Cisco Nexus 3548 スイッチ NX-OS リリース 6.x セキュリティ コンフィギュレーション ガイド

初版：2013 年 05 月 21 日

最終更新：2016 年 05 月 31 日

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

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

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

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

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

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

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

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

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

© 2013-2016 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xiii

対象読者 xiii

表記法 xiii

マニュアルに関するフィードバック xv

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

概要 3

Authentication, Authorization, and Accounting（認証、許可、およびアカウンティング） 3

RADIUS および TACACS+ セキュリティ プロトコル 4

SSH および Telnet 5

IP ACL 5

認証、許可、アカウンティングの設定 7

AAA の概要 7

AAA セキュリティ サービス 7

AAA を使用する利点 8

リモート AAA サービス 8

AAA サーバ グループ 9

AAA サービス設定オプション 9

ユーザ ログインの認証および許可プロセス 10

リモート AAA の前提条件 12

AAA の注意事項と制約事項 12

AAA の設定 12

コンソール ログイン認証方式の設定 12

デフォルトのログイン認証方式の設定 14

ログイン認証失敗メッセージのイネーブル化 15

AAA コマンド許可の設定 15

MSCHAP 認証のイネーブル化 17
デフォルトの AAA アカウンティング方式の設定 19
AAA サーバの VSA の使用 20
VSA 20
VSA の形式 21
AAA サーバ上でのスイッチのユーザ ロールと SNMPv3 パラメータの指定 21
ローカル AAA アカウンティング ログのモニタリングとクリア 22
AAA 設定の確認 22
AAA の設定例 23
デフォルトの AAA 設定 23
RADIUS の設定 25
RADIUS の設定 25
RADIUS の概要 25
RADIUS ネットワーク環境 25
RADIUS の操作について 26
RADIUS サーバのモニタリング 27
ベンダー固有属性 27
RADIUS の前提条件 28
RADIUS の注意事項と制約事項 28
RADIUS サーバの設定 28
RADIUS サーバ ホストの設定 29
RADIUS のグローバルな事前共有キーの設定 30
RADIUS サーバの事前共有キーの設定 31
RADIUS サーバ グループの設定 32
RADIUS サーバ グループのためのグローバル発信元インターフェイスの設定 33
ログイン時にユーザによる RADIUS サーバの指定を許可 34
グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定 35
サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定 36
RADIUS サーバのアカウンティングおよび認証属性の設定 37
RADIUS サーバの定期的モニタリングの設定 38
デッド タイム間隔の設定 39

RADIUS サーバまたはサーバ グループの手動モニタリング 40
RADIUS 設定の確認 41
RADIUS サーバ統計情報の表示 41
RADIUS サーバ統計情報のクリア 41
RADIUS の設定例 41
RADIUS のデフォルト設定 42
TACACS+ の設定 43
TACACS+ の設定について 43
TACACS+ の設定に関する情報 43
TACACS+ の利点 43
TACACS+ を使用したユーザ ログイン 44
デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー 45
TACACS+ サーバのコマンド許可サポート 45
TACACS+ サーバのモニタリング 45
TACACS+ の前提条件 46
TACACS+ の注意事項と制約事項 46
TACACS+ の設定 47
TACACS+ サーバの設定プロセス 47
TACACS+ のイネーブル化 47
TACACS+ サーバ ホストの設定 48
TACACS+ のグローバルな事前共有キーの設定 49
TACACS+ サーバの事前共有キーの設定 50
TACACS+ サーバ グループの設定 50
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 52
ログイン時の TACACS+ サーバの指定 53
TACACS+ サーバでの AAA 許可の設定 53
TACACS+ サーバでのコマンド許可の設定 55
TACACS+ サーバでのコマンド許可のテスト 56
コマンド許可検証のイネーブル化とディセーブル化 57
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 57
権限ロールのユーザ コマンドの許可または拒否 59

グローバルな TACACS+ タイムアウト間隔の設定 60
サーバのタイムアウト間隔の設定 61
TCP ポートの設定 62
TACACS+ サーバの定期的モニタリングの設定 63
デッド タイム間隔の設定 64
TACACS+ サーバまたはサーバ グループの手動モニタリング 65
TACACS+ のディセーブル化 65
TACACS+ 統計情報の表示 66
TACACS+ の設定の確認 66
TACACS+ の設定例 66
TACACS+ のデフォルト設定 67
SSH および Telnet の設定 69
SSH および Telnet の設定 69
SSH および Telnet の概要 69
SSH サーバ 69
SSH クライアント 69
SSH サーバ キー 70
Telnet サーバ 70
SSH の注意事項および制約事項 70
SSH の設定 71
SSH サーバ キーの生成 71
ユーザ アカウント用 SSH 公開キーの指定 71
Open SSH 形式による SSH 公開キーの指定 72
IETF SECSH 形式による SSH 公開キーの指定 72
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 73
リモート デバイスとの SSH セッションの開始 74
SSH ホストのクリア 74
SSH サーバのディセーブル化 75
SSH サーバ キーの削除 75
SSH セッションのクリア 76
SSH の設定例 76

Telnet の設定 77
Telnet サーバのディセーブル化 77
Telnet サーバの再イネーブル化 78
リモート デバイスとの Telnet セッションの開始 78
Telnet セッションのクリア 78
SSH および Telnet の設定の確認 79
SSH のデフォルト設定 79
アクセス コントロール リストの設定 81
ACL の概要 81
IP ACL のタイプと適用 82
適用順序 83
ルール 83
送信元と宛先 83
プロトコル 83
暗黙のルール 83
その他のフィルタリング オプション 84
シーケンス番号 84
論理演算子と論理演算ユニット 85
ACL TCAM リージョン 86
ACL のライセンス要件 87
ACL の前提条件 87
ACL の注意事項と制約事項 87
デフォルトの ACL 設定 88
IP ACL の設定 89
IP ACL の作成 89
IP ACL の変更 90
IP ACL の削除 91
IP ACL 内のシーケンス番号の変更 92
mgmt0 への IP-ACL の適用 92
ポート ACL としての IP ACL の適用 93
ルータ ACL としての IP ACL の適用 94
IP ACL の設定の確認 95

IP ACL の統計情報のモニタリングとクリア 96
VLAN ACL の概要 96
VACL とアクセス マップ 96
VACL とアクション 96
統計情報 97
VACL の設定 97
VACL の作成または変更 97
VACL の削除 98
VACL の VLAN への適用 98
VACL の設定の確認 99
VACL 統計情報の表示と消去 99
VACL の設定例 100
ACL TCAM リージョン サイズの設定 100
デフォルトの TCAM リージョン サイズに戻す 102
仮想端末回線の ACL の設定 103
VTY 回線の ACL の確認 104
VTY 回線の ACL の設定例 104
DHCP スヌーピングの設定 107
DHCP スヌーピングの概要 107
機能のイネーブル化とグローバルなイネーブル化 108
信頼できる送信元と信頼できない送信元 109
DHCP スヌーピング バインディング データベース 109
DHCP リレー エージェントの概要 110
DHCP リレー エージェント 110
DHCP リレー エージェントに対する VRF サポート 110
DHCP リレー バインディング データベース 111
DHCP スヌーピングのライセンス要件 111
DHCP スヌーピングの前提条件 112
DHCP スヌーピングの注意事項および制約事項 112
DHCP スヌーピングのデフォルト設定 112
DHCP スヌーピングの設定 113
DHCP スヌーピングの最小設定 113

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 114
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 114
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 115
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 116
Option 82 ユーザ定義データの挿入および削除のイネーブル化またはディセーブル化 117
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 118
インターフェイスの信頼状態の設定 119
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 120
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 121
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 122
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 124
インターフェイスへの DHCP サーバ アドレスの設定 125
DHCP スタティック バインディングの作成 127
DHCP スヌーピング設定の確認 128
DHCP バインディングの表示 128
DHCP スヌーピング バインディング データベースのクリア 129
DHCP リレー統計情報のクリア 130
DHCP のモニタリング 130
DHCP スヌーピングの設定例 130
MAC ACL の設定 133
MAC ACL の概要 133
MAC パケット分類 133
MAC ACL のデフォルト設定 134
MAC ACL の設定 134
MAC ACL の作成 134
MAC ACL の変更 135
MAC ACL 内のシーケンス番号の変更 137
MAC ACL の削除 138

ポート ACL としての MAC ACL の適用 139
MAC パケット分類のイネーブル化またはディセーブル化 141
MAC ACL の設定の確認 142
MAC ACL 統計情報のクリア 142
ユニキャスト RPF の設定 143
ユニキャスト RPF の概要 143
Unicast RPF 144
Global Statistics 144
ユニキャスト RPF のライセンス要件 145
ユニキャスト RPF の注意事項と制約事項 145
ユニキャスト RPF のデフォルト設定 146
ユニキャスト RPF の設定 146
ユニキャスト RPF の設定例 148
ユニキャスト RPF の設定の確認 148
コントロール プレーン ポリシングの設定 149
CoPP の概要 150
コントロール プレーン保護 151
コントロール プレーンのパケット タイプ 151
CoPP の分類 152
レート制御メカニズム 152
CoPP ポリシー テンプレート 153
デフォルト CoPP ポリシー 153
レイヤ 2 CoPP ポリシー 154
レイヤ 3 CoPP ポリシー 156
CoPP クラス マップ 157
1 秒間あたりのパケットのクレジット制限 157
CoPP と管理インターフェイス 157
CoPP のライセンス要件 158
CoPP の注意事項と制約事項 158
CoPP のアップグレードに関する注意事項 159
CoPP の設定 160
コントロール プレーン クラス マップの設定 160
コントロール プレーン ポリシー マップの設定 161

コントロール プレーン サービス ポリシーの設定 163
CoPP show コマンド 163
CoPP 設定ステータスの表示 165
CoPP のモニタリング 165
CoPP 統計情報のクリア 166
CoPP の設定例 166
CoPP の設定例 168
例：セットアップ ユーティリティによるデフォルト CoPP ポリシーの変更または再適用 170

はじめに

ここでは、次の項について説明します。

- 対象読者，xiii ページ
- 表記法，xiii ページ
- マニュアルに関するフィードバック，xv ページ

対象読者

このマニュアルは、Cisco Nexus デバイスのコンフィギュレーションおよびメンテナンスを担当するネットワーク管理者を対象としています。

表記法

（注） お客様のニーズを満たすためにドキュメントを更新するという継続的な取り組みの一環として、シスコでは設定タスクの文書化方法を変更しました。そのため、本ドキュメントには、従来とは異なるスタイルでの設定タスクが説明されている部分もあります。ドキュメントに新たに組み込まれるようになったセクションには、以下のセクションが含まれます。

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。

表記法	説明
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、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に記載されていない参照資料を紹介しています。

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。

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（ciscodfa-docfeedback@cisco.com）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。

第 1 章

新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

- 新機能および変更された機能に関する情報，1 ページ

新機能および変更された機能に関する情報

次の表では、このコンフィギュレーション ガイドでの重要な変更点の概要を示します。この表は、このマニュアルのすべての変更点、または特定のリリースのすべての新機能をまとめたリストではありません。

表 *1*：新機能

機能	説明	リリース	参照先
DHCP スヌーピング	ユーザ定義データの挿入および削除のための Option 82 のイネーブル化またはディセーブル化のサポートが追加されました。	6.0(2)A8(1)	Option 82 ユーザ定義データの挿入および削除のイネーブル化またはディセーブル化，（117 ページ）
ユニキャスト RPF の設定	Cisco NX-OS デバイス上で出力トラフィックのレート制限を設定する手順について説明します。	6.0(2)A7(1)	ユニキャスト RPF の概要，（143 ページ）

新機能および変更された機能に関する情報

機能	説明	リリース	参照先
MAC ACL	MAC ACL は、パケットのレイヤ 2 ヘッダーを使用してトラフィックをフィルタリングする ACL です。バーチャライゼーションのサポートなど、MAC ACL の基本的な機能の多くは IP ACL と共通です。Cisco NX-OS Release 6.0(2)A4(1) では、Cisco Nexus 3500 シリーズ スイッチで MAC ACL のサポートが導入されています。	6.0(2)A4(1)	MAC ACL の概要, （133 ページ）
スタティック NAT	この章は削除されてダイナミック NAT 機能と統合されました。		『Cisco Nexus 3548 Switch NX-OS Interfaces Configuration Guide, Release 6.0(2)A1(1)』

第 2 章

概要

この章の内容は、次のとおりです。

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

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

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

認証

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

許可

ワンタイム許可またはサービスごとの許可、ユーザ単位のアカウント リストとプロファイル、ユーザ グループ サポート、および IP、IPX、ARA、Telnet のサポートなど、リモート アクセスの制御方法を提供します。
RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てることで機能します。これらの属性とデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制限事項が決定されます。

アカウンティング

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

（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。

RADIUS および TACACS+ セキュリティ プロトコル

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

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

RADIUS

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

TACACS+

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

SSH および Telnet

セキュア シェル（SSH）サーバを使用すると、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。

IP ACL

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

第 3 章

認証、許可、アカウンティングの設定

この章の内容は、次のとおりです。

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

AAA の概要

AAA セキュリティ サービス

認証、許可、アカウンティング（AAA）機能では、Cisco Nexus デバイスを管理するユーザの ID 確認、アクセス権付与、およびアクション追跡を実行できます。Cisco Nexus デバイスは、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control device Plus（TACACS+）プロトコルをサポートします。

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

リモート AAA サービス

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

- ファブリック内の各スイッチに関するユーザ パスワード リストを簡単に管理できます。
- AAA サーバはすでに企業内に幅広く導入されており、簡単に AAA サービスに使用できます。
- ファブリック内のすべてのスイッチのアカウンティング ログを集中管理できます。
- スイッチ上のローカルデータベースを使用する方法に比べて、ファブリック内の各スイッチのユーザ属性は管理が簡単です。

AAA 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 オプションには障害が発生しているものと見なされます。必要に応じて、複数のサーバ グループを指定できます。スイッチが最初のグループ内のサーバからエラーを受信すると、次のサーバ グループのサーバが試行されます。

AAA サービス設定オプション

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

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

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 デバイスは、設定されている RADIUS サーバのグローバル プールから、設定された順序で RADIUS サーバを選択します。このグローバル プールからのサーバは、Cisco Nexus デバイス上の RADIUS サーバ グループ内で選択的に設定できるサーバです。

次の表に、AAA サービスに対して設定できる AAA 認証方式を示します。

表 *3*：*AAA* サービスの *AAA* 認証方式

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

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

ユーザ ログインの認証および許可プロセス

ユーザ ログインの認証および許可プロセスは、次のように実行されます。

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

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

  設定されているすべての認証方式が失敗した場合、ローカルデータベースを使用して認証が実行されます。

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

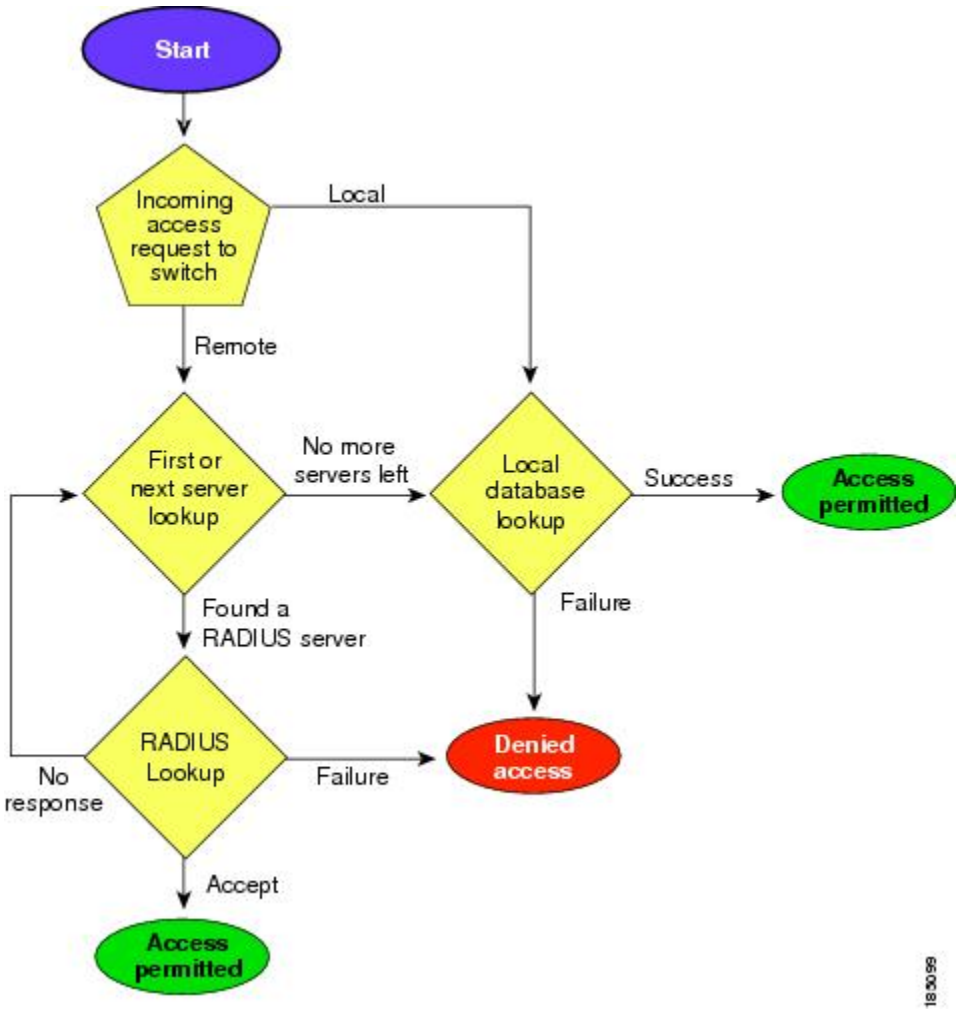
AAA サーバ プロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザ ロールが認証応答とともにダウンロードされます。

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

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

次の図に、認証および許可プロセスのフロー チャートを示します。

図 *1*：ユーザ ログインの認証および許可のフロー



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

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

リモート AAA の前提条件

リモート AAA サーバには、次の前提条件があります。

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

AAA の注意事項と制約事項

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

注意 すべて数字のユーザ名でユーザ アカウントを作成しないでください。

AAA の設定

コンソール ログイン認証方式の設定

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS サーバまたは TACACS+ サーバの名前付きサブセット
- Cisco Nexus デバイス上のローカル データベース
- ユーザ名のみ（**none**）

デフォルトの方式は、ローカルです。

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login console** {**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** を指定すると、RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group* を指定すると、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが認証に使用されます。 **local** 方式では、ローカル データベースが認証に使用されます。**none** 方式では、ユーザ名のみが使用されます。 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**	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa authentication**	（任意） コンソール ログイン認証方式の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、コンソール ログインの認証方式を設定する例を示します。

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

デフォルトのログイン認証方式の設定

デフォルトの方式は、ローカルです。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login default** {**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** を指定すると、RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group* を指定すると、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが認証に使用されます。 **local** 方式では、ローカル データベースが認証に使用されます。**none** 方式では、ユーザ名のみが使用されます。 デフォルトのログイン方式は **local** です。これは、方式が一切設定されていない場合、および設定済みのどの方式でも応答が得られなかった場合に使用されます。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show aaa authentication**	（任意） デフォルトのログイン認証方式の設定を表示します。

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

ログイン認証失敗メッセージのイネーブル化

ユーザがログインして、リモート AAA サーバが応答しなかった場合は、ローカル ユーザ データベースによってログインが処理されます。ログイン失敗メッセージの表示をイネーブルにしていた場合は、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**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login error-enable**	ログイン認証失敗メッセージをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show aaa authentication**	（任意） ログイン失敗メッセージの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

AAA コマンド許可の設定

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

許可方式には、次のものがあります。

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

デフォルトの方式は、Local です。

（注） コンソール セッションでの認証は、Cisco Nexus 5000 プラットフォームではサポートされません。Cisco Nexus 5500 プラットフォーム リリース 6.x 以降ではサポートされています。

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 コマンドの許可には、**config-commands** キーワードを使用します。
		許可方式を指定するには、**group**、**local**、または **none** キーワードを使用します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MSCHAP 認証のイネーブル化

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

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

次の表に、MSCHAP に必要な RADIUS VSA を示します。

表 *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**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login mschap enable**	MS-CHAP 認証をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show aaa authentication login mschap**	（任意） MS-CHAP 設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの AAA アカウンティング方式の設定

Cisco Nexus デバイスは、アカウンティングに TACACS+ 方式と RADIUS 方式をサポートします。スイッチは、ユーザ 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 デバイスは、これらの属性をアカウンティング レコードとして報告します。そのアカウンティング レコードは、セキュリティ サーバ上のアカウンティング ログに格納されます。

特定のアカウンティング方式を定義するデフォルト方式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**	グローバル コ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** を指定すると、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* を指定すると、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットがアカウン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。 デフォルトの方式は **local** です。サーバ グループが設定されていないとき、または設定済みのすべてのサーバ グループから応答がないときに、このデフォルト方式が使用されます。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show aaa accounting**	（任意） デフォルトの AAA アカウン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 デバイスのユーザ ロールおよび SNMPv3 パラメータを指定できます。

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間での VSA の通信のための方式を規定する標準を作成しています。IETF は属性 26 を使用します。ベンダーはVSAを使用して、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。値は次の形式のストリングです。

```
protocol : attribute seperator value *
```

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

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

VSA の形式

次の VSA プロトコル オプションが、Cisco Nexus デバイスでサポートされています。

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

次の属性がCisco Nexus デバイスでサポートされています。

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

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

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

```
shell:roles="roleA roleB …"
```

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

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

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

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

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

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

ローカルAAAアカウンティングログのモニタリングとクリア

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

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。

コマンド	目的
show aaa accounting	AAA アカウンティングの設定を表示します。
show aaa authentication [**login** {**error-enable** | **mschap**}]	AAA 認証情報を表示します。
show aaa authorization	AAA 許可の情報を表示します。
show aaa groups	AAA サーバ グループの設定を表示します。
show running-config aaa [**all**]	実行コンフィギュレーションの AAA 設定を表示します。
show startup-config aaa	スタートアップ コンフィギュレーションのAAA設定を表示します。

AAA の設定例

次に、AAA を設定する例を示します。

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

デフォルトの AAA 設定

次の表に、AAA パラメータのデフォルト設定を示します。

表 *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，25 ページ

RADIUS の設定

RADIUS の概要

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

RADIUS ネットワーク環境

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

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

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

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

- すでに RADIUS を使用中のネットワーク。

  RADIUS を使用した Cisco Nexus デバイスをネットワークに追加できます。この作業は、AAA サーバに移行するときの最初の手順になります。

- リソース アカウンティングが必要なネットワーク。

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

- 認証プロファイルをサポートするネットワーク。

  ネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルをセットアップできます。ユーザごとのプロファイルにより、Cisco Nexus デバイスは、既存の RADIUS ソリューションを使用してポートを管理できると同時に、共有リソースを効率的に管理してさまざまなサービス レベル契約を提供できます。

RADIUS の操作について

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

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

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

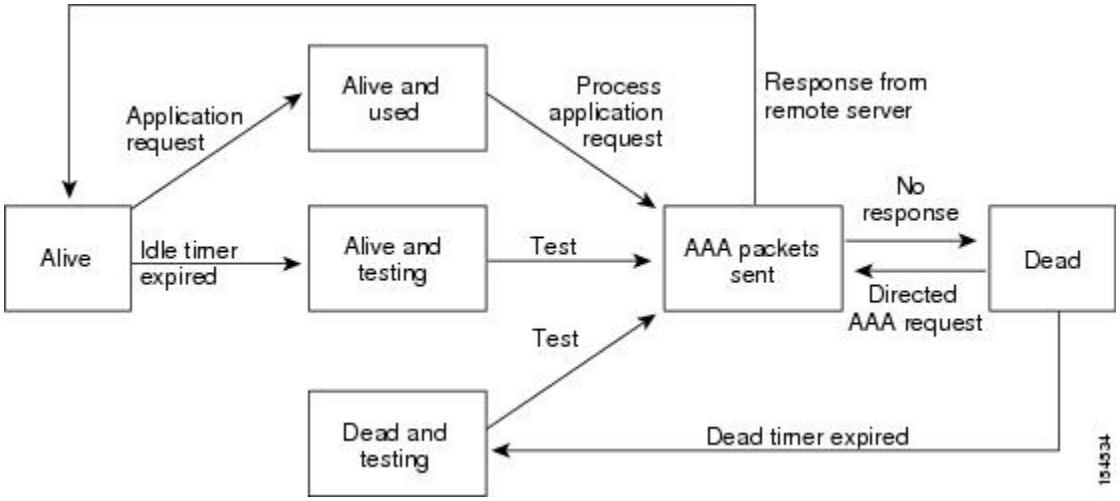
- ユーザがアクセス可能なサービス（Telnet、rlogin、またはローカルエリア トランスポート（LAT）接続、ポイントツーポイント プロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービスなど）
- 接続パラメータ（ホストまたはクライアントの IPv4 アドレス、アクセス リスト、ユーザ タイムアウト）

RADIUS サーバのモニタリング

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

次の図に、さまざまな RADIUS サーバの状態を示します。

図 *2*：*RADIUS* サーバの状態



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

ベンダー固有属性

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間でのベンダー固有属性（VSA）の通信のための方式を規定する標準を作成しています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つ

のベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。値は次の形式のストリングです。

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

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

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

次の VSA プロトコル オプションが、Cisco Nexus デバイスでサポートされています。

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

Cisco Nexus デバイスでは、次の属性がサポートされています。

- roles：ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られた複数のロール名をリストするストリングです。
- accountinginfo：標準の RADIUS アカウンティング プロトコルで処理される属性に加えて、アカウンティング情報が格納されます。この属性は、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分だけに送信されます。この属性と共に使用できるのは、アカウンティングのプロトコル データ ユニット（PDU）だけです。

RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IP アドレス（IPv4）またはホスト名を取得すること。
- RADIUS サーバから事前共有キーを取得すること。
- Cisco Nexus デバイスが、AAA サーバの RADIUS クライアントとして設定されていること。

RADIUS の注意事項と制約事項

RADIUS 設定時の注意事項と制限事項は次のとおりです。

- Cisco Nexus デバイス上に設定できる 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 デバイスと RADIUS サーバとの接続を確立します。

ステップ 2 RADIUS サーバの事前共有秘密キーを設定します。

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

ステップ 4 必要に応じて、次のオプションのパラメータを設定します。

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

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

RADIUS サーバ ホストの設定

認証に使用する各 RADIUS サーバについて、IP アドレス（IPv4）、または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* | *host-name*}	RADIUS サーバの IPv4 アドレス、またはホスト名を指定します。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

RADIUS のグローバルな事前共有キーの設定

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

はじめる前に

リモートの RADIUS サーバの事前共有キー値を取得していること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server key** [**0** | **7**] *key-value*	すべての RADIUS サーバで使用する事前共有キーを指定します。クリア テキスト形式（**0**）または暗号化形式（**7**）事前共有キーを指定できます。デフォルトの形式はクリア テキストです。 最大で 63 文字です。 デフォルトでは、事前共有キーは設定されません。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。 （注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

RADIUS サーバの事前共有キーの設定

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

はじめる前に

リモートの RADIUS サーバの事前共有キー値を取得していること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-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**）事前共有キーを指定できます。デフォルトの形式はクリア テキストです。 最大で 63 文字です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。 （注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、RADIUS 事前共有キーを設定する例を示します。

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

RADIUS サーバ グループの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch (config)# **aaa group server 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* |*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。 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。

	コマンドまたはアクション	目的
		（注） **source-interface** コマンドを使用して、**ip radius source-interface** コマンドによって割り当てられたグローバル ソース インターフェイスをオーバーライドします。
ステップ 6	switch(config-radius)# **exit**	設定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、変更を継続的に保存します。

次に、RADIUS サーバ グループを設定する例を示します。

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

次の作業

AAA サービスに RADIUS サーバ グループを適用します。

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip radius source-interface** *interface*	このデバイスで設定されているすべての RADIUS サーバ グループ用のグローバル発信元インターフェイスを設定します。発信元インターフェイス

	コマンドまたはアクション	目的
		は、管理または VLAN インターフェイスにすることができます。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定情報を表示します。
ステップ 5	switch# **copy running-config startup config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

ログイン時にユーザによる RADIUS サーバの指定を許可

ログイン時に RADIUS サーバを指定することをユーザに許可できます。

手順

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

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

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

グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server retransmit***count*	すべての RADIUS サーバの再送信回数を指定します。デフォルトの再送信回数は 1 で、範囲は 0 ～ 5 です。
ステップ 3	switch(config)# **radius-server timeout***seconds*	RADIUS サーバの送信タイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	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。また、スイッチがタイムアウトエラーを宣言する前にRADIUSサーバからの応答を待機するタイムアウト間隔を設定することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *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* | *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。 （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**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

RADIUS サーバのアカウン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* | | *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。 範囲は 0 ～ 65535 です。
ステップ 3	switch(config)# **radius-server host** {*ipv4-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* | | *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。 範囲は 0 ～ 65535 です。
ステップ 5	switch(config)# **radius-server host** {*ipv4-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**	設定モードを終了します。
ステップ 7	switch(config)# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、RADIUS サーバのアカウン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* | *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。 有効な範囲は、0 ～ 1440 分です。 （注） RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	switch(config)# **radius-server 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。 有効な範囲は 1 ～ 1440 分です。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **exit**	設定モードを終了します。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

デッド タイム間隔の設定

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

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

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
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* | *server-name*} [**vrf** *vrf-name*] *username password***test aaa server radius** {*ipv4-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

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*}	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*}	（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*}	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

この章の内容は、次のとおりです。

- TACACS+ の設定について，43 ページ

TACACS+ の設定について

TACACS+ の設定に関する情報

Terminal Access Controller Access Control System Plus（TACACS+）セキュリティ プロトコルは、Cisco Nexus デバイスにアクセスしようとするユーザの検証を集中的に行います。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されます。設定済みの TACACS+ 機能をCisco Nexus デバイス上で使用するには、TACACS+ サーバへのアクセス権を持ち、このサーバを設定する必要があります。

TACACS+では、認証、許可、アカウン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 デバイスは、TACACS+ プロトコルを使用して集中型の認証を行います。

TACACS+ の利点

TACACS+ には、RADIUS 認証にはない次の利点があります。

- 独立した AAA ファシリティを提供する。たとえば、Cisco Nexus デバイスは、認証を行わずにアクセスを許可できます。

- AAA クライアントとサーバ間のデータ送信に TCP トランスポート プロトコルを使用しているため、コネクション型プロトコルによる確実な転送を実行します。
- スイッチと AAA サーバ間でプロトコル ペイロード全体を暗号化して、高度なデータ機密性を実現します。RADIUS プロトコルはパスワードだけを暗号化します。

TACACS+ を使用したユーザ ログイン

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

1. Cisco Nexus デバイスが接続を確立すると、TACACS+ デーモンにアクセスして、ユーザ名とパスワードを取得します。

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

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

   Cisco Nexus デバイスで許可がイネーブルになっている場合は、この後、許可フェーズの処理が実行されます。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合、Cisco Nexus デバイスは、再度、TACACS+ デーモンにアクセスします。デーモンは ACCEPT または REJECT 許可応答を返します。ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT 応答により、ユーザがアクセス可能なサービスが決まります。

この場合のサービスは次のとおりです。

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

デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー

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

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

TACACS+ サーバのコマンド許可サポート

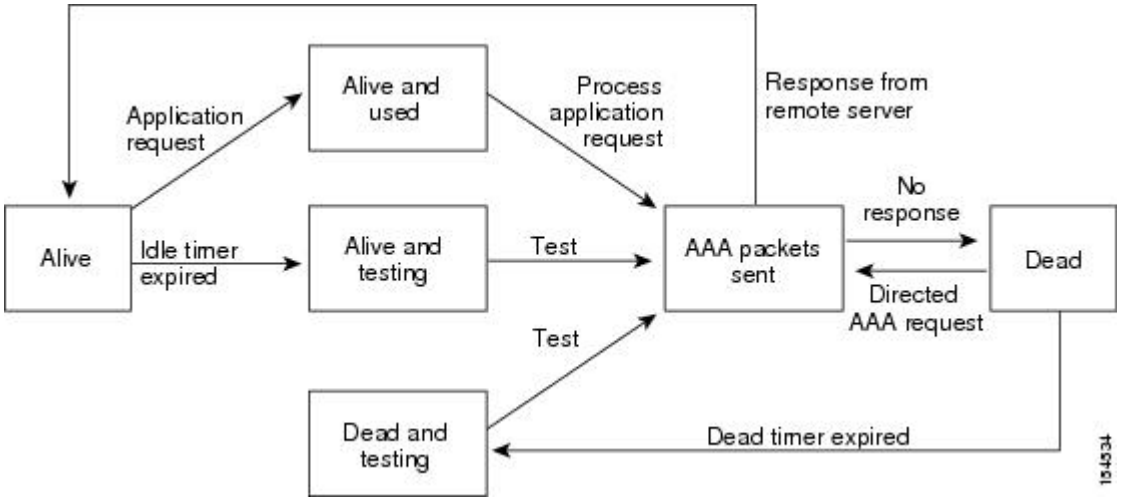
デフォルトでは、認証されたユーザがコマンドライン インターフェイス（CLI）でコマンドを入力したときに、Cisco NX-OS ソフトウェアのローカル データベースに対してコマンド許可が行われます。また、TACACS+ を使用して、認証されたユーザに対して許可されたコマンドを確認することもできます。

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 デバイスは定期的に TACACS+ サーバをモニタリングし、TACACS+ サーバが応答を返す（アライブ）かどうかを調べることができます。Cisco Nexus デバイスは、応答を返さない TACACS+ サーバをデッド（dead）としてマークし、デッド TACACS+ サーバには AAA 要求を送信しません。また、Cisco Nexus デバイスは定期的にデッド TACACS+ サーバをモニタリングし、それらのサーバが応答を返すようになった時点でアライブ状態に戻します。このプロセスでは、TACACS+ サーバが稼働状態であることを確認してから、実際の AAA 要求がサーバに送信されます。TACACS+ サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco Nexus デバイスによって、パフォーマンスに影響が出る前に、障害が発生していることを知らせるエラーメッセージが表示されます。

次の図に、さまざまな TACACS+ サーバの状態を示します。

図 *3* : *TACACS+* サーバの状態



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

TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

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

TACACS+ の注意事項と制約事項

TACACS+ に関する注意事項と制約事項は次のとおりです。

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

TACACS+ の設定

TACACS+ サーバの設定プロセス

ここでは、TACACS+ サーバを設定する方法について説明します。

手順

ステップ 1 TACACS+ をイネーブルにします。

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

ステップ 3 TACACS+ サーバの事前共有秘密キーを設定します。

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

ステップ 5 必要に応じて、次のオプションのパラメータを設定します。

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

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

TACACS+ のイネーブル化

デフォルトでは、Cisco Nexus デバイスで TACACS+ 機能はディセーブルに設定されています。TACACS+ 機能をイネーブルに設定すると、認証に関するコンフィギュレーション コマンドと検証コマンドを使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **feature tacacs+**	TACACS+ をイネーブルにします。
ステップ 3	switch(config)# **exit**	設定モードを終了します。

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

TACACS+ サーバ ホストの設定

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

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

TACACS+ サーバ ホストを設定する前に、次の点を確認してください。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*}	TACACS+ サーバの IPv4 アドレスまたはホスト名を指定します。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	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デバイスで使用するすべてのサーバについて、グローバル レベルで事前共有キーを設定できます。事前共有キーとは、Cisco Nexus デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

事前共有キーを設定する前に、次の点を確認してください。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**tacacs-server key** [**0** | **6** |**7**] *key-value*	すべての TACACS+ サーバ用の TACACS+ キーを指定します。*key-value* がクリアテキスト（**0**）の形式か、タイプ 6 暗号化（**6**）形式か、タイプ 7 暗号化（**7**）形式かを指定できます。デフォルトの形式はクリア テキストです。最大で 63 文字です。 デフォルトでは、事前共有キーは設定されません。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。 （注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、グローバルな事前共有キーを設定する例を示します。

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

TACACS+ サーバの事前共有キーの設定

TACACS+ サーバの事前共有キーを設定できます。事前共有キーとは、Cisco Nexus デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-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**）事前共有キーを指定できます。デフォルトの形式はクリア テキストです。最大で 63 文字です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	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**	グローバル コ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 host** {*ipv4-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**）事前共有キーを指定できます。デフォルトの形式はクリア テキストです。最大で 63 文字です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 4	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。
ステップ 5	switch(config-tacacs+)# **source-interface***interface*	（任意） 特定の TACACS+ サーバ グループに発信元インターフェイスを割り当てます。 サポートされているインターフェイスのタイプは管理および VLAN です。 （注） **source-interface** コマンドを使用して、**ip tacacs source-interface** コマンドによって割り当てられたグローバル ソース インターフェイスをオーバーライドします。
ステップ 6	switch(config-tacacs+)# **exit**	設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 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**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip tacacs source-interface** *interface* 例： `switch(config)# ip tacacs source-interface mgmt 0`	このデバイスで設定されているすべての TACACS+ サーバ グループ用のグローバル発信元インターフェイスを設定します。発信元インターフェイスは、管理または VLAN インターフェイスにすることができます。

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

ステップ 4	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定情報を表示します。

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

ログイン時の TACACS+ サーバの指定

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server directed-request**	ログイン時にユーザが認証要求の送信先となる TACACS+ サーバを指定できるようにします。デフォルトでは無効になっています。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **show tacacs-server directed-request**	（任意） TACACS+ の directed request の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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 許可が使用されないように指定します。

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# 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ロールベース許可コントロール（RBAC）がディセーブルになります。

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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。

	コマンドまたはアクション	目的
		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） 許可用の正しいコマンドを送信しないと、結果の信頼性が低くなります。

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*	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。

	コマンドまたはアクション	目的
	例： `switch# test aaa authorization command-type commands user TestUser command reload`	（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、ロールベース アクセス コントロール（RBAC）を使用します。両方のタイプのデバイスを同じ TACACS+ サーバ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
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。

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 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。デフォルトではディセーブルになっています。
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。デフォルトではディセーブルになっています。 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。

	コマンドまたはアクション	目的
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。デフォルトではディセーブルになっています。 **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。
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つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。 *command-string* 引数には、空白スペースを含めることができます。 （注） 256個の規則に対してこのコマンドを繰り返します。

ステップ 4	**exit**
	
	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 デバイスが、タイムアウト エラーを宣言する前に、すべての TACACS+ サーバからの応答を待機するグローバルなタイムアウト間隔も設定できます。タイムアウト間隔には、スイッ

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server 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**	設定モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

サーバのタイムアウト間隔の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **timeout***seconds*	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 （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**	設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	switch# **show 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 デバイスは、すべての TACACS+ 要求にポート 49 を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **port***tcp-port*	TACACS+ アカウンティング メッセージ用の UDP ポートを指定します。デフォルトの TCP ポートは 49 です。有効な範囲は 1 ～ 65535 です。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	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 デバイスがテスト パケットを送信するかを指定します。このオプションを設定して、サーバを定期的にテストしたり、1 回だけテストを実行できます。

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-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 デバイスが、前回応答しなかった TACACS+ サーバをチェックするまでの時間（分）を指定します。デフォルト値は 0 分、指定できる範囲は 0 ～ 1440 分です。
ステップ 4	switch(config)# **exit**	設定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。

	コマンドまたはアクション	目的
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ サーバの定期的モニタリングを設定する例を示します。

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

デッド タイム間隔の設定

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

（注） デッド タイム間隔が 0 分の場合、TACACS+ サーバは、応答を返さない場合でも、デッ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**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server deadtime***minutes*	グローバルなデッド タイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	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* | *host-name*} [**vrf***vrf-name*] *usernamepassword*	TACACS+ サーバにテスト メッセージを送信して可用性を確認します。
ステップ 2	switch# **test aaa 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**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature tacacs+**	TACACS+ をディセーブルにします。
ステップ 3	switch(config)# **exit**	設定モードを終了します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ 統計情報の表示

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

手順

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

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

TACACS+ の設定の確認

TACACS+ の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*] [**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# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ikvhw10"
switch(config)# tacacs-server host 1.1.1.1
switch(config)# tacacs-server host 1.1.1.2

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

TACACS+ のデフォルト設定

次の表に、TACACS+ パラメータのデフォルト設定を示します。

表 *7*：*TACACS+* のデフォルト パラメータ

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

第 6 章

SSH および Telnet の設定

この章の内容は、次のとおりです。

- SSH および Telnet の設定，69 ページ

SSH および Telnet の設定

SSH および Telnet の概要

SSH サーバ

セキュア シェル（SSH）プロトコル サーバ機能を使用すると、SSH クライアントは Cisco Nexus デバイスとの間で、セキュアな暗号化された接続を確立できます。SSH は強化暗号化を使用して認証を行います。Cisco Nexus デバイス スイッチの SSH サーバは、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 スイッチとの間、または SSH サーバを稼働している他の任意のデバイスとの間でセキュアな暗号化された接続を確立できます。この接続は、暗号化されたアウトバウンド接続を実現します。認証と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

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

SSH サーバ キー

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

- Rivest, Shamir, and Adelman（RSA）公開キー暗号化を使用した SSH バージョン 2
- Digital System 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限事項があります。

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

SSH の設定

SSH サーバ キーの生成

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ssh key**{**dsa** [**force**] | **rsa** [*bits* [**force**]]}	SSH サーバ キーを生成します。 *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**	グローバル コ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**	グローバル 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**	グローバル 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 デバイスからリモート デバイスに接続する SSH セッションを開始できます。

手順

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

SSH ホストのクリア

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

手順

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

SSH サーバのディセーブル化

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **[no] feature ssh**	SSH サーバをイネーブル/ディセーブルにします。デフォルトではイネーブルになっています。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# **show ssh server**	（任意） SSH サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH サーバ キーの削除

SSH サーバをディセーブルにした後、SSH サーバ キーを削除できます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature ssh**	SSH サーバをディセーブルにします。
ステップ 3	switch(config)# **no ssh key** [**dsa** | **rsa**]	SSH サーバ キーを削除します。 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

Cisco Nexus デバイスから SSH セッションをクリアできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show users**	ユーザ セッション情報を表示します。
ステップ 2	switch# **clear 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になっているため、この手順は必要ありません。

ステップ 3 SSH サーバ キーを表示します。

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

ssh-rsa
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 デバイスの Telnet サーバをディセーブルにできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **[no] feature telnet**	Telnet サーバをイネーブル/ディセーブルにします。デフォルトではイネーブルになっています。

Telnet サーバの再イネーブル化

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **[no] 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ます。必要に応じて、リモート デバイスのユーザ名も取得します。
- Cisco Nexus デバイス上で Telnet サーバをイネーブルにします。
- リモート デバイス上で Telnet サーバをイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **telnet***hostname*	リモート デバイスとの Telnet セッションを作成します。引数 *hostname* には、IPv4 アドレスまたはデバイス名を指定します。

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**]

コマンドまたはアクション	目的
switch# **show running-config security**[**all**]	実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。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

アクセス コントロール リストの設定

この章の内容は、次のとおりです。

- ACL の概要，81 ページ
- IP ACL の設定，89 ページ
- VLAN ACL の概要，96 ページ
- VACL の設定，97 ページ
- VACL の設定例，100 ページ
- ACL TCAM リージョン サイズの設定，100 ページ
- 仮想端末回線の ACL の設定，103 ページ

ACL の概要

アクセスコントロールリスト（ACL）とは、トラフィックのフィルタリングに使用する順序付きのルール セットのことです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。スイッチは、あるパケットに対してあるACLを適用するかどうかを判断するとき、そのパケットをACL内のすべてのルールの条件に対してテストします。一致する条件が最初に見つかった時点で、パケットを許可するか拒否するかが決まります。一致する条件が見つからないと、スイッチは適用可能なデフォルトのルールを適用します。許可されたパケットについては処理が続行され、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ハイパー テキスト トランスファ プロトコル（HTTP）トラフィックが流入するのを禁止できます。また、特定のサイトへの HTTP トラフィックだけを許可することもできます。その場合は、サイトの IP アドレスが、IP ACL に指定されているかどうかによって判定します。

IP ACL のタイプと適用

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

表 *9*：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
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には、先に VLAN インターフェイスをグローバルにイネーブルにする必要があります。 • 物理層 3 インターフェイス • レイヤ 3 イーサネット サブインターフェイス • レイヤ 3 イーサネット ポート チャネル インターフェイス • レイヤ 3 イーサネット ポート チャネル サブインターフェイス • トンネル • 管理インターフェイス	IPv4 ACL
VLAN ACL（VACL）	アクセス マップを使用して ACL をアクションにアソシエートし、そのアクセス マップを VLAN に適用する場合、その ACL は VACL と見なされます。	IPv4 ACL
VTY ACL	VTY	IPv4 ACL

適用順序

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

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

ルール

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

インターネット プロトコル番号を表す整数でプロトコルを指定できます。

暗黙のルール

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

すべての IPv4 ACL には、次の暗黙のルールがあります。

```
deny ip any any
```

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

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

すべての MAC ACL には、次の暗黙のルールがあります。

`deny any any` *protocol*

この暗黙ルールによって、デバイスは、トラフィックのレイヤ 2 ヘッダーに指定されているプロトコルに関係なく、不一致トラフィックを確実に拒否します。

その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。IPv4 ACL には、次の追加フィルタリング オプションが用意されています。

- レイヤ 4 プロトコル
- TCP/UDP ポート
- ICMP タイプおよびコード
- IGMP タイプ
- 優先レベル
- DiffServ コード ポイント（DSCP）値
- ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
- 確立済み TCP 接続

シーケンス番号

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

- 既存のルールの間に新規のルールを追加する：シーケンス番号を指定することによって、ACL 内での新規ルールの挿入場所を指定します。たとえば、ルール番号 100 と 110 の間に新しいルールを挿入する必要がある場合は、シーケンス番号 105 を新しいルールに割り当てます。
- ルールを削除する：シーケンス番号を使用しない場合は、ルールを削除するのに、次のようにルール全体を入力する必要があります。

  ```
  switch(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  このルールに 101 番のシーケンス番号が付いていれば、次コマンドだけでルールを削除できます。

  ```
  switch(config-acl)# no 101
  ```

- ルールを移動する：シーケンス番号を使用すれば、同じ ACL 内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号を使用せずにルールを入力すると、デバイスはそのルールを ACL の最後に追加し、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号を割り当てます。たとえば、ACL 内の最後のルールのシーケンス番号が 225 で、シーケンス番号を指定せずにルールを追加した場合、デバイスはその新しいルールにシーケンス番号 235 を割り当てます。

また、デバイスでは、ACL 内ルールのシーケンス番号を再割り当てすることができます。シーケンス番号の再割り当ては、ACL 内に、100、101 のように連続するシーケンス番号のルールがある場合、それらのルールの間に 1 つ以上のルールを挿入する必要があるときに便利です。

論理演算子と論理演算ユニット

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

Cisco Nexus デバイスは、演算子とオペランドの組み合わせを論理演算ユニット（LOU）というレジスタ内に格納し、IP ACL で指定された TCP および UDP ポート上で演算（より大きい、より小さい、等しくない、包含範囲）を行います。

（注） range 演算子は境界値も含みます。

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

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

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

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

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

  たとえば、あるルールによって、演算子とオペランドの組み合わせ「gt 10」が送信元ポートに、別のルールによって同じ組み合わせ「gt 10」が宛先ポートに適用される場合、両方の組み合わせが LOU の半分に格納され、結果として 1 つの LOU 全体が使用されることになりま

す。このため、「gt 10」を使用するルールが追加されても、これ以上 LOU は使用されません。

ACL TCAM リージョン

ハードウェアの ACL Ternary Content Addressable Memory（TCAM）リージョンのサイズを変更できます。

IPv4 TCAM はシングル幅です。

TCAM リージョン サイズには、次の注意事項と制約事項があります。

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

表 *10* : *ACL* リージョンによる *TCAM* サイズ

TCAM ACL リージョン	デフォルト サイズ	最小サイズ	インクリメンタルサイズ
SUP（入力）	112	48	16
PACL（入力）	400	0	16
VACL（入力）、VACL（出力）	640（入力）、640（出力）	0（入力）、0（出力）	16
RACL（入力）	1536	0	16

TCAM ACL リージョン	デフォルト サイズ	最小サイズ	インクリメンタルサイズ
QOS（入力）、QOS（出力）	192（入力）、64（出力）	16（入力）、64（出力）	16
E-VACL（出力）	640	0	16
E-RACL（出力）	256	0	16
NAT	256	0	16

ACL のライセンス要件

次の表に、この機能のライセンス要件を示します。

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

ACL の前提条件

IP ACL の前提条件は次のとおりです。

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

VACL の前提条件は次のとおりです。

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

ACL の注意事項と制約事項

IP ACL の設定に関する注意事項と制約事項は次のとおりです。

- 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。

- レイヤ 3 最大伝送単位チェックに失敗し、そのためにフラグメント化を要求しているパケット
- IP オプションがある IPv4 パケット（追加された IP パケット ヘッダーのフィールドは、宛先アドレス フィールドの後）
- IP ACL を VLAN インターフェイスに適用するためには、VLAN インターフェイスをグローバルにイネーブル化する必要があります。
- 1 つの VLAN アクセス マップでは、1 つの IP ACL だけを照合できます。
- 1 つの IP ACL に、複数の許可/拒否 ACE を設定することができます。
- 1 つの VLAN に適用できるアクセス マップは 1 つだけです。
- 出力 RACL と VACL はワープ モードでは適用できません。
- 出力 ACL は、マルチキャスト トラフィックには適用できません。
- SVI 上の入力 RACL をマルチキャスト トラフィックに適用することはできません。
- PACL はワープ モードでは適用できません。
- SVI とレイヤ 3 インターフェイスの同じ入力 RACL では TCAM リソースを共有できないため、それぞれが個別に TCAM リソースを使用します。ただし、ACL 統計情報リソースは共有されます。アップグレード前に RACL TCAM をほとんど使い切っている場合、アップグレード後に RACL アプリケーションで障害が発生する可能性があります。その場合は、RACL TCAM を切り分けることができます。
- ARP ACL は Nexus 3500 プラットフォームではサポートされません。

デフォルトの ACL 設定

次の表は、IP ACL パラメータのデフォルト設定をリスト表示しています。

表 *11*：*IP ACL* のデフォルト パラメータ

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

次の表に、VACL パラメータのデフォルト設定を示します。

表 *12*：*VACL* のデフォルト パラメータ

パラメータ	デフォルト
VACL	デフォルトの IP ACL は存在しません。

パラメータ	デフォルト
ACL ルール	すべての ACL に暗黙のルールが適用されます。

IP ACL の設定

IP ACL の作成

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **ip access-list***name*	IP ACL を作成して、IP ACL コンフィギュレーション モードを開始します。*name* 引数は 64 文字以内で指定します。
ステップ 3	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocolsourcedestination*	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『*Command Reference*』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 access-lists***name*	（任意） IP ACL の設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、IPv4 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ip access-list acl-01
```

```
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics
```

IP ACL の変更

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

既存のルールの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**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ipaccess-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**} *protocolsourcedestination*	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『*Command Reference*』を参照してください。
ステップ 5	switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocolsourcedestination*}	（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『*Command Reference*』を参照してください。
ステップ 6	switch(config-acl)# [**no**] **statistics**	（任意） ACL のルールと一致するパケットのグローバル統計をスイッチが維持するように設定します。 **no** オプションを指定すると、ACL のグローバルな統計情報がスイッチ内に維持されなくなります。

	コマンドまたはアクション	目的
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，（92 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**	グローバル コ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)# **noipaccess-list***name*	名前で指定したIPACL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IPACL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。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **resequenceip access-list***namestarting-sequence-numberincrement*	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# **showipaccess-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。

mgmt0 への IP-ACL の適用

管理インターフェイス（mgmt0）に IPv4 ACL を適用できます。

はじめる前に

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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	**interfacemgmt***port*
	
	例：
	`switch(config)# interface mgmt0`
	`switch(config-if)#`
		管理インターフェイスのコンフィギュレーション モードを開始します。

ステップ 3	**ip access-group** *access-list* {**in** | **out**} 例： `switch(config-if)#ip access-group acl-120 out`	IPv4 ACL を、指定方向のトラフィックのレイヤ 3 インターフェイスに適用します。各方向にルータ ACL を 1 つ適用できます。
ステップ 4	**show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	（任意） ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連項目

- IP ACL の作成

ポート ACL としての IP ACL の適用

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel***channel-number*}	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **ip port access-group** *access-list***in**	IPv4 ACL を、インターフェイスまたはポート チャネルに適用します。ポート ACL では、インバウンド フィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。
ステップ 4	switch# **show running-config**	（任意） ACL の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ルータ ACL としての IP ACL の適用

IPv4 ACL は、次のタイプのインターフェイスに適用できます。

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

これらのインターフェイス タイプに適用された ACL はルータ ACL と見なされます。

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • switch(config)# **interfaceethernet***slot*/*port*[**.***number*] • switch(config)# **interfaceport-channel***channel-number*[**.***number*] • switch(config)# **interfacetunnel***tunnel-number* • switch(config)# **interfacevlan***vlan-ID* • switch(config)# **interfacemgmt***port*	指定したインターフェイス タイプのコンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **ipaccess-group** *access-list* {**in** | **out**}	IPv4 ACL を、指定方向のトラフィックのレイヤ3インターフェイスに適用します。各方向にルータ ACL を 1 つ適用できます。
ステップ 4	switch(config-if)# **show running-config aclmgr**	（任意） ACL の設定を表示します。
ステップ 5	switch(config-if)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL の設定の確認

IP ACL 設定情報を表示するには、次のいずれかの作業を実行します。

- 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『*Command Reference*』を参照してください。

IP ACL の統計情報のモニタリングとクリア

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

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

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

VLAN ACL の概要

VLAN ACL（VACL）は、IP ACL の適用例の 1 つです。VACL を設定して、VLAN 内でブリッジされているすべてのパケットに適用できます。VACL は、セキュリティ パケットのフィルタリングだけに使用します。VACL は方向（入力または出力）で定義されることはありません。

VACL とアクセス マップ

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

VACL とアクション

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

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

- ドロップ：トラフィックをドロップします。

統計情報

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

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

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

VACL の設定

VACL の作成または変更

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **vlan access-map***map-name*	指定したアクセス マップのアクセス マップ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-access-map)# **matchipaddress***ip-access-list*	マップの IPv4 ACL を指定します。
ステップ 4	switch(config-access-map)# **action** {**drop** | **forward**}	スイッチが、ACL に一致したトラフィックに適用するアクションを指定します。
ステップ 5	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。

	コマンドまたはアクション	目的
		no オプションを指定すると、VACL のグローバルな統計情報がスイッチ内に保持されなくなります。
ステップ 6	switch(config-access-map)# **show running-config**	（任意） ACL の設定を表示します。
ステップ 7	switch(config-access-map)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL の削除

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no vlan access-map***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**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **vlan filter***map-name* **vlan-list***list*	指定したリストによって、VACL を VLAN に適用します。**no** オプションを使用すると、VACL の適用が解除されます。 **vlan-list** コマンドで指定できる VLAN は最大 32 個ですが、複数の **vlan-list** コマンドを設定すると、32 個を超える VLAN を指定できます。
ステップ 3	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
```

ACL TCAM リージョン サイズの設定

ハードウェアの ACL Ternary Content Addressable Memory（TCAM）リージョンのサイズを変更できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** } *tcam_size*	ACL TCAM リージョン サイズを変更します。 • **arpacl**：アドレス解決プロトコル（ARP）の ACL（ARPACL）TCAM リージョン サイズを設定します。 • **e-racl**：出力ルータ ACL（ERACL）TCAM リージョン サイズを設定します。 • **e-vacl**：出力の VLAN ACL（EVACL）TCAM リージョン サイズを設定します。 • **ifacl**：インターフェイス ACL（ifacl）TCAM リージョン サイズを設定します。エントリの最大数は 1500 です。 • **nat**：NAT TCAM リージョンのサイズを設定します。 • **qos**：Quality of Service（QoS）TCAM リージョン サイズを設定します。

	コマンドまたはアクション	目的
		• **qoslbl**：QoS ラベル（qoslbl）TCAM リージョン サイズを設定します。 • **racl**：ルータの ACL（RACL）TCAM リージョン サイズを設定します。 • **vacl**：VLAN ACL（VACL）TCAM リージョン サイズを設定します。 • *tcam_size*：TCAM サイズ。有効な範囲は 0 ～ 2,147,483,647 エントリです。 （注） **vacl** および **e-vacl** TCAM リージョンを同じサイズに設定する必要があります。
ステップ 3	**copy running-config startup-config** **例**： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 4	switch(config)# **show hardware profile tcam region** **例**： `switch(config)# show hardware profile tcam region`	スイッチの次回のリロード時に適用される TCAM サイズを表示します。
ステップ 5	switch(config)# **reload** **例**： `switch(config)# reload`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 （注） **copy running-config to startup-config** を保存した後、次回のリロード時に新しいサイズ値が有効になります。

次に、RACL TCAM リージョンのサイズを変更する例を示します。

```
switch(config)# hardware profile tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

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

次に、スイッチで TCAM VLAN ACL を設定する例を示します。

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

```
switch(config-sync-sp)# hardware profile tcam region vacl 512
switch(config-sync-sp)# hardware profile tcam region e-vacl 512
switch(config-sync-sp)#
```

次に、変更を確認するために、TCAM リージョンのサイズを表示する例を示します。

```
switch(config)# show hardware profile tcam region
         sup size =   16
        vacl size =  640
       ifacl size =  496
         qos size =  256
       rbacl size =    0
        span size =    0
        racl size = 1536
      e-racl size =  256
      e-vacl size =  640
      qoslbl size =    0
      arpacl size =    0
```

デフォルトの TCAM リージョン サイズに戻す

手順

	コマンドまたはアクション	目的

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

ステップ 2	switch(config)# **no hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** } *tcam_size*	デフォルト ACL TCAM サイズに設定を戻します。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 4	switch(config)# **reload**	スイッチをリロードします。

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

```
switch(config)# no hardware profile tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

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

仮想端末回線の ACL の設定

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

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

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

はじめる前に

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

手順

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

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

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

ステップ 4	switch(config-line)# **no access-class access-list-number {in | out}**
	
	例：
	`switch(config-line)# no access-class ozi2 in`
	`switch(config-line)# no access-class ozi3 out`
	`switch(config)#`
		（任意）
		着信または発信アクセス制限を削除します。

	コマンドまたはアクション	目的

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。

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


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

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

```
switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
switch(config)# ip access-list ozi2
switch(config-acl)# statistics per-entry
switch(config-acl)# deny tcp 172.18.217.83/32 any
switch(config-acl)# exit

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

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

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

次に、VTY 回線でアクセス制限を削除する例を示します。

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

第 8 章

DHCP スヌーピングの設定

この章は、次の項で構成されています。

- DHCP スヌーピングの概要，107 ページ
- DHCP リレー エージェントの概要，110 ページ
- DHCP スヌーピングのライセンス要件，111 ページ
- DHCP スヌーピングの前提条件，112 ページ
- DHCP スヌーピングの注意事項および制約事項，112 ページ
- DHCP スヌーピングのデフォルト設定，112 ページ
- DHCP スヌーピングの設定，113 ページ
- DHCP スヌーピング設定の確認，128 ページ
- DHCP バインディングの表示，128 ページ
- DHCP スヌーピング バインディング データベースのクリア，129 ページ
- DHCP リレー統計情報のクリア，130 ページ
- DHCP のモニタリング，130 ページ
- DHCP スヌーピングの設定例，130 ページ

DHCP スヌーピングの概要

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

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

- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

DHCP スヌーピングは、VLAN ベースごとにイネーブルに設定されます。デフォルトでは、すべての VLAN でこの機能は非アクティブです。この機能は、1 つの VLAN または特定の VLAN 範囲でイネーブルにできます。

機能のイネーブル化とグローバルなイネーブル化

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

機能のイネーブル化

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

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

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

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

グローバルなイネーブル化

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

DHCP スヌーピングをグローバルにイネーブルにすると、DHCP スヌーピングがイネーブルになっている VLAN の信頼できない各インターフェイスについて、受信した DHCP メッセージの検証が開始され、DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

DHCP スヌーピングをグローバルにディセーブルにすると、DHCP メッセージの検証と、信頼できないホストからの以降の要求の検証を停止します。DHCP スヌーピング バインディング データベースも削除されます。DHCP スヌーピングをグローバルにディセーブルにしても、DHCP スヌーピングの設定や、DHCP スヌーピング機能に依存するその他の機能の設定は削除されません。

信頼できる送信元と信頼できない送信元

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

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

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

Cisco Nexus デバイスでは、接続インターフェイスの信頼状態を設定することにより送信元が信頼されることを示します。

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

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

DHCP スヌーピング バインディング データベース

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

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

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

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

DHCP スヌーピング バインディング データベースの各エントリには、ホストの MAC アドレス、リース IP アドレス、リース期間、バインディング タイプ、VLAN 番号、およびホストに関連するインターフェイス情報が保存されます。

clear ip dhcp snooping binding コマンドを使用すると、バインディング データベースからエントリ削除できます。

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

（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 サーバにそれが転送されます。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 スヌーピングのライセンス要件

この機能には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

DHCP スヌーピングの前提条件

DHCP スヌーピングまたは DHCP リレー エージェントを設定するためには、DHCP についての知識が必要です。

DHCP スヌーピングの注意事項および制約事項

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

- DHCP スヌーピング データベースには 2,000 のバインディングを格納できます。
- DHCP をグローバルにイネーブル化し、さらに少なくとも 1 つの VLAN で DHCP スヌーピングをイネーブルにするまで、DHCP スヌーピングはアクティブになりません。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレーエージェントとして機能するスイッチが設定され、イネーブルになっていることを確認してください。
- DHCP スヌーピングを使用して設定を行っている VLAN で VLAN ACL（VACL）が設定されている場合、その VACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。
- DHCP スヌーピングおよび DHCP リレー機能は、同一の VLAN ポート上ではサポートされません。

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 *13*：*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 リレー エージェントに対する VRF サポート	ディセーブル

パラメータ	デフォルト
DHCP リレー エージェント	ディセーブル

DHCP スヌーピングの設定

DHCP スヌーピングの最小設定

1 DHCP スヌーピング機能をイネーブルにします。

2

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, （114 ページ）を参照してください。
ステップ 2	DHCP スヌーピングをグローバルにイネーブルにします。	詳細については、DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化, （114 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, （115 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, （119 ページ）を参照してください。

DHCP スヌーピング機能のイネーブル化またはディセーブル化

スイッチの DHCP スヌーピング機能をイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP スヌーピングはディセーブルです。

はじめる前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **feature dhcp** 例： `switch(config)# feature dhcp`	DHCP スヌーピング機能をイネーブルにします。**no** オプションを使用すると、DHCP スヌーピング機能がディセーブルになり、DHCP スヌーピングの設定がすべて消去されます。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
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	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip dhcp snooping** 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	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VLANに対するDHCPスヌーピングのイネーブル化またはディセーブル化

1 つまたは複数の VLAN に対して DHCP スヌーピングをイネーブルまたはディセーブルに設定できます。

はじめる前に

デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。

DHCP スヌーピングがイネーブルになっていることを確認してください。

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ipdhcp snooping vlan** *vlan-list* 例： `switch(config)# ip dhcp snooping vlan 100,200,250-252`	*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	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Option 82 データの挿入および削除のイネーブル化またはディセーブル化

DHCP リレー エージェントを使用せずに転送された DHCP パケットへの Option 82 情報の挿入および削除をイネーブルまたはディセーブルにできます。デフォルトでは、デバイスはDHCPパケットに Option 82 情報を挿入しません。

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

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip dhcp snooping information option** 例： `switch(config)# ip dhcp snooping information option`	DHCP パケットの Option 82 情報の挿入および削除をイネーブルにします。**no** オプションを使用すると、Option 82 情報の挿入および削除がディセーブルになります。
ステップ 3	[**no**] **ip dhcp snooping sub-option circuit-id format-type string format** 例： `switch(config)# ip dhcp snooping sub-option circuit-id format-type string format`	（任意） 入力 ifindex 名、またはホスト名、またはその両方の組み合わせにエンコード文字列形式を使用するよう Option 82 を設定します。（ホスト名の場合は「%h」、ifindex の場合は「%p」、ホスト名と ifindex 名の両方の場合は「%h」と「%p」の組み合わせ）
ステップ 4	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Option 82 ユーザ定義データの挿入および削除のイネーブル化またはディセーブル化

サーバに転送された DHCP パケットへの Option 82 ユーザ定義情報の挿入および削除をイネーブルまたはディセーブルに設定できます。この設定は、ポートごとに適用され、エンコード文字列形式の入力 ifindex 名を使用する Option82 グローバル コンフィギュレーションよりも優先されます。SVI 上で DHCP リレーを設定すると、入力物理 *ifindex* に基づくユーザ定義文字列が、リレー対象の DHCP パケットに付加されます。

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

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

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**config t**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ip dhcp snooping information option**	DHCP パケットの Option 82 情報の挿入および削除をイネーブルにします。**no** オプションを使用すると、Option 82 情報の挿入および削除がディセーブルになります。
ステップ 3	**interface ethernet***slot*/*port*	インターフェイス コンフィギュレーション モードを開始します。slot/port は、Option 82 文字列を設定するレイヤ 2 イーサネット入力インターフェイスです。
ステップ 4	**ip dhcp option82 suboption circuit-id***user-defined-circuit-id* 例： switch(config-if)# ip dhcp option82 suboption circuit-id po5-option82-string	ユーザが定義した Option82 文字列をポート チャネル 5 で入力します。「po5-option82-string」という文字列が、ポート チャネル 5 で入力中の DHCP パケットに付加されます。イーサネットインターフェイスでも同じように設定されます。
ステップ 5	**show ip dhcp option82 suboption info interface po5**	（任意） DHCP Option 82 の情報と統計情報を表示します。
ステップ 6	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP パケットの厳密な検証のイネーブル化またはディセーブル化

DHCP スヌーピング機能では、DHCP パケットの厳密な検証をイネーブルまたはディセーブルにできます。デフォルトでは、DHCP パケットの厳密な検証はディセーブルになっています。

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip dhcp packet strict-validation** 例： `switch(config)# ip dhcp packet strict-validation`	DHCP スヌーピング機能で、DHCP パケットの厳密な検証をイネーブルにします。**no** オプションを使用すると、DHCP パケットの厳密な検証がディセーブルになります。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの信頼状態の設定

各インターフェイスが DHCP メッセージの送信元として信頼できるかどうかを設定できます。DHCP の信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 ポート チャネル インターフェイス

はじめる前に

デフォルトでは、すべてのインターフェイスは信頼できません。

DHCP スヌーピングがイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的

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

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***port*/*slot*
	• **interfaceport-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	**showrunning-config dhcp** 例： `switch(config-if)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー エージェントのイネーブル化またはディセーブル化

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

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip dhcp relay** 例： `switch(config)# ip dhcp relay`	DHCP リレーエージェントをイネーブルにします。**no** オプションを使用すると、リレーエージェントがディセーブルになります。
ステップ 3	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 4	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

デバイスに対し、リレー エージェントによって転送された DHCP パケットへの Option 82 情報の挿入と削除をイネーブルまたはディセーブルにできます。

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip dhcp relay** 例： `switch(config)# ip dhcp relay`	DHCP リレー機能をイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 3	[**no**] **ip dhcp relay information option** 例： `switch(config)# ip dhcp relay information option`	DHCP リレー エージェントによって転送されるパケットに対する Option 82 情報の挿入および削除をイネーブルにします。Option 82 情報は、デフォルトでバイナリ ifIndex 形式です。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 4	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 5	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

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	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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 機能がイネーブルになっていることを確認します。

DHCP リレー エージェントがイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface slot/port*
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。*slot/port* は、DHCP リレー エージェントに対するサブネット ブロードキャスト サポートをイネーブルまたはディセーブルにするインターフェイスです。

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	**showip 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	**showrunning-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。

インターフェイスへの DHCP サーバ アドレスの設定

1 つのインターフェイスに複数の DHCP サーバ IP アドレスを設定できます。インバウンド DHCP BOOTREQUEST パケットがインターフェイスに着信すると、リレー エージェントはそのパケットを指定されたすべての DHCP サーバ IP アドレスに転送します。リレー エージェントは、すべての DHCP サーバからの応答を、要求を送信したホストへ転送します。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCP サーバが正しく設定されていることを確認します。

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

DHCP サーバがインターフェイスとは異なる VRF インスタンスに含まれている場合、VRF サポートがイネーブルになっていることを確認します。

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

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	次のいずれかのオプションを使用します。
	• **interfaceethernet***slot*/*port*[**.***number*]
	• **interfacevlan***vlan-id*
	• **interfaceport-channel***channel-id*[*.subchannel-id*]
	
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		• インターフェイス コンフィギュレーション モードを開始します。*slot*/*port* は、DHCP サーバ IP アドレスを設定する物理イーサネット インターフェイスです。サブインターフェイスを設定する場合は、*number* 引数を使用してサブインターフェイス番号を指定します。
		• インターフェイス コンフィギュレーション モードを開始します。*vlan-id* は、DHCP サーバ IP アドレスを設定する VLAN の ID です。
		• インターフェイス コンフィギュレーション モードを開始します。*channel-id* は、DHCP サーバ IP アドレスを設定するポート チャネルの ID です。サブチャネルを設定する場合は、*subchannel-id* 引数を使用してサブチャネル ID を指定します。

ステップ 3	**ip dhcp relay address** *IP-address* [**use-vrf** *vrf-name*] 例： `switch(config-if)# ip dhcp relay address 10.132.7.120 use-vrf red`	リレー エージェントがこのインターフェイスで受信した BOOTREQUEST パケットを転送する DHCP サーバの IP アドレスを設定します。 複数の IP アドレスを設定するには、アドレスごとに **ip dhcp relay address** コマンドを使用します。
ステップ 4	**showip dhcp relay address** 例： `switch(config-if)# show ip dhcp relay address`	（任意） 設定済みのすべての DHCP サーバ アドレスを表示します。

	コマンドまたはアクション	目的
ステップ 5	**showrunning-config dhcp** 例： `switch(config-if)# 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-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 スタティック バインディングの作成

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

はじめる前に

DHCP スヌーピング機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**ip source binding** *IP-address MAC-address* **vlan** *vlan-id* {**interface ethernet** *slot/port* | **port-channel** *channel-no*} 例： `switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3`	レイヤ 2 イーサネット インターフェイスにスタティックな送信元アドレスをバインドします。
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。

	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)# 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、Cisco Nexus デバイスの『System Management Configuration Guide』を参照してください。

コマンド	目的
show running-config dhcp	DHCP スヌーピング設定を表示します。
show ip dhcp relay	DHCP リレーの設定を表示します。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。

DHCP バインディングの表示

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

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

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

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

```
 500

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

DHCP スヌーピング バインディング データベースのクリア

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

はじめる前に

DHCP スヌーピングがイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ip dhcp snooping binding** 例： `switch# clear ip dhcp snooping binding`	（任意） DHCP スヌーピング バインディング データベースからすべてのエントリをクリアします。
ステップ 2	**clear ip dhcp snooping binding interface ethernet** *slot*/*port*[.*subinterface-number*] 例： `switch# clear ip dhcp snooping binding interface ethernet 1/4`	（任意） DHCP スヌーピング バインディング データベースから、特定のイーサネット インターフェイスに関連するエントリをクリアします。
ステップ 3	**clear ip dhcp snooping binding interface port-channel** *channel-number*[.*subchannel-number*] 例： `switch# clear ip dhcp snooping binding interface port-channel 72`	（任意） DHCP スヌーピング バインディング データベースから、特定のポート チャネル インターフェイスに関連するエントリをクリアします。
ステップ 4	**clear ip dhcp snooping binding vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface** {**ethernet** *slot*/*port*[.*subinterface-number* | **port-channel** *channel-number*[.*subchannel-number*] }	（任意） DHCP スヌーピング バインディング データベースから、特定のエントリをクリアします。

	コマンドまたはアクション	目的
	例： `switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface ethernet 2/11`	
ステップ 5	**show ip dhcp snooping binding** 例： `switch# show ip dhcp snooping binding`	（任意） DHCP スヌーピング バインディング データベースを表示します。

DHCP リレー統計情報のクリア

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

特定のインターフェイスの DHCP リレーの統計情報をクリアするには、**clear ip dhcp relay statistics interface** *interface* コマンドを使用します。

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

DHCP のモニタリング

DHCP スヌーピングをモニタするには、**show ip dhcp snooping statistics** コマンドを使用します。

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

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

DHCP スヌーピングの設定例

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

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

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

第 9 章

MAC ACL の設定

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

この章の内容は、次のとおりです。

- MAC ACL の概要，133 ページ
- MAC ACL のデフォルト設定，134 ページ
- MAC ACL の設定，134 ページ
- MAC ACL の設定の確認，142 ページ
- MAC ACL 統計情報のクリア，142 ページ

MAC ACL の概要

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

MAC パケット分類

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

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

MAC ACL のデフォルト設定

次の表に、MAC ACL パラメータのデフォルト設定を示します。

表 *14* : *MAC ACL* のデフォルト パラメータ

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

MAC ACL の設定

MAC ACL の作成

MAC ACL を作成し、これにルールを追加できます。

手順

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

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **macaccess-list***name*	MAC ACL を作成して、ACL コンフィギュレーション モードを開始します。
ステップ 3	switch(config-mac-acl)# {**permit** | **deny**}*sourcedestination protocol*	MAC ACL 内にルールを作成します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	switch(config-mac-acl)# **statistics per-entry**	（任意） そのACLのルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。
ステップ 5	switch(config-mac-acl)# **show mac access-lists***name*	（任意） MAC ACL の設定を表示します。
ステップ 6	switch(config-mac-acl)# **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 を作成する例を示します。

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

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

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

MAC ACL の変更

MAC ACL をデバイスから削除できます。

はじめる前に

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

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)# **macaccess-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**}*sourcedestination protocol*	（任意） 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**}*sourcedestination 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 per-entry**	（任意） その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 **no** オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 6	switch(config-mac-acl)# **show mac access-lists***name*	（任意） MAC ACL の設定を表示します。
ステップ 7	switch(config-mac-acl)# **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 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# 80 permit 00c0.4f00.00 0000.00ff.ffff any
switch(config-mac-acl)# no 80
switch(config-mac-acl)# statistics per-entry
switch(config-mac-acl)# show mac access-lists acl-mac-01
```

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

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

MAC ACL 内のシーケンス番号の変更

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

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)# **resequence mac access-list***namestarting-sequence-numberincrement*	ACL内に記述されているルールにシーケンス番号を付けます。 starting-sequence number に指定したシーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。
ステップ 3	switch(config)# **show mac access-lists***name*	（任意） MAC 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。

次に、MAC ACL のシーケンスを変更する例を示します。

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

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

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

MAC ACL の削除

MAC ACL をデバイスから削除できます。

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)# **nomacaccess-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(config)# **show mac access-lists***name***summary**	（任意） MAC ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	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、MAC ACL を削除する例を示します。

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

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

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

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

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

ポート ACL としての MAC ACL の適用

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

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

はじめる前に

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

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)# **interfaceethernet***slot*/*port* • switch(config)# **interfaceport-channel***channel-number*	• レイヤ2またはレイヤ3のインターフェイス コンフィギュレーション モードを開始します。 • レイヤ 2 またはレイヤ 3 のポート チャネル インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **mac port access-group***access-list*	MAC ACL をインターフェイスに適用します。
ステップ 4	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。

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

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

!Command: show running-config aclmgr
```

```
!Time: Sat Jul 19 23:36:04 2014

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

...

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

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

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

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

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

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


...

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

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

MAC パケット分類のイネーブル化またはディセーブル化

MAC パケット分類は、VLAN 単位でイネーブルまたはディセーブルにすることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **feature interface-vlan**	インターフェイス VLAN 機能をイネーブルにします。
ステップ 3	switch(config)# **interface vlan***interface-vlan-number*	VLANインターフェイスを作成します。number の範囲は 1 ～ 4094 です。
ステップ 4	switch(config-if)# [**no**] **mac packet-classify**	インターフェイスの MAC パケット分類をイネーブルにします。**no** オプションを使用すると、インターフェイスのMACパケット分類がディセーブルになります。
ステップ 5	switch(config-if)# **show running-config interface vlan***interface-vlan-number*	（任意） VLAN インターフェイスの実行コンフィギュレーションを表示します。
ステップ 6	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。

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

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

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

version 6.0(2)A4(1)

interface Vlan50
  mac packet-classify

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

MAC ACL の設定の確認

MAC ACL の設定情報を表示するには、次のいずれかの作業を実行します。

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

MAC ACL 統計情報のクリア

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

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

第 10 章

ユニキャスト RPF の設定

この章では、Cisco NX-OS デバイス上で出力トラフィックのレート制限を設定する手順について説明します。

この章は、次の項で構成されています。

- ユニキャスト RPF の概要，143 ページ
- ユニキャスト RPF のライセンス要件，145 ページ
- ユニキャスト RPF の注意事項と制約事項，145 ページ
- ユニキャスト RPF のデフォルト設定，146 ページ
- ユニキャスト RPF の設定，146 ページ
- ユニキャスト RPF の設定例，148 ページ
- ユニキャスト RPF の設定の確認，148 ページ

ユニキャスト RPF の概要

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

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

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

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

（注） ユニキャスト RPF では、コストが等しいすべての「最良」リターン パスが有効と見なされます。つまり、複数のリターン パスが存在していても、各パスのルーティング コスト（ホップ カウントや重みなど）が他のパスと等しく、そのルートが FIB 内にある限り、ユニキャスト RPF は機能します。ユニキャスト RPF は、Enhanced Interior Gateway Routing Protocol（EIGRP）バリアントが使用されていて、送信元 IP アドレスに戻る同等でない候補パスが存在する場合にも機能します。

Unicast RPF

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

Global Statistics

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

ユニキャスト RPF のライセンス要件

製品	ライセンス要件
Cisco NX-OS	ユニキャスト RPF にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ユニキャスト RPF の注意事項と制約事項

ユニキャスト RPF に関する注意事項と制約事項は次のとおりです。

- Cisco Nexus 3548 シリーズ スイッチの固有機能であるワープ モードで URPF を有効にすると、マルチキャスト エントリ数が半分になり、8 k から 4 k になります。同様に、ホスト エントリの数も、8 k の半分の 4 k になります。通常モードでは、サポートされる LPM エントリの数が半分に（24 k から 12 k に）なりますが、これは Cisco Nexus 3000 シリーズ スイッチの場合と同じです。
- ユニキャスト RPF は、ネットワーク内のより大きな部分からのダウンストリームのインターフェイスで適用する必要があります（ネットワークのエッジに適用するのが望ましい）。
- なるべくダウンストリームでユニキャスト RPF を適用する方が、アドレス スプーフィングの軽減やスプーフされたアドレスの送信元の特定の精度が高くなります。たとえば、集約デバイスでユニキャスト RPF を適用すると、多くのダウンストリーム ネットワークまたはクライアントからの攻撃を軽減できるとともに、管理が簡単になりますが、攻撃の送信元は特定できません。ネットワーク アクセス サーバにユニキャスト RPF を適用すると、攻撃の範囲を絞り、攻撃元を追跡しやすくなります。ただし、多数のサイトにユニキャスト RPF を展開すると、ネットワーク運用の管理コストが増加します。
- インターネット、イントラネット、およびエクストラネットのリソース全体でユニキャスト RPF を配布するエンティティが多いほど、インターネット コミュニティを通じた大規模なネットワークの中断が軽減される可能性が高くなり、攻撃の送信元をトレースできる可能性も高くなります。
- ユニキャスト RPF は、総称ルーティング カプセル化（GRE）トンネルのようなトンネルでカプセル化された IP パケットは検査しません。トンネリングとカプセル化のレイヤがパケットから除かれてからユニキャスト RPF がネットワーク トラフィックを処理するように、ホーム ゲートウェイにユニキャスト RPF を設定する必要があります。

- ユニキャスト RPF は、ネットワークからのアクセス ポイントが 1 つだけ、またはアップストリーム接続が 1 つだけの「単一ホーム」環境で使用できます。アクセス ポイントが 1 つのネットワークは対称ルーティングを提供します。これはつまり、パケットがネットワークに入るインターフェイスはその IP パケットの送信元への最良のリターン パスでもあるということです。
- ネットワーク内部のインターフェイスにはユニキャストRPFを使用しないでください。内部インターフェイスは、ルーティングを非対称にする可能性が高く、パケットの送信元へのルートが複数存在する場合が多いからです。ユニキャストRPFを設定するのは、元々対称であるか、対称に設定されている場合だけにしてください。ストリクト ユニキャスト RPF を設定しないでください。
- ユニキャスト RPF を使用すると、送信元が 0.0.0.0 で宛先が 255.255.255.255 のパケットを通過させて、ブートストラップ プロトコル（BOOTP）と Dynamic Host Configuration Protocol（DHCP）を正しく動作させることができます。

ユニキャスト RPF のデフォルト設定

次の表に、ユニキャスト RPF パラメータのデフォルト設定を示します。

表 *15*：ユニキャスト *RPF* パラメータのデフォルト設定

パラメータ	デフォルト
Unicast RPF	ディセーブル

ユニキャスト RPF の設定

入力インターフェイスに次のいずれかのユニキャスト RPF モードを設定できます。

ストリクト ユニキャスト RPF モード

厳格モードでは、ユニキャストRPFがFIBで一致するパケット送信元アドレスを見つけて、パケットを受信した入力インターフェイスが FIB 内のユニキャスト RPF インターフェイスのいずれかと一致した場合に、チェックに合格します。チェックに合格しないと、パケットは廃棄されます。このタイプのユニキャスト RPF チェックは、パケット フローが対称であると予想される場合に使用できます。

ルーズ ユニキャスト RPF モード

緩和モードでは、FIB でのパケット送信元アドレスのルックアップで一致が戻り、FIB の結果からその送信元が少なくとも1つの実インターフェイスで到達可能であることが示された場合に、チェックに合格します。パケットを受信した入力インターフェイスがFIB内のインターフェイスのいずれかと一致する必要はありません。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		イーサネット インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**ip verify unicast source reachable-via** {**any** [**allow-default**] | **rx**} 例： `switch(config-if)# ip verify unicast source reachable-via any`	IPv4 用インターフェイスにユニキャスト RPF を設定します。 **any** キーワードはルーズ モードのユニキャスト RPF を指定します。 **allow-default** キーワードを指定すると、送信元アドレスのルックアップでデフォルト ルートと一致させることが可能になり、それを検証に使用できます。 **rx** キーワードは厳格モードのユニキャスト RPF を指定します。

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

ステップ 5	**show ip interface ethernet***slot*/*port* 例： `switch(config)# show ip interface ethernet 2/3`	（任意） インターフェイスの IP 情報を表示します。
ステップ 6	**show running-config interface ethernet***slot*/*port* 例： `switch(config)# show running-config interface ethernet 2/3`	（任意） 実行コンフィギュレーション内のインターフェイスの情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユニキャスト RPF の設定例

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

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

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

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

ユニキャスト RPF の設定の確認

ユニキャスト RPF の設定情報を表示するには、次のいずれかの作業を行います。

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

第 11 章

コントロール プレーン ポリシングの設定

この章の内容は、次のとおりです。

- CoPP の概要，150 ページ
- コントロール プレーン保護，151 ページ
- CoPP ポリシー テンプレート，153 ページ
- CoPP クラス マップ，157 ページ
- 1 秒間あたりのパケットのクレジット制限，157 ページ
- CoPP と管理インターフェイス，157 ページ
- CoPP のライセンス要件，158 ページ
- CoPP の注意事項と制約事項，158 ページ
- CoPP のアップグレードに関する注意事項，159 ページ
- CoPP の設定，160 ページ
- CoPP show コマンド，163 ページ
- CoPP 設定ステータスの表示，165 ページ
- CoPP のモニタリング，165 ページ
- CoPP 統計情報のクリア，166 ページ
- CoPP の設定例，166 ページ
- CoPP の設定例，168 ページ
- 例：セットアップユーティリティによるデフォルト CoPP ポリシーの変更または再適用，170 ページ

CoPP の概要

コントロール プレーン ポリシング（CoPP）はコントロール プレーンを保護し、それをデータ プレーンから分離することによって、ネットワークの安定性、到達可能性、およびパケット配信を保証します。

この機能により、コントロールプレーンにポリシーマップを適用できるようになります。このポリシー マップは通常の QoS ポリシーのように見え、ルータまたはレイヤ 3 スイッチの任意の IP アドレスに宛てられたすべてのトラフィックに適用されます。ネットワーク デバイスへの一般的な攻撃ベクトルは、過剰なトラフィックがデバイス インターフェイスに転送されるサービス拒絶（DoS）攻撃です。

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

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

データ プレーン

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

制御プレーン

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

管理プレーン

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

スーパーバイザ モジュールには、マネージメント プレーンとコントロール プレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。スーパーバイザ モジュールの動作が途絶したり、スーパーバイザ モジュールが攻撃されたりすると、重大なネットワークの停止につながります。たとえばスーパーバイザに過剰なトラフィックが加わると、スーパーバイザ モジュールが過負荷になり、NX-OS デバイス全体のパフォーマンスが低下する可能性があります。またたとえば、スーパーバイザ モジュールに対する DoS 攻撃は、コントロール プレーンに対して非常に高速に IP トラフィック ストリームを生成することがあります。これにより、コントロール プレーンは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

次に、DoS 攻撃の例を示します。

- インターネット制御メッセージ プロトコル（ICMP）エコー要求

- IP フラグメント
- TCP SYN フラッディング

これらの攻撃によりデバイスのパフォーマンスが影響を受け、次のようなマイナスの結果をもたらします。

- サービス品質の低下（音声、ビデオ、または重要なアプリケーション トラフィックの低下など）
- ルート プロセッサまたはスイッチ プロセッサの高い CPU 使用率
- ルーティング プロトコルのアップデートまたはキープアライブの消失によるルート フラップ
- 不安定なレイヤ 2 トポロジ
- CLI との低速な、または応答を返さない対話型セッション
- メモリやバッファなどのプロセッサ リソースの枯渇
- 着信パケットの無差別のドロップ

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

コントロール プレーン保護

コントロール プレーンを保護するために、Cisco NX-OS デバイスはコントロール プレーンに向かうさまざまなパケットを異なるクラスに分離します。クラスの識別が終わると、Cisco NX-OS デバイスはパケットをポリシングします。これにより、スーパーバイザ モジュールに過剰な負担がかからないようになります。

コントロール プレーンのパケット タイプ

コントロール プレーンには、次のような異なるタイプのパケットが到達します。

受信パケット

ルータの宛先アドレスを持つパケット。宛先アドレスには、レイヤ2アドレス（ルータ MAC アドレスなど）やレイヤ 3 アドレス（ルータ インターフェイスの IP アドレスなど）があります。これらのパケットには、ルータ アップデートとキープアライブ メッセージも含まれます。ルータが使用するマルチキャスト アドレス宛てに送信されるマルチキャスト パケットも、このカテゴリに入ります。

例外パケット

スーパーバイザ モジュールによる特殊な処理を必要とするパケット。たとえば、宛先アドレスが Forwarding Information Base（FIB; 転送情報ベース）に存在せず、結果としてミスとなった場合は、スーパーバイザ モジュールが送信側に到達不能パケットを返します。他には、IP オプションがセットされたパケットもあります。

リダイレクト パケット

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

収集パケット

宛先 IP アドレスのレイヤ 2 MAC アドレスが FIB に存在していない場合は、スーパーバイザ モジュールがパケットを受信し、ARP 要求をそのホストに送信します。

これらのさまざまなパケットはすべて、コントロール プレーンへの悪意ある攻撃に利用され、Cisco NX-OS デバイスに過剰な負荷をかける可能性があります。CoPP は、これらのパケットを異なるクラスに分類し、これらのパケットをスーパーバイザが受信する速度を個別に制御するメカニズムを提供します。

CoPP の分類

効果的に保護するために、Cisco NX-OS デバイスはスーパーバイザ モジュールに到達するパケットを分類して、パケット タイプに基づいた異なるレート制御ポリシーを適用できるようにします。たとえば、Hello メッセージなどのプロトコル パケットには厳格さを緩め、IP オプションがセットされているためにスーパーバイザ モジュールに送信されるパケットには厳格さを強めることが考えられます。クラスマップとポリシーマップを使用して、パケットの分類およびレート制御ポリシーを設定します。

パケットの分類には、次のパラメータを使用できます。

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

レート制御メカニズム

パケットの分類が終わると、Cisco NX-OS デバイスにはスーパーバイザ モジュールに到達するパケットのレートを制御するメカニズムがあります。

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

CoPP ポリシー テンプレート

Cisco NX-OS デバイスの初回起動時には、DoS 攻撃からスーパーバイザ モジュールを保護するためのデフォルト copp-system-policy が Cisco NX-OS ソフトウェアによってインストールされます。最初のセットアップ ユーティリティで、次のいずれかの CoPP ポリシー オプションを選択することにより、展開シナリオの CoPP ポリシー テンプレートを選択できます。

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

オプションを選択しなかった場合や、セットアップ ユーティリティを実行しなかった場合には、Cisco NX-OS ソフトウェアにより Default ポリシングが適用されます。最初はこのデフォルト ポリシーを使用し、必要に応じて CoPP ポリシーを変更することを推奨します。

デフォルトの copp-system-policy ポリシーには、基本的なデバイス操作に最も適した値が設定されています。使用する DoS に対する保護要件に適合するよう、特定のクラスやアクセス コントロール リスト（ACL）を追加する必要があります。

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

デフォルト CoPP ポリシー

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

このポリシーの設定は次のとおりです。

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

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

レイヤ 2 CoPP ポリシー

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

このポリシーの設定は次のとおりです。

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

```
    police pps 100
```

レイヤ 3 CoPP ポリシー

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

このポリシーの設定は次のとおりです。

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

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

CoPP クラス マップ

ポリシー内のクラスには、次の 2 つのタイプがあります。

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

（注） copp-s-x という名前のクラスはスタティック クラスです。

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

1 秒間あたりのパケットのクレジット制限

特定のポリシーの 1 秒間あたりのパケット（PPS）の合計（ポリシーの各クラス部分の PPS の合計）の上限は、PPS のクレジット制限（PCL）の上限になります。特定のクラスの PPS が増加して PCL 超過すると、設定が拒否されます。目的の PPS を増やすには、PCL を超える PPS の分を他のクラスから減少させる必要があります。

CoPP と管理インターフェイス

Cisco NX-OS デバイスは、管理インターフェイス（mgmt0）をサポートしないハードウェア ベースの CoPP だけをサポートします。アウトオブバンド mgmt0 インターフェイスは CPU に直接接続するため、CoPP が実装されているインバンド トラフィック ハードウェアは通過しません。

mgmt0 インターフェイスで、ACL を設定して、特定タイプのトラフィックへのアクセスを許可または拒否することができます。

CoPP のライセンス要件

この機能には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべてCisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

CoPP の注意事項と制約事項

CoPP に関する注意事項と制約事項は次のとおりです。

- 導入のシナリオに応じてデフォルト、L2、またはL3 ポリシーを選択し、観察された動作に基づいて、CoPP ポリシーを後で変更することを推奨します。
- fast-reload を実行した後、トラフィックが完全に収束してから、トラフィックにおいて +/- 2 ～ 5 % の不規則性が約 30 ～ 40 秒間発生する場合は、ARP パケットに関する CoPP 値を大きくします。
- CoPP のカスタマイズは継続的なプロセスです。CoPP を設定するときには、特定の環境で使用されるプロトコルや機能に加えて、サーバ環境に必要なスーパーバイザ機能を考慮する必要があります。これらのプロトコルや機能が変更されたら、CoPP を変更する必要があります。
- Release 6.0(2)U6(1) の場合、**write erase** コマンドとリロードにより、**copp-s-bfd** コマンドに関して、ポリシングの1秒間あたりのパケット（PPS）のデフォルト値が900に変更されます。
- CoPP を継続的にモニタすることを推奨します。ドロップが発生した場合は、CoPP がトラフィックを誤ってドロップしたのか、または誤動作や攻撃に応答してドロップしたのかを判定してください。どちらの場合も、状況を分析して、別の CoPP ポリシーを使用するか、またはカスタマイズ済み CoPP ポリシーを変更する必要があるかどうかを評価します。
- Cisco NX-OS ソフトウェアは、出力 CoPP とサイレント モードをサポートしません。CoPP は入力だけでサポートされます。**service-policy output copp** は、コントロールプレーン インターフェイスには適用できません。
- 新しい CoPP ポリシーの作成はサポートされていません。
- glean（キャッシュ モードのクラス デフォルトのクラス マップ）に関するハードウェア カウンタはありません。
- 通常モードのクラス デフォルトに関するハードウェア カウンタはありません。
- MTU 障害クラス マップに関するカウンタはありません。
- 現時点では、BPDU、CDP、LACP、およびLLDPに関してハードウェア カウンタが共有されます。
- NAT に関するハードウェア カウンタはありません。
- DHCPREQ/DHCPRESP に関するハードウェア カウンタはありません。

- l3destmiss に関するハードウェア カウンタはありません。
- TTL1 に関するハードウェア カウンタはありません。
- IPMCMISS に関するハードウェア カウンタはありません。
- スタティック クラス マップには match acl ステートメントを追加できません。
- Release 6.0(2)U5(1) 以降では、トンネルが設定されていない場合、Cisco Nexus 3000 シリーズ スイッチは、すべてのパケットをドロップします。また、トンネルが設定されている場合でも、トンネルインターフェイスが設定されていないか、トンネルインターフェイスがシャットダウン状態のときは、パケットがドロップされます。

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

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

CoPP のアップグレードに関する注意事項

CoPP には、アップグレードに関する次の注意事項があります。

- CoPP 機能をサポートしない Cisco NX-OS リリースから CoPP 機能をサポートする Cisco NX-OS リリースにアップグレードする場合は、スイッチの起動時にデフォルト ポリシーを使って CoPP が自動的にイネーブルにされます。別のポリシー（デフォルト、l3、l2）をイネーブルにするには、アップグレード後にセットアップ スクリプトを実行する必要があります。CoPP 保護を設定しない場合、NX-OS デバイスは DoS 攻撃に対して脆弱な状態のままになります。
- CoPP 機能をサポートする Cisco NX-OS リリースから、新しいプロトコルの追加クラスを含む CoPP 機能をサポートする Cisco NX-OS リリースにアップグレードする場合は、CoPP の新しいクラスを使用可能にするためにセットアップ ユーティリティを実行する必要があります。
- セットアップ スクリプトは、CPU に着信するさまざまなフローに対応するポリシング レートを変更するため、デバイスにトラフィックが発生する時間ではなく、スケジュールされたメンテナンス期間にセットアップ スクリプトを実行することを推奨します。

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

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

CoPP の設定

コントロール プレーン クラス マップの設定

コントロール プレーン ポリシーのコントロール プレーン クラス マップを設定する必要があります。

トラフィックを分類するには、既存の ACL に基づいてパケットを照合します。ACL キーワード permit および deny は、マッチング時には無視されます。

はじめる前に

クラス マップ内で ACE ヒット カウンタを使用する場合は、IP ACL が設定してあることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**class-map type control-plane match-any** *class-map-name*
	
	例：
	`switch(config)# class-map type control-plane ClassMapA`
	`switch(config-cmap)#`
		コントロール プレーン クラス マップを指定し、クラス マップ コンフィギュレーション モードを開始します。デフォルトのクラス一致は match-any です。名前は最大 64 文字で、大文字と小文字は区別されます。
		（注） class-default、match-all、または match-any をクラス マップ名に使用できません。

ステップ 3	**match access-group name***access-list-name* 例： `switch(config-cmap)# match access-group name MyAccessList`	（任意） IP ACL のマッチングを指定します。複数の IP ACL のマッチングを行う場合は、このステップを繰り返します。

	コマンドまたはアクション	目的
		（注） ACL キーワード **permit** および **deny** は、CoPP マッチング時には無視されます。

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

ステップ 5	**show class-map type control-plane** [*class-map-name*] 例： `switch(config)# show class-map type control-plane`	（任意） コントロール プレーン クラス マップの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `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。

コントロール プレーン ポリシー マップの設定

CoPP のポリシー マップを設定する必要があります。ポリシー マップにはポリシング パラメータを含めます。クラスのポリサーを設定しなかった場合、デフォルトの PPS をサポートします。

IPv4 パケットのポリシーを設定できます。

はじめる前に

コントロール プレーン クラス マップが設定してあることを確認します。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的

ステップ 2	**policy-map type control-plane***policy-map-name*
	
	例：
	`switch(config)# policy-map type control-plane copp-system-policy`
	`switch(config-pmap)#`
		コントロール プレーン ポリシー マップを指定し、ポリシー マップ コンフィギュレーション モードを開始します。ポリシーマップ名は大文字と小文字が区別されます。
		（注） ポリシーマップ名は変更できません。ポリシー マップの **copp-system-policy** 名のみを使用できます。単一の **type control-plane** ポリシー マップのみを設定できます。

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

ステップ 4	**police** [**pps**] {*pps-value*} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**] 例： `switch(config-pmap-c)# police pps 100 bc 10`	1 秒間あたりのパケット（PPS）およびコミット済みバースト（BC）に関するレート制限を指定します。PPS の範囲は 0 ～ 20,000 です。デフォルト PPS は 0 です。BC の範囲は 0 ～ 512000000 です。デフォルト BC サイズの単位はバイトです。

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

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

ステップ 7	**show policy-map type control-plane** [**expand**] [**name***class-map-name*] 例： `switch(config)# show policy-map type control-plane`	（任意） コントロール プレーン ポリシー マップの設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

コントロール プレーン サービス ポリシーの設定

はじめる前に

コントロール プレーン ポリシー マップを設定します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**control-plane**
	
	例：
	`switch(config) # control-plane`
	`switch(config-cp)#`
		コントロール プレーン コンフィギュレーション モードを開始します。

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

ステップ 4	**show running-config copp** [**all**] 例： `switch(config)# show running-config copp`	（任意） CoPP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

CoPP show コマンド

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

コマンド	目的
show ip access-lists [*acl-name*]	CoPP の ACL を含め、システム内で設定されているすべての IPv4 ACL を表示します。
show class-map type control-plane [*class-map-name*]	このクラス マップにバインドされている ACL を含め、コントロール プレーン クラス マップの設定を表示します。
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	コントロール プレーン ポリシー マップと関連するクラス マップおよびPPSの値を表示します。
show running-config copp [**all**]	実行コンフィギュレーション内の CoPP 設定を表示します。
show running-config aclmgr [**all**]	実行コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。**all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show startup-config copp [**all**]	スタートアップ コンフィギュレーション内の CoPP 設定を表示します。
show startup-config aclmgr [**all**]	スタートアップ コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。**all** オプションを使用すると、スタートアップコンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

CoPP 設定ステータスの表示

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# **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。

次に、CoPP をモニタする例を示します。

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

service-policy  input: copp-system-policy

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


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

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

CoPP 統計情報のクリア

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show policy-map interface control-plane**	（任意） 現在適用されている CoPP ポリシーおよびクラスごとの統計情報を表示します。
ステップ 2	switch# **clear copp statistics**	CoPP 統計情報をクリアします。

次に、インターフェース環境で、CoPP 統計情報をクリアする例を示します。

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

CoPP の設定例

IP ACL の作成

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

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

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

関連する IP ACL を使用したサンプル CoPP クラスの作成

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

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

次に、CoPP ポリシーにクラスを追加する例を示します。

```
policy-map type control-plane copp-system-policy
Class copp-sample-class
 Police pps 100
```

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

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

既存または新規の CoPP のクラスと ACL を関連付ける

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

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

CoPP ポリシーにクラスを追加

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

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

ARP ACL ベースのダイナミック クラスの作成

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

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

ARP ACL の作成

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

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

CoPP クラスの作成と ARP ACL の関連付け

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

CoPP ポリシーからのクラスの削除

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

システムからのクラスの削除

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

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

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

CoPP の設定例

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

```
IP access list copp-system-acl-eigrp
        10 permit eigrp any 224.0.0.10/32
IP access list copp-system-acl-icmp
        10 permit icmp any any
IP access list copp-system-acl-igmp
        10 permit igmp any any
IP access list copp-system-acl-ntp
        10 permit udp any any eq ntp
        20 permit udp any eq ntp any
IP access list copp-system-acl-pimreg
        10 permit pim any any
IP access list copp-system-acl-ping
        10 permit icmp any any echo
        20 permit icmp any any echo-reply
IP access list copp-system-acl-routingproto1
        10 permit tcp any gt 1024 any eq bgp
        20 permit tcp any eq bgp any gt 1024
        30 permit udp any 224.0.0.0/24 eq rip
        40 permit tcp any gt 1024 any eq 639
        50 permit tcp any eq 639 any gt 1024
        70 permit ospf any any
        80 permit ospf any 224.0.0.5/32
        90 permit ospf any 224.0.0.6/32
IP access list copp-system-acl-routingproto2
        10 permit udp any 224.0.0.0/24 eq 1985
        20 permit 112 any 224.0.0.0/24
IP access list copp-system-acl-snmp
        10 permit udp any any eq snmp
        20 permit udp any any eq snmptrap
IP access list copp-system-acl-ssh
        10 permit tcp any any eq 22
        20 permit tcp any eq 22 any
IP access list copp-system-acl-stftp
        10 permit udp any any eq tftp
        20 permit udp any any eq 1758
        30 permit udp any eq tftp any
        40 permit udp any eq 1758 any
        50 permit tcp any any eq 115
        60 permit tcp any eq 115 any
IP access list copp-system-acl-tacacsradius
        10 permit tcp any any eq tacacs
        20 permit tcp any eq tacacs any
        30 permit udp any any eq 1812
        40 permit udp any any eq 1813
        50 permit udp any any eq 1645
        60 permit udp any any eq 1646
        70 permit udp any eq 1812 any
        80 permit udp any eq 1813 any
        90 permit udp any eq 1645 any
        100 permit udp any eq 1646 any
IP access list copp-system-acl-telnet
        10 permit tcp any any eq telnet
        20 permit tcp any any eq 107
        30 permit tcp any eq telnet any
        40 permit tcp any eq 107 any
IP access list copp-system-dhcp-relay
        10 permit udp any eq bootps any eq bootps
IP access list test
        statistics per-entry
        10 permit ip 1.2.3.4/32 5.6.7.8/32 [match=0]
        20 permit udp 11.22.33.44/32 any [match=0]
        30 deny udp 1.1.1.1/32 any [match=0]


class-map type control-plane match-any copp-icmp
```

```
  match access-group name copp-system-acl-icmp
class-map type control-plane match-any copp-ntp
  match access-group name copp-system-acl-ntp
class-map type control-plane match-any copp-s-arp
class-map type control-plane match-any copp-s-bfd
class-map type control-plane match-any copp-s-bpdu
class-map type control-plane match-any copp-s-dai
class-map type control-plane match-any copp-s-default
class-map type control-plane match-any copp-s-dhcpreq
  match access-group name copp-system-acl-dhcps6
class-map type control-plane match-any copp-s-dhcpresp
  match access-group name copp-system-acl-dhcpc6
  match access-group name copp-system-dhcp-relay
class-map type control-plane match-any copp-s-eigrp
  match access-group name copp-system-acl-eigrp
  match access-group name copp-system-acl-eigrp6
class-map type control-plane match-any copp-s-glean
class-map type control-plane match-any copp-s-igmp
  match access-group name copp-system-acl-igmp
class-map type control-plane match-any copp-s-ipmcmiss
class-map type control-plane match-any copp-s-l2switched
class-map type control-plane match-any copp-s-l3destmiss
class-map type control-plane match-any copp-s-l3mtufail
class-map type control-plane match-any copp-s-l3slowpath
class-map type control-plane match-any copp-s-pimautorp
class-map type control-plane match-any copp-s-pimreg
  match access-group name copp-system-acl-pimreg
class-map type control-plane match-any copp-s-ping
  match access-group name copp-system-acl-ping
class-map type control-plane match-any copp-s-ptp
class-map type control-plane match-any copp-s-routingProto1
  match access-group name copp-system-acl-routingproto1
  match access-group name copp-system-acl-v6routingproto1
class-map type control-plane match-any copp-s-routingProto2
  match access-group name copp-system-acl-routingproto2
class-map type control-plane match-any copp-s-selfIp
class-map type control-plane match-any copp-s-ttl1
class-map type control-plane match-any copp-s-v6routingProto2
  match access-group name copp-system-acl-v6routingProto2
class-map type control-plane match-any copp-snmp
  match access-group name copp-system-acl-snmp
class-map type control-plane match-any copp-ssh
  match access-group name copp-system-acl-ssh
class-map type control-plane match-any copp-stftp
  match access-group name copp-system-acl-stftp
class-map type control-plane match-any copp-tacacsradius
  match access-group name copp-system-acl-tacacsradius
class-map type control-plane match-any copp-telnet
  match access-group name copp-system-acl-telnet
policy-map type control-plane copp-system-policy
  class copp-s-selfIp
    police pps 500
  class copp-s-default
    police pps 400
  class copp-s-l2switched
    police pps 200
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-l3slowpath
    police pps 100
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
```

```
    police pps 300
  class copp-s-dai
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 1300
  class copp-s-v6routingProto2
    police pps 1300
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 1000
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bfd
    police pps 350
  class copp-s-bpdu
    police pps 12000
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
control-plane
  service-policy input copp-system-policy
```

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

セットアップ ユーティリティを使用して、デフォルト CoPP ポリシーを変更または再適用する例を次に示します。

```
switch# setup

         ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

  Create another login account (yes/no) [n]: n
```

```
  Configure read-only SNMP community string (yes/no) [n]: n

  Configure read-write SNMP community string (yes/no) [n]: n

  Enter the switch name : switch

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

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

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

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

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

  Configure CoPP System Policy Profile ( default / l2 / l3 ) [default]: l2

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

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

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

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

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

索 引

A

ACL の暗黙のルール 83

C

CoPP 152

I

IP ACL の暗黙のルール 83

M

MAC ACL の暗黙のルール 83

R

RADIUS サーバの事前共有キー 31
RADIUS のグローバルな事前共有キー 30
RADIUS、サーバの定期的なモニタリング 38

S

SSH クライアント 69
SSH サーバ 69
SSH サーバ キー 70

T

Telnet サーバ 70

こ

コントロール プレーン保護、分類 152

さ

サーバ グループ 9

て

デフォルト CoPP ポリシー 153

へ

ベンダー固有属性 20

ほ

ポート ACL 93

る

ルータ ACL 94