* **bootflash:** *filename*	サーバから IETF SECSH 形式の SSH キーを含むファイルをダウンロードします。 File Transfer Protocol（FTP）、SCP、SSH File Transfer Protocol（SFTP）、または Trivial File Transfer Protocol（TFTP）サーバを利用できます。
ステップ 2	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 3	switch(config)# **username** *username* **sshkey file** *filename*	SSH 形式で SSH 公開キーを設定します。
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	switch# **show user-account**	（任意） ユーザ アカウントの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **copy** *server-file* **bootflash:** *filename*	サーバから PEM フォーマット化された公開キー証明書形式の SSH キーを含むファイルをダウンロードします。 FTP、SCP、SFTP、または TFTP サーバを利用できます。

	コマンドまたはアクション	目的
ステップ 2	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 3	switch# **show user-account**	（任意） ユーザ アカウントの設定を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

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 SSH セッションを開始して、リモート デバイスと接続できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **ssh** {*hostname* | *username@hostname*} [**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、IPv6アドレス、またはホスト名を指定します。

SSH ホストのクリア

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

手順

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

SSH サーバのディセーブル化

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

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 モードを開始します。
ステップ 2	switch(config)# **no feature ssh**	SSH サーバをディセーブルにします。デフォルトはイネーブルです。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# **show ssh server**	（任意） SSH サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH サーバ キーの削除

SSH サーバをディセーブルにした後、SSH サーバ キーを削除できます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature ssh**	SSH サーバをディセーブルにします。
ステップ 3	switch(config)# **no ssh key** [**dsa** | **rsa**]	SSH サーバ キーを削除します。 デフォルトでは、すべての SSH キーが削除されます。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	switch# **show ssh key**	（任意） SSH サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH セッションのクリア

SSH セッションを Cisco Nexus デバイスからクリアできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show users**	ユーザ セッション情報を表示します。
ステップ 2	switch# **clear 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。

手順

ステップ 1　SSH サーバ キーを生成します。

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

ステップ 2　SSH サーバをイネーブルにします。

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

（注）　SSH サーバはデフォルトでイネーブルなので、この手順は必要ありません。

ステップ 3 SSH サーバ キーを表示します。

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

ssh-rsa
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 サーバのディセーブル化

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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 telnet**	Telnet サーバをディセーブルにします。 デフォルトはイネーブルです。

Telnet サーバの再イネーブル化

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **feature telnet**	Telnet サーバ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、必要なら、リモート デバイスのユーザ名も取得します。
- Cisco Nexus デバイス上で Telnet サーバをイネーブルにします。
- リモート デバイス上で Telnet サーバをイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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、IPv6 アドレス、またはデバイス名を指定します。

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

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

Telnet セッションのクリア

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show users**	ユーザ セッション情報を表示します。
ステップ 2	switch# **clear 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。

- switch# **show ssh key** [**dsa** | **rsa**]
  SSH サーバ キー ペアの情報を表示します。
- 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。 キーワード **all** を指定すると、SSH およびユーザ アカウントのデフォルト値が表示されます。
- switch# **show ssh server**
  SSH サーバの設定を表示します。
- switch# **show user-account**
  ユーザ アカウント情報を表示します。

SSH のデフォルト設定

次の表に、SSH パラメータのデフォルト設定を示します。

表 *8*：デフォルトの *SSH* パラメータ

パラメータ	デフォルト
SSH サーバ	イネーブル
SSH サーバ キー	1024 ビットで生成された RSA キー
RSA キー生成ビット数	1024
Telnet サーバ	イネーブル

第 7 章

Cisco TrustSec の設定

この章では、Cisco NX-OS デバイスに Cisco TrustSec を設定する手順について説明します。

この章は、次の内容で構成されています。

Cisco TrustSec の概要

ここでは、Cisco TrustSec について説明します。

Cisco TrustSec のアーキテクチャ

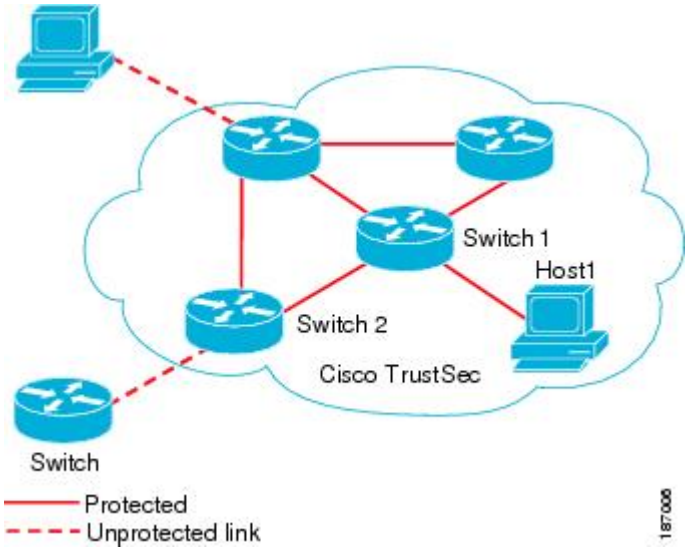
Cisco TrusSec のセキュリティ アーキテクチャは、信頼できるネットワーク デバイスのクラウドを確立することによってセキュア ネットワークを構築します。 また Cisco TrustSec は、認証時に取得されたデバイス情報を、ネットワークに入る際のパケットの分類またはカラリングに使用します。 このパケット分類は、Cisco TrustSec ネットワークへの入力時にパケットにタグ付けされることにより維持されます。タグによってパケットはデータ パス全体を通じて正しく識別され、セ

キュリティおよびその他のポリシー基準が適用されます。 このタグは、Security Group Tag（SGT; セキュリティ グループ タグ）と呼ばれることもあります。エンドポイント装置が SGT に応じてトラフィックをフィルタリングできるようにすることにより、アクセスコントロールポリシーをネットワークに強制できます。

（注） 入力とは、宛先へのパス上のパケットが最初の Cisco TrustSec 対応デバイスに入ることです。出力とは、パス上の最後の Cisco TrustSec 対応デバイスを出ることです。

次の図に、Cisco TrustSec クラウドの例を示します。 この例では、Cisco TrustSec クラウド内に、ネットワーク接続されたデバイスが数台とエンドポイント装置が 1 台あります。 1 台のエンド ポイント装置と 1 台のネットワーク接続されたデバイスは、Cisco TrustSec 対応デバイスではないため、クラウドの外部にあります。

図 *4*： *Cisco TrustSec* ネットワーク クラウドの例



Cisco TrustSec アーキテクチャは、主に次のコンポーネントで構成されています。

認証

Cisco TrustSec ネットワークにデバイスを加入させる前に、各デバイスの識別情報を検証します。

許可

認証されたデバイスの識別情報に基づいて、Cisco TrustSec ネットワークのリソースに対するデバイスのアクセス権のレベルを決定します。

アクセス コントロール

各パケットのソース タグを使用して、パケット単位でアクセス ポリシーを適用します。

Cisco TrustSec ネットワークには、次のエンティティがあります。

オーセンティケータ（AT）

すでに Cisco TrustSec ネットワークに含まれているデバイス

許可サーバ（AS）

認証情報、許可情報、またはその両方を提供できるサーバ

リンクが最初にアップ状態になったときに、許可が実行され、リンクの両側は、SGT および ACL などのリンクに適用されるポリシーを取得します。

認証

Cisco TrustSec は、デバイスのネットワーク加入を許可する前にデバイスを認証します。

デバイス ID

Cisco TrustSec はデバイスの ID として IP アドレスも MAC アドレスも使用しません。 その代わり、各 Cisco TrustSec 対応 Cisco NX-OS デバイスに、Cisco TrustSec ネットワークで一意に識別できる名前（デバイス ID）を手動で割り当てる必要があります。 このデバイス ID は次の操作に使用されます。

- 認証ポリシーの検索
- 認証時におけるデータベース内のパスワードの検索

デバイスのクレデンシャル

Cisco TrustSec はパスワードベースのクレデンシャルをサポートしています。認証サーバは、代わりに自己署名式の証明書を使用する場合もあります。Cisco TrustSec はパスワードでサプリカントを認証し、MSCHAPv2 を使用することにより、たとえ認証サーバの証明書を検証できなくても、相互認証が可能です。

認証サーバは、Cisco TrustSec ネットワークにサプリカントが最初に加入する際に、一時的に設定されたパスワードをそのサプリカントの認証に使用します。サプリカントが最初に Cisco TrustSec ネットワークに加入する際に、認証サーバは証明書を作成してサプリカントを認証し、強力なパスワードを生成して、これを PAC でサプリカントに送信します。 認証サーバはさらに、データベースに新しいパスワードを保存します。

ユーザの証明書

Cisco TrustSec には、エンドポイント装置の特定タイプのユーザ クレデンシャルは必要ありません。ユーザに対して任意のタイプの認証方式（MSCHAPv2、LEAP、Generic Token Card（GTC）、または OTP など）を選択し、対応するクレデンシャルを使用できます。

SGACL と SGT

Security Group Access List（SGACL; セキュリティ グループ アクセス リスト）を使用すると、割り当てられたセキュリティ グループに基づいてユーザが実行できる操作を制御できます。 許可をロールにまとめることにより、セキュリティ ポリシーの管理が容易になります。 Cisco NX-OS デバイスにユーザを追加する際に、1 つ以上のセキュリティ グループを割り当てれば、ユーザは適切な許可を即座に受信できます。セキュリティグループを変更することにより、新しい許可を追加したり、現在の許可を制限することもできます。

Cisco TrustSec はセキュリティ グループに、Security Group Tag（SGT; セキュリティ グループ タグ）という 16 ビットの固有のタグを割り当てます。 Cisco NX-OS デバイス内の SGT の数は認証済みのネットワーク エンティティの数に制限されます。 SGTは全社内の送信元の許可を示す単一ラベルです。 範囲は Cisco TrustSec ネットワーク内でグローバルです。

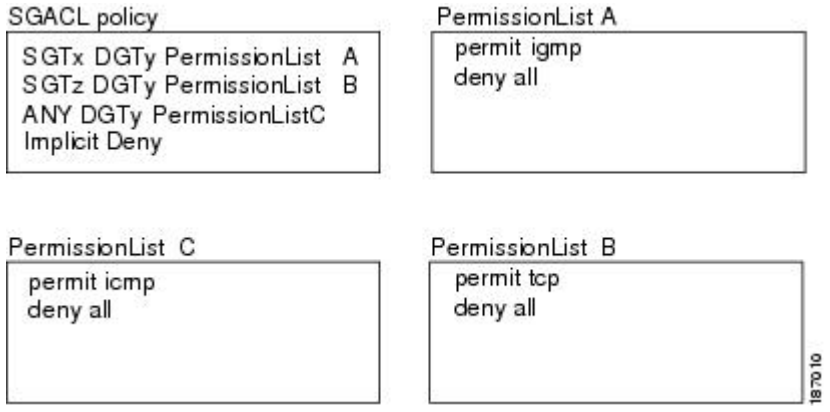
管理サーバは、セキュリティ ポリシーの設定に基づいて SGT を引き出します。 これらを手動で設定する必要はありません。

いったん認証されると、Cisco TrustSec はデバイスを送信元とするすべてのパケットに、そのデバイスが割り当てられているセキュリティ グループを表す SGT を付けます。 タグ付けされたパケットはネットワークを通じて Cisco TrustSec ヘッダーで SGT を運びます。 このタグは、送信元のグループを表しているので、送信元の SGT として参照されます。 Cisco TrustSec は、ネットワークの出口で、パケットの宛先デバイスに割り当てられているグループを判断し、アクセス コントロール ポリシーを適用します。

Cisco TrustSec はセキュリティ グループ間のアクセス コントロール ポリシーを定義します。 Cisco TrustSec は、ネットワーク内のデバイスをセキュリティ グループに割り当て、セキュリティ グループ間およびセキュリティ グループ内でアクセスコントロールを適用することにより、ネットワーク内での原則的なアクセス コントロールを行います。

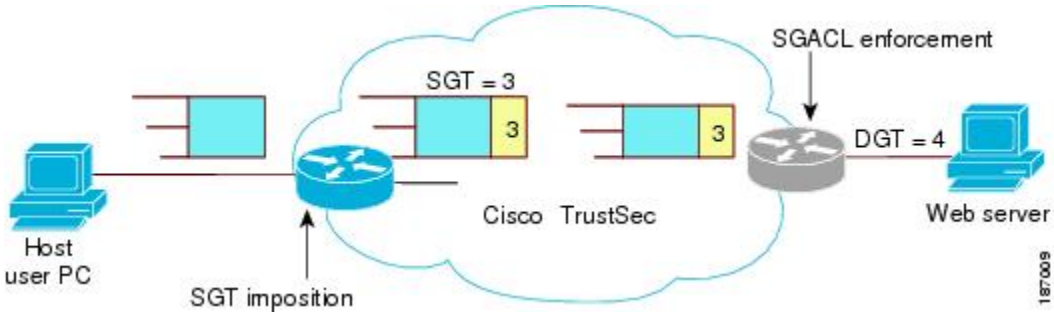
次の図に SGACL ポリシーの例を示します。

図 *5*： *SGACL* ポリシーの例



Cisco TrustSec ネットワークでは、次の図のように SGT の割り当てと SGACL の強制が実行されます。

図 *6*： *Cisco TrustSec* ネットワークでの *SGT* と *SGACL*



Cisco NX-OS デバイスは、従来の ACL の IP アドレスではなく、デバイス グループに Cisco TrustSec アクセス コントロール ポリシーを定義します。 このような組み合わせの解除によって、ネットワーク全体でネットワーク デバイスを自由に移動し、IP アドレスを変更できます。ネットワーク トポロジ全体を変更することが可能です。 ロールと許可が同じであれば、ネットワークが変更されてもセキュリティ ポリシーには影響しません。 この機能によって、ACL のサイズが大幅に節約され、保守作業も簡単になります。

従来の IP ネットワークでは、設定されている Access Control Entry（ACE; アクセス コントロール エントリ）の数は次のようにして決まります。

ACE の数=（指定されている送信元の数）X（指定されている宛先の数）X（指定されている許可の数）

Cisco TrustSec では、次の式を使用します。

ACE の数 = 指定されている許可の数

送信元セキュリティ グループの判断

Cisco TrustSec クラウドの入口のネットワーク デバイスは、Cisco TrustSec クラウドにパケットを転送する際に、パケットに SGT をタグ付けできるように、Cisco TrustSec クラウドに入るパケットの SGT を判断する必要があります。 出口のネットワーク デバイスは、SGACL を適用できるように、パケットの SGT を判断する必要があります。

ネットワーク デバイスは、次のいずれかの方法でパケットの SGT を判断できます。

- ポリシー取得時に送信元の SGT を取得する：Cisco TrustSec 認証フェーズ後、ネットワーク デバイスは認証サーバからポリシーを取得します。 認証サーバは、ピア デバイスが信頼できるかどうかを伝えます。 ピア デバイスが信頼できる場合、認証サーバはそのピア デバイスから着信するすべてのパケットに適用する SGT も提供します。
- Cisco TrustSec ヘッダーの送信元 SGT フィールドを取得する：信頼できるピア デバイスからパケットが着信した場合、そのパケットにとってネットワーク デバイスが Cisco TrustSec クラウド内の最初のネットワーク デバイスではない場合に、Cisco TrustSec ヘッダーの SGT フィールドで正しい値が伝送されます。

宛先セキュリティ グループの判断

Cisco TrustSec クラウドの出口のネットワーク デバイスは、SGACL を適用する宛先グループを判断します。 場合によっては、入口のデバイスまたは出口以外のその他のデバイスが、使用できる宛先グループの情報を持っていることもあります。 このような場合、SGACL は出口のデバイスではなくこれらのデバイスに適用されます。

Cisco TrustSec は、宛先 IP アドレスに基づいてパケットの宛先グループを決定します。

宛先 SGT を設定して、FEX または vEthernet ポート上の出力ブロードキャスト、マルチキャスト、および不明なユニキャスト トラフィックに対して Cisco TrustSec を強制することはしません。 代わりに、DST をゼロ（不明）に設定します。 次に、正しい設定の例を示します。

```
cts role-based access-list acl-on-fex-egress
     deny udp
     deny ip
cts role-based sgt 9 dst 0 access-list acl-on-fex-egress
```

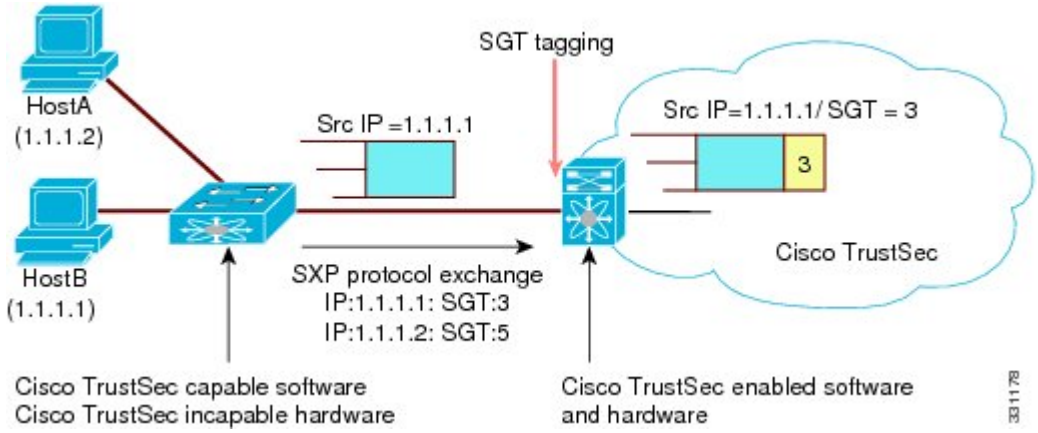
SXP によるレガシー アクセス ネットワークへの SGT の伝播

アクセス レイヤの Cisco NX-OS デバイス ハードウェアは Cisco TrustSec をサポートしています。 Cisco TrustSec ハードウェアがないと、Cisco TrustSec ソフトウェアはパケットに SGT をタグ付けできません。 SXP を使用すると、Cisco TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播できます。

SXP はアクセス レイヤ デバイスと宛先レイヤ デバイスの間で動作します。 アクセス レイヤ デバイスは SXP を使用して、SGT とともに Cisco TrustSec 認証デバイスの IP アドレスをディストリビューション スイッチに渡します。 Cisco TrustSec 対応のソフトウェアとハードウェアを両方備えたディストリビューション デバイスはこの情報を使用して、パケットに適切にタグを付け、SGACL ポリシーを強制します。

次の図に、SXP を使用して、従来のネットワークで SGT 情報を伝播する方法を示します。

図 *7*：*SXP* を使用した *SGT* 情報の伝播



パケットへの SGT のタグ付けには、ハードウェアによるサポートが必要です。 ネットワーク内に、パケットにSGTのタグ付けを行えないデバイスが含まれている可能性もあります。 これらのデバイスから Cisco TrustSec 対応のハードウェアを搭載しているデバイスに IP アドレスと SGT のマッピングを送信できるようにするには、SXP 接続を手動で設定する必要があります。 SXP 接続の手動での設定には、次のことが必要です。

- SXP データの整合性と認証が必要になる場合は、ピア デバイスの両方に同じ SXP パスワードを設定する必要があります。 SXPパスワードは各ピア接続に対して明示的に指定することも、デバイスに対してグローバルに設定することもできます。 SXPパスワードは必須ではありません。
- 各ピアを SXP 接続に SXP スピーカーまたは SXP リスナーとして設定する必要があります。 スピーカー デバイスはリスナー デバイスに SXP 情報を渡します。

（注） Cisco Nexus 5000 シリーズ スイッチには SXP リスナーになる機能はありません。 SXP スピーカーになることだけができます。

- 送信元 IP アドレスを指定して各ピアの関係付けに使用したり、特定の送信元 IP アドレスを設定していないピア接続に対してデフォルトの送信元IPアドレスを設定したりすることができます。

環境データのダウンロード

Cisco TrustSec 環境データは、Cisco TrustSec ノードとしてのデバイスの機能を支援するひとまとまりの情報またはポリシーです。 デバイスは、Cisco TrustSec クラウドに最初に加入する際に、認証サーバから環境データを取得しますが、一部のデータをデバイスに手動で設定することもできます。 たとえば、Cisco TrustSec のシード デバイスには認証サーバの情報を設定する必要がありますが、この情報は、デバイスが認証サーバから取得するサーバ リストを使用して、後から追加することができます。

デバイスは、期限前に Cisco TrustSec 環境データをリフレッシュする必要があります。 また、このデータの有効期限が切れていなければ、データをキャッシュし、リブート後に再利用することもできます。

デバイスは RADIUS を使用して、認証サーバから次の環境データを取得します。

サーバ リスト

クライアントがその後の RADIUS 要求に使用できるサーバのリスト（認証および許可の両方）

デバイス SGT

そのデバイス自体が属しているセキュリティ グループ

有効期間

Cisco TrustSec デバイスが環境データをリフレッシュする頻度を左右する期間

Cisco TrustSec のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	Cisco TrustSec にはライセンスは必要ありません。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS のライセンス スキームの詳細は、『*License and Copyright Information for Cisco NX-OS Software*』を参照してください。

Cisco TrustSec の前提条件

Cisco TrustSec の前提条件は次のとおりです。

- Cisco TrustSec 機能をイネーブルにする前に、802.1X 機能をイネーブルにする必要があります。 802.1X インターフェイス レベルの機能が使用できませんが、デバイスが RADIUS で認証するためには 802.1X が必要です。
- Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec の注意事項と制約事項

Cisco TrustSec に関する注意事項と制約事項は次のとおりです。

- Cisco TrustSec は、Cisco Nexus 5500 シリーズ スイッチ上でサポートされます。 Cisco Nexus 5000 シリーズ スイッチ上ではサポートされません。
- Cisco TrustSec は認証に RADIUS を使用します。
- Cisco TrustSec の AAA 認証および認可は、Cisco Secure Access Control Server（ACS）でだけサポートされています。
- Cisco TrustSec は IPv4 アドレスだけをサポートします。
- SXP は管理（mgmt 0）インターフェイスを使用できません。
- 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。
- ポリシーをクリアしても、すぐには有効になりません。フラップが発生する必要があります。 さらに、ポリシーがクリアされる方法は、SGT がスタティックまたはダイナミックのどちらであるかによって異なります。 スタティック SGT の場合、フラップが発生した後で SGT

が 0 にリセットされます。 ダイナミック SGT の場合、フラップが発生した後で SGT が RADIUS サーバから再度ダウンロードされます。

- Cisco TrustSec は、ルーティングされたスイッチ仮想インターフェイス（SVI）ではなく、管理 SVI をサポートしています。
- Cisco TrustSec 機能をイネーブルにする前に、802.1X 機能がイネーブルになっている必要があります。 ただし、802.1X のインターフェイス レベルの機能はいずれも使用できません。802.1X 機能は、RADIUS でのデバイスの認証にのみ使用されます。
- RBACL は、ブリッジされたイーサネット トラフィック上にのみ実装され、ルーティング VLAN またはルーティング インターフェイス上でイネーブルにすることはできません。
- ピアが信頼できるかどうかの判定や、出力に SGT を伝播する機能は、物理インターフェイス レベルで実行されます。
- ポート チャネル メンバ上の Cisco TrustedSec インターフェイス設定は、正確に同じである必要があります。 あるポート チャネル メンバが他のポート チャネル メンバと一致していない場合、そのポート チャネル メンバはエラー ディセーブル状態になります。
- vPC ドメインでは、Cisco TrustSec 設定がピア間で確実に同期されるようにするために、設定同期モード（config-sync）を使用してスイッチ プロファイルを作成します。 同じ vPC を 2 つのピア スイッチ上で異なった方法で設定すると、トラフィックは異なった方法で処理されます。
- Nexus 5500 スイッチでは、RBACL TCAM エントリの最大数は 128 であり、デフォルトではそのうちの 4 つのエントリが使用され、残りの 124 のエントリはユーザが設定できます。
- Cisco TrustSec は、レイヤ 3 インターフェイスまたは仮想ルーティング/転送（VRF）インターフェイスではサポートされていません。
- **cts-manual**、**sgt value**、**cts trusted mode**、**no-propagate sgt** の各設定は、同じポート チャネル上のすべてのポート チャネル メンバ、および同じファブリック ポート上のすべての FEX ポートまたは vEthernet ポート間で一致している必要があります。 これらの設定が一致していない場合、インターフェイスはエラー ディセーブル状態になります。

Cisco TrustSec のデフォルト設定

次の表に、Cisco TrustSec パラメータのデフォルト設定を示します。

表 *9*：*Cisco TrustSec* パラメータのデフォルト設定

パラメータ	デフォルト
Cisco TrustSec	ディセーブル
SXP	ディセーブル
SXP デフォルト パスワード	なし

パラメータ	デフォルト
SXP 復帰期間	120 秒（2 分）
SXP リトライ期間	60 秒（1 分）
RBACL ロギング	ディセーブル
RBACL 統計情報	ディセーブル

Cisco TrustSec の設定

ここでは、Cisco TrustSec の設定作業について説明します。

Cisco TrustSec 機能のイネーブル化

Cisco TrustSec を設定する前に、Cisco NX-OS デバイス上の 802.1X 機能および Cisco TrustSec の機能をイネーブルにする必要があります。 ただし、802.1X のインターフェイス レベルの機能はいずれも使用できません。 802.1X 機能は、RADIUS でのデバイスの認証にのみ使用されます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**feature dot1x** 例： `switch(config)# feature dot1x`	802.1X 機能をイネーブルにします。
ステップ 3	**feature cts** 例： `switch(config)# feature cts`	Cisco TrustSec 機能をイネーブルにします。

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。

	コマンドまたはアクション	目的
ステップ 5	**show cts** 例： `switch# show cts`	（任意） Cisco TrustSec の設定を表示します。
ステップ 6	**show feature** 例： `switch# show feature`	（任意） 機能がイネーブルになったステータスを表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec デバイスのクレデンシャルの設定

ネットワーク内の Cisco TrustSec 対応 Cisco NX-OS デバイス各々に、固有の Cisco TrustSec クレデンシャルを設定する必要があります。 Cisco TrustSec はクレデンシャルのパスワードをデバイスの認証に使用します。

（注） Cisco Secure ACS にも Cisco NX-OS デバイスの Cisco TrustSec クレデンシャルを設定する必要があります。（次の URL のマニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_and_configuration_guides_list.html）。

はじめる前に

Cisco TrustSec 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)#`
		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	**cts device-id** *name* **password** *password* 例： `switch(config)# cts device-id MyDevice1 password CiscO321`	固有のデバイス ID およびパスワードを設定します。 *name* 引数は、最大 32 文字で大文字と小文字を区別します。

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

ステップ 4	**show cts** 例： `switch# show cts`	（任意） Cisco TrustSec の設定を表示します。
ステップ 5	**show cts environment** 例： `switch# show cts environment`	（任意） Cisco TrustSec 環境データを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化 , （92 ページ）

Cisco TrustSec の AAA の設定

Cisco TrustSec の認証に Cisco Secure ACS を使用できます。 ネットワーク クラウド内の Cisco TrustSec 対応 Cisco NX-OS デバイスの 1 つに、RADIUS サーバ グループを設定し、デフォルトの AAA 認証および許可を指定する必要があります。

（注） Cisco TrustSec をサポートしているのは、Cisco Secure ACS だけです。

Cisco TrustSec Cisco NX-OS デバイスでの AAA の設定

ここでは、Cisco TrustSec ネットワーク クラウド内の Cisco NX-OS デバイスで AAA を設定する手順を説明します。

はじめる前に

Cisco ACS の IPv4 のアドレスまたはホスト名を取得します。

Cisco TrustSec 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	**radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **key** [**0** | **7**] *key* **pac** 例： `switch(config)# radius-server host 10.10.1.1 key L1a0K2s9 pac`	キーと PAC を使用して RADIUS サーバ ホストを設定します。 *hostname* 引数、*key* 引数は英数字であり、大文字と小文字を区別し、最大長は 63 文字です。 **0** オプションは、キーがクリア テキストであることを示します。 **7** オプションは、キーが暗号化されていることを示します。 デフォルトはクリア テキストです。
ステップ 3	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。

ステップ 4	**aaa group server radius** *group-name*
	
	例：
	`switch(config)# aaa group server radius Rad1`
	`switch(config-radius)#`
		RADIUS サーバ グループを指定し、RADIUS サーバ グループ コンフィギュレーション モードを開始します。

ステップ 5	**server** {*ipv4-address* | *ipv6-address* | *hostname*} 例： `switch(config-radius)# server 10.10.1.1`	RADIUS サーバ ホストのアドレスを指定します。
ステップ 6	**use-vrf** *vrf-name* 例： `switch(config-radius)# use-vrf management`	AAA サーバ グループの管理 VRF を指定します。 （注） 管理 VRF を使用する場合、ネットワーク クラウド内の デバイスにそれ以上の設定を行う必要はありません。 異なる VRF を使用する場合は、 デバイスに VRF を設定する必要があります。

	コマンドまたはアクション	目的

ステップ 7	**exit**
	
	例：
	`switch(config-radius)# exit`
	`switch(config)#`
		RADIUS サーバ グループ コンフィギュレーション モードを終了します。

ステップ 8	**aaa authentication cts default group** *group-name* 例： `switch(config)# aaa authentication cts default group Rad1`	Cisco TrustSec 認証に使用する RADIUS サーバ グループを指定します。
ステップ 9	**aaa authorization cts default group** *group-name* 例： `switch(config)# aaa authentication cts default group Rad1`	Cisco TrustSec 認証に使用する RADIUS サーバ グループを指定します。

ステップ 10	**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 11	**show radius-server groups** [*group-name*] 例： `switch# show radius-server group rad1`	（任意） RADIUS サーバ グループの設定を表示します。
ステップ 12	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） AAA 認証の設定を表示します。
ステップ 13	**show aaa authorization** 例： `switch# show aaa authorization`	（任意） AAA 認可設定を表示します。
ステップ 14	**show cts pacs** 例： `switch# show cts pacs`	（任意） Cisco TrustSec PAC 情報を表示します。
ステップ 15	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）

手動での Cisco TrustSec 認証の設定

Cisco NX-OS デバイスに Cisco Secure ACS 接続の両側のインターフェイスに手動で設定する必要があります。

注意 手動モードでの Cisco TrustSec の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** { **ethernet** | **vethernet** } *slot/port*
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		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	**cts manual**
	
	例：
	`switch(config-if)# cts manual`
	`switch(config-if-cts-manual)#`
		Cisco TrustSec 手動コンフィギュレーション モードを開始します。
		（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。

ステップ 4	**policy dynamic identity** *peer-name* 例： `switch(config-if-cts-manual)# policy dynamic identity MyDevice2`	（任意） ダイナミック許可ポリシーのダウンロードを設定します。 *peer-name* 引数は、ピア デバイスの Cisco TrustSec デバイス ID です。 ピア名では、大文字と小文字が区別されます。

	コマンドまたはアクション	目的
		（注） Cisco TrustSec クレデンシャルが設定されていることおよび Cisco TrustSec の AAA が設定されていることを確認します。 （注） **policy dynamic** コマンドと **policy static** コマンドは同時に使用できません。一度に 1 つしか適用できません。 交互に変更するには、他のコマンドを設定する前に、このコマンドの **no** 形式を使用して設定を削除する必要があります。
ステップ 5	**policy static sgt** *tag* [**trusted**] 例： `switch(config-if-cts-manual)# policy static sgt 0x2`	（任意） スタティック許可ポリシーを設定します。*tag* 引数は、0x2 から 0xffef の 16 進形式で指定します。**trusted** キーワードを指定すると、SGT 付きでインターフェイスにトラフィックが着信した場合、そのタグは上書きされません。 （注） **policy dynamic** コマンドと **policy static** コマンドは同時に使用できません。一度に 1 つしか適用できません。 交互に変更するには、他のコマンドを設定する前に、このコマンドの **no** 形式を使用して設定を削除する必要があります。

ステップ 6	**exit**
	
	例：
	`switch(config-if-cts-manual)# exit`
	`switch(config-if)#`
		Cisco TrustSec 手動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	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 8	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。

ステップ 9	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**show cts interface all** 例： `switch# show cts interface all`	（任意） インターフェイスの Cisco TrustSec 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`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）

インターフェイスでの Cisco TrustSec のポーズ フレームの暗号化または復号化の設定

ポーズ フレームは、イーサネット フロー制御に使用される MAC 制御フレームです。 一部のラインカードのポートは、ポーズ フレームの暗号化と復号化を実行します。一方、他のラインカードのポートにはこの機能がありません。 このような不一致により相互運用性の問題が発生し、ポートはポーズ フレームを廃棄するか、無視します。

Cisco NX-OS Release 5.2 以降では、ポーズ フレームを暗号化するかしないかを個々 のインターフェイス上で設定できます。 接続の両側のインターフェイスを設定する必要があります。dot1x または手動モードのいずれかを使用して実行できます。 2 つのポートが CTS リンクを実現するように接続され、一方がクリア Pause Capable、他方がセキュア（暗号化/復号化）Pause Capable である場合、ポーズフレームは、正しく送受信するために、クリアテキストでリンク間に送信する必要があります。

（注） F1 シリーズ モジュールおよび N7K-M132XP-12(L) モジュールはクリア ポーズ フレームだけをサポートします。 他の M1 シリーズ モジュールはすべてセキュア（暗号化および復号化）およびクリア ポーズ フレームをサポートします。

（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。 インターフェイスが半二重モードに設定されているかどうかを調べるには、**show interface** コマンドを使用します。

注意 ポーズ フレームの暗号化または復号化の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

flowcontrol {**send** | **receive**} コマンドを使用して、インターフェイスでフロー制御をイネーブルにしたことを確認します。

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 ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		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	**cts dot1x** または **cts manual**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec dot1x または手動コンフィギュレーション モードを開始します。
		（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。

ステップ 4	[**no**] **encrypt pause-frame**
	
	例：
	`switch(config-if-cts-dot1x)#`
	`no encrypt pause-frame`
		インターフェイスの Cisco TrustSec のポーズ フレームの暗号化または復号化を設定します。 **no encrypt pause-frame** が設定されている場合、ポーズ フレームはクリア テキストで送信されます。 **encrypt pause-frame** が設定されている場合、ポーズ フレームは CTS リンク上で暗号化されて送信されます。

ステップ 5	**exit**
	
	例：
	`switch(config-if-cts-dot1x)#`
	`exit`
	`switch(config-if)#`
		Cisco TrustSec dot1x または手動コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 7	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにしたり、インターフェイス上で Cisco TrustSec のポーズフレームの暗号化または復号化をイネーブルにしたりします。

ステップ 8	**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 9	**show cts interface all** 例： `switch# show cts interface all`	（任意） インターフェイスの Cisco TrustSec 設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SGACL ポリシーの設定

ここでは、SGACL ポリシーの設定作業について説明します。

SGACL ポリシーの設定プロセス

Cisco TrustSec の SGACL ポリシーを設定するには、次の手順を行います。

手順

ステップ 1 レイヤ 2 インターフェイスの場合は、Cisco TrustSec がイネーブルになっているインターフェイスがある VLAN に対して、SGACL ポリシーの強制をイネーブルにします。

ステップ 2 SGACL ポリシーの設定のダウンロードに Cisco Secure ACS 上の AAA を使用しない場合は、SGACL のマッピングとポリシーを手動で設定します。

VLAN に対する SGACL ポリシーの強制のイネーブル化

SGACL を使用する場合、Cisco TrustSec がイネーブルになっているレイヤ 2 インターフェイスがある VLAN 内で、SGACL ポリシーの強制をイネーブルにする必要があります。

（注） この操作は、FCoE VLAN では実行できません。

はじめる前に

Cisco TrustSec 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)#`
		コ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-id*
	
	例：
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		VLAN を指定し、VLAN コンフィギュレーション モードを開始します。

ステップ 3	**cts role-based enforcement** 例： `switch(config-vlan)# cts role-based enforcement`	VLAN に対する Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN 設定を保存し、VLAN コンフィギュレーション モードを終了します。

ステップ 5	**show cts role-based enable** 例： `switch(config)# show cts role-based enable`	（任意） Cisco TrustSec SGACL 強制の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化 , （92 ページ）

Cisco TrustSec SGT の手動設定

このデバイスから発信されるパケットに、固有の Cisco TrustSec Security Group Tag（SGT）を手動で設定できます。

はじめる前に

Cisco TrustSec 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)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**cts sgt** *tag* 例： `switch(config)# cts sgt 0x00a2`	デバイスから送信されるパケットの SGT を設定します。 *tag* 引数は、**0x***hhhh* の形式の 16 進値です。 指定できる範囲は 0x2 ～ 0xffef です。

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

ステップ 4	**show cts environment-data** 例： `switch# show cts environment-data`	（任意） Cisco TrustSec の環境データ情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化 , （92 ページ）

VLAN に対する IPv4 アドレスと SGACL SGT のマッピングの手動設定

SGT ポリシーが ACS サーバからダウンロードされる、または SXP モードを使用している場合に SGT マッピングがリスナーにリレーされるように、IPv4 アドレスを VLAN の SGACL SGT マッピングに手動で設定することができます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

VLAN の SGACL ポリシーの強制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)#`
		コ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-id*
	
	例：
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		VLANを指定し、VLANコンフィギュレーション モードを開始します。

ステップ 3	**cts role-based sgt-map** *ipv4-address tag* 例： `switch(config-vlan)# cts role-based sgt-map 10.10.1.1 100`	VLAN に対する SGACL ポリシーの SGT マッピングを設定します。

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN設定を保存し、VLANコンフィギュレーション モードを終了します。

ステップ 5	**show cts role-based sgt-map** 例： `switch(config)# show cts role-based sgt-map`	（任意） Cisco TrustSec SGACL SGT のマッピング設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）
VLAN に対する SGACL ポリシーの強制のイネーブル化，（102 ページ）

VRF に対する IPv4 アドレスと SGACL SGT のマッピングの手動設定

SGACL ポリシー設定のダウンロードに Cisco Secure ACS を使用できない場合は、IPv4 アドレスと SGACL SGT のマッピングを VRF に手動で設定できます。 Cisco NX-OS デバイスで、Cisco Secure ACSを使用できない場合は、この機能を使用できます。 VRF の IPv4 SGT マッピングは SXP スピーカーに役立ちます。

（注） **cts role based enforcement** コマンドは、VRF ではサポートされません。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

レイヤ 3 モジュール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)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**vrf context** *vrf-name*
	
	例：
	`switch(config)# vrf accounting`
	`switch(config-vrf)#`
		VRF を指定し、VRF 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	**cts role-based sgt-map** *ipv4-address tag* 例： `switch(config-vrf)# cts role-based sgt-map 10.10.1.1 100`	VLAN に対する SGACL ポリシーの SGT マッピングを設定します。

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

	コマンドまたはアクション	目的
ステップ 5	**show cts role-based sgt-map** 例： `switch(config)# show cts role-based sgt-map`	（任意） Cisco TrustSec SGACL SGT のマッピング設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SGACL ポリシーの手動設定

SGACL ポリシー設定のダウンロードに Cisco Secure ACS を使用しない場合は、Cisco NX-OS デバイスに手動で SGACL ポリシーを設定できます。 ロールベース アクセス コントロール リスト（RBACL）ロギングをイネーブルにすることもできます。これにより、ユーザは、Cisco NX-OS デバイスに着信する特定タイプのパケットをモニタできるようになります。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

Cisco TrustSec ロギングを機能させるには、Cisco TrustSec カウンタまたは統計情報をイネーブルにする必要があります。

VLAN に対する SGACL ポリシーの強制がイネーブルになっていることを確認します。

RBACL ロギングをイネーブルにする場合は、VLAN に対する RBACL ポリシーの強制がイネーブルになっていることを確認します。

RBACL ロギングをイネーブルにする場合は、CTS マネージャ syslog のログ レベルが 6 以下に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。

	コマンドまたはアクション	目的

ステップ 2	**cts role-based access-list** *list-name*
	
	例：
	`switch(config)# cts role-based access-list MySGACL`
	`switch(config-rbacl)#`
		SGACL を指定し、ロールベース アクセス リスト コンフィギュレーション モードを開始します。*list-name* 引数には、大文字と小文字を区別して、最大 32 文字の英数字で値を指定します。

ステップ 3	{**deny** | **permit**} **all** [**log**] 例： `switch(config-rbacl)# deny all log`	（任意） すべてのトラフィックを拒否または許可します。必要に応じて **log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。
ステップ 4	{**deny** | **permit**} **icmp** [**log**] 例： `switch(config-rbacl)# permit icmp`	（任意） インターネット制御メッセージ プロトコル（ICMP）トラフィックを拒否または許可します。必要に応じて **log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。
ステップ 5	{**deny** | **permit**} **igmp** [**log**] 例： `switch(config-rbacl)# deny igmp`	（任意） インターネット グループ管理プロトコル（IGMP）トラフィックを拒否または許可します。 必要に応じて **log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。
ステップ 6	{**deny** | **permit**} **ip** [**log**] 例： `switch(config-rbacl)# permit ip`	（任意） IP トラフィックを拒否または許可します。 必要に応じて **log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。
ステップ 7	{**deny** | **permit**} **tcp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}] [**log**] 例： `switch(config-rbacl)# deny tcp dst eq 100`	（任意） TCP トラフィックを拒否または許可します。 デフォルトではすべての TCP トラフィックが許可されます。 *port-number*、*port-number1*、port-number2 の引数の範囲は 0 ～ 65535 です。 必要に応じて **log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。
ステップ 8	{**deny** | **permit**} **udp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range** *port-number1 port-number2*}] [**log**]	UDP トラフィックを拒否または許可します。 デフォルトではすべての UDP トラフィックが許可されます。 *port-number*、*port-number1*、port-number2 の引数の範囲は 0 ～ 65535 です。 必要に応じて

	コマンドまたはアクション	目的
	例： `switch(config-rbacl)# permit udp src eq 1312`	**log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。
ステップ 9	**exit** 例： `switch(config-rbacl)# exit switch(config)#`	ロールベース アクセス リスト コンフィギュレーション モードを終了します。
ステップ 10	**cts role-based sgt** {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list** *list-name* 例： `switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL`	SGT 値と SGACL をマッピングします。 *sgt-value* 引数と *dgt-value* 引数の範囲は、0 ～ 65519 です。 （注） SGT と SGACL をマッピングするには、あらかじめ SGACL を作成しておく必要があります。
ステップ 11	**show cts role-based access-list** 例： `switch(config)# show cts role-based access-list`	（任意） Cisco TrustSec SGACL の設定を表示します。
ステップ 12	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）
VLAN に対する SGACL ポリシーの強制のイネーブル化，（102 ページ）

ダウンロードされた SGACL ポリシーの表示

Cisco TrustSec のデバイス クレデンシャルと AAA の設定後、Cisco Secure ACS からダウンロードされた Cisco TrustSec SGACL ポリシーを検証できます。 Cisco NX-OS ソフトウェアは、インターフェイスに対する認証および許可、または IPv4 アドレスおよび SGACL SGT の手動マッピングによって新しい SGT を学習すると、SGACL ポリシーをダウンロードします。

はじめる前に

Cisco TrustSec 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	**show cts role-based access-list** 例： `switch# show cts role-based access-list`	Cisco TrustSec SGACL を表示します（Cisco Secure ACS からダウンロードされたものと Cisco NX-OS デバイスに手動で設定されたものの両方）。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）

ダウンロードされた SGACL ポリシーのリフレッシュ

Cisco Secure ACS によって Cisco NX-OS デバイスにダウンロードされた SGACL ポリシーをリフレッシュできます。

はじめる前に

Cisco TrustSec 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	**cts refresh role-based policy** 例： `switch# cts refresh policy`	Cisco Secure ACS からの Cisco TrustSec SGACL をリフレッシュします。
ステップ 2	**show cts role-based policy** 例： `switch# show cts role-based policy`	（任意） Cisco TrustSec SGACL ポリシーを表示します。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）

RBACL の統計情報のイネーブル化

Role-Based Access Control List（RBACL; ロールベース アクセス コントロール リスト）ポリシーと一致するパケット数のカウントを要求できます。 この統計情報は、ACE ごとに収集されます。

（注） RBACL 統計情報は、Cisco NX-OS デバイスのリロード時または統計情報を故意にクリアしたときにだけ失われます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

RBACL 統計情報をイネーブルにする場合は、VLAN に対する RBACL ポリシーの強制がイネーブルになっていることを確認します。

RBACL 統計情報をイネーブルにするには、ハードウェアのエントリが各ポリシーに 1 つずつ必要です。ハードウェアに十分な領域が残っていない場合は、エラーメッセージが表示され、統計情報をイネーブルにできません。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コ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] cts role-based counters enable** 例： `switch(config)# cts role-based counters enable`	RBACL 統計情報をイネーブルまたはディセーブルにします。 デフォルトはディセーブルです。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ステップ 4	**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 5	**show cts role-based counters** 例： `switch# show cts role-based counters`	（任意） RBACL 統計情報の設定ステータスを表示し、すべての RBACL ポリシーの統計情報を一覧表示します。
ステップ 6	**clear cts role-based counters** 例： `switch# clear cts role-based counters`	（任意） すべてのカウンタが 0 にリセットされるように、RBACL 統計情報をクリアします。

Cisco TrustSec の SGACL ポリシーのクリア

Cisco TrustSec の SGACL ポリシーをクリアできます。

（注） ポリシーをクリアしても、すぐには有効になりません。フラップが発生する必要があります。さらに、ポリシーがクリアされる方法は、SGT がスタティックまたはダイナミックのどちらであるかによって異なります。 スタティック SGT の場合、フラップが発生した後で SGT が 0 にリセットされます。 ダイナミック SGT の場合、フラップが発生した後で SGT が RADIUS サーバから再度ダウンロードされます。

はじめる前に

Cisco TrustSec 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	**show cts role-based policy** 例： `switch# clear cts policy all`	（任意） Cisco TrustSec RBACL ポリシーの設定を表示します。
ステップ 2	**clear cts policy** {**all** | **peer** *device-name* | **sgt** *sgt-value*} 例： `switch# clear cts policy all`	Cisco TrustSec 接続情報のポリシーをクリアします。

関連トピック

Cisco TrustSec 機能のイネーブル化 , （92 ページ）

SXP の手動設定

SGT Exchange Protocol（SXP）を使用すると、Cisco TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播できます。 ここでは、ネットワーク内の Cisco NX-OS デバイスに Cisco TrustSec SXP を設定する手順について説明します。

Cisco TrustSec SXP の設定プロセス

Cisco TrustSec SXP の手動による設定手順は次のとおりです。

手順

ステップ 1 Cisco TrustSec 機能をイネーブルにします。

ステップ 2 Cisco TrustSec SXP をイネーブルにします。

ステップ 3 SXP ピア接続を設定します。

（注） SXP には管理（mgmt 0）接続は使用できません。

関連トピック

VLAN に対する SGACL ポリシーの強制のイネーブル化，（102 ページ）
VLAN に対する IPv4 アドレスと SGACL SGT のマッピングの手動設定，（104 ページ）
SGACL ポリシーの手動設定，（106 ページ）
Cisco TrustSec 機能のイネーブル化，（92 ページ）
Cisco TrustSec SXP のイネーブル化，（112 ページ）
Cisco TrustSec SXP のピア接続の設定，（113 ページ）

Cisco TrustSec SXP のイネーブル化

ピアの接続を設定する前に、Cisco TrustSec SXP をイネーブルにする必要があります。

はじめる前に

Cisco TrustSec 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)#`
		コンフィギュレーションモードを開始します。

ステップ 2	**cts sxp enable** 例： `switch(config)# cts sxp enable`	Cisco TrustSec の SXP をイネーブルにします。

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

	コマンドまたはアクション	目的
ステップ 4	**show cts sxp** 例： `switch# show cts sxp`	（任意） SXP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）

Cisco TrustSec SXP のピア接続の設定

両方のデバイスでSXP ピア接続を設定する必要があります。一方のデバイスはスピーカーで、他方のデバイスはリスナーになります。パスワード保護を使用している場合は、必ず両エンドに同じパスワードを使用してください。

（注） デフォルトの SXP 送信元 IP アドレスが設定されていない場合に、接続の SXP 送信元アドレスを指定しないと、Cisco NX-OS ソフトウェアは既存のローカル IP アドレスから SXP 送信元 IP アドレスを抽出します。その Cisco NX-OS デバイスから開始される各 TCP 接続で SXP 送信元アドレスが異なる可能性があります。

（注） Cisco Nexus 5000 シリーズ スイッチでは、SXP のスピーカー モードだけがサポートされます。そのため、任意の SXP ピアをリスナーとして設定する必要があります。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

SXP がイネーブルになっていることを確認します。

VRF に対する SGACL ポリシーの強制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)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp connection peer** *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** *password*} **mode listener** [**vrf** *vrf-name*] 例： `switch(config)# cts sxp connection peer 10.10.1.1 source 20.20.1.1 password default mode listener`	SXP アドレス接続を設定します。 source キーワードには発信元デバイスの IPv4 アドレスを指定します。 デフォルトの発信元は、**cts sxp default source-ip** コマンドを使用して設定した IPv4 アドレスです。 password キーワードには、SXP で接続に使用するパスワードを指定します。次のオプションがあります。 **default** **cts sxp default password** コマンドを使用して設定したデフォルトの SXP パスワードを使用します。 **none** パスワードを使用しません。 **required** このコマンドで指定したパスワードを使用します。 vrf キーワードでは、ピアに対する VRF を指定します。 デフォルトはデフォルト VRF です。 mode listener キーワードでは、リモート ピア デバイスのロールを指定します。 Cisco Nexus 5000 シリーズ スイッチは接続でスピーカーとしてのみ機能するため、ピアをリスナーとして設定する必要があります。 （注） SXP には管理（mgmt 0）インターフェイスを使用できません。

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

	コマンドまたはアクション	目的
ステップ 4	**show cts sxp connections** 例： `switch# show cts sxp connections`	（任意） SXP 接続と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`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）
Cisco TrustSec SXP のイネーブル化，（112 ページ）

デフォルトの SXP パスワードの設定

デフォルトでは、SXP は接続のセットアップ時にパスワードを使用しません。 Cisco NX-OS デバイスにデフォルトの SXP パスワードを設定できます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

SXP 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)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp default password** *password* 例： `switch(config)# cts sxp default password A2Q3d4F5`	SXP のデフォルト パスワードを設定します。

	コマンドまたはアクション	目的

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

ステップ 4	**show cts sxp** 例： `switch# show cts sxp`	（任意） SXP の設定を表示します。
ステップ 5	**show running-config cts** 例： `switch# show running-config cts`	（任意） 実行コンフィギュレーションの SXP 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`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）
Cisco TrustSec SXP のイネーブル化，（112 ページ）

デフォルトの SXP 送信元 IPv4 アドレスの設定

Cisco NX-OS ソフトウェアは、送信元 IPv4 アドレスが指定されないと、新規の TCP 接続すべてにデフォルトの送信元 IPv4 アドレスを使用します。 デフォルト SXP 送信元 IPv4 アドレスを設定しても、既存の TCP 接続には影響しません。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

SXP 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)#`
		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	**cts sxp default source-ip** *src-ip-addr* 例： `switch(config)# cts sxp default source-ip 10.10.3.3`	SXP のデフォルトの送信元 IPv4 アドレスを設定します。

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

ステップ 4	**show cts sxp** 例： `switch# show cts sxp`	（任意） SXP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）
Cisco TrustSec SXP のイネーブル化，（112 ページ）

SXP リトライ期間の変更

SXP リトライ期間によって、Cisco NX-OS ソフトウェアが SXP 接続を再試行する頻度が決まります。 SXP 接続が正常に確立されなかった場合、Cisco NX-OS ソフトウェアは SXP リトライ期間タイマーの終了後に、新たな接続の確立を試行します。 デフォルト値は 60 秒（1 分）です。 SXP リトライ期間を 0 秒に設定すると、タイマーがディセーブルになり、再試行は実行されません。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

SXP 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)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp retry-period** *seconds* 例： `switch(config)# cts sxp retry-period 120`	SXP リトライ タイマー期間を変更します。デフォルト値は 60 秒（1 分）です。 範囲は 0 ～ 64000 です。

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

ステップ 4	**show cts sxp** 例： `switch# show cts sxp`	（任意） SXP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

関連トピック

Cisco TrustSec 機能のイネーブル化，（92 ページ）
Cisco TrustSec SXP のイネーブル化，（112 ページ）

Cisco TrustSec の設定の確認

Cisco TrustSec 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 cts	Cisco TrustSec の情報を表示します。
show cts credentials	EAP-FAST の Cisco TrustSec クレデンシャルを表示します。

コマンド	目的
show cts environment-data	Cisco TrustSec の環境データを表示します。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。
show cts role-based access-list	Cisco TrustSec の SGACL 情報を表示します。
show cts role-based counters	RBACL 統計情報の設定ステータスを表示し、すべての RBACL ポリシーの統計情報を一覧表示します。
show cts role-based enable	Cisco TrustSec の SGACL 強制の状態を表示します。
show cts role-based policy	Cisco TrustSec の SGACL ポリシー情報を表示します。
show cts role-based sgt-map	Cisco TrustSec SGACL SGT マップの設定を表示します。
show cts sxp	Cisco TrustSec SXP の情報を表示します。
show running-config cts	実行コンフィギュレーションの Cisco TrustSec 情報を表示します。

Cisco TrustSec の設定例

ここでは、Cisco TrustSec の設定例を示します。

Cisco TrustSec のイネーブル化

Cisco TrustSec をイネーブルにする例を示します。

```
feature cts
cts device-id device1 password Cisco321
```

Cisco NX-OS デバイスへの Cisco TrustSec AAA の設定

次の例では、Cisco NX-OS デバイスに Cisco TrustSec の AAA を設定します。

```
radius-server host 10.10.1.1 key Cisco123 pac
aaa group server radius Rad1
  server 10.10.1.1
  use-vrf management
aaa authentication cts default group Rad1
aaa authorization cts default group Rad1
```

手動での Cisco TrustSec 認証の設定

次の例では、インターフェイスに手動スタティック ポリシーで Cisco TrustSec 認証を設定します。

```
interface ethernet 2/1
  cts manual
    policy static sgt 0x20
    no propagate-sgt
```

次の例では、インターフェイスに手動ダイナミック ポリシーで Cisco TrustSec 認証を設定します。

```
interface ethernet 2/2
  cts manual
    policy dynamic identity device2
```

VLAN に対する Cisco TrustSec ロールベース ポリシー強制の設定

次の例では、VLAN に対して Cisco TrustSec のロールベース ポリシー強制をイネーブルにします。

```
vlan 10
  cts role-based enforcement
```

デフォルト VRF に対する IPv4 アドレスと SGACL SGT のマッピングの設定

次の例では、デフォルト VRF に対して Cisco TrustSec ロールベース ポリシーの IPv4 アドレス対 SGACL SGT マッピングを手動で設定します。

```
cts role-based sgt-map 10.1.1.1 20
```

VLAN に対する IPv4 アドレスと SGACL SGT のマッピングの設定

次の例では、VLAN に対して Cisco TrustSec ロールベース ポリシーの IPv4 アドレス対 SGACL SGT マッピングを手動で設定します。

```
vlan 10
  cts role-based sgt-map 20.1.1.1 20
```

Cisco TrustSec SGACL の手動設定

次に、Cisco TrustSec SGACL を手動で設定する例を示します。

```
cts role-based access-list abcd
  permit icmp
cts role-based sgt 10 dgt 20 access-list abcd
```

次に、RBACL ロギングをイネーブルにする例を示します。

```
cts role-based access-list RBACL1
  deny tcp src eq 1111 dest eq 2222 log
cts role-based sgt 10 dgt 20 access-list RBACL1
```

この設定では、次の ACLLOG syslog が生成されます。

```
%$ VDC-1 %$ %CTS-6-CTS_RBACL_STAT_LOG: CTS ACE permit all log, Threshold exceeded: Hit count
 in 10s period = 4
```

（注） ACLLOG syslog には、一致した RBACL ポリシーの Destination Group Tag（DGT）情報が含まれていません。

次に、RBACL 統計情報をイネーブルおよび表示する例を示します。

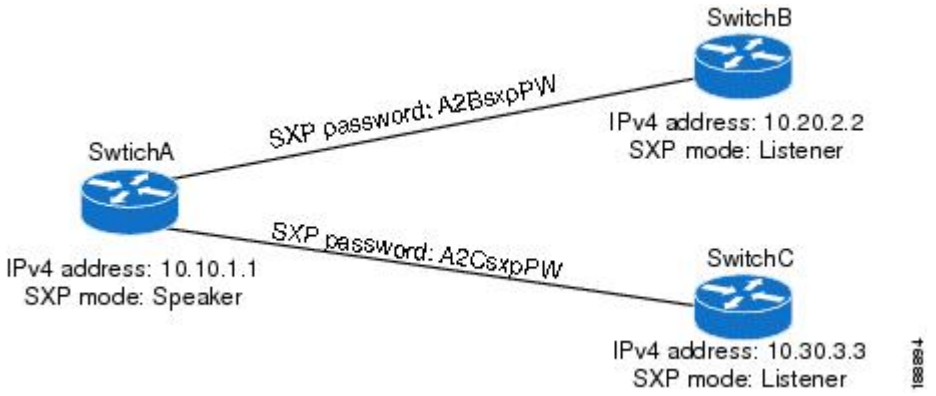
```
cts role-based counters enable
show cts role-based counters

RBACL policy counters enabled
Counters last cleared: 06/08/2009 at 01:32:59 PM
rbacl:abc
        deny tcp dest neq 80                              [0]
        deny tcp dest range 78 79                         [0]
rbacl:def
        deny udp                                          [0]
        deny ip                                           [0]
        deny igmp                                         [0]
```

SXP ピア接続の手動設定

次の図に、デフォルト VRF での SXP ピア接続の例を示します。

（注） Nexus 5000 シリーズ スイッチは SXP のスピーカー モードしかサポートしていないため、この例では SwitchA としてのみ設定できます。

図 *8*： *SXP* ピア接続の例



次に、SwitchA に SXP ピア接続を設定する例を示します。

```
feature cts
cts sxp enable
cts sxp connection peer 10.20.2.2 password required A2BsxpPW mode listener
cts sxp connection peer 10.30.3.3 password required A2CsxpPW mode listener
```

次に、SwitchB に SXP ピア接続を設定する例を示します。

```
feature cts
cts sxp enable
cts sxp connection peer 10.10.1.1 password required A2BsxpPW mode speaker
```

次に、SwitchC に SXP ピア接続を設定する例を示します。

```
feature cts
cts sxp enable
cts sxp connection peer 10.10.1.1 password required A2CsxpPW mode speaker
```

Cisco TrustSec に関する追加情報

ここでは、Cisco TrustSec の実装に関する追加情報について説明します。

関連資料

関連項目	参照先
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』

関連項目	参照先
コマンド リファレンス	『*Cisco Nexus 5000 Series NX-OS TrustSec Command Reference*』

Cisco TrustSec の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *10*：*Cisco TrustSec* の機能の履歴

機能名	リリース	機能情報
Cisco TrustSec	5.1(3)N1(1)	この機能が導入されました。

第 8 章

アクセス コントロール リストの設定

この章の内容は、次のとおりです。

ACL 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 HyperText Transfer Protocol（HTTP; ハイパー テキスト トランスファ プロトコル）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、IPv6、MAC の各 ACL をサポートしています。 スイッチでは、次の表に示すように、ポートの ACL、VLAN ACL、およびルータの ACL として、IP アクセス コントロール リスト（ACL）を使用できます。

表 *11*：セキュリティ *ACL* の適用

アプリケーション	サポートするインターフェイス	サポートする ACL のタイプ
ポート ACL	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 IPv6 ACL MAC ACL
ルータ ACL	• VLAN インターフェイス （注） VLANインターフェイスを設定する前に、VLANインターフェイスをグローバルで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 IPv6 ACL （注） MAC ACL（MAC パケット分類をイネーブルにする場合だけ、レイヤ 3 インターフェイスでサポートされます）。
VLAN ACL（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 MAC ACL

アプリケーション	サポートするインターフェイス	サポートする **ACL** のタイプ
VTY ACL	VTY	IPv4 ACL IPv6 ACL

適用順序

デバイスは、パケットを処理する際に、そのパケットの転送パスを決定します。 デバイスがトラフィックに適用する ACL はパスによって決まります。 デバイスは、次の順序で ACL を適用します。

1. ポート ACL
2. 入力 VACL
3. 入力ルータ ACL
4. 出力ルータ ACL
5. 出力 VACL

ルール

アクセス リスト コンフィギュレーション モードでルールを作成するには、**permit** または **deny** コマンドを使用します。 スイッチは、許可ルールに指定された基準に一致するトラフィックを許可し、拒否ルールに指定された基準に一致するトラフィックをブロックします。 ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。 指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。

プロトコル

IPv4、IPv6、および MAC の ACL では、トラフィックをプロトコルで識別できます。 指定の際の手間を省くために、一部のプロトコルは名前で指定できます。 たとえば、IPv4 ACL では、ICMP を名前で指定できます。

インターネット プロトコル番号を表す整数でプロトコルを指定できます。 たとえば、Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）を指定するには、115 を使用します。

暗黙のルール

IP ACL および MAC ACL には暗黙ルールがあります。暗黙ルールは、実行コンフィギュレーションには設定されていませんが、ACL 内の他のルールと一致しない場合にスイッチがトラフィックに適用するルールです。

すべての IPv4 ACL には、次の暗黙のルールがあります。

```
deny ip any any
```

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

すべての IPv6 ACL には、次の暗黙のルールがあります。

```
deny ipv6 any any
```

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

IPv6 ACL は、次の追加フィルタリング オプションをサポートしています。

- レイヤ 4 プロトコル
- 認証ヘッダー プロトコル
- カプセル化セキュリティ ペイロード
- ペイロード圧縮プロトコル
- ストリーム制御転送プロトコル（SCTP）
- SCTP、TCP、および UDP の各ポート
- ICMP タイプおよびコード
- IGMP タイプ
- フロー ラベル
- DSCP 値

- ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
- 確立済み TCP 接続
- パケット長

MAC ACL は、次の追加フィルタリング オプションをサポートしています。

- レイヤ 3 プロトコル
- VLAN ID
- Class of Service（CoS）

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ています。 入力するすべてのルールにシーケンス番号が割り当てられます（ユーザによる割り当てまたはデバイスによる自動割り当て）。 シーケンス番号によって、次の ACL 設定作業が容易になります。

- 既存のルールの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。

スイッチは、演算子とオペランドの組み合わせを、Logical Operator Unit（LOU; 論理演算ユニット）と呼ばれるレジスタ内に格納します。

「eq」演算子で LOU を使用しても、LOU への格納は行われません。 range 演算子は境界値も含みます。

演算子とオペランドの組み合わせが LOU に格納され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。

統計情報と ACL

このデバイスは IPv4、IPv6、および MAC の ACLに設定した各ルールのグローバル統計を保持できます。 1 つの ACL が複数のインターフェイスに適用される場合、ルール統計には、その ACL が適用されるすべてのインターフェイスと一致する（ヒットする）パケットの合計数が維持されます。

（注） インターフェイスレベルの ACL 統計はサポートされていません。

設定する ACL ごとに、その ACL の統計情報をデバイスが維持するかどうかを指定できます。これにより、ACL によるトラフィック フィルタリングが必要かどうかに応じて ACL 統計のオン、オフを指定できます。また、ACL 設定のトラブルシューティングにも役立ちます。

デバイスには ACL の暗黙ルールの統計情報は維持されません。 たとえば、すべての IPv4 ACL の末尾にある暗黙の **deny ip any any** ルールと一致するパケットのカウントはデバイスに維持されません。 暗黙ルールの統計情報を維持する場合は、暗黙ルールと同じルールを指定した ACL を明示的に設定する必要があります。

ACL のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ACL を使用するためにライセンスは必要ありません。

ACL の前提条件

IP ACL の前提条件は次のとおりです。

- IP ACL を設定するためには、IP アドレッシングおよびプロトコルに関する知識が必要です。
- ACL を設定するインターフェイス タイプについての知識が必要です。

VACL の前提条件は次のとおりです。

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

ACL の注意事項および制約事項

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。 この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。 この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。
- 時間範囲を使用する ACL を適用すると、デバイスはその ACL エントリで参照される時間範囲の開始時または終了時に ACL エントリをアップデートします。 時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。 時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。
- 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。

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。
- DHCP スヌーピング機能がイネーブルのときには、ACL の統計情報はサポートされません。

- M1 シリーズ モジュールでは、**mac packet-classify** コマンドによってポートおよび VLAN ポリシーの MAC ACL がイネーブルになります

VACL の設定に関する注意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。 この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。
- DHCP スヌーピング機能がイネーブルのときには、ACL の統計情報はサポートされません。

デフォルトの ACL 設定

次のテーブルは、IP ACL パラメータのデフォルト設定をリスト表示しています。

表 *12*：*IP ACL* のデフォルト パラメータ

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

次のテーブルは、MAC ACL パラメータのデフォルト設定をリスト表示しています。

表 *13*：*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	デフォルトの 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。

次の表に、VACL パラメータのデフォルト設定を示します。

表 *14*：デフォルトの *VACL* 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 または IPv6 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 モードを開始します。
ステップ 2	switch(config)# {**ip** | **ipv6**} **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 リファレンスを参照してください。
ステップ 4	switch(config-acl)# **statistics**	（任意） 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	switch# **show** {**ip** | **ipv6**} **access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 6	switch# **show ip access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 7	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、IPv4 ACL を作成する例を示します。

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

次に、IPv6 ACL を作成する例を示します。

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

IP ACL の変更

既存の IPv4 ACL または IPv6 ACL のルールの追加および削除を実行できます。 既存のルールは変更できません。 ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

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

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 モードを開始します。
ステップ 2	switch(config)# {**ip** | **ipv6**} **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 デバイスのコマンド リファレンスを参照してください。
ステップ 5	switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}	（任意） 指定したルールを IP ACL から削除します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、Cisco Nexus デバイスのコマンド リファレンスを参照してください。

	コマンドまたはアクション	目的
ステップ 6	switch(config-acl)# [**no**] **statistics**	（任意） 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。 **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	switch#**show ip access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 8	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

IP ACL 内のシーケンス番号の変更，（136 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。

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を開始します。
ステップ 2	switch(config)# no {**ip** | **ipv6**} **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	switch# **show running-config**	（任意） ACL の設定を表示します。 削除された IP ACL は表示されないはずです。

	コマンドまたはアクション	目的
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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** | **ipv6**} **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	switch# **show** {**ip** | **ipv6**} **access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ACL ロギングの設定

特定のプロトコルとアドレスのトラフィックをロギングするためのアクセス コントロール リストを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# {**ip** | **ipv6**} **access-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)# **permit** *protocol source destination* **log**	指定したプロトコルのトラフィックをログに記録するルールを syslog ファイルに作成します。 IP ACL において *protocol* 引数の有効な値は次のとおりです。 • **icmp**：ICMP • **igmp**：IGMP • **ip**：IPv4 • **ipv6**：IPV6 • **tcp**：TCP • **udp**：UDP • **sctp**：SCTP（IPv6 のみ） source 引数および destination 引数は、ネットワークのワイルド カード（IPv4 のみ）での IP アドレス、IP アドレスおよび可変長サブネット マスク、ホスト アドレス、または任意アドレスを指定する **any** に指定するなどがあります。 詳細については、『*Cisco Nexus 5000 Series NX-OS System Management Configuration Guide*』および*Cisco Nexus 5000* シリーズコマンド リファレンスを参照してください。
ステップ 4	switch(config-acl)# **exit**	現在のコンフィギュレーション モードを終了します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次の例では、あらゆる送信元および宛先からの IPv4 TCP トラフィックと一致するエントリを記録するための ACL を作成する例を示します。

```
switch# configuration terminal
switch(config)# ip access-list tcp_log
switch(config-acl)# permit tcp any any log
```

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

mgmt0 への IP-ACL の適用

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

はじめる前に

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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 または IPv6 ACL を、指定方向のトラフィックのレイヤ 3 インターフェイスに適用します。 各方向にルータ ACL を 1 つ適用できます。
ステップ 4	**show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	（任意） ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連資料

- IP ACL の作成

ルータ ACL としての IP ACL の適用

IPv4 ACL または IPv6 ACL は、次のタイプのインターフェイスに適用できます。

- 物理レイヤ 3 インターフェイスおよびサブインターフェイス
- 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。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
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	次のいずれかのコマンドを入力します。 • switch(config-if)# **ip access-group** *access-list* {**in** | **out**} • switch(config-if)# **ipv6 traffic-filter** *access-list* {**in** | **out**}	IPv4 ACL または IPv6 ACL を、指定方向のトラフィックのレイヤ 3 インターフェイスに適用します。各方向にルータ ACL を 1 つ適用できます。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **show running-config aclmgr**	（任意） ACL の設定を表示します。
ステップ 5	switch(config-if)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL のポート ACL としての適用

IPv4 または IPv6 の ACL は、物理イーサネット インターフェイスまたはポートチャネルに適用できます。 これらのインターフェイス タイプに適用された ACL は、ポート ACL と見なされます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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*}	特定の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)# {**ip port access-group** | **ipv6 port traffic-filter**} *access-list* **in**	IPv4 または IPv6 ACL をインターフェイスまたはポートチャネルに適用します。 ポート ACL では、インバウンド フィルタリングだけがサポートされています。 1 つのインターフェイスに 1 つのポート ACL を適用できます。
ステップ 4	switch# **show running-config**	（任意） ACL の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

- 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。

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 デバイスのコマンド リファレンスを参照してください。

IP ACL の統計情報のモニタリングとクリア

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

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

- switch# **show** {**ip** | **ipv6**} **access-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** コマンドと **show ipv6 access-list** コマンドの出力に、各ルールに一致したパケットの数が表示されます。
- switch#**show ip access-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** {**ip** | **ipv6**} **access-list counters** [*access-list-name*]
  すべての IP ACL、または特定の IP ACL の統計情報を消去します。
- switch# **clear ip access-list counters** [*access-list-name*]
  すべての IP ACL、または特定の IP ACL の統計情報を消去します。

MAC ACL の設定

MAC ACL の作成

MAC ACL を作成し、その MAC ACL にルールを追加する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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# **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)# [*sequence-number*] {**permit** | **deny**} *source destination protocol*	MAC ACL 内にルールを作成します。 **permit** オプションと **deny** オプションには、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。 詳細は、Cisco Nexus 5000 シリーズのコマンド リファレンスを参照してください。
ステップ 4	switch(config-mac-acl)# **statistics**	（任意） 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	switch# **show mac access-lists** *name*	（任意） MAC ACL の設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、MAC ACL を作成して、ルールを追加する例を示します。

```
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
```

MAC ACL の変更

既存の MAC ACL 内で、ルールの追加または削除を実行できます。 既存のルールは変更できません。 ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

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

MAC ACL を変更する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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	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	switch(config-mac-acl)# **no** {*sequence-number* | {**permit**|**deny**} *source destination protocol*}	（任意） 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	switch(config-mac-acl)# [**no**] **statistics**	（任意） 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。 **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 6	switch# **show mac access-lists** *name*	（任意） MAC ACL の設定を表示します。
ステップ 7	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、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 mac 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# statistics
```

MAC ACL の削除

スイッチから MAC ACL を削除できます。

ACLがインターフェイスに適用されているかどうかを確認してください。削除できるのは、現在適用されている ACL だけです。 ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。 スイッチは、削除対象の ACL が空であると見なします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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	switch# **show mac access-lists**	（任意） MAC ACL の設定を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

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する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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。

	コマンドまたはアクション	目的
ステップ 3	switch# **show mac access-lists** *name*	（任意） MAC ACL の設定を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ルール，（127 ページ）

MAC ACL のポート ACL としての適用

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。

- イーサネット インターフェイス
- EtherChannel インターフェイス

適用する ACL が存在しており、この適用で要求されているとおりに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。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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*}	特定のイーサネット 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	switch# **show running-config**	（任意） ACL の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

IP ACL の作成, （133 ページ）

MAC ACL の設定の確認

MAC ACL 設定情報を表示するには、次のいずれかの作業を実行します。

- switch# **show mac access-lists**
  MAC ACL の設定を表示します。
- switch# **show running-config**
  ACL の設定（MAC ACL と MAC 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 を適用したインターフェイスの設定を表示します。

MAC ACL 統計情報の表示と消去

MAC 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 mac access-lists** コマンドを使用します。

- switch# **show mac access-lists**
  MAC ACL の設定を表示します。 MAC ACL に **statistics** コマンドが指定されている場合は、**show mac 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 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。

MAC ACL の設定例

次に、acl-mac-01 という名前の MAC ACL を作成して、Ethernet インターフェイス 1/1 に適用する例を示します。

```
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)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# mac access-group acl-mac-01
```

VLAN ACL の概要

VLAN ACL（VACL）は、MAC ACL または IP ACL の適用例の 1 つです。 VACL を設定して、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 または MAC ACL をアクションとリンクさせます。 スイッチは、VACL によって許可されたパケットに設定されているアクションを実行します。

VACL とアクション

アクセスマップ コンフィギュレーション モードでは、**action** コマンドを使用して、次のいずれかのアクションを指定します。

- フォワード：スイッチの通常の動作によって決定された宛先にトラフィックを送信します。
- ドロップ：トラフィックをドロップします。

統計情報

Cisco Nexus デバイスは、VACL 内の各ルールについて、グローバルな統計情報を保持できます。VACL を複数の VLAN に適用した場合、保持されるルール統計情報は、その VACL が適用されている各インターフェイス上で一致（ヒット）したパケットの総数になります。

（注） Cisco Nexus デバイスは、インターフェイス単位の VACL 統計情報はサポートしていません。

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

VACL の設定

VACL の作成または変更

VACL を作成または変更できます。 VACL の作成には、IP ACL または MAC 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。

VACL を作成または変更する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **vlan access-map** *map-name*	指定したアクセス マップのアクセス マップ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-access-map)# **match ip address** *ip-access-list*	マップの IPv4 および IPV6 ACL を指定します。
ステップ 4	switch(config-access-map)# **match mac address** *mac-access-list*	マップの MAC ACL を指定します。
ステップ 5	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 6	switch(config-access-map)# [**no**] **statistics**	（任意） VACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。 **no** オプションを指定すると、VACL のグローバルな統計情報がスイッチ内に保持されなくなります。
ステップ 7	switch(config-access-map)# **show running-config**	（任意） ACL の設定を表示します。

	コマンドまたはアクション	目的
ステップ 8	switch(config-access-map)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL の削除

VACL を削除できます。これにより、VLAN アクセス マップも削除されます。

VACL が VLAN に適用されているかどうかを確認してください。 削除できるのは、現在適用されている VACL だけです。 VACL を削除しても、その VACL が適用されていた VLAN の設定は影響を受けません。 スイッチは、削除対象の VACL が空であると見なします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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	switch(config)# **show running-config**	（任意） ACL の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL の VLAN への適用

VACL を VLAN に適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コ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** 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** コマンドを設定すれば 32 個を超える VLAN を指定できます。
ステップ 3	switch(config)# **show running-config**	（任意） ACL の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL の設定の確認

VACL 設定情報を表示するには、次のいずれかの作業を実行します。

- switch# **show running-config aclmgr**
  VACL 関連の設定を含む、ACL の設定を表示します。
- switch# **show vlan filter**
  VLAN に適用されている VACL の情報を表示します。
- switch# **show vlan access-map**
  VLAN アクセス マップに関する情報を表示します。

VACL 統計情報の表示と消去

VACL 統計情報を表示または消去するには、次のいずれかの作業を実行します。

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

VACL の設定例

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

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

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で IPv4 または IPv6 の着信接続と発信接続を制限するには、ライン コンフィギュレーション モードで **access-class** コマンドを使用します。アクセス制限を解除するには、このコマンドの **no** 形式を使用します。

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

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

はじめる前に

適用する ACL が存在しており、この適用に対してトラフィックをフィルタリングするように設定されていることを確認してください。

手順

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

ステップ 2	switch(config)# **line vty**
	
	例：
	`switch(config)# line vty`
	`switch(config-line)#`
		ライン コンフィギュレーション モードを開始します。

ステップ 3	switch(config-line)# **access-class access-list-number {in | out}**
	
	例：
	`switch(config-line)# access-class ozi2 in`
	`switch(config-line)#access-class ozi3`
		着信または発信アクセス制限を指定します。

	コマンドまたはアクション	目的
	out switch(config)#	
ステップ 4	switch(config-line)# **no access-class access-list-number {in | out}** 例： switch(config-line)# no access-class ozi2 in switch(config-line)# no access-class ozi3 out switch(config)#	（任意） 着信または発信アクセス制限を削除します。
ステップ 5	switch(config-line)# **exit** 例： switch(config-line)# exit switch#	ライン コンフィギュレーション モードを終了します。
ステップ 6	switch# **show running-config aclmgr** 例： switch# show running-config aclmgr	（任意） スイッチの ACL の実行コンフィギュレーションを表示します。
ステップ 7	switch# **copy running-config startup-config** 例： switch# copy running-config startup-config	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

VTY 回線の ACL の確認

VTY 回線の ACL 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
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。

- ipv6 access-list ozi7 コマンドを VTY 回線の in 方向に適用すると、すべての IPv6 ホストへの VTY 接続が拒否されます。
- ipv6 access-list ozip6 コマンドを VTY 回線の out 方向に適用すると、すべての IPv6 ホストへの VTY 接続が許可されます。

```
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
ipv6 access-list ozi7
  10 deny tcp any any
ipv6 access-list ozip6
  10 permit tcp any any

line vty
  access-class ozi in
  access-class ozi2 out
  ipv6 access-class ozi7 in
  ipv6 access-class ozip6 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# conf t
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# conf t
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

ポート セキュリティの設定

この章は、次の内容で構成されています。

ポート セキュリティの概要

ポート セキュリティを使用すると、レイヤ 2 物理インターフェイス、レイヤ 2 ポート チャネル インターフェイス、および仮想ポートチャネル（vPC）を、MACアドレスの限定されたセットからのインバウンド トラフィックだけを許可するように設定できます。 この限定セットの MAC アドレスをセキュア MAC アドレスといいます。 さらに、デバイスは、同じ VLAN 内の別のインターフェイスでは、これらのMACアドレスからのトラフィックを許可しません。 セキュア MAC アドレスの数は、インターフェイス単位で設定します。

（注） 特に指定されていない限り、インターフェイスという用語は物理インターフェイス、ポート チャネル インターフェイス、および vPC を示します。同様に、レイヤ *2* インターフェイスという用語は、レイヤ 2 物理インターフェイスとレイヤ 2 ポート チャネル インターフェイスの両方を示します。

セキュア MAC アドレスの学習

MACアドレスは学習というプロセスによってセキュア アドレスになります。 MACアドレスは、1つのインターフェイスだけでセキュアMACアドレスになることができます。デバイスは、ポート セキュリティがイネーブルに設定されたインターフェイスごとに、スタティック、ダイナミック、またはスティッキの方式で、限られた数のMACアドレスを学習できます。デバイスがセキュアMACアドレスを格納する方法は、デバイスがセキュアMACアドレスを学習した方法によって異なります。

（注） 学習された MAC アドレスはすべて、vPC ピア間で同期されます。

スタティック方式

スタティック学習方式では、ユーザが手動でインターフェイスの実行コンフィギュレーションにセキュアMACアドレスを追加したり、設定から削除したりできます。 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーすると、デバイスを再起動してもスタティック セキュア MAC アドレスには影響がありません。

スタティック セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- ユーザが明示的に設定からアドレスを削除した場合。
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合。

スタティック方式では、ダイナミック方式またはスティッキ方式のアドレス学習がイネーブルになっているかどうかに関係なく、セキュア アドレスを追加できます。

ダイナミック方式

デフォルトでは、インターフェイスのポート セキュリティをイネーブルにすると、ダイナミック学習方式がイネーブルになります。 この方式では、デバイスは、入力トラフィックがインターフェイスを通過するときに MAC アドレスをセキュア アドレスにします。 このようなアドレスがまだセキュア アドレスではなく、デバイスのアドレス数が適用可能な最大数に達していなければ、デバイスはそのアドレスをセキュア アドレスにして、トラフィックを許可します。

デバイスは、ダイナミック セキュア MAC アドレスをメモリに保存します。 ダイナミック セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- デバイスが再起動した場合。
- インターフェイスが再起動した場合。
- アドレスが、ユーザによって設定されたインターフェイスのエージング期限に達した場合。
- ユーザがアドレスを明示的に削除した場合。
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合。

スティッキ方式

スティッキ方式をイネーブルにすると、デバイスは、ダイナミック アドレス学習と同じ方法で MAC アドレスをセキュア アドレスにしますが、この方法で学習されたアドレスは NVRAM に保存されます。 そのため、スティッキ方式で学習されたアドレスは、デバイスの再起動後も維持されます。 スティッキ セキュア MAC アドレスは、インターフェイスの実行コンフィギュレーション内にはありません。

ダイナミックとスティッキのアドレス学習は両方同時にイネーブルにできません。 あるインターフェイスのスティッキ学習をイネーブルにした場合、デバイスはダイナミック学習を停止して、代わりにスティッキ学習を実行します。 スティッキ学習をディセーブルにすると、デバイスはダイナミック学習を再開します。

スティッキ セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- ユーザがアドレスを明示的に削除した場合。
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合。

ダイナミック アドレスのエージング

デバイスは、ダイナミック方式で学習された MAC アドレスのエージングを行い、エージングの期限に達すると、アドレスをドロップします。 エージングの期限は、インターフェイスごとに設定できます。 有効な範囲は 0 ～ 1440 分です。0 を設定すると、エージングはディセーブルになります。

vPC ドメインでは、ダイナミック MAC アドレスは、両方の vPC ピアでエージング期限に達した後にのみドロップされます。

MAC アドレスのエージングを判断するためにデバイスが使用する方法も設定できます。 アドレス エージングの判断には、次に示す 2 つの方法が使用されます。

非アクティブ

適用可能なインターフェイス上のアドレスからデバイスが最後にパケットを受信して以降の経過時間。

絶対

デバイスがアドレスを学習して以降の経過時間。 これがデフォルトのエージング方法ですが、デフォルトのエージング時間は 0 分（エージングはディセーブル）です。

セキュア MAC アドレスの最大数

デフォルトでは、各インターフェイスのセキュアMACアドレスは1つだけです。 各インターフェイス、またはインターフェイス上の各VLANに許容可能な最大MACアドレス数を設定できます。最大数は、ダイナミック、スティッキ、スタティックのいずれの方式で学習された MAC アドレスにも適用されます。

（注） vPC ドメインでは、プライマリ vPC の設定が有効になります。

ヒント アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、そのデバイスにはポートの全帯域幅が保証されます。

各インターフェイスに許容されるセキュア MAC アドレスの数は、次の 3 つの制限によって決定されます。

最大デバイス数

デバイスが許容できるセキュア MAC アドレスの最大数は 8192 です。この値は変更できません。 新しいアドレスを学習するとデバイスの最大数を超過してしまう場合、たとえインターフェイスや VLAN の最大数に達していなくても、デバイスは新しいアドレスの学習を許可しません。

最大インターフェイス数

ポート セキュリティで保護されるインターフェイスごとに、1025 のセキュア MAC アドレスの最大数を設定できます。 デフォルトでは、インターフェイスの最大アドレス数は 1 です。 インターフェイスの最大数を、デバイスの最大数より大きくすることはできません。

vPC ドメインでは、プライマリ vPC スイッチのセキュア MAC アドレスの最大数を設定します。 最大数のセキュア MAC アドレスがセカンダリ スイッチに設定されている場合でも、プライマリ vPC スイッチではカウントを確認します。

最大 VLAN 数

ポート セキュリティで保護される各インターフェイスについて、VLAN あたりのセキュア MAC アドレスの最大数を設定できます。 VLAN の最大数は、インターフェイスに設定されている最大数より大きくできません。 VLAN 最大数の設定が適しているのは、トランク ポートの場合だけです。 VLAN の最大数には、デフォルト値はありません。

インターフェイスあたりの、VLAN とインターフェイスの最大数は必要に応じて設定できます。ただし、新しい制限値が、適用可能なセキュア アドレス数よりも少ない場合は、まず、セキュア MAC アドレスの数を減らす必要があります。

セキュリティ違反と処理

次の 2 つのイベントのいずれかが発生すると、ポート セキュリティ機能によってセキュリティ違反がトリガーされます。

MAX カウント違反

あるインターフェイスにセキュア MAC アドレス以外のアドレスから入力トラフィックが着信し、そのアドレスを学習するとセキュア MAC アドレスの適用可能な最大数を超えてしまう場合。 ブロックされたエントリは、Cisco Nexus 5000 シリーズ スイッチ上の Forwarding Module（FWM）に追加されます。

あるインターフェイスに VLAN とインターフェイスの両方の最大数が設定されている場合は、どちらかの最大数を超えると、違反が発生します。 たとえば、ポート セキュリティが設定されている単一のインターフェイスについて、次のように想定します。

- VLAN 1 の最大アドレス数は 5 です。
- このインターフェイスの最大アドレス数は 10 です。

デバイスは、次のいずれかが発生すると違反を検出します。

- VLAN 1 のアドレスをすでに 5 つ学習していて、6 つめのアドレスからのインバウンド トラフィックが VLAN 1 のインターフェイスに着信した場合。
- このインターフェイス上のアドレスをすでに 10 個学習していて、11 番めのアドレスからのインバウンド トラフィックがこのインターフェイスに着信した場合。

MAC 移動違反

あるインターフェイスのセキュア MAC アドレスになっているアドレスからの入力トラフィックが、そのインターフェイスと同じ VLAN 内の別のインターフェイスに着信した場合。 ブロックされたエントリが、ドロップ エントリとしてポート セキュリティ テーブルに追加されます。

セキュリティ違反が発生すると、デバイスは、インターフェイスのセキュリティ違反カウンタの値を増加させ、インターフェイスのポート セキュリティ設定に指定されている処理を実行します。 セキュア MAC アドレスからの入力トラフィックが、そのアドレスをセキュア アドレスにし

たインターフェイスとは異なるインターフェイスに着信したことにより違反が発生した場合、デバイスはトラフィックを受信したインターフェイスに対して処理を実行します。

デバイスが実行できる処理は次のとおりです。

シャットダウン

違反をトリガーしたパケットの受信インターフェイスをシャットダウンします。 このインターフェイスはエラー ディセーブル状態になります。 これがデフォルトの処理です。 インターフェイスの再起動後も、セキュアMACアドレスを含めて、ポートセキュリティの設定は維持されます。

シャットダウン後にデバイスが自動的にインターフェイスを再起動するように設定するには、**errdisable** グローバル コンフィギュレーション コマンドを使用します。あるいは、**shutdown** および **no shut down** のインターフェイス コンフィギュレーション コマンドを入力することにより、手動でインターフェイスを再起動することもできます。

Cisco Nexus 5010 および 5020 スイッチでは、MAC アドレスはセキュアでないポートに移動せず、セキュアでないポートのフレームは転送されます。 Cisco Nexus 5500 スイッチでは、MAC アドレスはセキュアでないポートに移動せず、セキュアでないポートのフレームはドロップされます。

制限

セキュアでない MAC アドレスからの入力トラフィックをドロップします。そして、この MAC アドレスを、ブロックされた MAC エントリとしてポート セキュリティ テーブルに追加します。

（注） vPC ドメインでは、制限モードで違反が発生したためにポート セキュリティ テーブルに追加されたブロックされた MAC アドレスは、vPC ピア間で同期されません。

デバイスはドロップされたパケットの数を保持します。これはセキュリティ違反カウントと呼ばれます。 アドレス ラーニングはインターフェイス上で最大回数のセキュリティ違反が発生するまで続行されます。 最初のセキュリティ違反のあとに学習されたアドレスからのトラフィックはドロップされます。

MAX カウント違反の最大数（10）に到達した後、インターフェイスはシャット ダウンされ、Cisco Nexus 5010 スイッチおよび 5020 スイッチで **errdisabled** 状態に置かれ、Cisco Nexus 5500 スイッチの保護モードに移動されます。

保護

これ以上の違反の発生を防止します。 セキュリティ違反をトリガーしたアドレスは学習されますが、そのアドレスからのトラフィックはドロップされます。 それ以降、アドレス学習は実行されなくなります。

（注） 保護のアクションは、Cisco Nexus 5500 スイッチでのみサポートされています。

（注） vPC では、プライマリ vPC スイッチに設定された違反アクションが有効になります。 そのため、セキュリティ違反がトリガーされた場合は常に、プライマリ vPC スイッチ上で定義されているセキュリティの処理が実行されます。

MAX移動違反の最大数（10）に到達した後、インターフェイスはシャットダウンされ、**errdisable** 状態に置かれます。

ポート タイプの変更

レイヤ2インターフェイスにポート セキュリティを設定し、そのインターフェイスのポート タイプを変更した場合、デバイスは次のように動作します。

アクセス ポートからトランク ポート

レイヤ 2 インターフェイスをアクセス ポートからトランク ポートに変更すると、デバイスはダイナミック方式で学習されたすべてのセキュア アドレスをドロップします。 デバイスは、スタティック方式またはスティッキ方式で学習したアドレスをネイティブ トランク VLAN に移行します。

トランク ポートからアクセス ポート

レイヤ 2 インターフェイスをトランク ポートからアクセス ポートに変更すると、デバイスはダイナミック方式で学習されたすべてのセキュア アドレスをドロップします。 ネイティブ トランク VLAN でスティッキ方式で学習されたアドレスはすべて、アクセス VLAN に移行されます。 ネイティブ トランク VLAN でない場合、スティッキ方式で学習されたセキュア アドレスはドロップされます。

スイッチド ポートからルーテッド ポート

インターフェイスをレイヤ 2 インターフェイスからレイヤ 3 インターフェイスに変更すると、デバイスはそのインターフェイスのポート セキュリティをディセーブルにし、そのインターフェイスのすべてのポート セキュリティ設定を廃棄します。 デバイスは、学習方式に関係なく、そのインターフェイスのセキュア MAC アドレスもすべて廃棄します。

ルーテッド ポートからスイッチド ポート

インターフェイスをレイヤ 3 インターフェイスからレイヤ 2 インターフェイスに変更すると、デバイス上のそのインターフェイスのポート セキュリティ設定はなくなります。

ポート セキュリティのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ポートセキュリティにはライセンスは必要ありません。 ライセンス パッケージに含まれていない機能は、Cisco NX-OS デバイス イメージにバンドルされており、追加料金なしで利用できます。 Cisco NX-OS ライセンス方式についての詳細は、『*License and Copyright Information for Cisco NX-OS Software*』次の URL で入手可能です。 http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html を参照してください。

ポート セキュリティの前提条件

ポート セキュリティの前提条件は次のとおりです。

- ポート セキュリティで保護するデバイスのポート セキュリティをグローバルにイネーブル化すること。
- vPC ドメインでは、両方の vPC ピアと、vPC ピアの両方の vPC インターフェイスで、ポート セキュリティをグローバルでイネーブルにする必要があります。 **config sync** コマンドを使用して、両方の vPC ピア間で設定に矛盾がないことを確認してください。

ポート セキュリティの注意事項と制約事項

ポート セキュリティを設定する場合は、次の注意事項に従ってください。

- ポート セキュリティは、PVLAN ポート上でサポートされます。
- ポート セキュリティは、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先ポートをサポートしません。
- ポート セキュリティは他の機能に依存しません。

- ポート セキュリティは、vPC ピア リンク上ではサポートされません。
- ポート セキュリティは、ネットワーク インターフェイス（NIF）ポート、Flex Link ポート、または vEthernet インターフェイス上ではサポートされません。

vPC 上のポート セキュリティの注意事項と制約事項

ポート セキュリティに関する注意事項と制約事項に加えて、vPC 上のポート セキュリティに関する追加の注意事項と制約事項があります。 vPC 上のポート セキュリティを設定する場合は、次の注意事項に従ってください。

- vPC ドメイン内の両方の vPC ピアで、ポート セキュリティをグローバルにイネーブルにする必要があります。
- 両方の vPC ピアの vPC インターフェイス上でポート セキュリティをイネーブルにする必要があります。
- プライマリ vPC ピアでスタティック セキュア MAC アドレスを設定する必要があります。 この MAC アドレスは、セカンダリ vPC ピアと同期されます。 セカンダリ ピアでスタティック セキュア MAC アドレスを設定しないでください。 この MAC アドレスはセカンダリ vPC 設定に表示されますが、有効にはなりません。
- 学習された MAC アドレスはすべて、vPC ピア間で同期されます。
- 両方の vPC ピアは、ダイナミックまたはスティッキ MAC アドレスの学習方式で設定できます。 ただし、両方の vPC ピアが同じ方式に設定されていることを推奨します。
- ダイナミック MAC アドレスは、両方の vPC ピアでエージング期限に達した後にのみドロップされます。
- セキュア MAC アドレスの最大数は、プライマリ vPC スイッチ上で設定します。 最大数のセキュア MAC アドレスがセカンダリ スイッチに設定されている場合でも、プライマリ vPC スイッチではカウントを確認します。
- 違反時の処理は、プライマリ vPC 上で設定します。 そのため、セキュリティ違反がトリガーされた場合は常に、プライマリ vPC スイッチ上で定義されているセキュリティの処理が実行されます。
- ポート セキュリティ機能が両方の vPC ピアでイネーブルになっており、かつポート セキュリティが vPC ピアの両方の vPC インターフェイス上でイネーブルになっている場合に、ポート セキュリティは vPC インターフェイス上でイネーブルになります。 設定が正しいことを確認するには、**config sync** コマンドを使用できます。
- スイッチでインサービス ソフトウェア アップグレード（ISSU）が実行されている間、ポート セキュリティの動作はそのピア スイッチ上で停止されます。 ピア スイッチはどの新しい MAC アドレスも学習せず、この動作中に発生した MAC の移動は無視されます。 ISSU が完了すると、ピア スイッチに通知され、通常のポート セキュリティ機能が再開します。
- 上位バージョンへの ISSU がサポートされていますが、下位バージョンへの ISSU はサポートされていません。

ポート セキュリティの設定

ポートセキュリティのグローバルなイネーブル化またはディセーブル化

デバイスに対してポート セキュリティ機能のグローバルなイネーブル化またはディセーブル化が可能です。 デフォルトで、ポート セキュリティはグローバルにディセーブルになっています。

ポート セキュリティをグローバルにディセーブルにすると、すべてのセキュア MAC アドレスを含むすべてのポート セキュリティ設定が失われます。

（注） vPC ドメインのポートセキュリティをイネーブル、またはディセーブルにするには、vPC ピアの両方でポート セキュリティをグローバルにイネーブル化またはディセ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	[**no**] **feature port-security** 例： `switch(config)# feature port-security`	ポートセキュリティをグローバルにイネーブル化します。 **no** オプションを使用するとポートセキュリティはグローバルにディセーブル化されます。
ステップ 3	**show port-security** 例： `switch(config)# show port-security`	ポートセキュリティのステータスを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 5	vPC ドメインのポート セキュリティが設定されている場合、ポートセキュリティをグローバルでイネーブルにするには、	—

	コマンドまたはアクション	目的
	vPC ピアでステップ 1 ～ 4 を繰り返します。 例：	

レイヤ2インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化

レイヤ 2 インターフェイスに対してポート セキュリティ機能のイネーブル化またはディセーブル化が可能です。デフォルトでは、ポートセキュリティはすべてのインターフェイスでディセーブルです。

インターフェイスのポート セキュリティをディセーブルにすると、そのインターフェイスのすべてのスイッチポートのポート セキュリティ設定が失われます。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

vPC ドメインにポート セキュリティを設定する場合、両方の vPC ピアでポート セキュリティをグローバルにイネーブル化しておく必要があります。

レイヤ 2 イーサネット インターフェイスがポート チャネル インターフェイスのメンバである場合、レイヤ 2 イーサネット インターフェイスに対するポート セキュリティはイネーブルまたはディセーブルにできません。

セキュア レイヤ 2 ポート チャネル インターフェイスのメンバのいずれかのポート セキュリティがイネーブルになっている場合、先にポートチャネルインターフェイスからセキュア メンバ ポートをすべて削除しない限り、そのポートチャネルインターフェイスのポートセキュリティをディセーブルにできません。

手順

	コマンドまたはアクション	目的

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

ステップ 2	次のいずれかのコマンドを入力します。 • **interface ethernet** *slot*/*port*	ポート セキュリティを設定するイーサネット インターフェイスまたはポート チャネル インターフェイスのインター

	コマンドまたはアクション	目的

	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		フェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport** 例： `switch(config-if)# switchport`	そのインターフェイスを、レイヤ 2 インターフェイスとして設定します。
ステップ 4	[**no**] **switchport port-security** 例： `switch(config-if)# switchport port-security`	インターフェイス上でポート セキュリティをイネーブルにします。 **no** オプションを使用すると、そのインターフェイスのポートセキュリティがディセーブルになります。
ステップ 5	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 7	vPC ドメインのポートセキュリティを設定している場合、vPC インターフェイスのポート セキュリティをイネーブルにするには vPC ピアへの手順 1 ～ 6 を繰り返します。	—

スティッキ MAC アドレス ラーニングのイネーブル化またはディセーブル化

インターフェイスのスティッキ MAC アドレス ラーニングをディセーブルまたはイネーブルに設定できます。 スティッキ学習をディセーブルにすると、そのインターフェイスはダイナミック MAC アドレス ラーニング（デフォルトの学習方式）に戻ります。

デフォルトでは、スティッキ MAC アドレス ラーニングはディセーブルです。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		スティッキ MAC アドレス ラーニングを設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport** 例： `switch(config-if)# switchport`	そのインターフェイスを、レイヤ 2 インターフェイスとして設定します。
ステップ 4	[**no**] **switchport port-security mac-address sticky** 例： `switch(config-if)# switchport port-security mac-address sticky`	そのインターフェイスのスティッキ MAC アドレス ラーニングをイネーブルにします。 **no** オプションを使用するとスティッキ MAC アドレス ラーニングがディセーブルになります。
ステップ 5	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポートセキュリティの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスのスタティック セキュア MAC アドレスの追加

レイヤ 2 インターフェイスにスタティック セキュア MAC アドレスを追加できます。

（注） MAC アドレスが任意のインターフェイスでセキュア MAC アドレスである場合、その MAC アドレスがすでにセキュア MAC アドレスとなっているインターフェイスからその MAC アドレスを削除するまで、その MAC アドレスをスタティック セキュア MAC アドレスとして別のインターフェイスに追加することはできません。

デフォルトでは、インターフェイスにスタティック セキュア MAC アドレスは設定されません。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

インターフェイスのセキュア MAC アドレス最大数に達していないことを確認します。 必要に応じて、セキュア MAC アドレスを削除するか、インターフェイスの最大アドレス数を変更できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **switchport port-security mac-address** *address* [**vlan** *vlan-ID*] 例： `switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE`	現在のインターフェイスのポート セキュリティにスタティック MAC アドレスを設定します。 そのアドレスからのトラフィックを許可する VLAN を指定する場合は、**vlan** キーワードを使用します。

	コマンドまたはアクション	目的
ステップ 4	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスのスタティック セキュア MAC アドレスの削除

レイヤ 2 インターフェイスのスタティック セキュア MAC アドレスを削除できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		スタティック セキュア MAC アドレスを削除するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport port-security mac-address** *address* 例： `switch(config-if)# no switchport port-security mac-address 0019.D2D0.00AE`	現在のインターフェイスのポート セキュリティからスタティック セキュア MAC アドレスを削除します。

	コマンドまたはアクション	目的
ステップ 4	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ダイナミック セキュア MAC アドレスの削除

ダイナミックに学習されたセキュア MAC アドレスを削除できます。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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	**clear port-security dynamic** {**interface ethernet** *slot*/*port* | **address** *address*} [**vlan** *vlan-ID*] 例： `switch(config)# clear port-security dynamic interface ethernet 2/1`	ダイナミックに学習されたセキュア MAC アドレスを削除します。次の方法で指定できます。 **interface** キーワードを使用すると、指定したインターフェイスでダイナミックに学習されたアドレスがすべて削除されます。 **address** キーワードを使用すると、指定した単一のダイナミック学習アドレスが削除されます。 特定の VLAN のアドレスを削除するようにコマンドに制限を加えるには、**vlan** キーワードを使用します。

	コマンドまたはアクション	目的
ステップ 3	**show port-security address** 例： `switch(config)# show port-security address`	セキュア MAC アドレスを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC アドレスの最大数の設定

レイヤ 2 インターフェイスで学習可能な MAC アドレスまたはスタティックに設定可能な MAC アドレスの最大数を設定できます。 レイヤ 2 インターフェイス上の VLAN 単位でも MAC アドレスの最大数を設定できます。 インターフェイスに設定できる最大アドレス数は 1025 です。 システムの最大アドレス数は 8192 です。

デフォルトでは、各インターフェイスのセキュア MAC アドレスの最大数は 1 です。 VLAN には、セキュア MAC アドレス数のデフォルトの最大値はありません。

（注） インターフェイスですでに学習されているアドレス数またはインターフェイスにスタティックに設定されたアドレス数よりも小さい数を最大数に指定すると、デバイスはこのコマンドを拒否します。 ダイナミック方式で学習されたアドレスをすべて削除するには、**shutdown** および **no shutdown** のコマンドを使用して、インターフェイスを再起動します。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	例：
	`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。*slot* は、MACアドレスの最大数を設定するインターフェイスです。

ステップ 3	[**no**] **switchport port-security maximum** *number* [**vlan** *vlan-ID*] 例： `switch(config-if)# switchport port-security maximum 425`	現在のインターフェイスで学習可能な MAC アドレスまたはスタティックに設定可能な MACアドレスの最大数を設定します。*number* の最大値は 1025 です。 **no** オプションを使用すると、MAC アドレスの最大数がデフォルト値（1）にリセットされます。 最大数を適用する VLAN を指定する場合は、**vlan** キーワードを使用します。
ステップ 4	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

アドレス エージングのタイプと期間の設定

MAC アドレス エージングのタイプと期間を設定できます。デバイスは、ダイナミック方式で学習された MAC アドレスがエージング期限に到達する時期を判断するためにこれらの設定を使用します。

デフォルトのエージング タイプは絶対エージングです。

デフォルトのエージング タイムは 0 分（エージングはディセーブル）です。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		MAC エージングのタイプと期間を設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**[no] switchport port-security aging type** {**absolute** | **inactivity**} 例： `switch(config-if)# switchport port-security aging type inactivity`	ダイナミックに学習された MAC アドレスにデバイスが適用するエージング タイプを設定します。 **no** オプションを使用すると、エージング タイプがデフォルト値（絶対エージング）にリセットされます。
ステップ 4	**[no] switchport port-security aging time** *minutes* 例： `switch(config-if)# switchport port-security aging time 120`	ダイナミックに学習された MAC アドレスがドロップされるまでのエージング タイムを分単位で設定します。 *minutes* の最大値は 1440 です。 **no** オプションを使用すると、エージング タイムがデフォルト値である 0（エージングはディセーブル）にリセットされます。
ステップ 5	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

セキュリティ違反時の処理の設定

セキュリティ違反が発生した場合にデバイスが実行する処理を設定できます。 違反時の処理は、ポート セキュリティをイネーブルにしたインターフェイスごとに設定できます。

デフォルトのセキュリティ処理では、セキュリティ違反が発生したポートがシャットダウンされます。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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** *slot*/*port*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		セキュリティ違反時の処理を設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **switchport port-security violation** {**protect** | **restrict** | **shutdown**} 例： `switch(config-if)# switchport port-security violation restrict`	現在のインターフェイスのポート セキュリティにセキュリティ違反時の処理を設定します。 **no** オプションを使用すると、違反時の処理がデフォルト値（インターフェイスのシャットダウン）にリセットされます。
ステップ 4	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポートセキュリティの設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ポート セキュリティの設定の確認

ポートセキュリティの設定情報を表示するには、次のいずれかの作業を行います。このコマンドの出力フィールドの詳細については、『*Cisco Nexus 5000 NX-OS* コマンド リファレンス』を参照してください。

コマンド	目的
show running-config port-security	ポート セキュリティの設定を表示します。
show port-security	デバイスのポートセキュリティのステータスを表示します。
show port-security interface	特定のインターフェイスのポートセキュリティのステータスを表示します。
show port-security address	セキュア MAC アドレスを表示します。
show running-config interface	実行コンフィギュレーションにあるインターフェイスを表示します。
show mac address-table	MAC アドレス テーブルの内容を表示します。
show system internal port-security info global	デバイスのポートセキュリティの設定を表示します。

セキュア **MAC** アドレスの表示

セキュア MAC アドレスを表示するには、**show port-security address** コマンドを使用します。 このコマンドの出力フィールドの詳細については、『*Cisco Nexus 5000 Series NX-OS Command Reference*』を参照してください。

ポート セキュリティの設定例

次に示す例は、VLAN とインターフェイスのセキュア アドレス最大数が指定されているイーサネット 2/1 インターフェイスのポート セキュリティ設定です。 この例のインターフェイスはトランク ポートです。 違反時の処理は Restrict（制限）に設定されています。

```
feature port-security
interface Ethernet 2/1
  switchport
  switchport port-security
  switchport port-security maximum 10
  switchport port-security maximum 7 vlan 10
  switchport port-security maximum 3 vlan 20
  switchport port-security violation restrict
```

vPC ドメインでのポート セキュリティの設定例

次に、vPC ドメインで vPC ピア上のポート セキュリティをイネーブルにして設定する例を示します。 最初のスイッチがプライマリ vPC ピアであり、2 番目のスイッチがセカンダリ vPC ピアです。 ドメイン 103 がすでに作成されていることを前提にしています。

```
primary_switch(config)# feature port-security
primary_switch(config-if)# int e1/1
primary_switch(config-if)# switchport port-security
primary_switch(config-if)# switchport port-security max 1025
primary_switch(config-if)# switchport port-security violation restrict
primary_switch(config-if)# switchport port-security aging time 4
primary_switch(config-if)# switchport port-security aging type absolute
primary_switch(config-if)# switchport port-security mac sticky
primary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
primary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# int e103/1/1
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# copy running-config startup-config
```

ポート セキュリティのデフォルト設定

次の表に、ポート セキュリティ パラメータのデフォルト設定を示します。

表 *15*：ポート セキュリティ パラメータのデフォルト値

パラメータ	デフォルト
ポートセキュリティがグローバルにイネーブルかどうか	ディセーブル
インターフェイス単位でポートセキュリティがイネーブルかどうか	ディセーブル
MAC アドレス ラーニング方式	ダイナミック

パラメータ	デフォルト
セキュア MAC アドレスのインターフェイス最大数	1
セキュリティ違反時の処理	シャットダウン

ポート セキュリティに関する追加情報

関連資料

関連項目	参照先
レイヤ 2 スイッチング	『*Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide*』
vPC	『*Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide*』
ポート セキュリティ コマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 5000 Series NX-OS Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

MIB

Cisco NX-OS はポート セキュリティに関して読み取り専用の SNMP をサポートしています。

MIB	MIB のリンク
• CISCO-PORT-SECURITY-MIB （注） トラップは、セキュア MAC アドレスの違反の通知についてサポートされています。	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

ポート セキュリティの機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *16*：ポート セキュリティの機能の履歴

機能名	リリース	機能情報
ポート セキュリティ	5.1(3)N1(1)	このリリースで導入された機能。

第 10 章

DHCP スヌーピングの設定

この章では、Cisco NX-OS デバイスで Dynamic Host Configuration Protocol（DHCP）スヌーピングを設定する手順について説明します。

DHCP スヌーピングの概要

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

- 信頼できないソースからの 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する。
- DHCP スヌーピング バインディング データベースを構築し、管理する。このデータベースには、リース IP アドレスを持つ、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する。

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 上または VLAN の特定の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。

信頼できるソースおよび信頼できないソース

DHCP スヌーピングがトラフィックの送信元を信頼するかどうかを設定できます。 信頼できないソースの場合、トラフィック攻撃やその他の敵対的アクションが開始される可能性があります。こうした攻撃を防ぐため、DHCP スヌーピングは信頼できない送信元からのメッセージをフィルタリングします。

企業ネットワークでは、信頼できる送信元はその企業の管理制御下にあるスイッチです。 これらのスイッチには、ネットワーク内のスイッチ、ルータ、およびサーバが含まれます。 ファイアウォールを越えるスイッチやネットワーク外のスイッチは信頼できない送信元です。 一般的に、ホスト ポートは信頼できない送信元として扱われます。

サービス プロバイダーの環境では、サービス プロバイダー ネットワークにないスイッチは、信頼できない送信元です（カスタマー スイッチなど）。 ホスト ポートは、信頼できないソースです。

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、信頼できない状態です。 DHCP サーバ インターフェイスは、信頼できるインターフェイスとして設定する必要があります。 ユーザのネットワーク内でスイッチ（スイッチまたはルータ）に接続されている場合、他のインターフェイスも信頼できるインターフェイスとして設定できます。 ホスト ポート インターフェイスは、通常、信頼できるインターフェイスとしては設定しません。

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

DHCP スヌーピング バインディング データベース

DHCP スヌーピングは、代行受信した DHCP メッセージから抽出した情報を使用し、ダイナミックにデータベースを構築し維持します。 ホストが、DHCP スヌーピングがイネーブルになっている VLAN に関連付けられている場合、このデータベースには、リース IP アドレスを含む信頼できない各ホストのエントリが含まれています。 データベースには、信頼できるインターフェイスを介して接続するホストに関するエントリは保存されません。

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

スイッチが特定の DHCP メッセージを受信すると、DHCP スヌーピングはデータベースをアップデートします。 たとえば、サーバからの DHCPACK メッセージをスイッチで受信すると、この機能により、データベースにエントリが追加されます。 IP アドレスのリース期限が切れると、また

はホストからの DHCPRELEASE メッセージをスイッチで受信すると、この機能により、データベースのエントリが削除されます。

DHCP スヌーピング バインディング データベース内の各エントリには、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、およびホストに関連付けられた VLAN 番号とインターフェイスの情報が含まれています。

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 スヌーピングの Option 82 データの挿入

DHCP は多数の加入者に対する IP アドレスの割り当てを一元的に管理できます。 Option 82 をイネーブルにすると、デバイスは、ネットワークに接続されている加入者デバイス（および、その MAC アドレス）を識別します。 加入者 LAN 上のマルチ ホストをアクセス デバイスの同一ポートに接続でき、これらは一意に識別されます。

Cisco NX-OS デバイスで Option 82 をイネーブルにすると、次の一連のイベントが発生します。

1. ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
2. Cisco NX-OS デバイスは、この DHCP 要求を受信すると、パケット内に Option 82 情報を追加します。 Option 82 情報には、デバイスの MAC アドレス（リモート ID サブオプション）と、受信されたパケットの発信元のポート ID である vlan-mod-port（回線 ID サブオプション）が含まれます。 ポート チャネルの背後に存在するホストの場合、回線 ID には、そのポート チャネルの if_index が入力されます。

（注） vPC ピア スイッチの場合、リモート ID サブオプションには、両方のスイッチで一意である vPC スイッチ MAC アドレスが含まれます。 この MAC アドレスは、vPC ドメイン ID を使用して計算されます。 Option 82 情報は、DHCP 要求が最初に受信されたスイッチで挿入された後、他の vPC ピア スイッチに転送されます。

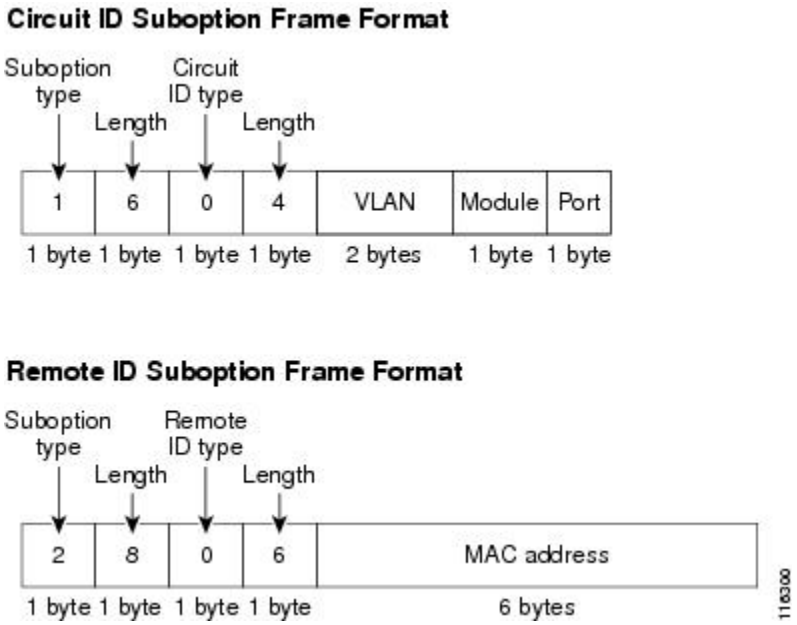
3. デバイスは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
4. DHCP サーバはこのパケットを受信します。 サーバは、Option 82 に対応している場合、リモート ID、回線 ID、またはその両方を使用して IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることのできる IP アドレスの数の制限などのポリシーを実装したりできます。 DHCP サーバは、Option 82 フィールドを DHCP 応答内にエコーします。
5. DHCP サーバは、その応答を Cisco NX-OS デバイスに送信します。 Cisco NX-OS デバイスは、リモート ID フィールドや、場合によっては回線 ID フィールドを検査することによって、そのデバイスが Option 82 データを最初に挿入したことを確認します。 Cisco NX-OS デバイスは、Option 82 フィールドを削除し、DHCP 要求を送信した DHCP クライアントに接続されているインターフェイスにそのパケットを転送します。

上記の一連のイベントが発生した場合、次の値は変更されません。

- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - 回線 ID タイプの長さ

次の図は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示しています。 Cisco NX-OS デバイスは、DHCP スヌーピングをグローバルにイネーブルにしたときや、Option 82 データの挿入と削除をイネーブルにしたときにこれらのパケット形式を使用します。 回線 ID サブオプションの場合、モジュール フィールドはモジュールのスロット番号になります。

図 *9*： サブオプションのパケット形式



vPC 環境での DHCP スヌーピング

仮想ポート チャネル（vPC）では、2 台の Cisco NX-OS スイッチを 3 番目のスイッチに 1 つの論理ポート チャネルとして認識させることができます。 3 番目のスイッチは、スイッチ、サーバ、またはポートチャネルをサポートするその他のネットワーク スイッチのいずれかにすることができます。

標準的な vPC 環境では、DHCP 要求は一方の vPC ピア スイッチに到達でき、応答は他方の vPC ピア スイッチに到達できるため、一方のスイッチには部分的な DHCP（IP-MAC）バインディング エントリが生成され、他方のスイッチにはバインディング エントリが生成されません。 Cisco NX-OS Release 5.1 から、この問題は Cisco Fabric Service over Ethernet（CFSoE）分散を使用して、すべての DHCP パケット（要求および応答）が両方のスイッチに確実に認識されるようにすることで対処されます。これにより、vPC リンクの背後に存在するすべてのクライアントについて、両方のスイッチで同じバインディング エントリが作成および管理されるようになります。

CFSoE 分散ではまた、vPC リンク上の DHCP 要求および応答を 1 台のスイッチのみが転送するようにもできます。 vPC 以外の環境では、両方のスイッチが DHCP パケットを転送します。

DHCP スヌーピング バインディング エントリの同期

ダイナミック DHCP バインディング エントリは、次のシナリオで同期される必要があります。

- リモート vPC がオンラインになったとき、その vPC リンクのすべてのバインディング エントリがピアと同期する必要があります。
- DHCP スヌーピングがピア スイッチでイネーブルの場合、リモートでアップ状態であるすべての vPC リンク用のダイナミック バインディング エントリは、ピアと同期する必要があります。

パケット検証

スイッチは、DHCP スヌーピングがイネーブルの VLAN にある信頼できないインターフェイスで受信された DHCP パケットを検証します。 次の条件が発生（この場合パケットは破棄される）しない限り、スイッチでは、DHCP パケットが転送されます。

- 信頼できないインターフェイスで DHCP 応答パケット（DHCPACK、DHCPNAK、または DHCPOFFER などのパケット）を受信した場合。
- 信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合。 このチェックは、DHCP スヌーピングの MAC アドレス検証オプションがオンの場合だけ、実行されます。
- DHCP スヌーピング バインディング テーブル内にエントリを持つ信頼できないホストから DHCPRELEASE または DHCPDECLINE メッセージを受信したが、バインディング テーブル内のインターフェイス情報が、このメッセージを受信したインターフェイスと一致しない場合。

- リレー エージェントの IP アドレス（0.0.0.0 以外）を含む DHCP パケットを受信した場合。

さらに、DHCP パケットの厳密な検証をイネーブルにすることもできます。これにより、DHCP パケットのオプション フィールドが確認されます。これには、オプション フィールドの最初の 4 バイト内の「マジック クッキー」値も含まれます。デフォルトでは、厳密な検証はディセーブルになっています。 これを **ip dhcp packet strict-validation** コマンドによりイネーブルにすると、DHCP スヌーピングで無効なオプション フィールドを含むパケットを処理した場合に、パケットがドロップされます。

DHCP リレー エージェントの概要

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 をイネーブルにした後に、デバイスは、デフォルトでバイナリ ifIndex 形式を使用します。 必要に応じて、符号化された文字列形式を使用するように、Option 82 設定を変更できます。

（注） 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 情報を設定したインターフェイスに DHCP 要求が着信した場合、DHCP サーバのアドレスが、別の VRF のメンバであるインターフェイスのネットワークに属する

ものであれば、デバイスは要求に Option 82 情報を挿入し、サーバの VRF の DHCP サーバに転送されます。 Option 82 情報は次のとおりです。

VPN 識別子

DHCP 要求を受信するインターフェイスが属する VRF の名前。

リンクの選択

DHCP 要求を受信するインターフェイスのサブネット アドレス。

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。

（注） 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 サーバや DHCP リレーエージェントとして機能するスイッチが設定され、イネーブルになっていることを確認してください。
- DHCP スヌーピングを使用して設定を行っている VLAN で VLAN ACL（VACL）が設定されている場合、その VACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。
- デフォルトで、DHCP バインディングは、スイッチの再起動後に永続的に保存されません。スイッチの再起動後にも永続的なバインディングを保持するには、**copy r s** コマンドを使用します。 **copy r s** コマンドが発行されると、その時点で存在するすべてのバインディングは、スイッチの再起動後も永続的な状態になります。
- vPC リンク内のスイッチ間で DHCP 設定が同期されていることを確認します。 同期されていないと、ランタイム エラーが発生し、パケットがドロップされる場合があります。
- リモート DHCP サーバとローカル DHCP サーバの両方を使用するには、DHCP リレー機能を設定し、ローカル DHCP サーバのユニキャスト アドレスを定義し、またはローカル DHCP サーバが常駐するサブネットのローカル ブロードキャスト アドレスを設定する必要があります。 DHCP サーバのユニキャスト アドレスを定義せず、またはサブネットのローカル ブロードキャスト アドレスを設定しない場合、ローカル DHCP パケットは配信できません。たとえば、この状況は SVI に IP DHCP アドレスを適用する場合に発生することがあります。

次の注意事項および制約事項は、FabricPath を含む実装に適用されます。

- DHCP スヌーピングは、CE-Fabric 境界スイッチ上でイネーブルにする必要があります。
- アクセス レイヤでネットワークを保護するために、DHCP スヌーピングはすべてのアクセス レイヤ スイッチ上でイネーブルになっています。
- DHCP は、FabricPath モードで設定されたポート上のバインディング エントリを学習しません。 DHCP スヌーピングは、すべてのアクセス レイヤ スイッチで手動でイネーブルにする必要があります。
- ダイナミック ARP インスペクション（DAI）がイネーブルになっている場合、FabricPath ポート上で受信された ARP パケットは許可されます。
- FabricPath モードでは、ポート上で IPSG をイネーブルにすることはできません。
- システムのすべての FabricPath ポートは、信頼できるポートとして設定する必要があります。
- FabricPath の DHCP スヌーピングは、スイッチに設定されたすべての VLAN でイネーブルにする必要があります。 スイッチ上のすべての VLAN の FabricPath をイネーブルにしない場合、DHCP がイネーブルにされていない VLAN で DHCP パケットはドロップされます。

  DHCP パケットがドロップされないようにするには、次の設定すべてを実行する必要があります。

  - **feature dhcp** コマンドを使用して DHCP 機能をイネーブルにします。

- **feature-set fabricpath** および **feature-set fabricpath** コマンドを使用して FabricPath フィーチャ セットをインストールします。
- **ip dhcp snooping** コマンドを使用して、DHCP スヌーピングをグローバルにイネーブルにします。
- **ip dhcp snooping vlan** *vlan* コマンドを使用して、スイッチの設定済み VLAN ごとに DHCP スヌーピングをイネーブルにします。

DHCP スヌーピングのデフォルト設定

次の表に、DHCP スヌーピング パラメータのデフォルト設定を示します。

表 *17* : *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	No
DHCP スヌーピング VLAN	なし
DHCP スヌーピングの Option 82 サポート	ディセーブル
DHCP スヌーピング信頼状態	信頼できない

DHCP スヌーピングの設定

DHCP スヌーピングの最小設定

手順

	コマンドまたはアクション	目的
ステップ 1	DHCP スヌーピング機能をイネーブルにします。	DHCP スヌーピング機能がディセーブルになっていると、DHCP スヌーピングを設定できません。 詳細については、DHCP スヌーピング機能のイネーブル化またはディセーブル化, （189 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 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, （190 ページ）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, （191 ページ）を参照してください。
ステップ 4	DHCP サーバとスイッチが、信頼できるインターフェイスを使用し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, （193 ページ）を参照してください。

DHCP スヌーピング機能のイネーブル化またはディセーブル化

スイッチの DHCP スヌーピング機能をイネーブルまたはディセーブルに設定できます。 デフォルトでは、DHCP スヌーピングはディセーブルです。

はじめる前に

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

手順

	コマンドまたはアクション	目的

ステップ 1	**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**] **feature dhcp** 例： `switch(config)# feature dhcp`	DHCP スヌーピング機能をイネーブルにします。 **no** オプションを使用すると、DHCP スヌーピング機能がディセーブルになり、DHCP スヌーピングの設定がすべて消去されます。

	コマンドまたはアクション	目的
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

はじめる前に

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

手順

	コマンドまたはアクション	目的

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

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

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VLANに対するDHCPスヌーピングのイネーブル化またはディセーブル化

1 つまたは複数の VLAN に対して DHCP スヌーピングをイネーブルまたはディセーブルに設定できます。

はじめる前に

デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。

DHCP スヌーピングがイネーブルになっていることを確認してください。

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

手順

	コマンドまたはアクション	目的

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

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

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Option 82 データの挿入および削除のイネーブル化またはディセーブル化

DHCP リレー エージェントを使用せずに転送された DHCP パケットへの Option 82 情報の挿入および削除をイネーブルまたはディセーブルに設定できます。

はじめる前に

デフォルトでは、スイッチは DHCP パケットに Option 82 情報を挿入しません。

DHCP スヌーピングがイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**[no] ip dhcp snooping information option** 例： `switch(config)# ip dhcp snooping information option`	DHCP パケットの Option 82 情報の挿入および削除をイネーブルにします。 **no** オプションを使用すると、Option 82 情報の挿入および削除がディセーブルになります。
ステップ 3	**show running-config dhcp** 例： `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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP パケットの厳密な検証のイネーブル化またはディセーブル化

DHCP スヌーピング機能では、DHCP パケットの厳密な検証をイネーブルまたはディセーブルにできます。 デフォルトでは、DHCP パケットの厳密な検証はディセーブルになっています。

手順

	コマンドまたはアクション	目的

ステップ 1	**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 packet strict-validation** 例： `switch(config)# ip dhcp packet strict-validation`	DHCP スヌーピング機能で、DHCP パケットの厳密な検証をイネーブルにします。 **no** オプションを使用すると、DHCP パケットの厳密な検証がディセーブルになります。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの信頼状態の設定

各インターフェイスが DHCP メッセージの送信元として信頼できるかどうかを設定できます。 DHCP の信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 ポート チャネル インターフェイス

はじめる前に

デフォルトでは、すべてのインターフェイスは信頼できません。

DHCP スヌーピングがイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	次のいずれかのコマンドを入力します。
	• **interface ethernet** *port*/*slot*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		• 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** 例： `switch(config-if)# ip dhcp snooping trust`	DHCP スヌーピングに関してインターフェイスを信頼できるインターフェイスとして設定します。 **no** オプションを使用すると、ポートは信頼できないインターフェイスとして設定されます。
ステップ 4	**show running-config dhcp** 例： `switch(config-if)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー エージェントのイネーブル化またはディセーブル化

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

はじめる前に

DHCP 機能がイネーブル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	[**no**] **ip dhcp relay** 例： `switch(config)# ip dhcp relay`	DHCP リレーエージェントをイネーブルにします。 **no** オプションを使用すると、DHCP リレーエージェントがディセーブルになります。
ステップ 3	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 4	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

デバイスに対し、リレー エージェントによって転送された DHCP パケットへの Option 82 情報の挿入と削除をイネーブルまたはディセーブルに設定できます。

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

はじめる前に

DHCP 機能がイネーブル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	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)#[**no**] **ip dhcp relay information option**	DHCP リレーエージェントによって転送されるパケットに対する Option 82 情報の挿入および削除をイネーブルにします。 Option 82 情報は、デフォルトでバイナリ ifIndex 形式です。 **no** オプションを使用すると、この動作がディセーブルになります。
ステップ 3	switch(config)# **ip dhcp relay information sub-option circuit-id format-type string**	（任意） デフォルトの ifIndex バイナリ形式の代わりに符号化されたストリング形式を使用するように、オプション 82 を設定します。
ステップ 4	switch(config)# **show ip dhcp relay**	（任意） DHCP リレーの設定を表示します。
ステップ 5	switch(config)# **show running-config dhcp**	（任意） DHCP 設定を表示します。
ステップ 6	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

ある VRF のインターフェイスで受信した DHCP 要求を、別の VRF の DHCP サーバにリレーする機能をサポートするように、デバイスを設定できます。

はじめる前に

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	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 5	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ 3 インターフェイスの 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。

はじめる前に

DHCP 機能がイネーブルであ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。

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。

	コマンドまたはアクション	目的
ステップ 6	**show ip dhcp relay** 例： `switch# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 7	**show running-config dhcp** 例： `switch# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP スタティック バインディングの作成

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

はじめる前に

DHCP スヌーピング機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**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	**show ip dhcp snooping binding** 例： `switch(config)# ip dhcp snooping binding`	（任意） DHCP スヌーピングのスタティックおよびダイナミック バインディングを示します。
ステップ 4	**show ip dhcp snooping binding dynamic** 例： `switch(config)# ip dhcp snooping binding dynamic`	（任意） DHCP スヌーピングのダイナミック バインディングを示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、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、ご使用の 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 snooping	DHCP スヌーピングに関する一般的な情報を表示します。

DHCP バインディングの表示

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

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

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

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

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

DHCP スヌーピング バインディング データベースのクリア

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

はじめる前に

DHCP スヌーピングがイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ip dhcp snooping binding** 例： `switch# clear ip dhcp snooping binding`	（任意） DHCP スヌーピング バインディング データベースからすべてのエントリをクリアします。
ステップ 2	**clear ip dhcp snooping binding interface ethernet** *slot*/*port*[.*subinterface-number*] 例： `switch# clear ip dhcp snooping binding interface ethernet 1/4`	（任意） DHCP スヌーピング バインディング データベースから、特定のイーサネット インターフェイスに関連するエントリをクリアします。
ステップ 3	**clear ip dhcp snooping binding interface port-channel** *channel-number*[.*subchannel-number*] 例： `switch# clear ip dhcp snooping binding interface port-channel 72`	（任意） DHCP スヌーピング バインディング データベースから、特定のポート チャネル インターフェイスに関連するエントリをクリアします。

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

DHCP スヌーピングの設定例

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

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

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

第 11 章

ダイナミック ARP インスペクションの設定

この章では、Cisco Nexus 5000 シリーズ スイッチに Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）Inspection（DAI; ダイナミック ARP インスペクション）を設定する方法について説明します。

この章は、次の内容で構成されています。

DAI の概要

ARP

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。 たとえば、ホスト B がホスト A に情報を送信しようとして、ホスト B の ARP キャッシュにホスト A の MAC アドレスがないという場合、 ARP の用語では、ホスト B が送信者、ホスト A はターゲットになります。

ホスト B は、ホスト A の IP アドレスに関連付けられた MAC アドレスを取得するため、このブロードキャスト ドメイン内の全ホストに対してブロードキャスト メッセージを送信します。 ブ

ロードキャスト ドメイン内の全ホストはこの ARP 要求を受信し、これに対してホスト A は自身の MAC アドレスを返します。

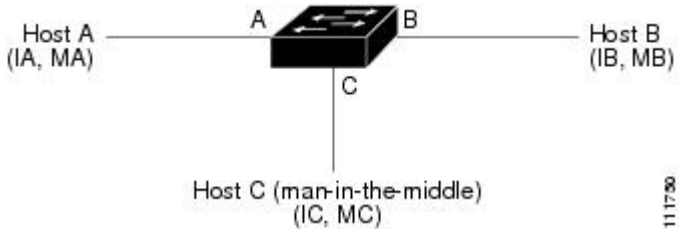
ARP スプーフィング攻撃

ARP では、たとえ ARP 要求を受信していなくても、ホストからの応答が可能なので、ARP スプーフィング攻撃と ARP キャッシュ ポイズニングが発生する可能性があります。 攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

ARP スプーフィング攻撃は、サブネットに接続されているデバイスの ARP キャッシュに偽りの情報を送信することにより、レイヤ 2 ネットワークに接続されているホスト、スイッチ、ルータに影響を及ぼす可能性があります。 ARP キャッシュに偽りの情報を送信することを ARP キャッシュ ポイズニングといいます。 スプーフ攻撃では、サブネット上の他のホストに対するトラフィックの代行受信も可能です。

次の図に、ARP キャッシュ ポイズニングの例を示します。

図 *10*： *ARP* キャッシュ ポイズニング



ホスト A、B、C は、それぞれインターフェイス A、B、C を介してデバイスに接続され、同一サブネットに属します。 カッコ内は、各ホストの IP および MAC アドレスを示します。たとえば、ホスト A は IP アドレス IA、および MAC アドレス MA を使用します。 ホスト A がホスト B に IP データを送信する必要がある場合、ホスト A は IP アドレス IB に関連付けられた MAC アドレスを求める ARP 要求をブロードキャストします。 デバイスとホスト B はこの ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持つホストの ARP バインディングを、それぞれの ARP キャッシュ内に書き込みます。たとえば、IP アドレス IA は MAC アドレス MA にバインドされます。 ホスト B が応答すると、デバイスとホスト A は、IP アドレス IB および MAC アドレス MB を持つホストのバインディングを、それぞれの ARP キャッシュ内に書き込みます。

ホスト C は、バインディングを伴う 2 つの偽造 ARP 応答をブロードキャストすることにより、デバイス、ホスト A、ホスト B の ARP キャッシュをポイズニングできます。偽造 ARP 応答の 1 つは、IP アドレス IA と MAC アドレス MC を持つホストの応答、もう 1 つは IP アドレス IB と MAC アドレス MC を持つホストの応答です。 これにより、ホスト B とデバイスは、IA を宛先とするトラフィックの宛先 MAC アドレスとして、MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。 同様に、ホスト A とデバイスは、IB を宛先とするトラフィックの宛先 MAC アドレスとして MAC アドレス MC を使用します。

ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送でき

ます。 このトポロジでは、ホスト C は、ホスト A からホスト B へのトラフィック ストリーム内に自身を割り込ませています。これは、*man-in-the-middle* 攻撃の典型的な例です。

DAI および ARP スプーフィング攻撃

DAI を使用することで、有効な ARP 要求および応答だけがリレーされるようになります。 DAI がイネーブルになり適切に設定されている場合、Cisco Nexus デバイスは次のアクティビティを実行します。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

DAI によって ARP パケットの有効性を判断するときの基準となる有効な IP-to-MAC バインディングは、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースに保存されています。 このデータベースは、VLAN とデバイス上で DHCP スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。 また、このデータベースにはユーザが作成するスタティック エントリも保存できます。 ARP パケットを信頼できるインターフェイス上で受信した場合は、デバイスはこのパケットを検査せずに転送します。 信頼できないインターフェイス上では、デバイスは有効性を確認できたパケットだけを転送します。

DAI では、パケット内の IP アドレスが無効な場合に ARP パケットをドロップするのか、または ARP パケット本体の MAC アドレスがイーサネット ヘッダーに指定されたアドレスと一致しない場合に ARP パケットをドロップするのかを設定できます。

関連トピック

DAI パケットのロギング, （207 ページ）
追加検証のイネーブル化またはディセーブル化, （212 ページ）

インターフェイスの信頼状態とネットワーク セキュリティ

DAI は、デバイスの各インターフェイスに信頼状態を関連付けます。 信頼できるインターフェイス上で受信されたパケットは、DAI のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、DAI の有効性検査が行われます。

一般的なネットワーク構成では、次の注意事項に従ってインターフェイスの信頼状態を設定します。

信頼できない

ホストに接続されているインターフェイス

信頼できる

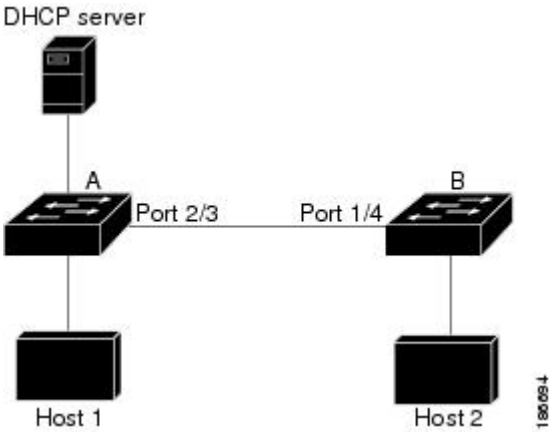
デバイスに接続されているインターフェイス

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

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

次の図では、デバイスAおよびデバイスBの両方が、ホスト1およびホスト2を収容するVLAN上でDAIを実行していると仮定します。 ホスト1およびホスト2が、デバイスAに接続されているDHCPサーバからIPアドレスを取得すると、デバイスAだけがホスト1のIP/MACアドレスをバインドします。 デバイスAとデバイスB間のインターフェイスが信頼できない場合は、ホスト1からのARPパケットはデバイスBではドロップされ、ホスト1およびホスト2の間の接続は切断されます。

図 *11*： *DAI* をイネーブルにした *VLAN* での *ARP* パケット検証



信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワークにセキュリティ ホールが生じる可能性があります。 デバイスAがDAIを実行していなければ、ホスト1はデバイスBのARPキャッシュを簡単にポイズニングできます（デバイス間のリンクが信頼できるものとして設定されている場合はホスト2も同様）。 この状況は、デバイスBがDAIを実行している場合でも起こりえます。

DAIは、DAIが稼働するデバイスに接続されているホスト（信頼できないインターフェイス上）がネットワーク内の他のホストのARPキャッシュをポイズニングしないように保証します。ただし、DAIが稼働するデバイスに接続されているホストのキャッシュがネットワークの他の部分のホストによってポイズニングされるのを防ぐことはできません。

VLAN内の一部のデバイスでDAIが稼働し、他のデバイスでは稼働していない場合は、DAIが稼働しているデバイス上のインターフェイスの信頼状態を次のガイドラインに従って設定します。

信頼できない

ホスト、または DAI を実行していないデバイスに接続されているインターフェイス

信頼できる

DAI を実行しているデバイスに接続されているインターフェイス

DAI が稼働していないデバイスからのパケットのバインディングを検証するには、DAI が稼働しているデバイスに ARP ACL を設定します。バインディングの有効性を判断できない場合は、DAI が稼働しているデバイスを DAI が稼働していないデバイスからレイヤ 3 で隔離します。

（注） ネットワークの設定によっては、VLAN 内の一部のデバイスで ARP パケットを検証できない場合もあります。

関連トピック

レイヤ 2 インターフェイスの DAI 信頼状態の設定, （210 ページ）

DAI パケットのロギング

Cisco NX-OS は処理された DAI パケットについてのログ エントリのバッファを維持しています。各ログエントリには、受信側の VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスといったフロー情報が記録されます。

ログに記録するパケットのタイプを指定することもできます。デフォルトでは、Cisco Nexus デバイスは DAI がドロップしたパケットだけをログに記録します。

ログ バッファがあふれると、デバイスは最も古い DAI ログ エントリを新しいエントリで上書きします。 バッファ内の最大エントリ数を設定できます。

（注） Cisco NX-OS は、ログに記録される DAI パケットに関するシステム メッセージを生成しません。

関連トピック

DAI のログ バッファ サイズの設定, （213 ページ）
DAI のログ フィルタリングの設定, （214 ページ）

DAI のライセンス要件

次の表に、DAI のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	DAIにはライセンスは必要ありません。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式に関する詳細は、『*Cisco NX-OS Licensing Guide*』を参照してください。

DAI の前提条件

- DHCP を設定するには、その前に DAI 機能をイネーブルにする必要があります。

DAI の注意事項と制約事項

DAI に関する注意事項と制約事項は次のとおりです。

- DAI は入力セキュリティ機能であり、出力検査は行いません。
- DAI は、DAI をサポートしないデバイス、またはこの機能がイネーブルにされていないデバイスに接続されているホストに対しては、効果がありません。 man-in-the-middle 攻撃は 1 つのレイヤ 2 ブロードキャスト ドメインに限定されるため、DAI が有効なドメインを、DAI が実行されないドメインから切り離す必要があります。 これにより、DAI が有効なドメイン内のホストの ARP キャッシュをセキュリティ保護できます。
- DAI では、DHCP スヌーピング バインディング データベース内のエントリを使用して、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスのバインディングを確認します。 DAI が ARP パケットの有効性を判断するのにスタティック IP-MAC アドレス バインディングを使用するように設定する場合、DHCP スヌーピングの設定はイネーブルにするだけで済みます。 DAI が ARP パケットの有効性を判断するのにダイナミック IP-MAC アドレス バインディングを使用するように設定する場合は、DAI を設定した VLAN と同じ VLAN に DHCP スヌーピングを設定する必要があります。
- **feature dhcp** コマンドを使用して DHCP 機能をイネーブルにすると、I/O モジュールが DHCP を受信する前、または DAI の設定前に約 30 秒の遅延が発生します。 この遅延は、DHCP 機能がディセーブルになった設定から、DHCP 機能がイネーブルになった設定に変更するために使用する方式には関係なく発生します。 たとえば、ロールバック機能を使用して、DHCP 機能をイネーブルにする設定に戻した場合、ロールバックを完了してから約 30 秒後に I/O モジュールが DHCP と DAI 設定を受信します。
- DAI は、アクセス ポート、トランク ポート、ポート チャネル ポート、およびプライベート VLAN ポートでサポートされます。

- ポート チャネルに対する DAI の信頼設定によって、そのポート チャネルに割り当てたすべての物理ポートの信頼状態が決まります。 たとえば、ある物理ポートを信頼できるインターフェイスとして設定し、信頼できないインターフェイスであるポート チャネルにその物理ポートを追加した場合、その物理ポートは信頼できない状態になります。
- ポート チャネルから物理ポートを削除した場合、その物理ポートはポート チャネルの DAI 信頼状態の設定を保持しません。
- ポートチャネルの信頼状態を変更すると、デバイスはそのチャネルを構成するすべての物理ポートに対し、新しい信頼状態を設定します。
- ARP パケットが有効かどうかを判定するために DAI でスタティック IP-MAC アドレス バインディングを使用するように設定する場合は、DHCP スヌーピングがイネーブルになっていること、およびスタティック IP-MAC アドレス バインディングを設定していることを確認します。
- ARP パケットが有効かどうかを判定するために DAI でダイナミック IP-MAC アドレス バインディングを使用するように設定する場合は、DHCP スヌーピングがイネーブルになっていることを確認します。

DAI のデフォルト設定

次の表に、DAI パラメータのデフォルト設定を示します。

表 *18*：デフォルトの *DAI* パラメータ

パラメータ	デフォルト
DAI	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
有効性検査	検査は実行されません。
ログ バッファ	DAI をイネーブルにした場合は、拒否または廃棄されたすべての ARP パケットが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは、1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

DAI の設定

VLAN での DAI のイネーブル化とディセーブル化

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

はじめる前に

DAI をイネーブルにする場合は、次の点を確認してください。

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip arp inspection vlan** *list* 例： `switch(config)# ip arp inspection vlan 13`	VLAN の特定のリストに対して DAI をイネーブルにします。 **no** オプションを使用すると、指定した VLAN の DAI がディセーブルになります。
ステップ 3	**show ip arp inspection vlan** *list* 例： `switch(config)# show ip arp inspection vlan 13`	（任意） VLAN の特定リストの DAI ステータスを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ 2 インターフェイスの DAI 信頼状態の設定

レイヤ 2 インターフェイスの DAI インターフェイス信頼状態を設定できます。 デフォルトでは、すべてのインターフェイスは信頼できません。

デバイスは、信頼できるレイヤ 2 インターフェイス上で受信した ARP パケットを転送しますが、検査は行いません。

信頼できないインターフェイス上では、デバイスはすべての ARP 要求および ARP 応答を代行受信します。デバイスは、ローカル キャッシュをアップデートして、代行受信したパケットを適切な宛先に転送する前に、そのパケットの IP-MAC アドレス バインディングが有効かどうかを検証します。 そのパケットのバインディングが無効であると判断すると、デバイスはそのパケットをドロップし、ロギングの設定に従ってログに記録します。

はじめる前に

DAI をイネーブルにする場合は、DHCP 機能がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *type number* / *slot*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **ip arp inspection trust** 例： `switch(config-if)# ip arp inspection trust`	インターフェイスを、信頼できる ARP インターフェイスとして設定します。 **no** オプションを使用すると、そのインターフェイスは信頼できない ARP インターフェイスとして設定されます。
ステップ 4	**show ip arp inspection interface** *type number* / *slot* 例： `switch(config-if)# show ip arp inspection interface ethernet 2/1`	（任意） 特定のインターフェイスの信頼状態および ARP パケット レートを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

インターフェイスの信頼状態とネットワーク セキュリティ，（205 ページ）

DAI のログ フィルタリングの設定，（214 ページ）

追加検証のイネーブル化またはディセーブル化

ARP パケットの追加検証をイネーブルまたはディセーブルにできます。デフォルトでは、ARP パケットの追加検証はイネーブルになりません。 追加検証が設定されていない場合、送信元 MAC アドレス、ARP パケットの IP/MAC バインディング エントリと照合する送信元 IP アドレスのチェックは、イーサネット送信元 MAC アドレス（ARP 送信者の MAC アドレスではない）と ARP 送信者の IP アドレスを使用して実行されます。

DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、記録、および廃棄します。宛先 MAC アドレス、送信元および宛先 IP アドレス、送信元 MAC アドレスに対し、追加検証をイネーブルにすることができます。

追加検証を実装するには、**ip arp inspection validate** コマンドで次のキーワードを使用します。

dst-mac

ARP 応答のイーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較して検査します。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。

ip

ARP 本文をチェックして、無効な IP アドレスや予期しない IP アドレスがないかを確認します。 アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。 送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。

src-mac

ARP 要求と応答のイーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信者 MAC アドレスと比較して検査します。 イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。

追加検証をイネーブルにする場合は、次の点に注意してください。

- 少なくとも 1 つのキーワードを指定する必要があります。 指定するキーワードは、1 つでも、2 つでも、3 つすべてでもかまいません。
- 各 **ip arp inspection validate** コマンドにより、それまでに指定したコマンドの設定が置き換えられます。 **ip arp inspection validate** コマンドによって src -mac および dst-mac 検証をイネーブルにし、2 つめの **ip arp inspection validate** コマンドで IP 検証をイネーブルにした場合は、2 つめのコマンドを入力した時点で src-mac と dst-mac の検証がディセーブルになります。

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} 例： `switch(config)# ip arp inspection validate src-mac dst-mac ip`	追加の DAI 検証をイネーブルにします。あるいは、**no** オプションを使用して、追加の DAI 検証をディセーブルにします。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI のログ バッファ サイズの設定

DAI のログ バッファ サイズを設定できます。 デフォルトのバッファ サイズは 32 メッセージです。

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip arp inspection log-buffer entries** *number* 例： `switch(config)# ip arp inspection log-buffer entries 64`	DAI のログ バッファ サイズを設定します。**no** オプションを使用すると、デフォルトのバッファ サイズ（32 メッセージ）に戻ります。設定できるバッファ サイズは、0 ～ 2048 メッセージです。

	コマンドまたはアクション	目的
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAIの設定も含めて、DHCPスヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI のログ フィルタリングの設定

DAI パケットを記録するかどうかをデバイスが判断する方法を設定できます。 デフォルトでは、デバイスはドロップされる DAI パケットをログに記録します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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。 • **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings all** • **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings none** • **ip arp inspection vlan** *vlan-list* **logging dhcp-bindingspermit** • **no ip arp inspection vlan** *vlan-list* **logging dhcp-bindings** {**all** | **none** | **permit**} 例： `switch(config)# ip arp inspection vlan 100 dhcp-bindings permit`	次のようにして、DAI ログ フィルタリングを設定します。 **no** オプションを使用すると、DAI ログ フィルタリングが削除されます。 • DHCP バインディングに一致するすべてのパケットを記録します。 • DHCP バインディングに一致するパケットを記録しません。 • DHCP バインディングによって許可されるパケットを記録します。 • DAI ログ フィルタリングを削除します。

	コマンドまたはアクション	目的
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI の設定の確認

DAI の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config arp	DAI の設定を表示します。
show ip arp inspection	DAI のステータスを表示します。
show ip arp inspection interface ethernet	特定のインターフェイスの信頼状態および ARP パケット レートを表示します。
show ip arp inspection vlan	特定の VLAN の DAI 設定を表示します。
show arp access-lists	ARP ACL を表示します。
show ip arp inspection log	DAI のログ設定を表示します。

DAI の統計情報のモニタリングとクリア

DAI の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドを使用します。 これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show ip arp inspection statistics	DAI の統計情報を表示します。

コマンド	目的
show ip arp ethernet	インターフェイス固有の DAI の統計情報を表示します。
clear ip arp inspection statistics	DAI 統計情報をクリアします。

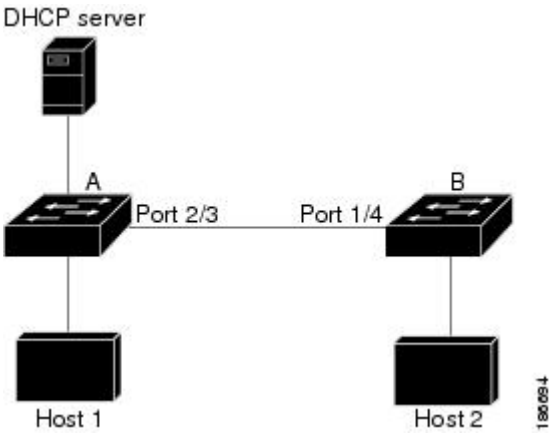
DAI の設定例

例 1：2 つのデバイスが DAI をサポートする場合

2 つのデバイスが DAI をサポートする場合の DAI の設定手順を次に示します。

次の図に、この例のネットワーク構成を示します。 ホスト 1 はデバイス A に、ホスト 2 はデバイス B にそれぞれ接続されています。 両方のデバイスは、これらのホストが置かれている VLAN 1 上で DAI を実行しています。 DHCP サーバはデバイス A に接続されています。 両方のホストは、同一の DHCP サーバから IP アドレスを取得します。 デバイス A はホスト 1 およびホスト 2 のバインディングを持ち、デバイス B はホスト 2 のバインディングを持ちます。 デバイス A のイーサネット インターフェイス 2/3 は、デバイス B のイーサネット インターフェイス 1/4 に接続されています。

図 *12*：*DAI* をサポートする *2* つのデバイス



DAI では、DHCP スヌーピング バインディング データベース内のエントリを使用して、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスのバインディングを確認します。 IP アドレスを動的に割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。

- この構成は、DHCP サーバがデバイス A から別の場所に移動されると機能しません。

- この構成によってセキュリティが損なわれないようにするには、デバイス A のイーサネット インターフェイス 2/3、およびデバイス B のイーサネット インターフェイス 1/4 を、信頼できるインターフェイスとして設定します。

デバイス A の設定

デバイス A で DAI をイネーブルにし、イーサネット インターフェイス 2/3 を信頼できるインターフェイスとして設定するには、次の作業を行います。

手順

ステップ 1 デバイス A にログインして、デバイス A とデバイス B の間の接続を確認します。

```
switchA# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchB                Ethernet2/3     177     R S I    WS-C2960-24TC Ethernet1/4
switchA#
```

ステップ 2 VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
switchA# config t
switchA(config)# ip arp inspection vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchA(config)#
```

ステップ 3 イーサネット インターフェイス 2/3 を、信頼できるインターフェイスとして設定します。

```
switchA(config)# interface ethernet 2/3
switchA(config-if)# ip arp inspection trust
switchA(config-if)# exit
switchA(config)# exit
switchA# show ip arp inspection interface ethernet 2/3
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet2/3      Trusted           15             5
```

ステップ 4 バインディングを確認します。

```
switchA# show ip dhcp snooping binding
MacAddress         IpAddress        LeaseSec  Type           VLAN  Interface
-----------------  ---------------  --------  -------------  ----  -------------
00:60:0b:00:12:89  10.0.0.1         0         dhcp-snooping  1     Ethernet2/3
```

```
switchA#
```

ステップ 5 DAI がパケットを処理する前、およびあとの統計情報を調べます。

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

ホスト 1 が IP アドレス 10.0.0.1 および MAC アドレス 0002.0002.0002 を持つ 2 つの ARP 要求を送信すると、両方の要求が許可されます。これは、次の統計情報で確認できます。

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

ホスト 1 が、IP アドレス 10.0.0.3 を持つ ARP 要求を送信しようとすると、このパケットはドロップされ、エラー メッセージがログに記録されます。

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Ethernet2/3, vlan
1.([0002.0002.0002/10.0.0.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Fri Jul 13 2008])
```

この場合に表示される統計情報は次のようになります。

```
switchA# show ip arp inspection statistics vlan 1
switchA#
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 2
ARP Res Dropped    = 0
DHCP Drops         = 2
DHCP Permits       = 2
```

```
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

デバイス B の設定

デバイス B で DAI をイネーブルにし、イーサネット インターフェイス 1/4 を信頼できるインターフェイスとして設定するには、次の作業を行います。

手順

ステップ 1 デバイス B にログインして、デバイス B とデバイス A の間の接続を確認します。

```
switchB# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchA                Ethernet1/4     120     R S I    WS-C2960-24TC Ethernet2/3
switchB#
```

ステップ 2 VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
switchB# config t
switchB(config)# ip arp inspection vlan 1
switchB(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchB(config)#
```

ステップ 3 イーサネット インターフェイス 1/4 を、信頼できるインターフェイスとして設定します。

```
switchB(config)# interface ethernet 1/4
switchB(config-if)# ip arp inspection trust
switchB(config-if)# exit
switchB(config)# exit
switchB# show ip arp inspection interface ethernet 1/4
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet1/4      Trusted           15             5
switchB#
```

ステップ 4 DHCP スヌーピング バインディングのリストを確認します。

```
switchB# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type           VLAN  Interface
------------------  ---------------  --------  -------------  ----  -------------
00:01:00:01:00:01  10.0.0.2         4995      dhcp-snooping  1     Ethernet1/4
switchB#
```

ステップ 5 DAI がパケットを処理する前、およびあとの統計情報を調べます。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

ホスト 2 が、IP アドレス 10.0.0.2 および MAC アドレス 0001.0001.0001 を持つ ARP 要求を送信すると、このパケットは転送され、統計情報が更新されます。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

ホスト 2 が IP アドレス 10.0.0.1 を持つ ARP 要求を送信しようとすると、この要求はドロップされ、システム メッセージがログに記録されます。

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Ethernet1/4, vlan
1.([0001.0001.0001/10.0.0.1/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri Jun 13 2008])
```

この場合に表示される統計情報は次のようになります。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
```

```
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 1
ARP Res Dropped    = 0
DHCP Drops         = 1
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

第 12 章

IP ソース ガードの設定

この章では、Cisco Nexus 5000 シリーズ スイッチ上で IP ソース ガードを設定する方法について説明します。

この章は、次の内容で構成されています。

IP ソース ガードの概要

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

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

信頼できる IP および MAC のアドレス バインディングのフィルタリングは、スプーフィング攻撃（有効なホストの IP アドレスを使用して不正なネットワーク アクセス権を取得する攻撃）の防止

に役立ちます。 IP ソース ガードを妨ぐためには、攻撃者は有効なホストの IP アドレスと MAC アドレスを両方スプーフィングする必要があります。

DHCP スヌーピングで信頼状態になっていないレイヤ 2 インターフェイスの IP ソース ガードをイネーブルにできます。 IP ソース ガードは、アクセス モードとトランク モードで動作するように設定されているインターフェイスをサポートしています。IP ソース ガードを最初にイネーブルにすると、次のトラフィックを除いて、そのインターフェイス上のインバウンド IP トラフィックがすべてブロックされます。

- DHCP パケット。DHCP パケットは、DHCP スヌーピングによって検査が実行され、その結果に応じて転送またはドロップされます。
- Cisco NX-OS デバイスに設定したスタティック IP ソース エントリからの IP トラフィック。

デバイスが IP トラフィックを許可するのは、DHCP スヌーピングによって IP パケットの IP アドレスと MAC アドレスのバインディング テーブル エントリが追加された場合、またはユーザがスタティック IP ソース エントリを設定した場合です。

パケットの IP アドレスと MAC アドレスがバインディング テーブル エントリにも、スタティック IP ソース エントリにもない場合、その IP パケットはドロップされます。 たとえば、**show ip dhcp snooping binding** コマンドによって、次のバインディング テーブル エントリが表示されるとします。

```
MacAddress          IpAddress    LeaseSec   Type         VLAN      Interface
------------------  -----------  ---------  -------      -------   ----------
00:02:B3:3F:3B:99   10.5.5.2       6943     dhcp-snooping  10      Ethernet2/3
```

IP アドレスが 10.5.5.2 の IP パケットをデバイスが受信した場合、IP ソース ガードによってこのパケットが転送されるのは、このパケットの MAC アドレスが 00:02:B3:3F:3B:99 のときだけです。

IP ソース ガードのライセンス要件

次の表に、IP ソース ガードのライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	IP ソース ガードにはライセンスは必要ありません。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式に関する詳細は、『*Cisco NX-OS Licensing Guide*』を参照してください。

IP ソース ガードの前提条件

IP ソース ガードの前提条件は次のとおりです。

- DHCP 機能をイネーブルにする必要があります。

IP ソース ガイドの注意事項と制約事項

IP ソース ガードに関する注意事項と制約事項は次のとおりです。

- IP ソース ガードは、インターフェイス上の IP トラフィックを、IP-MAC アドレス バインディング テーブル エントリまたはスタティック IP ソース エントリに送信元が含まれているトラフィックだけに制限します。 インターフェイス上の IP ソース ガードを初めてイネーブルにする際には、そのインターフェイス上のホストが DHCP サーバから新しい IP アドレスを受信するまで、IP トラフィックが中断されることがあります。
- IP ソース ガードの機能は、DHCP スヌーピング（IP-MAC アドレス バインディング テーブルの構築および維持に関して）、またはスタティック IP ソース エントリの手動での維持に依存しています。

IP ソース ガードのデフォルト設定

次の表に、IP ソース ガードのパラメータのデフォルト設定を示します。

表 *19* : *IP* ソース ガードのパラメータのデフォルト値

パラメータ	デフォルト
IPSG	各インターフェイスでディセーブル
IP ソース エントリ	なし。 デフォルトではスタティック IP ソース エントリはありません。デフォルトの IP ソース エントリもありません。

IP ソース ガードの設定

レイヤ2インターフェイスに対するIP ソース ガードのイネーブル化またはディセーブル化

レイヤ 2 インターフェイスに対して IP ソース ガード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、すべてのインターフェイスに対して IP ソース ガードはディセーブル。

はじめる前に

DHCP 機能がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet** *slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		特定のインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**[no] ip verify source dhcp-snooping-vlan** 例： `switch(config-if)# ip verify source dhcp-snooping vlan`	インターフェイスの IP ソース ガードをイネーブルにします。 **no** オプションを使用すると、そのインターフェイスの IP ソース ガードがディセーブルになります。
ステップ 4	**show running-config dhcp** 例： `switch(config-if)# show running-config dhcp`	（任意） IP ソース ガードの設定も含めて、DHCP スヌーピングの実行コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

スタティック IP ソース エントリの追加または削除, （226 ページ）

スタティック IP ソース エントリの追加または削除

デバイス上のスタティック IP ソース エントリの追加または削除を実行できます。 デフォルトでは、デバイスにはスタティック IP ソース エントリは設定されていません。

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip source binding** *IP-address MAC-address* **vlan** *vlan-ID* **interface ethernet** *slot*/*port* 例： `switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3`	現在のインターフェイスのスタティック IP ソース エントリを作成します。スタティック IP ソース エントリを削除する場合は、**no** オプションを使用します。
ステップ 3	**show ip dhcp snooping binding** [**interface ethernet** *slot*/*port*] 例： `switch(config)# show ip dhcp snooping binding interface ethernet 2/3`	（任意） スタティック IP ソース エントリを含めて、指定したインターフェイスの IP-MAC アドレス バインディングを表示します。 スタティック エントリは、Type カラムの表示で示されます。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

レイヤ 2 インターフェイスに対する IP ソース ガードのイネーブル化またはディセーブル化, （225 ページ）
IP ソース ガード バインディングの表示, （227 ページ）

IP ソース ガード バインディングの表示

IP-MAC アドレス バインディングを表示するには、**show ip verify source** コマンドを使用します。

IP ソース ガードの設定例

スタティック IP ソース エントリを作成し、インターフェイスの IP ソース ガードをイネーブルにする例を示します。

```
ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3
interface ethernet 2/3
  no shutdown
  ip verify source dhcp-snooping-vlan
```

IP ソース ガードに関する追加情報

関連資料

関連項目	参照先
IP ソース ガード コマンド：完全なコマンド構文、コマンドモード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
DHCP スヌーピングのコマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

第 13 章

コントロール プレーン ポリシングの設定

この章では、Cisco NX-OS デバイスでコントロール プレーン ポリシング（CoPP）を設定する手順を説明します。

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、非管理ポートからスイッチに入力されるすべてのトラフィックに適用されます。ネットワーク デバイスへの一般的な攻撃ベクトルは、過剰なトラフィックがデバイス インターフェイスに転送されるサービス拒絶（DoS）攻撃です。

Cisco NX-OS デバイスは、DoS 攻撃がパフォーマンスに影響しないようにするために CoPP を提供します。 このような攻撃は誤って、または悪意を持って実行される場合があり、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 Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）など、NX-OS デバイスを管理する目的のコンポーネントを実行します。

スーパーバイザ モジュールには、マネージメント プレーンとコントロール プレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。 スーパーバイザモジュールの動作が途絶したり、スーパーバイザ モジュールが攻撃されたりすると、重大なネットワークの停止につながります。 たとえばスーパーバイザに過剰なトラフィックが加わると、スーパーバイザモジュールが過負荷になり、NX-OS デバイス全体のパフォーマンスが低下する可能性があります。 たとえば、スーパーバイザ モジュールに対する DoS 攻撃は、コントロール プレーンに対して非常に高速に IP トラフィック ストリームを生成することがあります。これにより、コントロール プレーンは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

DoS 攻撃の例は次のとおりです。

- インターネット制御メッセージ プロトコル（ICMP）エコー要求
- IP フラグメント
- TCP SYN フラッディング

これらの攻撃によりデバイスのパフォーマンスが影響を受け、次のようなマイナスの結果をもたらします。

- サービス品質の低下（音声、ビデオ、または重要なアプリケーション トラフィックの低下など）
- ルート プロセッサまたはスイッチ プロセッサの高い CPU 使用率
- ルーティング プロトコルのアップデートまたはキープアライブの消失によるルート フラップ
- 不安定なレイヤ 2 トポロジ
- CLI との低速な、または応答を返さない対話型セッション
- メモリやバッファなどのプロセッサ リソースの枯渇
- 着信パケットの無差別のドロップ

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

コントロール プレーンの保護

コントロール プレーンを保護するため、Cisco NX-OS デバイスはコントロール プレーンに向かうさまざまなパケットを異なるクラスに分離します。 クラスの識別が終わると、Cisco NX-OS デバイスはパケットをポリシングします。これにより、スーパーバイザ モジュールに過剰な負担がかからないようになります。

コントロール プレーンのパケット タイプ

コントロール プレーンには、次のような異なるタイプのパケットが到達します。

受信パケット

ルータの宛先アドレスを持つパケット。 宛先アドレスには、レイヤ 2 アドレス（ルータ MAC アドレスなど）やレイヤ 3 アドレス（ルータ インターフェイスの IP アドレスなど）があります。 これらのパケットには、ルータ アップデートとキープアライブ メッセージも含まれます。 ルータが使用するマルチキャスト アドレス宛てに送信されるマルチキャスト パケットも、このカテゴリに入ります。

例外パケット

スーパーバイザ モジュールによる特殊な処理を必要とするパケット。 たとえば、宛先アドレスが Forwarding Information Base（FIB; 転送情報ベース）に存在せず、結果としてミスとなった場合は、スーパーバイザ モジュールが送信側に到達不能パケットを返します。 他には、IP オプションがセットされたパケットもあります。

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。 Dynamic Host Configuration Protocol（DHCP）スヌーピングやダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）インスペクションなどの機能は、パケットをスーパーバイザ モジュールにリダイレクトします。

収集パケット

宛先 IP アドレスのレイヤ 2 MAC アドレスが FIB に存在していない場合は、スーパーバイザ モジュールがパケットを受信し、ARP 要求をそのホストに送信します。

これらのさまざまなパケットはすべて、コントロール プレーンへの悪意ある攻撃に利用され、Cisco NX-OS デバイスに過剰な負荷をかける可能性があります。 CoPP は、これらのパケットを異なるクラスに分類し、これらのパケットをスーパーバイザが受信する速度を個別に制御するメカニズムを提供します。

CoPP の分類

効果的に保護するために、Cisco NX-OS デバイスはスーパーバイザ モジュールに到達するパケットを分類して、パケット タイプに基づいた異なるレート制御ポリシーを適用できるようにします。 たとえば、Hello メッセージなどのプロトコル パケットには厳格さを緩め、IP オプションがセットされているためにスーパーバイザ モジュールに送信されるパケットには厳格さを強めることが考えられます。

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 2 つの異なるメカニズム（ポリシングおよびレート制限）があります。

ハードウェア ポリサーを使用すると、トラフィックが所定の条件に一致する場合、または違反する場合について異なるアクションを定義できます。 このアクションには、パケットの送信、パケットのマーク付け、およびパケットのドロップがあります。

ポリシングには、次のパラメータを設定できます。

認定情報レート（CIR）

ビット レートとして指定する必要な帯域幅。

認定バースト（BC）

指定した時間枠内に CIR を超過する可能性があるが、スケジューリングには影響を与えないトラフィック バーストのサイズ。

CoPP クラス マップ

次の表に、使用可能なクラス マップとその設定を示します。

表 *20*：クラス マップの設定および説明

クラス マップ	設定	説明
class-map type control-plane match-any copp-system-class-arp	match protocol arp match protocol nd	クラスは、すべての ARP パケットに一致します。 クラスは、すべての ARP パケットおよび ND（NA、NS、RA および RS）パケットに一致します。
class-map type control-plane match-any copp-system-class-bgp	match protocol bgp	クラスはすべての BGP パケットに一致します。
class-map type control-plane match-any copp-system-class-bridging	match protocol bridging	クラスはすべての STP および RSTP フレームに一致します。
class-map type control-plane match-any copp-system-class-cdp	match protocol cdp	クラスはすべての CDP フレームに一致します。
class-map type control-plane match-any copp-system-class-default	match protocol default	クラスはすべてのフレームに一致します。 デフォルト ポリサーに使用します。
class-map type control-plane match-any copp-system-class-dhcp	match protocol dhcp	クラスは、すべての IPv4 DHCP パケットに一致します クラスは、すべての両方の IPv4 DHCP パケットに一致します
class-map type control-plane match-any copp-system-class-eigrp	match protocol eigrp match protocol eigrp6	クラスは、すべての IPv4 EIGRP パケットに一致します。 クラスは、IPv4 EIGRP パケットと IPv6 EIGRP パケットの両方に一致します。
class-map type control-plane match-any copp-system-class-exception	match protocol exception	Martian 宛先アドレスを持つパケットまたは MTU エラーが発生したパケットなど、クラスは IP ルーティングの目的で例外パケットとして扱われるすべての IP パケットに一致します（TTL 例外、IP フラグメント例外、および同一インターフェイス例外のパケットを除く）。

クラス マップ	設定	説明
class-map type control-plane match-any copp-system-class-excp-ip-frag	match protocol ip_frag	クラスはフラグメント化したすべての IP パケットに一致します。（これらのパケットは、IP ルーティングの観点から例外パケットとして扱われます）。
class-map type control-plane match-any copp-system-class-excp-same-if	match protocol same-if	クラスは、IP ルーティングの例外パケットとして扱われるすべての IP パケットに一致します。パケットが一致するのは、宛先とすべきインターフェイスから受信したためです。
class-map type control-plane match-any copp-system-class-excp-ttl	match protocol ttl	クラスは、IP ルーティングの観点から TTL 例外パケットとして扱われる（TTL が 0 の場合）すべてのパケットに一致します。
class-map type control-plane match-any copp-system-class-fip	match protocol fip	クラスは FCoE Initialization Protocol に属するすべてのパケットに一致します。
class-map type control-plane match-any copp-system-class-glean	match protocol glean	クラスは、宛先の MAC 情報が使用不可能であるためにネクスト ホップにルーティングできないすべての IP パケットに一致します。
class-map type control-plane match-any copp-system-class-hsrp-vrrp	match protocol hsrp_vrrp match protocol hsrp6	クラスは、HSRP パケットおよび VRRP パケットに一致します。 クラスは、IPv4 HSRP、VRRP、および IPv6 HSRP パケットに一致します
class-map type control-plane match-any copp-system-class-icmp-echo	match protocol icmp_echo	クラスは、すべての ICMP エコー（ping）パケットに一致します。
class-map type control-plane match-any copp-system-class-igmp	match protocol igmp	クラスはすべての IGMP パケットに一致します。

クラス マップ	設定	説明
class-map type control-plane match-any copp-system-class-isis	match protocol isis_dce	クラスはすべての ISIS プロトコル パケットに一致します。
class-map type control-plane match-any copp-system-class-l3dest-miss	match protocol unicast	クラスはFIBで宛先が見つからなかったすべてのユニキャスト ルーティングされたパケットに一致します。
class-map type control-plane match-any copp-system-class-lacp	match protocol lacp	クラスは、すべてのリンク アグリゲーション制御プロトコル（LACP）フレームに一致します。
class-map type control-plane match-any copp-system-class-lldp	match protocol lldp_dcx	クラスはすべてのLLDPフレームに一致します。
class-map type control-plane match-any copp-system-class-mcast-miss	match protocol multicast	クラスは、FIBにエントリがないためにルーティングできなかったすべての IP マルチキャスト フレームに一致します。
class-map type control-plane match-any copp-system-class-mgmt	match protocol mgmt	クラスは、SNMP、HTTP、NTP、Telnet、SSH など、管理に関連するすべてのフレームに一致します。
class-map type control-plane match-any copp-system-class-msdp	match protocol msdp	クラスは MSDP パケットに一致します。
class-map type control-plane match-any copp-system-class-ospf	match protocol ospf match protocol ospfv3	クラスは、OSPF パケットおよびOSPFv3プロトコルパケットに一致します。
class-map type control-plane match-any copp-system-class-pim-hello	match protocol pim	クラスはすべての PIM Hello パケットに一致します。
class-map type control-plane match-any copp-system-class-pim-register	match protocol reg	クラスはすべての PIM 登録パケットに一致します。
class-map type control-plane match-any copp-system-class-rip	match protocol rip	クラスはすべてのRIPパケットに一致します。

クラス マップ	設定	説明
class-map type control-plane match-any copp-system-class-udld	match protocol udld	クラスはすべてのUDLDフレームに一致します。

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、DoS 攻撃からスーパーバイザ モジュールを保護するためのデフォルトの copp-system-policy が Cisco NX-OS ソフトウェアによりインストールされます。最初のセットアップ ユーティリティで、次のいずれかの CoPP ポリシー オプションを選択することにより、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。

- デフォルト CoPP ポリシー（copp-system-policy-default）。
- 拡張レイヤ 2 CoPP ポリシー（copp-system-policy-scaled-l2）。
- 拡張レイヤ 3 CoPP ポリシー（copp-system-policy-scaled-l3）。
- カスタマイズされた CoPP ポリシー（copp-system-policy-customized）。

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。 このデフォルト ポリシーから開始して、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-default 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 Access Control List（ACL; アクセス コントロール リスト）を追加する必要があります。

コントロール プレーン コンフィギュレーション モードで **service-policy input** *policy-name* コマンドを使用して、使用する CoPP ポリシーを変更できます。

デフォルト CoPP ポリシー

copp-system-policy-default ポリシーが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、またはこれに関連付けられたクラスマップを変更することはできません。また、このポリシーのクラス マップ設定も変更できません。

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy-default
    class copp-system-class-igmp
      police cir 1024 kbps bc 65535 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 1024 kbps bc 3600000 bytes
    class copp-system-class-dhcp
```

```
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-mgmt
    police cir 12000 kbps bc 4800000 bytes
  class copp-system-class-lacp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-lldp
    police cir 2048 kbps bc 4800000 bytes
  class copp-system-class-udld
    police cir 2048 kbps bc 4800000 bytes
  class copp-system-class-isis
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-msdp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-cdp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-fip
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-bgp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-eigrp
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-exception
    police cir 64 kbps bc 4800000 bytes
  class copp-system-class-glean
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-hsrp-vrrp
    police cir 1024 kbps bc 4800000 bytes
  class copp-system-class-icmp-echo
    police cir 64 kbps bc 3600000 bytes
  class copp-system-class-ospf
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-pim-register
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-rip
    police cir 9600 kbps bc 4800000 bytes
  class copp-system-class-l3dest-miss
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-mcast-miss
    police cir 256 kbps bc 3200000 bytes
  class copp-system-class-excp-ip-frag
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-excp-same-if
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-excp-ttl
    police cir 64 kbps bc 3200000 bytes
  class copp-system-class-default
    police cir 2048 kbps bc 6400000 bytes
```

拡張レイヤ 2 CoPP ポリシー

copp-system-policy-scaled ポリシーには、デフォルト ポリシーと同じポリサー レートのほとんどのクラスがあります。 ただし、IGMP と ISIS に対しては、より高いポリサー レートが設定されています。 このポリシー、またはこれに関連付けられたクラスマップを変更することはできません。また、このポリシーのクラス マップ設定も変更できません。

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy-scaled-l2
    class copp-system-class-igmp
      police cir 4096 kbps bc 264000 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 1024 kbps bc 3600000 bytes
    class copp-system-class-dhcp
```

```
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-mgmt
  police cir 12000 kbps bc 4800000 bytes
class copp-system-class-lacp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-lldp
  police cir 2048 kbps bc 4800000 bytes
class copp-system-class-udld
  police cir 2048 kbps bc 4800000 bytes
class copp-system-class-isis
  police cir 2048 kbps bc 4800000 bytes
class copp-system-class-msdp
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-cdp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-fip
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-bgp
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-eigrp
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-exception
  police cir 64 kbps bc 4800000 bytes
class copp-system-class-glean
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-hsrp-vrrp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-icmp-echo
  police cir 64 kbps bc 3600000 bytes
class copp-system-class-ospf
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-pim-register
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-rip
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-l3dest-miss
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-mcast-miss
  police cir 256 kbps bc 3200000 bytes
class copp-system-class-excp-ip-frag
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-same-if
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-ttl
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-default
  police cir 2048 kbps bc 6400000 bytes
```

拡張レイヤ 3 CoPP ポリシー

copp-system-policy-scaled-l3 ポリシーには、デフォルト ポリシーと同じポリサー レートのほとんどのクラスがあります。 ただし、IGMP、ICMP エコー、ISIS、マルチキャスト欠落、および Glean に関連するクラスに対しては、より高いポリサー レートが設定されています。 このポリシー、またはこれに関連付けられたクラスマップを変更することはできません。また、このポリシーのクラス マップ設定も変更できません。

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy-scaled-l3
    class copp-system-class-igmp
      police cir 4096 kbps bc 264000 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
```

```
  police cir 4000 kbps bc 3600000 bytes
class copp-system-class-dhcp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-mgmt
  police cir 12000 kbps bc 4800000 bytes
class copp-system-class-lacp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-lldp
  police cir 2048 kbps bc 4800000 bytes
class copp-system-class-udld
  police cir 2048 kbps bc 4800000 bytes
class copp-system-class-isis
  police cir 2048 kbps bc 4800000 bytes
class copp-system-class-msdp
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-cdp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-fip
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-bgp
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-eigrp
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-exception
  police cir 64 kbps bc 4800000 bytes
class copp-system-class-glean
  police cir 4000 kbps bc 4800000 bytes
class copp-system-class-hsrp-vrrp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-icmp-echo
  police cir 4000 kbps bc 3600000 bytes
class copp-system-class-ospf
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-pim-register
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-rip
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-l3dest-miss
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-mcast-miss
  police cir 4000 kbps bc 3200000 bytes
class copp-system-class-excp-ip-frag
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-same-if
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-ttl
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-default
  police cir 2048 kbps bc 6400000 bytes
```

カスタマイズ可能な CoPP ポリシー

copp-system-policy-customized ポリシーは、デフォルト ポリシーと同様に設定され、別のクラス マップ情報のレートとバースト サイズ向けにカスタマイズできます。

このポリシーに設定されているクラス マップを追加または削除することはできません。

重要 このポリシーは上級ユーザ用です。 このポリシーを設定する場合は細心の注意を払い、実稼働ネットワークに導入する前に幅広いテストを行うことを推奨します。

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy-customized
```

```
class copp-system-class-igmp
  police cir 1024 kbps bc 65535 bytes
class copp-system-class-pim-hello
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-bridging
  police cir 20000 kbps bc 4800000 bytes
class copp-system-class-arp
  police cir 1024 kbps bc 3600000 bytes
class copp-system-class-dhcp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-mgmt
  police cir 12000 kbps bc 4800000 bytes
class copp-system-class-lacp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-lldp
  police cir 2048 kbps bc 4800000 bytes
class copp-system-class-udld
  police cir 2048 kbps bc 4800000 bytes
class copp-system-class-isis
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-msdp
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-cdp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-fip
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-bgp
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-eigrp
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-exception
  police cir 64 kbps bc 4800000 bytes
class copp-system-class-glean
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-hsrp-vrrp
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-icmp-echo
  police cir 64 kbps bc 3600000 bytes
class copp-system-class-ospf
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-pim-register
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-rip
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-l3dest-miss
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-mcast-miss
  police cir 256 kbps bc 3200000 bytes
class copp-system-class-excp-ip-frag
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-same-if
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-ttl
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-default
  police cir 2048 kbps bc 6400000 bytes
```

CoPP と管理インターフェイス

Cisco NX-OS デバイスは、管理インターフェイス（mgmt0）をサポートしないハードウェア ベースの CoPP だけをサポートします。 アウトオブバンド mgmt0 インターフェイスは CPU に直接接続するため、CoPP が実装されているインバンド トラフィック ハードウェアは通過しません。

mgmt0 インターフェイスで、ACL を設定して、特定タイプのトラフィックへのアクセスを許可または拒否することができます。

CoPP のライセンス要件

この機能にはライセンスは不要です。ライセンスパッケージに含まれていない機能はすべてCisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

CoPP の注意事項と制約事項

CoPP は、スイッチではデフォルトでイネーブルになっている機能です。 CoPP をイネーブルまたはディセーブルにすることはできません。

- 一度に 1 つのコントロール プレーン ポリシーだけを適用できます。
- CoPP ポリシーを削除すると、デフォルト CoPP ポリシーが適用されます。 このようにして、CoPP ポリシーが常に適用されます。
- クラスまたはポリシーの追加や削除はできません。
- クラスの順序の変更や、ポリシーのクラスの削除はできません。
- デフォルト、拡張レイヤ 2、または拡張レイヤ 3 ポリシーは変更できません。 ただし、カスタマイズされたポリシー内のクラスの情報レートやバースト サイズを変更することは可能です。
- カスタマイズされたポリシーが変更されていない限り、カスタマイズされたポリシー設定はデフォルトのポリシー設定と同じです。
- 以前のリリースからアップグレードしている場合は、デフォルト CoPP ポリシーがスイッチ上でデフォルトでイネーブルになります。
- カスタマイズされたポリシーを変更するか、または適用されたポリシーを変更すると、統計情報カウンタがリセットされます。
- ISSU を実行すると、統計情報カウンタがリセットされます。
- 最初にデフォルト CoPP ポリシーを使用した後、データセンターおよびアプリケーションの要件に基づいて、どの CoPP ポリシーを使用するかを後で決定することを推奨します。
- CoPP のカスタマイズは継続的なプロセスです。 CoPP は、特定の環境で使用されているプロトコルや機能のほか、サーバ環境に必要なスーパーバイザ機能に従って設定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。
- CoPP を継続的にモニタすることを推奨します。 ドロップが発生した場合は、CoPP がトラフィックを誤ってドロップしたのか、または誤動作や攻撃に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された 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。
- 他のクラスマップで指定しないトラフィックはすべて、最後のクラス（デフォルト クラス）に配置されます。

- Cisco NX-OS ソフトウェアは、出力 CoPP とサイレント モードをサポートしません。 CoPP は、入力でのみサポートされます（コントロール プレーン インターフェイスに対して **service-policy output copp** コマンドは使用できません）。

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

CoPP のデフォルト設定

次の表に、CoPP パラメータのデフォルト設定を示します。

表 *21*：*CoPP* パラメータのデフォルト設定

パラメータ	デフォルト
デフォルト ポリシー	copp-system-policy-default

CoPP の設定

スイッチへの CoPP ポリシーの適用

スイッチに次の CoPP ポリシーの 1 つを適用することができます。

- デフォルト CoPP ポリシー（copp-system-policy-default）。
- 拡張レイヤ 2 CoPP ポリシー（copp-system-policy-scaled-l2）。
- 拡張レイヤ 3 CoPP ポリシー（copp-system-policy-scaled-l3）。
- カスタマイズされた CoPP ポリシー（copp-system-policy-customized）。

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) # **control-plane**	control-plane モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-cp) # **service-policy input** *policy-map-name*	指定された CoPP ポリシー マップを適用します。*policy-map-name* には、copp-system-policy-default、copp-system-policy-scaled-l2、copp-system-policy-scaled-l3、または copp-system-policy-customized が適用可能です。
ステップ 4	switch(config-cp) # **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、変更を永続的に保存します。

次に、デバイスに CoPP ポリシーを適用する例を示します。

```
switch# configure terminal
switch(config)# control-plane
switch(config-cp) # service-policy input copp-system-policy-default
switch(config-cp) # copy running-config startup-config
```

カスタマイズされた CoPP ポリシーの変更

このポリシーに設定されたクラス マップの情報レートおよびバースト サイズだけを変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **policy-map type control-plane copp-system-policy-customized**	カスタマイズされた CoPP ポリシー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-pmap)# **class** *class-map-name*	定義済みポリシーの任意の CoPP にリスト表示された 28 の定義済みクラス マップのうちの 1 つを指定します。
ステップ 4	switch(config-pmap-c)# **police cir** *rate-value* **kbps bc** *buffer-size* **bytes**	認定情報レート（CIR）および認定バースト サイズ（BC）を設定します。 cir に指定できる範囲は 1 ～ 20480 です。 bc に指定できる範囲は 1500 ～ 6400000 です。
ステップ 5	switch(config-pmap-c) # **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

	コマンドまたはアクション	目的
		ションにコピーして、変更を永続的に保存します。

次に、カスタマイズされた CoPP ポリシーを変更する例を示します。

```
switch(config)# policy-map type control-plane copp-system-policy-customized
switch(config-pmap)# class copp-system-class-bridging
switch(config-pmap-c)# police cir 10000 kbps bc 2400000 bytes
```

CoPP の設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	関連するクラス マップのあるコントロール プレーン ポリシー マップを表示します。
show policy-map interface control-plane	ポリシーの値と関連するクラスマップ、およびポリシーごとまたはクラスマップごとのドロップが表示されます。
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。

CoPP 設定ステータスの表示

手順

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

次に、CoPP 設定ステータスを表示する例を示します。

```
switch# show copp status
```

CoPP のモニタ

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show policy-map interface control-plane**	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。 一致した、および違反したパケット カウンタなど。 統計情報は、OutPackets（コントロール プレーンに対して許可されたパケット）と DropPackets（レート制限によってドロップされたパケット）に関して指定します。

次に、CoPP をモニタする例を示します。

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

service-policy input: copp-system-policy-default

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

CoPP 統計情報のクリア

手順

	コマンドまたはアクション	目的
ステップ 1	switch#**show policy-map interface control-plane**	（任意） 現在適用されている CoPP ポリシーおよびクラスごとの統計情報を表示します。
ステップ 2	switch# **clear copp statistics**	CoPP 統計情報をクリアします。

次に、インターフェース環境で、CoPP 統計情報をクリアする例を示します。

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

CoPP に関する追加情報

ここでは、CoPP の実装に関する追加情報について説明します。

関連資料

関連項目	参照先
ライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 5000 Series NX-OS Security Command Reference*』

CoPP の機能の履歴

表 *22* : *CoPP* の機能の履歴

機能名	機能情報
CoPP	5.1(3)N1(1) で導入
CoPP	5.2(1)N1(1) での追加の IPv6 サポート

索 引

A

C

D

I

L

M

R

S

T

V

あ

か

き

く

け

こ

さ

し

せ

た