Cisco Nexus 3000 シリーズ NX-OS リリース 5.0(3)U2(2) セキュリティ コンフィギュレーション ガイド

初版：2011 年 10 月 13 日

最終更新：2012 年 02 月 24 日

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

Text Part Number: OL-25780-01-J

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

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

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

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

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

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

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

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

© 2011-2012 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xiii

対象読者 xiii

表記法 xiii

Nexus 3000 シリーズ NX-OS ソフトウェアの関連資料 xv

マニュアルの入手方法およびテクニカル サポート xvi

このリリースの新規および変更情報 1

新機能および変更された機能に関する情報 1

概要 3

認証、許可、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 について 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 サーバ設定オプション 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 16
MSCHAP 認証のイネーブル化 18
AAA アカウンティングのデフォルト方式の設定 19
AAA サーバの VSA の使用 21
VSA 21
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 22
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 23
AAA の設定例 24
デフォルトの AAA 設定 24
RADIUS の設定 25
RADIUS の設定 25
RADIUS について 25
RADIUS ネットワーク環境 25
RADIUS の操作について 26
RADIUS サーバ 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 29
RADIUS サーバ ホストの設定 29
RADIUS のグローバルな事前共有キーの設定 30
RADIUS サーバの事前共有キーの設定 32
RADIUS サーバ グループの設定 33
RADIUS サーバ グループのためのグローバル発信元インターフェイスの設定 34
ログイン時にユーザによる RADIUS サーバの指定を許可 35
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 36
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 37
RADIUS サーバのアカウンティングおよび認証属性の設定 39
RADIUS サーバの定期的モニタリングの設定 40

デッド タイム間隔の設定 42
RADIUS サーバまたはサーバ グループの手動モニタリング 43
RADIUS 設定の確認 43
RADIUS サーバの統計情報のモニタリング 44
RADIUS サーバ統計情報のクリア 44
RADIUS の設定例 45
RADIUS のデフォルト設定 45
TACACS+ の設定 47
TACACS+ の設定について 47
TACACS+ について 47
TACACS+ の利点 47
TACACS+ を使用したユーザ ログイン 48
デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー 49
TACACS+ サーバのコマンド許可サポート 49
TACACS+ サーバのモニタリング 49
TACACS+ の前提条件 50
TACACS+ の注意事項と制約事項 50
TACACS+ の設定 51
TACACS+ サーバの設定プロセス 51
TACACS+ のイネーブル化 51
TACACS+ サーバ ホストの設定 52
TACACS+ のグローバルな事前共有キーの設定 53
TACACS+ サーバの事前共有キーの設定 54
TACACS+ サーバ グループの設定 56
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 57
ログイン時の TACACS+ サーバの指定 58
TACACS+ サーバでの AAA 許可の設定 59
TACACS+ サーバでのコマンド許可の設定 60
TACACS+ サーバでのコマンド許可のテスト 62
コマンド許可検証のイネーブル化とディセーブル化 63
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 64

権限ロールのユーザ コマンドの許可または拒否 66
グローバルな TACACS+ タイムアウト間隔の設定 67
サーバのタイムアウト間隔の設定 68
TCP ポートの設定 69
TACACS+ サーバの定期的モニタリングの設定 70
デッド タイム間隔の設定 72
TACACS+ サーバまたはサーバ グループの手動モニタリング 73
TACACS+ のディセーブル化 73
TACACS+ 統計情報のモニタリング 74
TACACS+ の設定の確認 74
TACACS+ の設定例 75
TACACS+ のデフォルト設定 75
SSH および Telnet の設定 77
SSH および Telnet の設定 77
SSH および Telnet の概要 77
SSH サーバ 77
SSH クライアント 77
SSH サーバ キー 78
Telnet サーバ 78
SSH の注意事項および制約事項 78
SSH の設定 79
SSH サーバ キーの生成 79
ユーザ アカウント用 SSH 公開キーの指定 80
Open SSH 形式による SSH 公開キーの指定 80
IETF SECSH 形式による SSH 公開キーの指定 81
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 82
リモート デバイスとの SSH セッションの開始 83
SSH ホストのクリア 83
SSH サーバのディセーブル化 83
SSH サーバ キーの削除 84
SSH セッションのクリア 85

SSH の設定例 85
Telnet の設定 87
Telnet サーバのディセーブル化 87
Telnet サーバの再イネーブル化 87
リモート デバイスとの Telnet セッションの開始 87
Telnet セッションのクリア 88
SSH および Telnet の設定の確認 89
SSH のデフォルト設定 89
アクセス コントロール リストの設定 91
ACL について 91
IP ACL のタイプと適用 92
適用順序 93
ルール 93
送信元と宛先 93
プロトコル 93
暗黙のルール 94
その他のフィルタリング オプション 94
シーケンス番号 94
論理演算子と論理演算ユニット 95
ACL TCAM リージョン 96
ACL のライセンス要件 98
ACL の前提条件 98
ACL の注意事項および制約事項 98
デフォルトの ACL 設定 99
IP ACL の設定 100
IP ACL の作成 100
IP ACL の変更 101
IP ACL の削除 102
IP ACL 内のシーケンス番号の変更 103
mgmt0 への IP-ACL の適用 104
IP ACL のポート ACL としての適用 105
ルータ ACL としての IP ACL の適用 106

IP ACL の設定の確認 108
IP ACL の統計情報のモニタリングとクリア 108
VLAN ACL の概要 109
VACL とアクセス マップ 109
VACL とアクション 109
統計情報 109
VACL の設定 110
VACL の作成または変更 110
VACL の削除 111
VACL の VLAN への適用 112
VACL の設定の確認 113
VACL 統計情報の表示と消去 113
VACL の設定例 113
ACL TCAM リージョン サイズの設定 113
デフォルト TCAM リージョン サイズに戻す 116
仮想端末回線の ACL の設定 117
VTY 回線の ACL の確認 118
VTY 回線の ACL の設定例 119
DHCP スヌーピングの設定 121
DHCP スヌーピングの概要 121
機能のイネーブル化とグローバルなイネーブル化 122
信頼できるソースおよび信頼できないソース 123
DHCP スヌーピング バインディング データベース 123
DHCP リレー エージェントの概要 124
DHCP リレー エージェント 124
DHCP リレー エージェントに対する VRF サポート 124
DHCP リレー バインディング データベース 125
DHCP スヌーピングの注意事項および制約事項 125
DHCP スヌーピングのデフォルト設定 126
DHCP スヌーピングの設定 126
DHCP スヌーピングの最小設定 126
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 127

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 128
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 129
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 130
インターフェイスの信頼状態の設定 131
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 133
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 134
DHCP スタティック バインディングの作成 135
DHCP スヌーピング設定の確認 136
DHCP バインディングの表示 137
DHCP スヌーピング バインディング データベースのクリア 137
DHCP スヌーピングの設定例 138
ダイナミック ARP インスペクションの設定 139
DAI の概要 139
ARP 139
ARP スプーフィング攻撃 140
DAI および ARP スプーフィング攻撃 141
インターフェイスの信頼状態とネットワーク セキュリティ 141
DAI パケットのロギング 143
DAI のライセンス要件 143
DAI の前提条件 144
DAI の注意事項と制約事項 144
DAI のデフォルト設定 145
DAI の設定 146
VLAN での DAI のイネーブル化とディセーブル化 146
レイヤ 2 インターフェイスの DAI 信頼状態の設定 147
追加検証のイネーブル化またはディセーブル化 148
DAI のログ バッファ サイズの設定 150
DAI のログ フィルタリングの設定 150
DAI の設定の確認 152
DAI の統計情報のモニタリングとクリア 152
DAI の設定例 153

例 1：2 つのデバイスが DAI をサポートする場合 153
デバイス A の設定 154
デバイス B の設定 155
ユニキャスト RPF の設定 159
ユニキャスト RPF の概要 159
ユニキャスト RPF プロセス 160
グローバル統計情報 161
ユニキャスト RPF のライセンス要件 161
ユニキャスト RPF の注意事項と制約事項 162
ユニキャスト RPF のデフォルト設定 163
ユニキャスト RPF の設定 163
ユニキャスト RPF の設定例 165
ユニキャスト RPF の設定の確認 165
コントロール プレーン ポリシングの設定 167
CoPP の概要 168
コントロール プレーンの保護 169
コントロール プレーンのパケット タイプ 169
CoPP の分類 170
レート制御メカニズム 171
CoPP ポリシー テンプレート 171
デフォルト CoPP ポリシー 171
レイヤ 2 CoPP ポリシー 172
レイヤ 3 CoPP ポリシー 173
CoPP のクラス マップ 174
1 秒間あたりのパケットのクレジット制限 175
CoPP と管理インターフェイス 175
CoPP のライセンス要件 175
CoPP の注意事項と制約事項 175
CoPP のアップグレードの注意事項 176
CoPP の設定 176
コントロール プレーン クラス マップの設定 176
コントロール プレーン ポリシー マップの設定 178

コントロール プレーン サービス ポリシーの設定 179
CoPP show コマンド 181
CoPP 設定ステータスの表示 182
CoPP のモニタ 182
CoPP 統計情報のクリア 183
CoPP の設定例 184
CoPP の設定例 185
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 188
CoPP に関する追加情報 189
CoPP の機能の履歴 189

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
- Nexus 3000 シリーズ NX-OS ソフトウェアの関連資料，xv ページ
- マニュアルの入手方法およびテクニカル サポート，xvi ページ

対象読者

この出版物は Cisco Nexus シリーズ デバイスの設定と保守を行う経験豊富なネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	角カッコで囲まれているものは、省略可能な要素（キーワードまたは引数）です。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

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

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

Nexus 3000 シリーズ NX-OS ソフトウェアの関連資料

完全な Cisco NX-OS 3000 シリーズ マニュアル セットは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html

インストレーション ガイドおよびアップグレード ガイド

インストールおよびアップグレード ガイドは次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/prod_installation_guides_list.html

このカテゴリのマニュアルは次のとおりです。

- *Cisco Nexus 5000* シリーズ、*Cisco Nexus 3000* シリーズ、および *Cisco Nexus 2000* シリーズの安全に関する情報およびドキュメント
- 『*Regulatory, Compliance, and Safety Information for the Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series*』
- 『*Cisco Nexus 3000 Series Hardware Installation Guide*』

コンフィギュレーション ガイド

コンフィギュレーション ガイドは次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/products_installation_and_configuration_guides_list.html

このカテゴリのマニュアルは次のとおりです。

- 『*Fundamentals Configuration Guide*』
- 『*Interfaces Configuration Guide*』
- 『*Layer 2 Switching Configuration Guide*』
- 『*Multicast Configuration Guide*』
- 『*Quality of Service Configuration Guide*』
- 『*Security Configuration Guide*』
- 『*System Management Configuration Guide*』

- 『*Unicast Routing Configuration Guide*』
- 『*Verified Scalability Guide for Cisco NX-OS*』

テクニカル リファレンス

テクニカル リファレンスは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/prod_technical_reference_list.html

エラー メッセージおよびシステム メッセージ

エラー メッセージとシステム メッセージのリファレンス ガイドは次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/products_system_message_guides_list.html

マニュアルの入手方法およびテクニカル サポート

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

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

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

第 1 章

このリリースの新規および変更情報

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

- 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

この章では、『*Cisco Nexus 3000 Series NX-OS Security Configuration Guide*』に記載されている新機能および変更された各機能について、リリース固有の情報を示します。

このマニュアルの最新バージョンは、次のシスコ Web サイトから入手できます。

http://www.cisco.com/en/US/products/ps11541/products_installation_and_configuration_guides_list.html

Cisco Nexus 3000 シリーズ スイッチの Cisco NX-OS に関する最新情報を確認するには、次のシスコ Web サイトから入手できる『*Cisco Nexus 3000 Series Release Notes*』を参照してください。

http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html

表 *1*：*Cisco NX-OS Release 5.0(3)U2(2)* のセキュリティに関する新機能と変更された機能

機能	説明	参照先
コントロール プレーン ポリシング（CoPP）	コントロール プレーン ポリシングのサポート。	コントロール プレーン ポリシング
出力 RACL の L40p ポート比較のサポート	出力 RACL の制約事項の資料。	ルータ ACL としての IP ACL の適用，（106 ページ） VLAN ACL の概要

第 2 章

概要

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

- 認証、許可、アカウンティング，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

認証、許可、アカウンティング

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

認証

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

許可

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

RADIUS や TACACS+ などのリモート セキュリティ サーバでは、権限が定義された属性値（AV）のペアを、対象のユーザに関連付けることで、ユーザに対して特定の権限を認可します。 AAA 認可は、ユーザに認可されている操作を示す一連の属性を組み合わせて実行します。 これらの属性とデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制約事項が決定されます。

アカウンティング

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

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

関連トピック

AAA の設定

RADIUS および TACACS+ セキュリティ プロトコル

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

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

RADIUS

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

TACACS+

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

関連トピック

RADIUS の設定
TACACS+ の設定, （47 ページ）

SSH および Telnet

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

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

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

関連トピック

SSH および Telnet の設定, （77 ページ）

IP ACL

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

関連トピック

IP ACL の設定

第 3 章

認証、許可、アカウンティングの設定

この章では、Cisco Nexus 3000 シリーズ スイッチに認証、許可、アカウンティング（AAA）を設定する方法を説明します。 次のような構成になっています。

- AAA について，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，23 ページ
- AAA の設定例，24 ページ
- デフォルトの AAA 設定，24 ページ

AAA について

AAA セキュリティ サービス

認証、認可、アカウンティング（AAA）機能では、Cisco Nexus 3000 シリーズ スイッチを管理するユーザにつき、ID を確認し、アクセス権を付与し、アクションを追跡できます。 Cisco Nexus 3000 シリーズ スイッチは、Remote Access Dial-In User Service（RADIUS）または Terminal Access Controller Access Control device Plus（TACACS+）プロトコルをサポートします。

ユーザが入力したユーザ ID とパスワードに基づいて、スイッチは、ローカル データベースを使用してローカル認証/ローカル許可を実行するか、1 つまたは複数の AAA サーバを使用してリモート認証またはリモート許可を実行します。 スイッチと AAA サーバ間の通信は、事前共有秘密キーによって保護されます。 すべての AAA サーバ用または特定の AAA サーバ専用に共通秘密キーを設定できます。

AAA セキュリティは、次のサービスを実行します。

- 認証：ユーザを識別します。選択したセキュリティ プロトコルに応じて、ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージング サポート、暗号化などが行われます。
- 許可：アクセス コントロールを実行します。

  Cisco Nexus 3000 シリーズ スイッチでの許可は、AAA サーバからダウンロードされる属性により実行されます。 RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。
- アカウンティング：課金、監査、レポートのための情報収集、ローカルでの情報のロギング、および AAA サーバへの情報の送信の方式を提供します。

（注） Cisco NX-OS ソフトウェアは、認証、許可、アカウンティングをそれぞれ個別にサポートします。 たとえば、アカウンティングは設定せずに、認証と許可を設定したりできます。

AAA を使用する利点

AAA は、次のような利点を提供します。

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

リモート AAA サービス

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

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

AAA サーバ グループ

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

AAA サーバ設定オプション

Cisco Nexus 3000 シリーズ スイッチでは、次のサービスごとに異なった AAA 設定を作成できます。

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

次の表に、AAA サービス設定オプションの CLI コマンドを示します。

表 *2* : ***AAA*** **サービス コンフィギュレーション コマンド**

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

AAA サービスには、次の認証方式を指定できます。

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

（注） 方式がすべてRADIUSサーバになっており、特定のサーバ グループが指定されていない場合、Cisco Nexus 3000 シリーズ スイッチは、設定されている RADIUS サーバのグローバル プールから、設定の順序で、RADIUS サーバを選択します。 このグローバル プールのサーバは、Nexus 5000 シリーズ スイッチ上の RADIUS サーバ グループ内で選択的に設定可能なサーバです。

次の表に、AAA サービスに対して設定できる AAA 認証方式を示します。

表 *3*： *AAA* サービスのための *AAA* 認証方式

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

（注） コンソール ログイン認証、ユーザ ログイン認証、およびユーザ管理セッション アカウンティングでは、Cisco Nexus 3000 シリーズ スイッチは、各オプションを指定された順序で試行します。 その他の設定済みオプションが失敗した場合、ローカル オプションがデフォルト方式です。

ユーザ ログインの認証および許可プロセス

ユーザ ログインの認証および許可プロセスは、次のように実行されます。

- 目的の Cisco Nexus 3000 シリーズ スイッチにログインする際、Telnet、SSH、Fabric Manager または Device Manager、コンソール ログインのいずれかのオプションを使用できます。
- サーバ グループ認証方式を使用してAAAサーバ グループが設定してある場合は、Cisco Nexus 3000 シリーズ スイッチが、グループ内の最初の AAA サーバに認証要求を送信し、次のように処理されます。

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

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

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

- Cisco Nexus 3000 シリーズ スイッチがリモート AAA サーバでユーザの認証に成功した場合は、次の条件が適用されます。

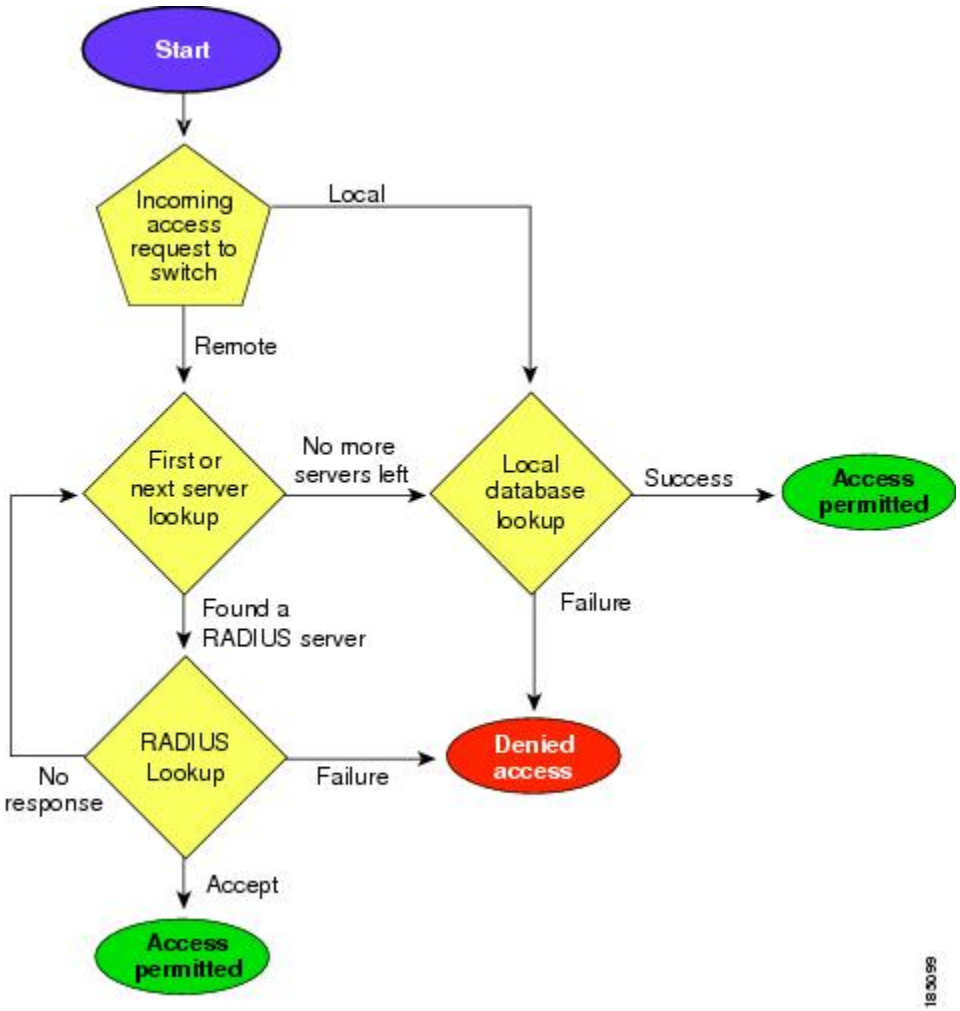
  AAA サーバ プロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザ ロールが認証応答とともにダウンロードされます。

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

- ユーザ名とパスワードがローカルで正常に認証された場合は、Cisco Nexus 3000 シリーズ スイッチにログインでき、ローカルデータベース内で設定されているロールが割り当てられます。

次の図には、認証および許可プロセスのフロー チャートを示します。

図 *1*：ユーザ ログインの認証および許可のフロー



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

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

リモート AAA の前提条件

リモート AAA サーバには、次の前提条件があります。

- 少なくとも 1 台の RADIUS サーバまたは TACACS+ サーバが、IP で到達可能であること。
- Cisco Nexus 3000 シリーズ スイッチが AAA サーバのクライアントとして設定されている。
- 事前に共有された秘密キーが Cisco Nexus 3000 シリーズ スイッチ上およびリモート AAA サーバ上で設定されている。
- リモート サーバが Cisco Nexus 3000 シリーズ スイッチからの AAA 要求に応答する。

AAA の注意事項と制約事項

Cisco Nexus 3000 シリーズ スイッチは、TACACS+ または RADIUS で作成されたか、ローカルに作成されたかに関係なく、すべて数字のユーザ名はサポートしません。 すべて数字のユーザ名が AAA サーバに存在し、ログイン時に入力された場合には、Cisco Nexus 3000 シリーズ スイッチはそのユーザをログインさせます。

注意 すべて数字のユーザ名でユーザ アカウントを作成しないでください。

AAA の設定

コンソール ログイン認証方式の設定

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS サーバまたは TACACS+ サーバの名前付きサブセット
- Cisco Nexus 3000 シリーズ スイッチ上のローカル データベース
- ユーザ名だけ（**none**）

デフォルトの方式は、local です。

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

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login console** {**group** *group-list* [**none**] | **local** | **none**}
3. switch(config)# **exit**
4. （任意） switch# **show aaa authentication**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login console** {**group** *group-list* [**none**]	**local**	**none**}	コンソールのログイン認証方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。 グループ名は、次のように指定します。 • **radius**：RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが認証に使用されます。 **local** 方式では、ローカル データベースが認証に使用されます。**none** 方式では、ユーザ名だけが使用されます。 デフォルトのコンソール ログイン方式は **local** です。この方式は、方式が一切設定されていない場合、および設定済みのどの方式でも応答が得られなかった場合に使用されます。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa authentication**	（任意） コンソール ログイン認証方式の設定を表示します。

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

次に、コンソール ログインの認証方式を設定する例を示します。

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

デフォルトのログイン認証方式の設定

デフォルトの方式は、local です。

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login default** {**group** *group-list* [**none**] | **local** | **none**}
3. switch(config)# **exit**
4. （任意） switch# **show aaa authentication**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login default** {**group** *group-list* [**none**]	**local**	**none**}	デフォルト認証方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。 グループ名は、次のように指定します。 • **radius**：RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが認証に使用されます。

	コマンドまたはアクション	目的
		local 方式では、ローカル データベースが認証に使用されます。**none** 方式では、ユーザ名だけが使用されます。 デフォルトのログイン方式は **local** です。この方式は、方式が一切設定されていない場合、および設定済みのどの方式でも応答が得られなかった場合に使用されます。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa authentication**	（任意） デフォルトのログイン認証方式の設定を表示します。
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.
```

手順の概要

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login error-enable**
3. switch(config)# **exit**
4. （任意） switch# **show aaa authentication**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login error-enable**	ログイン認証失敗メッセージをイネーブルにします。デフォルトはディセーブルです。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa authentication**	（任意） ログイン失敗メッセージの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

AAA コマンド許可の設定

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

許可方式には、次のものがあります。

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

デフォルトの方式は、Local です。

（注） コンソール セッション上の許可はありません。

はじめる前に

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

手順の概要

1. **configure terminal**
2. **aaa authorization** {**commands** | **config-commands**} {**default**} {{[**group** *group-name*] | [**local**]} | {[**group** *group-name*] | [**none**]}}

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**aaa authorization** {**commands** | **config-commands**} {**default**} {{[**group** *group-name*] | [**local**]} | {[**group** *group-name*] | [**none**]}}
	
	例：
	`switch(config)# aaa authorization config-commands default group tac1`
	
	例：
	`switch# aaa authorization commands default group tac1`
		許可パラメータを設定します。
		EXEC モード コマンドを許可するには、**commands** キーワードを使用します。
		コンフィギュレーション モード コマンドを許可するには、**config-commands** キーワードを使用します。
		許可方式を指定するには、**group**、**local**、または **none** キーワードを使用します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MSCHAP 認証のイネーブル化

Microsoft Challenge Handshake Authentication Protocol（MSCHAP; マイクロソフト チャレンジ ハンドシェーク認証プロトコル）は、マイクロソフト版の CHAP です。 リモート認証サーバ（RADIUS または TACACS+）を通じて、Cisco Nexus 3000 シリーズ スイッチへのユーザ ログインに MSCHAP を使用できます。

デフォルトでは、Cisco Nexus 3000 シリーズ スイッチはスイッチとリモート サーバの間で Password Authentication Protocol（PAP; パスワード認証プロトコル）認証を使用します。 MSCHAP がイネーブルの場合は、MSCHAP VSA（Vendor-Specific Attribute; ベンダー固有属性）を認識するように RADIUS サーバを設定する必要があります。

次の表に、MSCHAP に必要な RADIUS VSA を示します。

表 *4*： *MSCHAP RADIUS VSA*

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login mschap enable**
3. switch(config)# **exit**
4. （任意） switch# **show aaa authentication login mschap**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login mschap enable**	MS-CHAP 認証をイネーブルにします。 デフォルトはディセーブルです。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa authentication login mschap**	（任意） MS-CHAP 設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

VSA, （21 ページ）

AAA アカウンティングのデフォルト方式の設定

Cisco Nexus 3000 シリーズ スイッチは、アカウンティングに TACACS+ 方式と RADIUS 方式をサポートします。 スイッチは、ユーザアクティビティをアカウンティング レコードの形でTACACS+ セキュリティ サーバまたは RADIUS セキュリティ サーバに報告します。 各アカウンティング レコードに、アカウンティング属性値（AV）のペアが入っており、それが AAA サーバに格納されます。

AAA アカウンティングをアクティブにすると、Cisco Nexus 3000 シリーズ スイッチは、これらの属性をアカウンティング レコードとして報告します。そのアカウンティング レコードは、セキュリティ サーバ上のアカウンティング ログに格納されます。

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

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

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

はじめる前に

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **aaa accounting default** {**group** *group-list* | **local**}
3. switch(config)# **exit**
4. （任意） switch# **show aaa accounting**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa accounting default** {**group** *group-list* | **local**}	デフォルトのアカウンティング方式を設定します。 スペースで区切ったリストで、1 つまたは複数のサーバ グループ名を指定できます。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。 グループ名は、次のように指定します。 • **radius**：RADIUS サーバのグローバル プールがアカウンティングに使用されます。 • *named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットがアカウンティングに使用されます。 **local** 方式では、アカウンティングにローカル データベースが使用されます。

	コマンドまたはアクション	目的
		デフォルトのアカウンティング方式は **local** です。サーバ グループが設定されていないとき、または設定済みのすべてのサーバ グループから応答がないときに、このデフォルトの方式が使用されます。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show aaa accounting**	（任意） デフォルトの AAA アカウンティング方式の設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

AAA サーバの VSA の使用

VSA

ベンダー固有属性（VSA）を使用して、AAA サーバ上でのCisco Nexus 3000 シリーズのユーザ ロールおよび SNMPv3 パラメータを指定できます。

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

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

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

Cisco Nexus 3000 シリーズ スイッチでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。 この許可情報は、VSA で指定されます。

VSA の形式

次の VSA プロトコル オプションが、Cisco Nexus 3000 シリーズ スイッチでサポートされています。

- Shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されます。

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

次の属性が Cisco Nexus 3000 シリーズ スイッチでサポートされています。

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

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

AAA サーバで VSA cisco-av-pair を使用して、次の形式で、Cisco Nexus 3000 シリーズ スイッチのユーザ ロール マッピングを指定できます。

```
shell:roles="roleA roleB …"
```

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

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

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

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

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

詳細については、『』、『*Cisco Nexus 3000 Series NX-OS System Management Configuration Guide*』の「Configuring User Accounts and RBAC」の章を参照してください。

ローカルAAAアカウンティングログのモニタリングとクリア

Cisco Nexus 3000 シリーズ スイッチは、AAA アカウンティング アクティビティのローカル ログを保持しています。

手順の概要

1. switch# **show accounting log** [*size*] [**start-time** *year month day hh* **:** *mm* **:** *ss*]
2. （任意） switch# **clear accounting log**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show accounting log** [*size*] [**start-time** *year month day hh* **:** *mm* **:** *ss*]	アカウンティング ログを表示します。 このコマンド出力には、デフォルトで最大 250,000 バイトのアカウンティング ログが表示されます。 サイズ引数を指定すれば、コマンドの出力を制限できます。 指定できる範囲は 0 ～ 250000 バイトです。 ログ出力の開始時刻を指定することもできます。
ステップ 2	switch# **clear accounting log**	（任意） アカウンティング ログの内容をクリアします。

AAA 設定の確認

AAA の設定情報を表示するには、次のいずれかの作業を行います。

手順の概要

1. **show aaa accounting**
2. **show aaa authentication** [**login** {**error-enable** | **mschap**}]
3. **show aaa authorization**
4. **show aaa groups**
5. **show running-config aaa** [**all**]
6. **show startup-config aaa**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**show aaa groups**	AAA サーバ グループの設定を表示します。
ステップ 5	**show running-config aaa** [**all**]	実行コンフィギュレーションの AAA 設定を表示します。
ステップ 6	**show startup-config aaa**	スタートアップ コンフィギュレーションの AAA 設定を表示します。

AAA の設定例

次に、AAA を設定する例を示します。

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

デフォルトの AAA 設定

次の表に、AAA パラメータのデフォルト設定を示します。

表 *5*：デフォルトの *AAA* パラメータ

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

第 4 章

RADIUS の設定

この章の内容は、次のとおりです。

- RADIUS の設定，25 ページ

RADIUS の設定

RADIUS について

Remote Access Dial-In User Service（RADIUS）分散クライアント/ サーバ システムを使用すると、不正アクセスからネットワークを保護できます。 シスコの実装では、RADIUS クライアントは Cisco Nexus 3000 シリーズ スイッチで稼働し、すべてのユーザ認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウンティング要求を送信します。

RADIUS ネットワーク環境

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

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

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

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

- すでに RADIUS を使用中のネットワーク。

  RADIUS を使用した Cisco Nexus 3000 シリーズ スイッチをネットワークに追加できます。 この作業は、AAA サーバに移行するときの最初の手順になります。

- リソース アカウンティングが必要なネットワーク。

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

- 認証プロファイルをサポートするネットワーク

  ネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルをセットアップできます。 ユーザごとのプロファイルにより、Nexus 5000 シリーズ スイッチは、既存の RADIUS ソリューションを使用してポートを管理できると同時に、共有リソースを効率的に管理してさまざまなサービス レベル アグリーメントを提供できます。

RADIUS の操作について

ユーザがログインを試行し、RADIUS を使用して Cisco Nexus 3000 シリーズ スイッチに対する認証を行う際には、次のプロセスが実行されます。

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

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

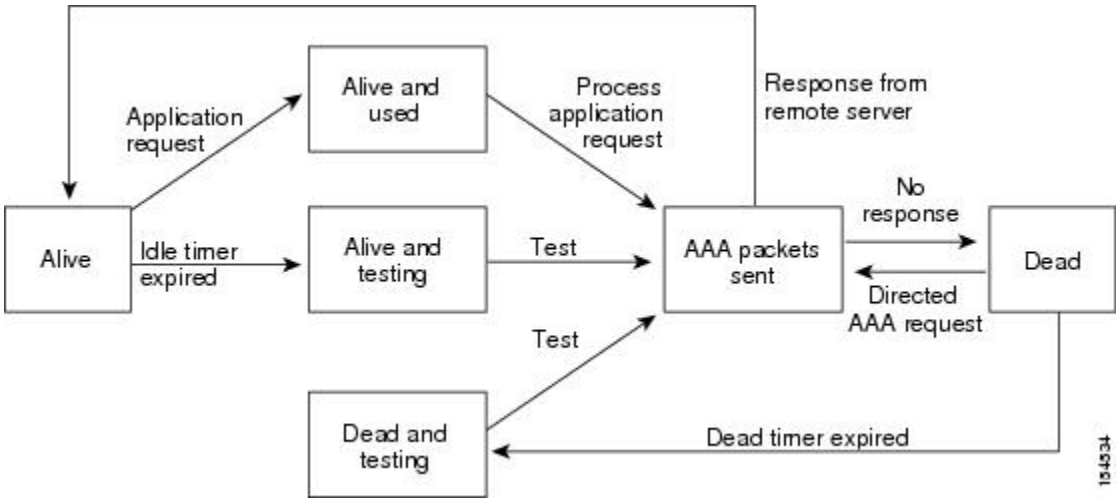
- ユーザがアクセス可能なサービス（Telnet、rlogin、または local-area transport（LAT; ローカル エリア トランスポート）接続、PPP（ポイントツーポイントプロトコル）、シリアルライン インターネット プロトコル（SLIP）、EXEC サービスなど）
- 接続パラメータ（ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセス リスト、ユーザ タイムアウト）

RADIUS サーバ モニタリング

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

次の図には、さまざまな RADIUS サーバの状態を示します。

図 *2*： *RADIUS* サーバの状態



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

ベンダー固有属性

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間でのベンダー固有属性（VSA）の通信のための方式を規定する標準を作成しています。 IETF は、属性 26 を使用します。 VSA を使用するとベンダーは、一般的な用途には適合しない独自の拡張属性をサポートできます。 シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。 シスコのベンダー ID は 9、サポー

トされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。 値は、次の形式のストリングです。

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

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

Cisco Nexus 3000 シリーズ スイッチでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。 この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションが、Cisco Nexus 3000 シリーズ スイッチでサポートされています。

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

Cisco Nexus 3000 シリーズ スイッチは、次の属性をサポートしています。

- roles：ユーザが属するすべてのロールの一覧です。 値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。
- accountinginfo：標準の RADIUS アカウンティング プロトコルで処理される属性に加えて、アカウンティング情報が格納されます。 この属性は、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分だけに送信されます。 この属性と共に使用できるのは、アカウンティングの Protocol Data Unit（PDU; プロトコル データ ユニット）だけです。

RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IPv4 または IPv6IP アドレスまたはホスト名を取得こと。
- RADIUS サーバから事前共有キーを取得すること。
- Cisco Nexus 3000 シリーズ スイッチが、AAA サーバの RADIUS クライアントとして設定されていること。

RADIUS の注意事項と制約事項

RADIUS 設定時の注意事項と制限事項は次のとおりです。

- スイッチ上に設定できる RADIUS サーバの最大数は 64 です。Cisco Nexus 3000 シリーズ

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。

手順の概要

1. Cisco Nexus 3000 シリーズ スイッチと RADIUS サーバとの接続を確立します。
2. RADIUS サーバの事前共有秘密キーを設定します。
3. 必要に応じて、AAA 認証方式用に、RADIUS サーバのサブセットを使用して RADIUS サーバ グループを設定します。
4. 必要に応じて、次のオプションのパラメータを設定します。
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。

手順の詳細

ステップ 1 Cisco Nexus 3000 シリーズ スイッチと RADIUS サーバとの接続を確立します。

ステップ 2 RADIUS サーバの事前共有秘密キーを設定します。

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

ステップ 4 必要に応じて、次のオプションのパラメータを設定します。

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

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

RADIUS サーバ ホストの設定

認証に使用する各 RADIUS サーバについて、IP アドレス（IPv4 または IPv6）、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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*}
3. switch(config)# **exit**
4. （任意） switch# **show radius-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*}	RADIUS サーバの IPv4 または IPv6 アドレス、またはホスト名を指定します。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

RADIUS のグローバルな事前共有キーの設定

Cisco Nexus 3000 シリーズ デバイスで使用するすべてのサーバについて、グローバル レベルで事前共有キーを設定できます。 事前共有キーとは、スイッチと RADIUS サーバ ホスト間の共有秘密テキスト ストリングです。

はじめる前に

リモートの RADIUS サーバの事前共有キー値を取得していること。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **radius-server key** [**0** | **7**] *key-value*
3. switch(config)# **exit**
4. （任意） switch# **show radius-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

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

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

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

RADIUS サーバの事前共有キーの設定

事前共有キーとは、Cisco Nexus 3000 シリーズ 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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **7**] *key-value*
3. switch(config)# **exit**
4. （任意） switch# **show radius-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **7**] *key-value*	特定の RADIUS サーバの事前共有キーを指定します。 クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。 デフォルトの形式はクリア テキストです。 最大で 63 文字の長さまで指定可能です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。 （注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。 暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、RADIUS 事前共有キーを設定する例を示します。

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

RADIUS サーバ グループの設定

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

手順の概要

1. switch# **configure terminal**
2. switch (config)# **aaa group server radius** *group-name*
3. switch (config-radius)# **server** {*ipv4-address* | *ipv6-address* | *server-name*}
4. （任意） switch (config-radius)# **deadtime** *minutes*
5. （任意） switch(config-radius)# **source-interface** *interface*
6. switch(config-radius)# **exit**
7. （任意） switch(config)# **show radius-server group** [*group-name*]
8. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch (config)# **aaa group server radius** *group-name*	RADIUS サーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション サブモードを開始します。 *group-name* 引数は、最大 127 文字の英数字のストリングで、大文字小文字が区別されます。
ステップ 3	switch (config-radius)# **server** {*ipv4-address* | *ipv6-address* | *server-name*}	RADIUS サーバを、RADIUS サーバ グループのメンバーとして設定します。 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。

	コマンドまたはアクション	目的
		（注） RADIUS サーバ グループのデッド タイム間隔が 0 より大きい場合は、この値がグローバルなデッド タイム値より優先されます。
ステップ 5	switch(config-radius)# **source-interface** *interface*	（任意） 特定の RADIUS サーバ グループに発信元インターフェイスを割り当てます。 サポートされているインターフェイスのタイプは管理および VLAN です。 （注） **source-interface** コマンドを使用して、**ip radius source-interface** コマンドによって割り当てられたグローバル ソース インターフェイスを上書きします。
ステップ 6	switch(config-radius)# **exit**	コンフィギュレーション モードを終了します。
ステップ 7	switch(config)# **show radius-server group** [*group-name*]	（任意） RADIUS サーバ グループの設定を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、RADIUS サーバ グループを設定する例を示します。

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

次の作業

AAA サービスに RADIUS サーバ グループを適用します。

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

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip radius source-interface** *interface*
3. switch(config)# **exit**
4. （任意） switch# **show radius-server**
5. （任意） switch# **copy running-config startup config**

手順の詳細

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

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

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

ログイン時にユーザによる RADIUS サーバの指定を許可

ログイン時にユーザによる RADIUS サーバの指定を許可できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **radius-server directed-request**
3. switch(config)# **exit**
4. （任意） switch# **show radius-server directed-request**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

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

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

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

グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定

すべての RADIUS サーバに対するグローバルな再送信リトライ回数とタイムアウト間隔を設定できます。 デフォルトでは、スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。 このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。 タイムアウト間隔は、Cisco Nexus 3000 シリーズ スイッチがタイムアウト エラーを宣言する前に、RADIUS サーバからの応答を待機する時間を決定します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **radius-server retransmit** *count*
3. switch(config)# **radius-server timeout** *seconds*
4. switch(config)# **exit**
5. （任意） switch# **show radius-server**
6. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server retransmit** *count*	すべての RADIUS サーバの再送信回数を指定します。 デフォルトの再送信回数は 1 で、範囲は 0 ～ 5 です。
ステップ 3	switch(config)# **radius-server timeout** *seconds*	RADIUS サーバの送信タイムアウト間隔を指定します。 デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。
ステップ 4	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

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

サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定

デフォルトでは、Cisco Nexus 3000 シリーズ スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。 このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。 スイッチが、タイムアウト エラーを宣言する前に、RADIUS サーバからの応答を待機するタイムアウト間隔も設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **retransmit** *count*
3. switch(config)#**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout** *seconds*
4. switch(config)# **exit**
5. （任意） switch# **show radius-server**
6. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **retransmit** *count*	特定のサーバに対する再送信回数を指定します。デフォルトはグローバル値です。 （注） 特定の RADIUS サーバに指定した再送信回数は、すべての RADIUS サーバに指定した再送信回数より優先されます。
ステップ 3	switch(config)#**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout** *seconds*	特定のサーバの送信タイムアウト間隔を指定します。デフォルトはグローバル値です。 （注） 特定の RADIUS サーバに指定したタイムアウト間隔は、すべての RADIUS サーバに指定したタイムアウト間隔より優先されます。
ステップ 4	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

RADIUS サーバのアカウンティングおよび認証属性の設定

RADIUS サーバをアカウンティング専用、または認証専用に使用するかを指定できます。 デフォルトでは、RADIUS サーバはアカウンティングと認証の両方に使用されます。 RADIUS のアカウンティングおよび認証メッセージの宛先 UDP ポート番号も指定できます。

手順の概要

1. switch# **configure terminal**
2. （任意） switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **acct-port** *udp-port*
3. （任意） switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting**
4. （任意） switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **auth-port** *udp-port*
5. （任意） switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication**
6. switch(config)# **exit**
7. （任意） switch(config)# **show radius-server**
8. switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **acct-port** *udp-port*	（任意） RADIUS アカウンティングのメッセージに使用する UDP ポートを指定します。 デフォルトの UDP ポートは 1812 です。 指定できる範囲は 0 ～ 65535 です。
ステップ 3	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting**	（任意） 特定の RADIUS サーバをアカウンティング用にのみ使用することを指定します。 デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **auth-port** *udp-port*	（任意） RADIUS 認証メッセージ用の UDP ポートを指定します。 デフォルトの UDP ポートは 1812 です。 指定できる範囲は 0 ～ 65535 です。

	コマンドまたはアクション	目的
ステップ 5	switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication**	（任意） 特定の RADIUS サーバを認証用にのみ使用することを指定します。 デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 6	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 7	switch(config)# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

RADIUS サーバの定期的モニタリングの設定

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

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

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

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
3. switch(config)# **radius-server deadtime** *minutes*
4. switch(config)# **exit**
5. （任意） switch# **show radius-server**
6. （任意） switch# **copy running-config startup-config**

手順の詳細

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

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

```
switch# configure terminal
```

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

デッド タイム間隔の設定

すべての RADIUS サーバのデッド タイム間隔を設定できます。 デッド タイム間隔には、Cisco Nexus 3000 シリーズ スイッチが RADIUS サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを判断するためにテスト パケットを送信するまでの間隔を指定します。 デフォルト値は 0 分です。

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **radius-server deadtime**
3. switch(config)# **exit**
4. （任意） switch# **show radius-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server deadtime**	デッド タイム間隔を設定します。 デフォルト値は 0 分です。 有効な範囲は 1 ～ 1440 分です。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

RADIUS サーバまたはサーバ グループの手動モニタリング

手順の概要

1. switch# **test aaa server radius** {*ipv4-address* | *ipv6-address* | *server-name*} [**vrf** *vrf-name*] *username password*
2. switch# **test aaa group** *group-name username password*

手順の詳細

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

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

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

RADIUS 設定の確認

手順の概要

1. switch# **show running-config radius** [**all**]
2. switch# **show startup-config radius**
3. switch# **show radius-server** [*server-name* | *ipv4-address*] [**directed-request** | **groups** | **sorted** | **statistics**]

手順の詳細

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

RADIUS サーバの統計情報のモニタリング

手順の概要

1. switch# **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

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

RADIUS サーバ統計情報のクリア

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

はじめる前に

Cisco NX-OS デバイスに RADIUS サーバを設定します。

手順の概要

1. （任意） switch# **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}
2. switch# **clear radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

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

RADIUS の設定例

次に、RADIUS を設定する例を示します。

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

RADIUS のデフォルト設定

次の表に、RADIUS パラメータのデフォルト設定を示します。

表 *6*：デフォルトの *RADIUS* パラメータ

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

第 5 章

TACACS+ の設定

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

- TACACS+ の設定について，47 ページ

TACACS+ の設定について

TACACS+ について

Terminal Access Controller Access Control System Plus（TACACS+）セキュリティ プロトコルは、Cisco Nexus 3000 シリーズ スイッチにアクセスしようとするユーザを集中的に検証します。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されます。 Cisco Nexus 3000 シリーズ スイッチに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ では、認証、許可、アカウンティングの各ファシリティを個別に提供します。 TACACS+ を使用すると、単一のアクセス コントロール サーバ（TACACS+ デーモン）で、各サービス（認証、許可、アカウンティング）を個別に提供できます。 各サービスは固有のデータベースにアソシエートされており、デーモンの機能に応じて、そのサーバまたはネットワーク上で使用可能な他のサービスを利用できます。

TACACS+ クライアント/サーバ プロトコルでは、トランスポート要件を満たすため TCP（TCP ポート 49）を使用します。 Cisco Nexus 3000 シリーズ スイッチは、TACACS+ プロトコルを使用して集中型の認証を行います。

TACACS+ の利点

TACACS+ には、RADIUS 認証にはない次の利点があります。

- 独立した AAA ファシリティを提供する。 たとえば、Cisco Nexus 3000 シリーズ スイッチは、認証を行わずにアクセスを許可できます。
- AAA クライアントとサーバ間のデータ送信に TCP トランスポート プロトコルを使用しているため、コネクション型プロトコルによる確実な転送を実行する。
- スイッチと AAA サーバ間でプロトコル ペイロード全体を暗号化して、高度なデータ機密性を実現する。 RADIUS プロトコルはパスワードだけを暗号化します。

TACACS+ を使用したユーザ ログイン

ユーザが TACACS+ を使用して、Cisco Nexus 3000 シリーズ スイッチに対し Password Authentication Protocol（PAP; パスワード認証プロトコル）によるログインを試行すると、次のプロセスが実行されます。

1. Cisco Nexus 3000 シリーズ スイッチが接続を確立すると、TACACS+ デーモンにアクセスして、ユーザ名とパスワードを取得します。

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

2. Cisco Nexus 3000 シリーズ スイッチが、TACACS+ デーモンから次のいずれかの応答を受信します。
   - ACCEPT：ユーザの認証に成功したので、サービスを開始します。 Cisco Nexus 3000 シリーズ スイッチがユーザの許可を要求している場合は、許可が開始されます。
   - REJECT：ユーザの認証に失敗しました。 TACACS+ デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン シーケンスを再試行するよう要求します。
   - ERROR：認証中に、デーモン内、またはデーモンと Cisco Nexus 3000 シリーズ スイッチ間のネットワーク接続でエラーが発生しました。 Cisco Nexus 3000 シリーズ スイッチが ERROR 応答を受信した場合、スイッチは代わりのユーザ認証方式を試します。

   Cisco Nexus 3000 シリーズ スイッチで許可がイネーブルになっている場合は、この後、許可フェーズの処理が実行されます。 ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合、Cisco Nexus 3000 シリーズ スイッチは、再度、TACACS+ デーモンにアクセスします。デーモンは ACCEPT または REJECT 許可応答を返します。 ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT 応答により、ユーザがアクセス可能なサービスが決まります。

サービスには次が含まれます。

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

デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー

TACACS+ サーバに対してスイッチを認証するには、TACACS+ 事前共有キーを設定する必要があります。 事前共有キーは、Cisco Nexus 3000 シリーズ スイッチと TACACS+ サーバ ホストの間で共有される秘密テキスト ストリングです。 キーの長さは 63 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用できません）。 Cisco Nexus 3000 シリーズ スイッチ上のすべての TACACS+サーバ設定で使用されるグローバルな事前共有秘密キーを設定できます。

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

TACACS+ サーバのコマンド許可サポート

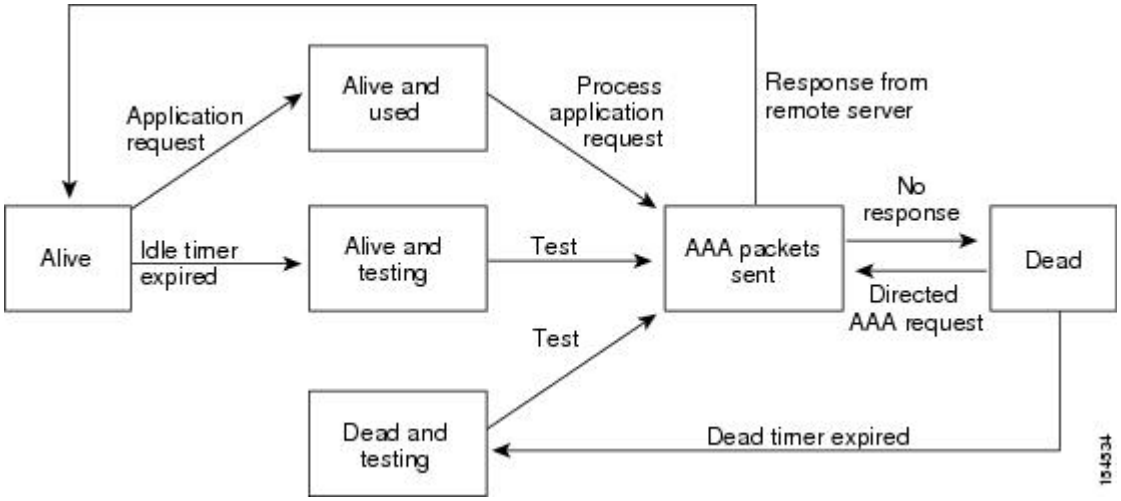
デフォルトでは、認証されたユーザがコマンドライン インターフェイス（CLI）でコマンドを入力したときに、Cisco NX-OS ソフトウェアのローカル データベースに対してコマンド許可が行われます。 また、TACACS+ を使用して、認証されたユーザに対して許可されたコマンドを確認することもできます。

TACACS+ サーバのモニタリング

応答を返さない TACACS+ サーバがあると、AAA 要求の処理に遅延が発生する可能性があります。 AAA 要求の処理時間を節約するため、Cisco Nexus 3000 シリーズ スイッチは定期的に TACACS+ サーバをモニタリングし、TACACS+ サーバが応答を返す（アライブ）かどうかを調べることができます。 Cisco Nexus 3000 シリーズ スイッチは、応答を返さない TACACS+ サーバをデッド（dead）としてマークし、デッド TACACS+ サーバには AAA 要求を送信しません。 またCisco Nexus 3000 シリーズ スイッチは、定期的にデッド TACACS+ サーバをモニタリングし、それらが応答を返したらアライブ状態に戻します。 このモニタリング プロセスでは、実際の AAA 要求がサーバに送信される前に、TACACS+ サーバが稼働状態であることを確認します。 TACACS+ サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco Nexus 3000 シリーズ スイッチによって、パフォーマンスに影響が出る前に、障害が発生していることを知らせるエラー メッセージが表示されます。

次の図では、さまざまな TACACS+ サーバの状態を示します。

図 *3*： *TACACS+* サーバの状態



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

TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバの IPv4 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 3000 シリーズ スイッチが、AAA サーバの TACACS+ クライアントとして設定されていること。

TACACS+ の注意事項と制約事項

TACACS+ に関する注意事項と制約事項は次のとおりです。

- Cisco Nexus 3000 シリーズ スイッチ上に設定できる TACACS+ サーバの最大数は 64 です。

TACACS+ の設定

TACACS+ サーバの設定プロセス

ここでは、TACACS+ サーバを設定する方法について説明します。

手順の概要

1. TACACS+ をイネーブルにします。
2. TACACS+ サーバと Cisco Nexus 3000 シリーズ スイッチとの接続を確立します。
3. TACACS+ サーバの事前共有秘密キーを設定します。
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。
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。
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。

手順の詳細

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 3000 シリーズ スイッチとの接続を確立します。

ステップ 3 TACACS+ サーバの事前共有秘密キーを設定します。

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

ステップ 5 必要に応じて、次のオプションのパラメータを設定します。

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

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

TACACS+ のイネーブル化

デフォルトでは、Cisco Nexus 3000 シリーズ スイッチで TACACS+ 機能はディセーブルに設定されています。認証に関するコンフィギュレーション コマンドと検証コマンドを使用するために、TACACS+ 機能をイネーブルにするには、次の作業を行います。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature tacacs+**
3. switch(config)# **exit**
4. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **feature tacacs+**	TACACS+ をイネーブルにします。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバ ホストの設定

リモートの TACACS+ サーバにアクセスするには、Cisco Nexus 3000 シリーズ スイッチ上に、TACACS+ サーバの 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 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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*}
3. switch(config)# **exit**
4. （任意） switch# **show tacacs-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *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**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

サーバ グループから TACACS+ サーバ ホストを削除できます。

TACACS+ のグローバルな事前共有キーの設定

Cisco Nexus 3000 シリーズ スイッチで使用するすべてのサーバについて、グローバル レベルで事前共有キーを設定できます。 事前共有キーとは、Cisco Nexus 3000 シリーズ スイッチと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

事前共有キーを設定する前に、次の点を確認してください。

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **tacacs-server key** [**0** | **7**] *key-value*
3. switch(config)# **exit**
4. （任意） switch# **show tacacs-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

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

次に、グローバルな事前共有キーを設定する例を示します。

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

関連トピック

TACACS+ のイネーブル化 , （51 ページ）

TACACS+ サーバの事前共有キーの設定

TACACS+ サーバの事前共有キーを設定できます。 事前共有キーとは、Cisco Nexus 3000 シリーズ スイッチと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value*
3. switch(config)# **exit**
4. （任意） switch# **show tacacs-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value*	特定の TACACS+ サーバの事前共有キーを指定します。 クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。 デフォルトの形式はクリア テキストです。 最大で 63 文字の長さまで指定可能です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。 （注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。 暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ 事前共有キーを設定する例を示します。

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

TACACS+ サーバ グループの設定

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

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

はじめる前に

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **aaa group server tacacs+** *group-name*
3. switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value*
4. （任意） switch(config-tacacs+)# **deadtime** *minutes*
5. （任意） switch(config-tacacs+)# **source-interface** *interface*
6. switch(config-tacacs+)# **exit**
7. （任意） switch(config)# **show tacacs-server groups**
8. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa group server tacacs+** *group-name*	TACACS+ サーバ グループを作成し、そのグループの TACACS+ サーバ グループ コンフィギュレーション モードを開始します。
ステップ 3	switch(config)# **tacacs-server 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**）の事前共有キーを指定できます。 デフォルトの形式はクリア テキストです。 最大で 63 文字の長さまで指定可能です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 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。

	コマンドまたはアクション	目的
		（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* 例： `switch(config-tacacs+)# source-interface mgmt 0`	（任意） 特定の TACACS+ サーバ グループに発信元インターフェイスを割り当てます。 サポートされているインターフェイスのタイプは管理および VLAN です。 （注） **source-interface** コマンドを使用して、**ip tacacs source-interface** コマンドによって割り当てられたグローバル ソース インターフェイスを上書きします。
ステップ 6	switch(config-tacacs+)# **exit**	コンフィギュレーション モードを終了します。
ステップ 7	switch(config)# **show tacacs-server groups**	（任意） TACACS+ サーバ グループの設定を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ サーバ グループを設定する例を示します。

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

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

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

手順の概要

1. **configure terminal**
2. **ip tacacs source-interface** *interface*
3. **exit**
4. （任意） **show tacacs-server**
5. （任意） **copy running-config startup config**

手順の詳細

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

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

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

ログイン時の TACACS+ サーバの指定

認証要求の送信先 TACACS+ サーバをユーザが指定できるようにスイッチを設定するには、directed-request オプションをイネーブルにします。 デフォルトでは、Cisco Nexus 3000 シリーズ スイッチは、デフォルトの AAA 認証方式に基づいて認証要求を転送します。 このオプションをイネーブルにすると、ユーザは *username@hostname* としてログインできます。ここで、*hostname* は設定済みの RADIUS サーバの名前です。

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **tacacs-server directed-request**
3. switch(config)# **exit**
4. （任意） switch# **show tacacs-server directed-request**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

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

TACACS+ サーバでの AAA 許可の設定

TACACS+ サーバのデフォルトの AAA 許可方式を設定できます。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **aaa authorization ssh-certificate default** {**group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. （任意） **show aaa authorization** [**all**]
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

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

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

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

TACACS+ サーバでのコマンド許可の設定

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

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

はじめる前に

TACACS+ をイネーブルにします。

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

手順の概要

1. **configure terminal**
2. **aaa authorization** {**commands** | **config-commands**} **default** [**group** *group-list* [**local**] | **local**]
3. **exit**
4. （任意） **show aaa authorization** [**all**]
5. （任意） **copy running-config startup-config**

手順の詳細

	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。

手順の概要

1. **test aaa authorization command-type** {**commands** | **config-commands**} **user** *username* **command** *command-string*

手順の詳細

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

コマンド許可検証のイネーブル化とディセーブル化

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

（注） 許可検証をイネーブルにした場合は、コマンドは実行されません。

手順の概要

1. **terminal verify-only** [**username** *username*]
2. **terminal no verify-only** [**username** *username*]

手順の詳細

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

TACACS+ サーバでの許可に使用する特権レベルのサポートの設定

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

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

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

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

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

手順の概要

1. **configure terminal**
2. [**no**] **feature privilege**
3. [**no**] **enable secret** [**0** | **5**] *password* [**priv-lvl** *priv-lvl* | **all**]
4. [**no**] **username** *username* **priv-lvl** *n*
5. （任意） **show privilege**
6. （任意） **copy running-config startup-config**
7. **exit**
8. **enable** *level*

手順の詳細

	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。 デフォルトはディセーブルです。
ステップ 3	[**no**] **enable secret** [**0** | **5**] *password* [**priv-lvl** *priv-lvl* | **all**] 例： `switch(config)# enable secret 5 def456 priv-lvl 15`	特定の特権レベルのシークレット パスワードをイネーブルまたはディセーブルにします。 特権レベルが上がるたびに、正しいパスワードを入力するようにユーザに要求します。 デフォルトはディセーブルです。 パスワードの形式としてクリア テキストを指定する場合は **0** を入力し、暗号化された形式を指定する場合は **5** を入力します。 *password* 引数に指定できる文字数は、最大 64 文字です。 *priv-lvl* 引数は、1 ～ 15 です。 （注） シークレット パスワードをイネーブルにするには、**feature privilege** コマンドを入力してロールの累積権限をイネーブルにする必要があります。
ステップ 4	[**no**] **username** *username* **priv-lvl** *n* 例： `switch(config)# username user2 priv-lvl 15`	ユーザの許可に対する特権レベルの使用をイネーブルまたはディセーブルにします。 デフォルトはディセーブルです。 **priv-lvl** キーワードはユーザに割り当てる権限レベルを指定します。 デフォルトの特権レベルはありません。 特権レベル 0 ～ 15（priv-lvl 0 ～ priv-lvl 15）は、ユーザ ロール priv-0 ～ priv-15 にマッピングされます。
ステップ 5	**show privilege** 例： `switch(config)# show privilege`	（任意） ユーザ名、現在の特権レベル、および累積権限のサポートのステータスを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的

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**。

手順の概要

1. **configure terminal**
2. [**no**] **role name priv-***n*
3. **rule** *number* {**deny** | **permit**} **command** *command-string*
4. **exit**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的

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

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

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

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

グローバルな TACACS+ タイムアウト間隔の設定

Cisco Nexus 3000 シリーズ スイッチがすべての TACACS+ サーバからの応答を待つグローバルなタイムアウト間隔を設定できます。これを過ぎるとタイムアウトエラーになります。タイムアウト間隔には、スイッチが TACACS+ サーバからの応答を待つ時間を指定します。これを過ぎるとタイムアウト エラーになります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **tacacs-server timeout** *seconds*
3. switch(config)# **exit**
4. （任意） switch# **show tacacs-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server timeout** *seconds*	TACACS+ サーバのタイムアウト間隔を指定します。 デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

サーバのタイムアウト間隔の設定

Cisco Nexus 3000 シリーズ スイッチが、タイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機するタイムアウト間隔を設定できます。 タイムアウト間隔は、スイッチがタイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機する時間を決定します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **timeout** *seconds*
3. switch(config)# **exit**
4. （任意） switch# **show tacacs-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **timeout** *seconds*	特定のサーバのタイムアウト間隔を指定します。 デフォルトはグローバル値です。 （注） 特定の TACACS+ サーバに指定したタイムアウト間隔は、すべての TACACS+ サーバに指定したタイムアウト間隔より優先されます。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、TACACS+ サーバ用に別の TCP ポートを設定できます。 デフォルトでは、Cisco Nexus 3000 シリーズ スイッチは、すべての TACACS+ 要求にポート 49 を使用します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **port** *tcp-port*
3. switch(config)# **exit**
4. （任意） switch# **show tacacs-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

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

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

次に、TCP ポートを設定する例を示します。

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

TACACS+ サーバの定期的モニタリングの設定

TACACS+ サーバの可用性をモニタリングできます。 パラメータとして、サーバに使用するユーザ名とパスワード、およびアイドル タイマーがあります。 アイドル タイマーには、TACACS+ サーバがどのくらいの期間要求を受信しなかった場合に、Cisco Nexus 3000 シリーズ スイッチがテスト パケットを送信するかを指定します。このオプションを設定して、サーバを定期的にテストしたり、1 回だけテストを実行できます。

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

テスト アイドル タイマーには、TACACS+ サーバがどのくらいの期間要求を受信しなかった場合に、Cisco Nexus 3000 シリーズ スイッチがテスト パケットを送信するかを指定します。

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

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

手順の概要

1. switch# **configure terminal**
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*]]}
3. switch(config)# **tacacs-server dead-time** *minutes*
4. switch(config)# **exit**
5. （任意） switch# **show tacacs-server**
6. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *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 3000 シリーズ スイッチが、前回応答しなかった TACACS+ サーバをチェックするまでの時間（分）を指定します。 デフォルト値は 0 分、指定できる範囲は 0 ～ 1440 分です。
ステップ 4	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 5	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ サーバの定期的モニタリングを設定する例を示します。

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

デッド タイム間隔の設定

すべての TACACS+ サーバのデッド タイム間隔を設定できます。 デッド タイム間隔には、Cisco Nexus 3000 シリーズ スイッチが TACACS+ サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを判断するためにテスト パケットを送信するまでの間隔を指定します。

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **tacacs-server deadtime** *minutes*
3. switch(config)# **exit**
4. （任意） switch# **show tacacs-server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server deadtime** *minutes*	グローバルなデッド タイム間隔を設定します。 デフォルト値は 0 分です。 有効な範囲は 1 ～ 1440 分です。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバまたはサーバ グループの手動モニタリング

手順の概要

1. switch# **test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password*
2. switch# **test aaa group** *group-name username password*

手順の詳細

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

次に、手動でテスト メッセージを送信する例を示します。

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

TACACS+ のディセーブル化

TACACS+ をディセーブルにできます。

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no feature tacacs+**
3. switch(config)# **exit**
4. （任意） switch# **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **no feature tacacs+**	TACACS+ をディセーブルにします。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードを終了します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ 統計情報のモニタリング

Cisco Nexus 3000 シリーズ スイッチが TACACS+ のアクティビティについて保持している統計情報を表示する手順は、次のとおりです。

手順の概要

1. switch# **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

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

このコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 3000* シリーズ *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。

手順の概要

1. switch# **show tacacs+** {**status** | **pending** | **pending-diff**}
2. switch# **show running-config tacacs** [**all**]
3. switch# **show startup-config tacacs**
4. switch# **show tacacs-serve** [*host-name* | *ipv4-address*] [**directed-request** | **groups** | **sorted** | **statistics**]

手順の詳細

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

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

TACACS+ のデフォルト設定

次の表に、TACACS+ パラメータのデフォルト設定を示します。

表 *7*：***TACACS+*** のデフォルト パラメータ

パラメータ	デフォルト
TACACS+	ディセーブル

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

第 6 章

SSH および Telnet の設定

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

- SSH および Telnet の設定，77 ページ

SSH および Telnet の設定

SSH および Telnet の概要

SSH サーバ

Secure Shell（SSH）サーバ機能を使用すると、SSH クライアントが Cisco Nexus 3000 シリーズ スイッチに対して、セキュアで暗号化された接続を確立できます。 SSH は強化暗号化を使用して認証を行います。 Cisco Nexus 3000 シリーズ 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、Cisco Nexus 3000 シリーズ スイッチは、別の Cisco Nexus 3000 シリーズ スイッチまたは SSH サーバを稼働している他の任意のデバイスと、セキュアな暗号化された接続を確立できます。 この接続は、暗号化されたアウトバウンド接続を実現します。 認証と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

Cisco Nexus 3000 シリーズ スイッチの 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 3000 シリーズ スイッチ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 3000 シリーズ スイッチは 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 3000 シリーズ スイッチでは、デフォルトで Telnet サーバがイネーブルになっています。

SSH の注意事項および制約事項

SSH には、次の注意事項および制約事項があります。

- Cisco Nexus 3000 シリーズ スイッチは、SSH バージョン 2（SSHv2）だけをサポートしています。

SSH の設定

SSH サーバ キーの生成

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]}
3. switch(config)# **exit**
4. （任意） switch# **show ssh key**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]}	SSH サーバ キーを生成します。 *bits* 引数には、キーの生成に使用するビット数を指定します。 有効な範囲は 768 ～ 2048 です。デフォルト値は 1024 です。 既存のキーを置き換える場合は、キーワード **force** を使用します。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# **show ssh key**	（任意） SSH サーバ キーを表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、SSH サーバ キーを生成する例を示します。

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

ユーザ アカウント用 SSH 公開キーの指定

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

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

Open SSH 形式による SSH 公開キーの指定

ユーザ アカウント用に SSH 形式で SSH 公開キーを指定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **username** *username* **sshkey** *ssh-key*
3. switch(config)# **exit**
4. （任意） switch# **show user-account**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

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

次に、Open SSH 形式で SSH 公開キーを指定する例を示します。

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

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

IETF SECSH 形式による SSH 公開キーの指定

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

手順の概要

1. switch# **copy** *server-file* **bootflash:** *filename*
2. switch# **configure terminal**
3. switch(config)# **username** *username* **sshkey file** *filename*
4. switch(config)# **exit**
5. （任意） switch# **show user-account**
6. （任意） switch# **copy running-config startup-config**

手順の詳細

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

	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、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。

手順の概要

1. switch# **copy** *server-file* **bootflash:** *filename*
2. switch# **configure terminal**
3. （任意） switch# **show user-account**
4. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **copy** *server-file* **bootflash:** *filename*	サーバから PEM フォーマット化された公開キー証明書形式の SSH キーを含むファイルをダウンロードします。FTP、SCP、SFTP、または TFTP サーバを利用できます。
ステップ 2	switch# **configure terminal**	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 3000 シリーズ スイッチから SSH セッションを開始して、リモート デバイスと接続できます。

手順の概要

1. switch# **ssh** {*hostname* | *username@hostname*} [**vrf** *vrf-name*]

手順の詳細

	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。

手順の概要

1. switch# **clear ssh hosts**

手順の詳細

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

SSH サーバのディセーブル化

Cisco Nexus 3000 シリーズ スイッチでは、デフォルトで SSH サーバがイネーブルになっています。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no feature ssh**
3. switch(config)# **exit**
4. （任意） switch# **show ssh server**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

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

SSH サーバ キーの削除

SSH サーバをディセーブルにした後、SSH サーバ キーを削除できます。

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no feature ssh**
3. switch(config)# **no ssh key** [**dsa** | **rsa**]
4. switch(config)# **exit**
5. （任意） switch# **show ssh key**
6. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature ssh**	SSH サーバをディセーブルにします。
ステップ 3	switch(config)# **no ssh key** [**dsa** | **rsa**]	SSH サーバ キーを削除します。 デフォルトでは、すべての SSH キーが削除されます。
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	switch# **show ssh key**	（任意） SSH サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH セッションのクリア

SSH セッションを Cisco Nexus 3000 シリーズ スイッチからクリアできます。

手順の概要

1. switch# **show users**
2. switch# **clear line** *vty-line*

手順の詳細

	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。

手順の概要

1. SSH サーバ キーを生成します。
2. SSH サーバをイネーブルにします。
3. SSH サーバ キーを表示します。
4. Open SSH 形式による SSH 公開キーを指定します。
5. 設定を保存します。

手順の詳細

ステップ 1 SSH サーバ キーを生成します。

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

ステップ 2 SSH サーバをイネーブルにします。

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

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

ステップ 3 SSH サーバ キーを表示します。

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

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/
cTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4ZXIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5/
Ninn0Mc=

bitcount:1024

fingerprint:
4b:4d:f6:b9:42:e9:d9:71:3c:bd:09:94:4a:93:ac:ca
*************************************
could not retrieve dsa key information
*************************************
```

ステップ 4 Open SSH 形式による SSH 公開キーを指定します。

```
switch(config)# username User1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
```

ステップ 5 設定を保存します。

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

Telnet の設定

Telnet サーバのディセーブル化

デフォルトでは、Telnet サーバはイネーブルに設定されています。 Cisco Nexus 3000 シリーズ スイッチで Telnet サーバをディセーブルにできます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature telnet**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **feature telnet**	Telnet サーバをディセーブルにします。 デフォルトはイネーブルです。

Telnet サーバの再イネーブル化

Cisco Nexus 3000 シリーズ スイッチの 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。

手順の概要

1. switch(config)# **feature telnet**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **feature telnet**	Telnet サーバを再度イネーブルにします。

リモート デバイスとの Telnet セッションの開始

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

- リモート デバイスのホスト名を取得し、必要なら、リモート デバイスのユーザ名も取得します。
- Cisco Nexus 3000 シリーズ スイッチ上で 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。

手順の概要

1. switch# **telnet** *hostname*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **telnet** *hostname*	リモート デバイスとの Telnet セッションを作成します。 引数 *hostname* には、IPv4 アドレス、IPv6 アドレス、またはデバイス名を指定します。

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

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

Telnet セッションのクリア

Cisco Nexus 3000 シリーズ スイッチから Telnet セッションをクリアできます。

手順の概要

1. switch# **show users**
2. switch# **clear line** *vty-line*

手順の詳細

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

SSH および Telnet の設定の確認

SSH の設定情報を表示するには、次のいずれかの作業を行います。

- switch# **show ssh key** [**dsa** | **rsa**]
  SSH サーバ キー ペアの情報を表示します。
- switch# **show running-config security** [**all**]
  実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。 キーワード **all** を指定すると、SSH およびユーザ アカウントのデフォルト値が表示されます。
- switch# **show ssh server**
  SSH サーバの設定を表示します。
- switch# **show user-account**
  ユーザ アカウント情報を表示します。

SSH のデフォルト設定

次の表に、SSH パラメータのデフォルト設定を示します。

表 *8*：デフォルトの *SSH* パラメータ

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

第 7 章

アクセス コントロール リストの設定

この章の内容は、次のとおりです。

- ACL について，91 ページ
- IP ACL の設定，100 ページ
- VLAN ACL の概要，109 ページ
- VACL の設定，110 ページ
- VACL の設定例，113 ページ
- ACL TCAM リージョン サイズの設定，113 ページ
- 仮想端末回線の ACL の設定，117 ページ

ACL について

アクセスコントロールリスト（ACL）とは、トラフィックのフィルタリングに使用する順序付きのルールセットのことです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。スイッチは、あるパケットに対してある ACL を適用するかどうかを判断するとき、そのパケットをACL内のすべてのルールの条件に対してテストします。一致する条件が最初に見つかった時点で、パケットを許可するか拒否するかが決まります。一致する条件が見つからないと、スイッチは適用可能なデフォルトのルールを適用します。許可されたパケットについては処理が続行され、拒否されたパケットはドロップされます。

ACL を使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。たとえば、ACLを使用して、厳重にセキュリティ保護されたネットワークからインターネットに HyperText Transfer Protocol（HTTP; ハイパー テキスト トランスファ プロトコル）トラフィックが流入するのを禁止できます。また、特定のサイトへの HTTP トラフィックだけを許可することもできます。その場合は、サイトの IP アドレスが、IP ACL に指定されているかどうかによって判定します。

IP ACL のタイプと適用

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 IPv6 ACL
ルータ ACL	• VLAN インターフェイス （注） VLAN インターフェイスを設定する前に、VLAN インターフェイスをグローバルでイネーブルにする必要があります。 • 物理層 3 インターフェイス • レイヤ 3 イーサネット サブインターフェイス • レイヤ 3 イーサネット ポート チャネル インターフェイス • レイヤ 3 イーサネット ポート チャネル サブインターフェイス • トンネル • 管理インターフェイス	IPv4 ACL IPv6 ACL
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

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

適用順序

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

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

ルール

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

送信元と宛先

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

プロトコル

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

インターネット プロトコル番号を表す整数でプロトコルを指定できます。

暗黙のルール

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

すべての IPv4 ACL には、次の暗黙のルールがあります。

```
deny ip any any
```

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

すべての IPv6 ACL には、次の暗黙のルールがあります。

```
deny ipv6 any any
```

その他のフィルタリング オプション

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

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

シーケンス番号

デバイスはルールのシーケンス番号をサポートしています。 入力されたすべてのルールには、ユーザによって、またはスイッチによって自動的に、シーケンス番号が付けられます。 シーケンス番号によって、次の ACL 設定作業が容易になります。

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

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

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

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

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

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

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

論理演算子と論理演算ユニット

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

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

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

演算子とオペランドの組み合わせが LOU に格納されるかどうかの判断基準を次に示します。

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

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

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

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

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。 ただし、IPv6 TCAM はダブル幅です。 たとえば、256 エントリの IPv6 TCAM を作成するには、IPv4 TCAM を 256 x 2（つまり 512）エントリ減らす必要があります。

IPv6 ポート ACL、VLAN ACL、ルータ ACL を作成して、QoS の IPv6 アドレスを照合できます。ただし、Cisco NX-OS ではすべてを同時に使用することをサポートしていません。 これらの新しい IPv6 TCAM をイネーブルにするには、既存の TCAM を削除するかサイズを縮小する必要があります。

TCAM リージョン サイズに関する注意事項および制約事項は次のとおりです。

- デフォルト ACL TCAM サイズに戻すには、**no hardware profile tcam region** コマンドを使用します。 **write erase** コマンドを使用してからスイッチをリロードする必要はなくなりました。
- プラットフォームによっては、各 TCAM リージョンが異なる最小/最大/集約サイズ制限を持つ可能性があります。
- ARPACL TCAM のデフォルト サイズはゼロです。 コントロールプレーン ポリシング（CoPP）ポリシーで ARP ACL を使用する前に、この TCAM のサイズをゼロ以外のサイズに設定する必要があります。
- VACL および出力 VLAN ACL（E-VACL）のサイズには、同じ値を設定する必要があります。
- IPv4 と IPv6 の両方のアドレスは、ダブル幅の TCAM 内であっても共存できません。
- 合計 TCAM 深度は、入力が 2000、出力が 1000 であり、256 エントリの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 サイズを 0 には設定できません。
- 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* リージョン別 *TCAM* サイズ

TCAM ACL リージョン	デフォルトサイズ	最小サイズ	インクリメンタル サイズ	最大サイズ
SUP（入力）	128 x 2	128 x 2	N/A	128 x 2
SPAN（入力）	128	128	N/A	128
ARPACL（入力）	0	0	128	128

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

ACL のライセンス要件

次の表に、この機能のライセンス要件を示します。

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

ACL の前提条件

IP ACL の前提条件は次のとおりです。

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

VACL の前提条件は次のとおりです。

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

ACL の注意事項および制約事項

IP ACL の設定に関する注意事項と制約事項は次のとおりです。

- ACL の設定には Session Manager を使用することを推奨します。 この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。 この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。
- レイヤ 3 最大伝送単位チェックに失敗し、そのためにフラグメント化を要求しているパケット
- IP オプションがある IPv4 パケット（追加された IP パケット ヘッダーのフィールドは、宛先アドレス フィールドの後）
- 時間範囲を使用する ACL を適用すると、デバイスは ACL エントリで参照される時間範囲の開始時または終了時に ACL エントリをアップデートします。 時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。 時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。
- IP ACL を VLAN インターフェイスに適用するためには、VLAN インターフェイスをグローバルにイネーブル化する必要があります。

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

VACL には、次の設定があります

- ACL の設定には Session Manager を使用することを推奨します。 この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。
- DHCP スヌーピング機能がイネーブルのときには、ACL の統計情報はサポートされません。
- VLAN ACL として適用される IPv4 ACL に、TCP/UDP ポート番号のための論理演算子を含む 1 つ以上の ACE が含まれている場合、ポート番号は入力方向では照合されますが、出力方向では無視されます。
- 1 つの VLAN アクセス マップは、1 つの IP ACL だけを照合できます。
- 1 つの IP ACL は、複数の許可/拒否 ACE を持てます。
- 1 つの VLAN には、1 つのアクセス マップだけを適用できます。

デフォルトの ACL 設定

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

表 *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*：デフォルトの *VACL* パラメータ

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

IP ACL の設定

IP ACL の作成

スイッチに IPv4 または IPv6 を作成し、その ACL にルールを追加できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip access-list** *name*
3. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*
4. （任意） switch(config-acl)# **statistics**
5. （任意） switch# **show** {**ip** | **ipv6**} **access-lists** *name*
6. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip access-list** *name*	IP ACL を作成して、IP ACL コンフィギュレーション モードを開始します。 *name* 引数は 64 文字以内で指定します。
ステップ 3	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*	IP ACL 内にルールを作成します。 多数のルールを作成できます。 *sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。 詳細は、『*Cisco Nexus 3000* シリーズ *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** | **ipv6**} **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
```

次に、IPv6 ACL を作成する例を示します。

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

IP ACL の変更

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

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# {**ip** | **ipv6**} **access-list** *name*
3. switch(config)#**ip access-list** *name*
4. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*
5. （任意） switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}
6. （任意） switch(config-acl)# [**no**] **statistics**
7. （任意） switch#**show ip access-lists** *name*
8. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# {**ip** | **ipv6**} **access-list** *name*	名前で指定した ACL の IP ACL コンフィギュレーション モードを開始します。
ステップ 3	switch(config)#**ip access-list** *name*	名前で指定した ACL の IP ACL コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*	IP ACL 内にルールを作成します。 シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。 シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。 *sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。 詳細は、『*Cisco Nexus 3000 シリーズ Command Reference*』を参照してください。
ステップ 5	switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}	（任意） 指定したルールを IP ACL から削除します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。 詳細は、『*Cisco Nexus 3000 シリーズ Command Reference*』を参照してください。
ステップ 6	switch(config-acl)# [**no**] **statistics**	（任意） ACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。 **no** オプションを指定すると、ACL のグローバルな統計情報がスイッチ内に保持されなくなります。
ステップ 7	switch#**show ip access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 8	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

IP ACL 内のシーケンス番号の変更, （103 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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# no {**ip** | **ipv6**} **access-list** *name*
3. switch(config)# no **ip access-list** *name*
4. （任意） switch# **show running-config**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# no {**ip** | **ipv6**} **access-list** *name*	名前で指定した IP ACL を実行コンフィギュレーションから削除します。
ステップ 3	switch(config)# no **ip access-list** *name*	名前で指定した IP ACL を実行コンフィギュレーションから削除します。
ステップ 4	switch# **show running-config**	（任意） ACL の設定を表示します。 削除された IP ACL は表示されないはずです。
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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **resequence ip access-list** *name starting-sequence-number increment*
3. （任意） switch# **show** {**ip** | **ipv6**} **access-lists** *name*
4. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **resequence ip access-list** *name starting-sequence-number increment*	ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。 後続の各ルールには、直前のルールよりも大きい番号が付けられます。 番号の間隔は、指定した増分によって決まります。 *starting-sequence-number* 引数と *increment* 引数は、1 ～ 4294967295 の整数で指定します。
ステップ 3	switch# **show** {**ip** | **ipv6**} **access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

mgmt0 への IP-ACL の適用

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

はじめる前に

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

手順の概要

1. **configure terminal**
2. **interface mgmt** *port*
3. **ip access-group** *access-list* {**in** | **out**}
4. （任意） **show running-config aclmgr**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface mgmt** *port*
	
	例：
	`switch(config)# interface mgmt0`
	`switch(config-if)#`
		管理インターフェイスのコンフィギュレーション モードを開始します。

ステップ 3	**ip access-group** *access-list* {**in** | **out**} 例： `switch(config-if)#ip access-group acl-120 out`	IPv4 ACL または IPv6 ACL を、指定方向のトラフィックのレイヤ 3 インターフェイスに適用します。 各方向にルータ ACL を 1 つ適用できます。
ステップ 4	**show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	（任意） ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連資料

- IP ACL の作成

IP ACL のポート ACL としての適用

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

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel** *channel-number*}
3. switch(config-if)# **ip port access-group** *access-list* **in**
4. （任意） switch# **show running-config**
5. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel** *channel-number*}	特定のインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **ip port access-group** *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 または IPv6 ACL は、次のタイプのインターフェイスに適用できます。

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

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

（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 エントリが必要な場合があります。

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。

手順の概要

1. switch# **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - switch(config)# **interface ethernet** *slot*/*port*[**.** *number*]
   - switch(config)# **interface port-channel** *channel-number*[**.** *number*]
   - switch(config)# **interface tunnel** *tunnel-number*
   - switch(config)# **interface vlan** *vlan-ID*
   - switch(config)# **interface mgmt** *port*
3. 次のいずれかのコマンドを入力します。
   - switch(config-if)# **ip access-group** *access-list* {**in** | **out**}
   - switch(config-if)# **ipv6 traffic-filter** *access-list* {**in** | **out**}
4. （任意） switch(config-if)# **show running-config aclmgr**
5. （任意） switch(config-if)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • switch(config)# **interface ethernet** *slot*/*port*[**.** *number*] • switch(config)# **interface port-channel** *channel-number*[**.** *number*] • switch(config)# **interface tunnel** *tunnel-number*	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。

	コマンドまたはアクション	目的
	• switch(config)# **interface vlan** *vlan-ID* • switch(config)# **interface mgmt** *port*	
ステップ 3	次のいずれかのコマンドを入力します。 • switch(config-if)# **ip access-group** *access-list* {**in** | **out**} • switch(config-if)# **ipv6 traffic-filter** *access-list* {**in** | **out**}	IPv4 ACL または IPv6 ACL を、指定方向のトラフィックのレイヤ 3 インターフェイスに適用します。 各方向にルータ ACL を 1 つ適用できます。
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に表示される各フィールドの詳細については、『*Cisco Nexus 3000* シリーズ *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** コマンドまたは **show ipv6 access-list** コマンドを使用します。 このコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 3000* シリーズ *Command Reference*』を参照してください。

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

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

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 によって許可されたパケットに設定されているアクションを実行します。

VACL とアクション

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

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

統計情報

スイッチは、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 3000 シリーズ スイッチでは、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。

VACL を作成または変更する手順は、次のとおりです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vlan access-map** *map-name*
3. switch(config-access-map)# **match ip address** *ip-access-list*
4. switch(config-access-map)# **action** {**drop** | **forward**}
5. （任意） switch(config-access-map)# [**no**] **statistics**
6. （任意） switch(config-access-map)# **show running-config**
7. （任意） switch(config-access-map)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **vlan access-map** *map-name*	指定したアクセスマップのアクセスマップ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-access-map)# **match ip address** *ip-access-list*	マップの IPv4 および IPV6 ACL を指定します。
ステップ 4	switch(config-access-map)# **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。

	コマンドまたはアクション	目的
ステップ 5	switch(config-access-map)# [**no**] **statistics**	（任意） VACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。 **no** オプションを指定すると、VACL のグローバルな統計情報がスイッチ内に保持されなくなります。
ステップ 6	switch(config-access-map)# **show running-config**	（任意） ACL の設定を表示します。
ステップ 7	switch(config-access-map)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL の削除

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

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no vlan access-map** *map-name*
3. （任意） switch(config)# **show running-config**
4. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no vlan access-map** *map-name*	指定したアクセスマップの VLAN アクセスマップの設定を削除します。

	コマンドまたはアクション	目的
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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# [**no**] **vlan filter** *map-name* **vlan-list** *list*
3. （任意） switch(config)# **show running-config**
4. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **vlan filter** *map-name* **vlan-list** *list*	指定したリストによって、VACL を VLAN に適用します。**no** を使用すると、VACL の適用が解除されます。 **vlan-list** コマンドで指定できる VLAN は最大 32 個ですが、複数の **vlan-list** コマンドを設定すれば 32 個を超える VLAN を指定できます。
ステップ 3	switch(config)# **show running-config**	（任意） ACL の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL の設定の確認

VACL 設定情報を表示するには、次のいずれかの作業を実行します。

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

VACL 統計情報の表示と消去

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

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

VACL の設定例

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

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

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。

手順の概要

1. **configure terminal**
2. **hardware profile tcam region** {**arpacl** | {**ipv6-e-racl** | **e-racl**} | **ifacl** | **ipsg** | {**ipv6-qos** | **qos**} |**qoslbl** | {**ipv6-racl** | **racl**} | **vacl** } *tcam_size*
3. **copy running-config startup-config**
4. switch(config)# **show hardware profile tcam region**
5. switch(config)# **reload**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**hardware profile tcam region** {**arpacl**	{**ipv6-e-racl**	**e-racl**}	**ifacl**	**ipsg**	{**ipv6-qos**	**qos**} |**qoslbl**	{**ipv6-racl**	**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）ACL（ARPACL）TCAM リージョンのサイズを設定します。 • **e-racl**：出力ルータ ACL（ERACL）TCAM リージョンのサイズを設定します。 • **e-vacl**：出力 VLAN ACL（EVACL）TCAM リージョンのサイズを設定します。 • **ifacl**：インターフェイス ACL（ifacl）TCAM リージョンのサイズを設定します。 • **ipsg**：IP ソース ガード（IPSG）TCAM リージョンのサイズを設定します。 • **qos**：Quality of Service（QoS）TCAM リージョンのサイズを設定します。 • **qoslbl**：QoS ラベル（qoslbl）TCAM リージョンのサイズを設定します。 • **racl**：ルータ ACL（RACL）TCAM リージョンのサイズを設定します。 • **vacl**：VLAN ACL（VACL）TCAM リージョンの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。

	コマンドまたはアクション	目的
		（注） **vacl** および **e-vacl** TCAM リージョンは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**	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**	スイッチで次のリロード時に適用される TCAM サイズを表示します。
ステップ 5	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、次にリロードして初めて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-configur startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

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

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

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

switch(config)# show hardware profile tcam region
   sup size = 128
  vacl size = 512
 ifacl size = 256
   qos size = 256
 rbacl size = 0
  span size = 128
  racl size = 256
e-racl size = 512
e-vacl size = 512
qoslbl size = 512
  ipsg size = 512
arpacl size = 128
switch(config)#
```

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)#
```

デフォルト TCAM リージョン サイズに戻す

手順の概要

1. **configure terminal**
2. switch(config)# **no hardware profile tcam region** { **arpacl** | **arpacl** *tcam_size*}
3. （任意） **copy running-config startup-config**
4. switch(config)# **reload**

手順の詳細

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

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

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

はじめる前に

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **line vty**
3. switch(config-line)# **access-class access-list-number {in | out}**
4. （任意） switch(config-line)# **no access-class access-list-number {in | out}**
5. switch(config-line)# **exit**
6. （任意） switch# **show running-config aclmgr**
7. （任意） switch# **copy running-config startup-config**

手順の詳細

	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。

	コマンドまたはアクション	目的

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

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

ステップ 6	switch# **show running-config aclmgr** 例： `switch# show running-config aclmgr`	（任意） スイッチの ACL の実行コンフィギュレーションを表示します。
ステップ 7	switch# **copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

VTY 回線の ACL の確認

VTY 回線の ACL 設定を表示するには、次のいずれかの作業を行います。

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

VTY 回線の ACL の設定例

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

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

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

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

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

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

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

次に、VTY 回線でアクセス制限を削除する例を示します。

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

第 8 章

DHCP スヌーピングの設定

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

- DHCP スヌーピングの概要，121 ページ
- DHCP リレー エージェントの概要，124 ページ
- DHCP スヌーピングの注意事項および制約事項，125 ページ
- DHCP スヌーピングのデフォルト設定，126 ページ
- DHCP スヌーピングの設定，126 ページ
- DHCP スヌーピング設定の確認，136 ページ
- DHCP バインディングの表示，137 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，137 ページ
- DHCP スヌーピングの設定例，138 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。

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

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

機能のイネーブル化とグローバルなイネーブル化

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

機能のイネーブル化

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

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

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

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

グローバルなイネーブル化

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

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

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

信頼できるソースおよび信頼できないソース

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

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

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

Cisco Nexus 3000 シリーズ スイッチでは、接続インターフェイスの信頼状態を設定することにより送信元が信頼されることを示します。

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

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

DHCP スヌーピング バインディング データベース

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

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

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

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

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

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

DHCP 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 identifier]、[link selection]、[server identifier override] 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。

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 スヌーピングの設定

DHCP スヌーピングの最小設定

手順の詳細

	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, （127 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化します。	詳細については、DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化, （128 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 3	少なくとも 1 つの VLAN で、DHCP スヌーピングをイネーブルにします。	デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。 詳細については、VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化, （129 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, （131 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。

手順の概要

1. **config t**
2. **[no] feature dhcp**
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**[no] feature dhcp** 例： `switch(config)# feature dhcp`	DHCP スヌーピング機能をイネーブルにします。 **no** オプションを使用すると、DHCP スヌーピング機能がディ

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

DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化

スイッチに対して DHCP スヌーピング機能のグローバルなイネーブル化またはディセーブル化が可能です。 DHCP スヌーピングをグローバルにディセーブルにすると、DHCP スヌーピングの実行や 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。

手順の概要

1. **config t**
2. **[no] ip dhcp snooping**
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	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。

	コマンドまたはアクション	目的
ステップ 2	[no] ip dhcp snooping 例： switch(config)# ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブル化します。 no オプションを使用すると DHCP スヌーピングがディセーブルになります。
ステップ 3	show running-config dhcp 例： switch(config)# show running-config dhcp	（任意） DHCP スヌーピングの設定を表示します。
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。

手順の概要

1. **config t**
2. [**no**] **ip dhcp snooping vlan** *vlan-list*
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip dhcp snooping vlan** *vlan-list* 例： `switch(config)# ip dhcp snooping vlan 100,200,250-252`	*vlan-list* で指定する VLAN の DHCP スヌーピングをイネーブルにします。 **no** オプションを使用すると、指定した VLAN の DHCP スヌーピングがディセーブルになります。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP パケットの厳密な検証のイネーブル化またはディセーブル化

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

手順の概要

1. **config t**
2. [**no**] **ip dhcp packet strict-validation**
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

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

インターフェイスの信頼状態の設定

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

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

はじめる前に

デフォルトでは、すべてのインターフェイスは信頼できません。

DHCP スヌーピングがイネーブルになっていることを確認してください。

手順の概要

1. **config t**
2. 次のいずれかのコマンドを入力します。
   - **interface ethernet** *port*/*slot*
   - **interface port-channel** *channel-number*
3. [**no**] **ip dhcp snooping trust**
4. （任意） **show running-config dhcp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	次のいずれかのコマンドを入力します。
	• **interface ethernet** *port*/*slot*
	• **interface port-channel** *channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		• インターフェイス コンフィギュレーション モードを開始します。*port*/*slot* は、DHCP スヌーピングで trusted または untrusted に設定するレイヤ 2 イーサネット インターフェイスです。
		• インターフェイス コンフィギュレーション モードを開始します。*port*/*slot* は、DHCP スヌーピングで trusted または untrusted に設定するレイヤ 2 ポートチャネル インターフェイスです。

ステップ 3	[**no**] **ip dhcp snooping trust** 例： `switch(config-if)# ip dhcp snooping trust`	DHCP スヌーピングに関してインターフェイスを信頼できるインターフェイスとして設定します。 **no** オプションを使用すると、ポートは信頼できないインターフェイスとして設定されます。
ステップ 4	**show running-config dhcp** 例： `switch(config-if)# show running-config dhcp`	（任意） DHCP スヌーピングの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー エージェントのイネーブル化またはディセーブル化

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

はじめる前に

DHCP 機能がイネーブルであることを確認します。

手順の概要

1. **config t**
2. **[no] ip dhcp relay**
3. （任意） **show ip dhcp relay**
4. （任意） **show running-config dhcp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

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

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

ある VRF のインターフェイスで受信した DHCP 要求を、別の VRF の DHCP サーバにリレーする機能をサポートするように、デバイスを設定できます。

はじめる前に

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

手順の概要

1. **config t**
2. **[no] ip dhcp relay information option vpn**
3. **[no] ip dhcp relay sub-option type cisco**
4. （任意） **show ip dhcp relay**
5. （任意） **show running-config dhcp**
6. （任意） **copy running-config startup-config**

手順の詳細

	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。

	コマンドまたはアクション	目的
ステップ 4	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 5	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

手順の概要

1. **config t**
2. **ip source binding** *IP-address MAC-address* **vlan** *vlan-id* {**interface ethernet** *slot/port* | **port-channel** *channel-no*}
3. （任意） **show ip dhcp snooping binding**
4. （任意） **show ip dhcp snooping binding dynamic**
5. （任意） **copy running-config startup-config**

手順の詳細

	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。

	コマンドまたはアクション	目的
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。
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。 これらのコマンド出力のフィールドの詳細については、『』、『*Cisco Nexus 3000 Series NX-OS System Management Configuration Guide*』を参照してください。

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

DHCP バインディングの表示

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

このコマンドの出力フィールドの詳細については、『』、『*Cisco Nexus 3000 Series NX-OS 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。

手順の概要

1. （任意） **clear ip dhcp snooping binding**
2. （任意） **clear ip dhcp snooping binding interface ethernet** *slot*/*port*[.*subinterface-number*]
3. （任意） **clear ip dhcp snooping binding interface port-channel** *channel-number*[.*subchannel-number*]
4. （任意） **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*] }
5. （任意） **show ip dhcp snooping binding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ip dhcp snooping binding** 例： `switch# clear ip dhcp snooping binding`	（任意） DHCP スヌーピング バインディング データベースからすべてのエントリをクリアします。
ステップ 2	**clear ip dhcp snooping binding interface ethernet** *slot*/*port*[.*subinterface-number*] 例： `switch# clear ip dhcp snooping binding interface ethernet 1/4`	（任意） DHCP スヌーピング バインディング データベースから、特定のイーサネット インターフェイスに関連するエントリをクリアします。
ステップ 3	**clear ip dhcp snooping binding interface port-channel** *channel-number*[.*subchannel-number*] 例： `switch# clear ip dhcp snooping binding interface port-channel 72`	（任意） DHCP スヌーピング バインディング データベースから、特定のポート チャネル インターフェイスに関連するエントリをクリアします。
ステップ 4	**clear ip dhcp snooping binding vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface** {**ethernet** *slot*/*port*[.*subinterface-number* | **port-channel** *channel-number*[.*subchannel-number*] } 例： `switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface ethernet 2/11`	（任意） DHCP スヌーピング バインディング データベースから、特定のエントリをクリアします。
ステップ 5	**show ip dhcp snooping binding** 例： `switch# show ip dhcp snooping binding`	（任意） DHCP スヌーピング バインディング データベースを表示します。

DHCP スヌーピングの設定例

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

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

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

第 9 章

ダイナミック ARP インスペクションの設定

この章では、Cisco Nexus 3000 シリーズ スイッチに Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）Inspection（DAI; ダイナミック ARP インスペクション）を設定する方法について説明します。

この章は、次の内容で構成されています。

- DAI の概要，139 ページ
- DAI のライセンス要件，143 ページ
- DAI の前提条件，144 ページ
- DAI の注意事項と制約事項，144 ページ
- DAI のデフォルト設定，145 ページ
- DAI の設定，146 ページ
- DAI の設定の確認，152 ページ
- DAI の統計情報のモニタリングとクリア，152 ページ
- DAI の設定例，153 ページ

DAI の概要

ARP

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。 たとえば、ホスト B がホスト A に情報を送信しようとして、ホスト B の ARP キャッシュにホスト A の MAC アドレスがないという場合、 ARP の用語では、ホスト B が送信者、ホスト A はターゲットになります。

ホスト B は、ホスト A の IP アドレスに関連付けられた MAC アドレスを取得するため、このブロードキャスト ドメイン内の全ホストに対してブロードキャスト メッセージを送信します。 ブ

ロードキャスト ドメイン内の全ホストはこの ARP 要求を受信し、これに対してホスト A は自身の MAC アドレスを返します。

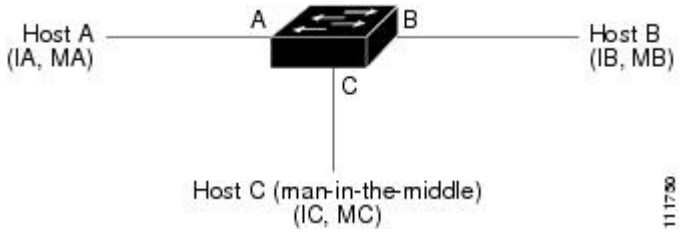
ARP スプーフィング攻撃

ARPでは、たとえARP要求を受信していなくても、ホストからの応答が可能なので、ARPスプーフィング攻撃と ARP キャッシュ ポイズニングが発生する可能性があります。 攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

ARPスプーフィング攻撃は、サブネットに接続されているデバイスのARPキャッシュに偽りの情報を送信することにより、レイヤ 2 ネットワークに接続されているホスト、スイッチ、ルータに影響を及ぼす可能性があります。 ARPキャッシュに偽りの情報を送信することをARPキャッシュポイズニングといいます。 スプーフ攻撃では、サブネット上の他のホストに対するトラフィックの代行受信も可能です。

次の図に、ARP キャッシュ ポイズニングの例を示します。

図 *4*： *ARP* キャッシュ ポイズニング



ホストA、B、Cは、それぞれインターフェイスA、B、Cを介してデバイスに接続されています。これらのインターフェイスは同一サブネットに属します。 カッコ内は、各ホストのIPおよびMACアドレスを示します。たとえば、ホスト A は IP アドレス IA、および MAC アドレス MA を使用します。 ホスト A がホスト B に IP データを送信する必要がある場合、ホスト A は IP アドレス IB に関連付けられた MAC アドレスを求める ARP 要求をブロードキャストします。 デバイスとホスト B はこの ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持つホストの ARP バインディングを、それぞれの ARP キャッシュ内に書き込みます。たとえば、IP アドレス IA は MAC アドレス MA にバインドされます。 ホスト B が応答すると、デバイスとホスト A は、IP アドレス IB および MAC アドレス MB を持つホストのバインディングを、それぞれの ARP キャッシュ内に書き込みます。

ホストCは、バインディングを伴う2つの偽造ARP応答をブロードキャストすることにより、デバイス、ホスト A、ホスト B の ARP キャッシュをポイズニングできます。偽造 ARP 応答の 1 つは、IP アドレス IA と MAC アドレス MC を持つホストの応答、もう 1 つは IP アドレス IB と MAC アドレス MC を持つホストの応答です。 これにより、ホスト B とデバイスは、IA を宛先とするトラフィックの宛先 MAC アドレスとして、MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。 同様に、ホスト A とデバイスは、IB を宛先とするトラフィックの宛先 MAC アドレスとして MAC アドレス MC を使用します。

ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。 このトポロジでは、ホスト C は、ホスト A からホスト B へのトラフィック ストリーム内に自身を割り込ませています。これは、*man-in-the-middle* 攻撃の典型的な例です。

DAI および ARP スプーフィング攻撃

DAI を使用することで、有効な ARP 要求および応答だけがリレーされるようになります。 DAI がイネーブルになり適切に設定されている場合、Cisco NX-OS デバイスは次のアクティビティを実行します。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

DAI によって ARP パケットの有効性を判断するときの基準となる有効な IP-to-MAC バインディングは、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースに保存されています。 このデータベースは、VLAN とデバイス上で DHCP スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。 また、このデータベースにはユーザが作成するスタティック エントリも保存できます。 ARP パケットを信頼できるインターフェイス上で受信した場合は、デバイスはこのパケットを検査せずに転送します。 信頼できないインターフェイス上では、デバイスは有効性を確認できたパケットだけを転送します。

DAI では、パケット内の IP アドレスが無効な場合に ARP パケットをドロップするのか、または ARP パケット本体の MAC アドレスがイーサネット ヘッダーに指定されたアドレスと一致しない場合に ARP パケットをドロップするのかを設定できます。

関連トピック

DAI パケットのロギング, （143 ページ）
追加検証のイネーブル化またはディセーブル化, （148 ページ）

インターフェイスの信頼状態とネットワーク セキュリティ

DAI は、デバイスの各インターフェイスに信頼状態を関連付けます。 信頼できるインターフェイス上で受信されたパケットは、DAI のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、DAI の有効性検査が行われます。

一般的なネットワーク構成では、次のガイドラインに従ってインターフェイスの信頼状態を設定します。

信頼できない

ホストに接続されているインターフェイス

信頼できる

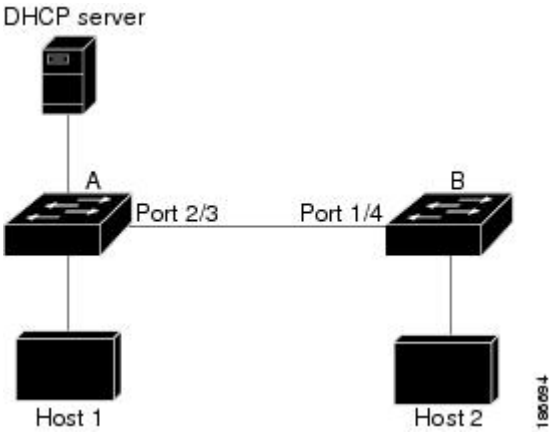
デバイスに接続されているインターフェイス

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

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

次の図では、デバイスAおよびデバイスBの両方が、ホスト1およびホスト2を収容するVLAN上でDAIを実行していると仮定します。 ホスト1およびホスト2が、デバイスAに接続されているDHCPサーバからIPアドレスを取得すると、デバイスAだけがホスト1のIP/MACアドレスをバインドします。 デバイスAとデバイスB間のインターフェイスが信頼できない場合は、ホスト1からのARPパケットはデバイスBではドロップされ、ホスト1およびホスト2の間の接続は切断されます。

図 *5*： *DAI* をイネーブルにした *VLAN* での *ARP* パケット検証



信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワークにセキュリティ ホールが生じる可能性があります。 デバイスAがDAIを実行していなければ、ホスト1はデバイスBのARPキャッシュを簡単にポイズニングできます（デバイス間のリンクが信頼できるものとして設定されている場合はホスト2も同様）。 この状況は、デバイスBがDAIを実行している場合でも起こりえます。

DAIは、DAIが稼働するデバイスに接続されているホスト（信頼できないインターフェイス上）がネットワーク内の他のホストのARPキャッシュをポイズニングしないように保証します。ただし、DAIが稼働するデバイスに接続されているホストのキャッシュがネットワークの他の部分のホストによってポイズニングされるのを防ぐことはできません。

VLAN内の一部のデバイスでDAIが稼働し、他のデバイスでは稼働していない場合は、DAIが稼働しているデバイス上のインターフェイスの信頼状態を次のガイドラインに従って設定します。

信頼できない

ホスト、または DAI が稼働していないデバイスに接続されているインターフェイス

信頼できる

DAI が稼働しているデバイスに接続されているインターフェイス

DAI が稼働していないデバイスからのパケットのバインディングを検証するには、DAI が稼働しているデバイスに ARP ACL を設定します。バインディングの有効性を判断できない場合は、DAI が稼働しているデバイスを DAI が稼働していないデバイスからレイヤ 3 で隔離します。

（注） ネットワークの設定によっては、VLAN 内の一部のデバイスで ARP パケットを検証できない場合もあります。

関連トピック

レイヤ 2 インターフェイスの DAI 信頼状態の設定, （147 ページ）

DAI パケットのロギング

Cisco NX-OS は処理された DAI パケットについてのログ エントリのバッファを維持しています。各ログエントリには、受信側の VLAN、ポート番号、送信元 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

ログに記録するパケットのタイプを指定することもできます。 デフォルトでは、Cisco NX-OS デバイスは DAI がドロップしたパケットだけをログに記録します。

ログ バッファがあふれると、デバイスは最も古い DAI ログ エントリを新しいエントリで上書きします。 バッファ内の最大エントリ数を設定できます。

（注） Cisco NX-OS は、ログに記録される DAI パケットに関するシステム メッセージを生成しません。

関連トピック

DAI のログ バッファ サイズの設定, （150 ページ）
DAI のログ フィルタリングの設定, （150 ページ）

DAI のライセンス要件

次の表に、DAI のライセンス要件を示します。

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

DAI の前提条件

- DHCP を設定するには、その前に DAI 機能をイネーブルにする必要があります。

DAI の注意事項と制約事項

DAI に関する注意事項と制約事項は次のとおりです。

- DAI は入力セキュリティ機能であり、出力検査は行いません。
- DAI は、DAI をサポートしないデバイス、またはこの機能がイネーブルにされていないデバイスに接続されているホストに対しては、効果がありません。 man-in-the-middle 攻撃は 1 つのレイヤ 2 ブロードキャスト ドメインに限定されるため、DAI が有効なドメインを、DAI が実行されないドメインから切り離す必要があります。 これにより、DAIが有効なドメイン内のホストの ARP キャッシュをセキュリティ保護できます。
- DAI では、DHCP スヌーピング バインディング データベース内のエントリを使用して、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスのバインディングを確認します。 DAI が ARP パケットの有効性を判断するのにスタティック IP-MAC アドレス バインディングを使用するように設定する場合、DHCP スヌーピングの設定はイネーブルにするだけで済みます。 DAI が ARP パケットの有効性を判断するのにダイナミック IP-MAC アドレス バインディングを使用するように設定する場合は、DAI を設定した VLAN と同じ VLAN に DHCP スヌーピングを設定する必要があります。
- **feature dhcp** コマンドを使用して DHCP 機能をイネーブルにすると、I/O モジュールが DHCP を受信する前、または DAI の設定前に約 30 秒の遅延が発生します。 この遅延は、DHCP 機能がディセーブルになった設定から、DHCP 機能がイネーブルになった設定に変更するために使用する方式には関係なく発生します。 たとえば、ロールバック機能を使用して、DHCP 機能をイネーブルにする設定に戻した場合、ロールバックを完了してから約 30 秒後に I/O モジュールが DHCP と DAI 設定を受信します。
- DAI は、アクセス ポート、トランク ポート、ポート チャネル ポート、およびプライベート VLAN ポートでサポートされます。

- ポート チャネルに対する DAI の信頼設定によって、そのポート チャネルに割り当てたすべての物理ポートの信頼状態が決まります。 たとえば、ある物理ポートを信頼できるインターフェイスとして設定し、信頼できないインターフェイスであるポート チャネルにその物理ポートを追加した場合、その物理ポートは信頼できない状態になります。
- ポート チャネルから物理ポートを削除した場合、その物理ポートはポート チャネルの DAI 信頼状態の設定を保持しません。
- ポートチャネルの信頼状態を変更すると、デバイスはそのチャネルを構成するすべての物理ポートに対し、新しい信頼状態を設定します。
- ARP パケットが有効かどうかを判定するために DAI でスタティック IP-MAC アドレス バインディングを使用するように設定する場合は、DHCP スヌーピングがイネーブルになっていること、およびスタティック IP-MAC アドレス バインディングを設定していることを確認します。
- ARP パケットが有効かどうかを判定するために DAI でダイナミック IP-MAC アドレス バインディングを使用するように設定する場合は、DHCP スヌーピングがイネーブルになっていることを確認します。

DAI のデフォルト設定

次の表に、DAI パラメータのデフォルト設定を示します。

表 *14*：デフォルトの *DAI* パラメータ

パラメータ	デフォルト
DAI	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
有効性検査	検査は実行されません。
ログ バッファ	DAI をイネーブルにした場合は、拒否または廃棄されたすべての ARP パケットが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは、1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

DAI の設定

VLAN での DAI のイネーブル化とディセーブル化

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

はじめる前に

DAI をイネーブルにする場合は、次の点を確認してください。

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

手順の概要

1. **configure terminal**
2. [**no**] **ip arp inspection vlan** *list*
3. （任意） **show ip arp inspection vlan** *list*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip arp inspection vlan** *list* 例： `switch(config)# ip arp inspection vlan 13`	VLAN の特定のリストに対して DAI をイネーブルにします。 **no** オプションを使用すると、指定した VLAN の DAI がディセーブルになります。
ステップ 3	**show ip arp inspection vlan** *list* 例： `switch(config)# show ip arp inspection vlan 13`	（任意） VLANの特定リストのDAIステータスを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ 2 インターフェイスの DAI 信頼状態の設定

レイヤ 2 インターフェイスの DAI インターフェイス信頼状態を設定できます。 デフォルトでは、すべてのインターフェイスは信頼できません。

デバイスは、信頼できるレイヤ 2 インターフェイス上で受信した ARP パケットを転送しますが、検査は行いません。

信頼できないインターフェイス上では、デバイスはすべての ARP 要求および ARP 応答を代行受信します。デバイスは、ローカル キャッシュをアップデートして、代行受信したパケットを適切な宛先に転送する前に、そのパケットの IP-MAC アドレス バインディングが有効かどうかを検証します。 そのパケットのバインディングが無効であると判断すると、デバイスはそのパケットをドロップし、ロギングの設定に従ってログに記録します。

はじめる前に

DAI をイネーブルにする場合は、DHCP 機能がイネーブルであることを確認します。

手順の概要

1. **configure terminal**
2. **interface** *type number* / *slot*
3. [**no**] **ip arp inspection trust**
4. （任意） **show ip arp inspection interface** *type number* / *slot*
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *type number* / *slot*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **ip arp inspection trust** 例： `switch(config-if)# ip arp inspection trust`	インターフェイスを、信頼できる ARP インターフェイスとして設定します。 **no** オプションを使用すると、そのインターフェイスは信頼できない ARP インターフェイスとして設定されます。

	コマンドまたはアクション	目的
ステップ 4	**show ip arp inspection interface** *type number / slot* 例： `switch(config-if)# show ip arp inspection interface ethernet 2/1`	（任意） 特定のインターフェイスの信頼状態およびARPパケット レートを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

インターフェイスの信頼状態とネットワーク セキュリティ，（141 ページ）
DAI のログ フィルタリングの設定，（150 ページ）

追加検証のイネーブル化またはディセーブル化

ARPパケットの追加検証をイネーブルまたはディセーブルにできます。デフォルトでは、ARPパケットの追加検証はイネーブルになりません。 追加検証が設定されていない場合、送信元 MAC アドレス、ARP パケットの IP/MAC バインディング エントリと照合する送信元 IP アドレスのチェックは、イーサネット送信元MACアドレス（ARP送信者のMACアドレスではない）と ARP 送信者の IP アドレスを使用して実行されます。

DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、記録、および廃棄します。宛先MACアドレス、送信元および宛先IPアドレス、送信元MACアドレスに対し、追加検証をイネーブルにすることができます。

追加検証を実装するには、**ip arp inspection validate** コマンドで次のキーワードを使用します。

dst-mac

ARP 応答のイーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較して検査します。イネーブルにすると、異なるMACアドレスを持つパケットは無効パケットとして分類され、廃棄されます。

ip

ARP 本文をチェックして、無効な IP アドレスや予期しない IP アドレスがないかを確認します。 アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。 送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。

src-mac

ARP 要求と応答のイーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信者 MAC アドレスと比較して検査します。 イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。

追加検証をイネーブルにする場合は、次の点に注意してください。

- 少なくとも 1 つのキーワードを指定する必要があります。 指定するキーワードは、1 つでも、2 つでも、3 つすべてでもかまいません。
- 各 **ip arp inspection validate** コマンドにより、それまでに指定したコマンドの設定が置き換えられます。 **ip arp inspection validate** コマンドによって src -mac および dst-mac 検証をイネーブルにし、2 つめの **ip arp inspection validate** コマンドで IP 検証をイネーブルにした場合は、2 つめのコマンドを入力した時点で src-mac と dst-mac の検証がディセーブルになります。

手順の概要

1. **configure terminal**
2. **[no] ip arp inspection validate {[src-mac] [dst-mac] [ip]}**
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**[no] ip arp inspection validate {[src-mac] [dst-mac] [ip]}** 例： `switch(config)# ip arp inspection validate src-mac dst-mac ip`	追加のDAI検証をイネーブルにします。あるいは、**no** オプションを使用して、追加の DAI 検証をディセーブルにします。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAIの設定も含めて、DHCPスヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI のログ バッファ サイズの設定

DAI のログ バッファ サイズを設定できます。 デフォルトのバッファ サイズは 32 メッセージです。

手順の概要

1. **configure terminal**
2. [**no**] **ip arp inspection log-buffer entries** *number*
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip arp inspection log-buffer entries** *number* 例： `switch(config)# ip arp inspection log-buffer entries 64`	DAI のログ バッファ サイズを設定します。 **no** オプションを使用すると、デフォルトのバッファ サイズ（32 メッセージ）に戻ります。 設定できるバッファ サイズは、0 ～ 2048 メッセージです。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI のログ フィルタリングの設定

DAI パケットを記録するかどうかをデバイスが判断する方法を設定できます。 デフォルトでは、デバイスはドロップされる DAI パケットをログに記録します。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings all**
   - **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings none**
   - **ip arp inspection vlan** *vlan-list* **logging dhcp-bindingspermit**
   - **no ip arp inspection vlan** *vlan-list* **logging dhcp-bindings** {**all** | **none** | **permit**}
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	次のいずれかのコマンドを入力します。 • **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings all** • **ip arp inspection vlan** *vlan-list* **logging dhcp-bindings none** • **ip arp inspection vlan** *vlan-list* **logging dhcp-bindingspermit** • **no ip arp inspection vlan** *vlan-list* **logging dhcp-bindings** {**all**	**none**	**permit**} 例： `switch(config)# ip arp inspection vlan 100 dhcp-bindings permit`	次のようにして、DAI ログ フィルタリングを設定します。 **no** オプションを使用すると、DAI ログ フィルタリングが削除されます。 • DHCP バインディングに一致するすべてのパケットを記録します。 • DHCP バインディングに一致するパケットを記録しません。 • DHCP バインディングによって許可されるパケットを記録します。 • DAI ログ フィルタリングを削除します。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAI の設定も含めて、DHCP スヌーピング設定を表示します。

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

DAI の設定の確認

DAI の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config arp	DAI の設定を表示します。
show ip arp inspection	DAI のステータスを表示します。
show ip arp inspection interface ethernet	特定のインターフェイスの信頼状態およびARP パケット レートを表示します。
show ip arp inspection vlan	特定の VLAN の DAI 設定を表示します。
show arp access-lists	ARP ACL を表示します。
show ip arp inspection log	DAI のログ設定を表示します。

DAI の統計情報のモニタリングとクリア

DAI の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドを使用します。 これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show ip arp inspection statistics	DAI の統計情報を表示します。
show ip arp ethernet	インターフェイス固有のDAIの統計情報を表示します。
clear ip arp inspection statistics	DAI 統計情報をクリアします。

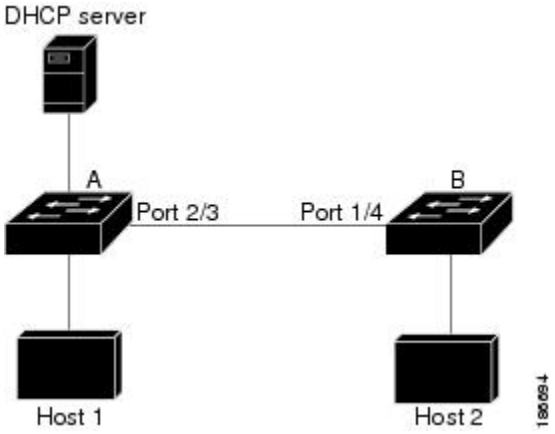
DAI の設定例

例 1：2 つのデバイスが DAI をサポートする場合

2 つのデバイスが DAI をサポートする場合の DAI の設定手順を次に示します。

次の図に、この例のネットワーク構成を示します。 ホスト 1 はデバイス A に、ホスト 2 はデバイス B にそれぞれ接続されています。 両方のデバイスは、これらのホストが置かれている VLAN 1 上で DAI を実行しています。 DHCP サーバはデバイス A に接続されています。 両方のホストは、同一の DHCP サーバから IP アドレスを取得します。 デバイス A はホスト 1 およびホスト 2 のバインディングを持ち、デバイス B はホスト 2 のバインディングを持ちます。 デバイス A のイーサネット インターフェイス 2/3 は、デバイス B のイーサネット インターフェイス 1/4 に接続されています。

図 *6*：*DAI* をサポートする *2* つのデバイス



DAI では、DHCP スヌーピング バインディング データベース内のエントリを使用して、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスのバインディングを確認します。 IP アドレスを動的に割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。

- この構成は、DHCP サーバがデバイス A から別の場所に移動されると機能しません。
- この構成によってセキュリティが損なわれないようにするには、デバイス A のイーサネット インターフェイス 2/3、およびデバイス B のイーサネット インターフェイス 1/4 を、信頼できるインターフェイスとして設定します。

デバイス A の設定

デバイス A で DAI をイネーブルにし、イーサネット インターフェイス 2/3 を信頼できるインターフェイスとして設定するには、次の作業を行います。

ステップ 1 デバイス A にログインして、デバイス A とデバイス B の間の接続を確認します。

例：
```
switchA# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchB                Ethernet2/3     177     R S I    WS-C2960-24TC Ethernet1/4
switchA#
```

ステップ 2 VLAN 1 で DAI をイネーブルにし、設定を確認します。

例：
```
switchA# config t
switchA(config)# ip arp inspection vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchA(config)#
```

ステップ 3 イーサネット インターフェイス 2/3 を、信頼できるインターフェイスとして設定します。

例：
```
switchA(config)# interface ethernet 2/3
switchA(config-if)# ip arp inspection trust
switchA(config-if)# exit
switchA(config)# exit
switchA# show ip arp inspection interface ethernet 2/3
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet2/3      Trusted           15             5
```

ステップ 4 バインディングを確認します。

例：
```
switchA# show ip dhcp snooping binding
MacAddress         IpAddress        LeaseSec  Type           VLAN  Interface
-----------------  ---------------  --------  -------------  ----  -------------
00:60:0b:00:12:89  10.0.0.1         0         dhcp-snooping  1     Ethernet2/3
switchA#
```

ステップ 5 DAI がパケットを処理する前、およびあとの統計情報を調べます。

例：
```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
```

```
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

ホスト 1 が IP アドレス 10.0.0.1 および MAC アドレス 0002.0002.0002 を持つ 2 つの ARP 要求を送信すると、両方の要求が許可されます。これは、次の統計情報で確認できます。

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

ホスト 1 が、IP アドレス 10.0.0.3 を持つ ARP 要求を送信しようとすると、このパケットはドロップされ、エラー メッセージがログに記録されます。

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Ethernet2/3, vlan
1.([0002.0002.0002/10.0.0.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Fri Jul 13 2008])
```

この場合に表示される統計情報は次のようになります。

```
switchA# show ip arp inspection statistics vlan 1
switchA#
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 2
ARP Res Dropped    = 0
DHCP Drops         = 2
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

デバイス B の設定

デバイス B で DAI をイネーブルにし、イーサネット インターフェイス 1/4 を信頼できるインターフェイスとして設定するには、次の作業を行います。

ステップ 1 デバイス B にログインして、デバイス B とデバイス A の間の接続を確認します。

例：
```
switchB# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchA                Ethernet1/4     120     R S I    WS-C2960-24TC Ethernet2/3
switchB#
```

ステップ 2 VLAN 1 で DAI をイネーブルにし、設定を確認します。

例：
```
switchB# config t
switchB(config)# ip arp inspection vlan 1
switchB(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchB(config)#
```

ステップ 3 イーサネット インターフェイス 1/4 を、信頼できるインターフェイスとして設定します。

例：
```
switchB(config)# interface ethernet 1/4
switchB(config-if)# ip arp inspection trust
switchB(config-if)# exit
switchB(config)# exit
switchB# show ip arp inspection interface ethernet 1/4
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet1/4      Trusted           15             5
switchB#
```

ステップ 4 DHCP スヌーピング バインディングのリストを確認します。

例：
```
switchB# show ip dhcp snooping binding
MacAddress         IpAddress        LeaseSec  Type           VLAN  Interface
-----------------  ---------------  --------  -------------  ----  -------------
00:01:00:01:00:01  10.0.0.2         4995      dhcp-snooping  1     Ethernet1/4
switchB#
```

ステップ 5 DAI がパケットを処理する前、およびあとの統計情報を調べます。

例：
```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
```

```
IP Fails-ARP Res   = 0
switchB#
```

ホスト 2 が、IP アドレス 10.0.0.2 および MAC アドレス 0001.0001.0001 を持つ ARP 要求を送信すると、このパケットは転送され、統計情報が更新されます。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

ホスト 2 が IP アドレス 10.0.0.1 を持つ ARP 要求を送信しようとすると、この要求はドロップされ、システム メッセージがログに記録されます。

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Ethernet1/4, vlan
1.([0001.0001.0001/10.0.0.1/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri Jun 13 2008])
```

この場合に表示される統計情報は次のようになります。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 1
ARP Res Dropped    = 0
DHCP Drops         = 1
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

第 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、次の内容で構成されています。

- ユニキャスト RPF の概要，159 ページ
- ユニキャスト RPF のライセンス要件，161 ページ
- ユニキャスト RPF の注意事項と制約事項，162 ページ
- ユニキャスト RPF のデフォルト設定，163 ページ
- ユニキャスト RPF の設定，163 ページ
- ユニキャスト RPF の設定例，165 ページ
- ユニキャスト RPF の設定の確認，165 ページ

ユニキャスト RPF の概要

ユニキャスト RPF 機能では、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ことによって緩和します。 たとえば、Smurf や Tribal Flood Network（TFN）など、いくつかの一般的な Denial of Service（DoS; サービス拒絶）攻撃は、偽造の送信元 IPv4 または IPv6 アドレスやすぐに変更される送信元 IPv4 または IPv6 アドレスを利用して、攻撃を突き止めたりフィルタリングしたりする手段を妨ぐことができます。 ユニキャスト RPF では、送信元アドレスが有効で IP ルーティング テーブルと一致するパケットだけを転送することにより、攻撃を回避します。

インターフェイス上でユニキャスト RPF をイネーブルにすると、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、かつパケットが受信された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 Forwarding Information Base（FIB; 転送情報ベース）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 パスで着信す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。

ユニキャスト RPF プロセス

ユニキャスト RPF には、キーの実装原則がいくつかあります。

- パケットは、パケットの送信元に対する最適なリターンパス（ルート）があるインターフェイスで受信する必要があります（このプロセスは対称ルーティングと呼ばれます）。 FIB に受信インターフェイスへのルートと一致するルートが存在する必要があります。 スタティック ルート、ネットワーク文、ダイナミック ルーティングによって FIB にルートが追加されます。
- 受信側インターフェイスでの IP 送信元アドレスは、そのインターフェイスのルーティング エントリと一致する必要があります。
- ユニキャスト RPF は入力機能であり、接続のアップストリーム エンドのデバイスの入力インターフェイスだけに適用されます。

ダウンストリーム ネットワークにインターネットへの他の接続があっても、ダウンストリーム ネットワークにユニキャスト RPF を使用できます。

注意 攻撃者が送信元アドレスへの最良パスを変更する可能性があるので、加重やローカルプリファレンスなどのオプションのBGP属性を使用する際には、十分に注意してください。 変更によって、ユニキャスト RPF の操作に影響が出ます。

ユニキャスト RPF と ACL を設定したインターフェイスでパケットが受信されると、Cisco NX-OS ソフトウェアは次の動作を行います。

手順の概要

1. インバウンド インターフェイスで入力 ACL をチェックします。
2. ユニキャストRPFを使用し、FIBテーブル内のリバースルックアップを実行することにより、そのパケットが送信元への最良リターン パスで着信したことを確認します。
3. パケットの転送を目的として FIB ルックアップを実行します。
4. アウトバウンド インターフェイスで出力 ACL をチェックします。
5. パケットを転送します。

手順の詳細

ステップ 1 インバウンド インターフェイスで入力 ACL をチェックします。

ステップ 2 ユニキャストRPFを使用し、FIBテーブル内のリバースルックアップを実行することにより、そのパケットが送信元への最良リターン パスで着信したことを確認します。

ステップ 3 パケットの転送を目的として FIB ルックアップを実行します。

ステップ 4 アウトバウンド インターフェイスで出力 ACL をチェックします。

ステップ 5 パケットを転送します。

グローバル統計情報

Cisco NX-OS デバイスがユニキャスト RPF チェックの失敗によりインターフェイスでパケットをドロップするたびに、その情報がForwarding Engine（FE;転送エンジン）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 のライセンス方式に関する詳細は、*Cisco NX-OS* ライセンス ガイド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。

- 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、攻撃の範囲を限定し、攻撃の送信元をトレースできますが、多くのサイトにユニキャストRPFを配布するため、ネットワーク運用の管理コストが増大します。
- 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。
- 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、Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）と Dynamic Host Configuration Protocol（DHCP）を正しく動作させることができます。

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

ユニキャスト RPF のデフォルト設定

次の表に、ユニキャスト RPF パラメータのデフォルト設定を示します。

表 *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
ユニキャスト RPF	ディセーブル

ユニキャスト RPF の設定

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

ストリクト ユニキャスト RPF モード

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

ルーズ ユニキャスト RPF モード

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

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **ip verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
4. **ipv6 verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
5. **exit**
6. （任意） **show ip interface ethernet** *slot*/*port*
7. （任意） **show running-config interface ethernet** *slot*/*port*
8. （任意） **copy running-config startup-config**

手順の詳細

	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** キーワードは緩和モードのユニキャスト RPF を指定します。 **allow-default** キーワードを指定すると、送信元アドレスのルックアップでデフォルト ルートと一致させることが可能であり、これを検証に使用できます。 **rx** キーワードは厳格モードのユニキャスト RPF を指定します。

ステップ 4	**ipv6 verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
	
	例：
	`Example:`
	`switch(config-if)# ipv6 verify unicast source reachable-via any`
		IPv6 用インターフェイスにユニキャスト RPF を設定します。
		any キーワードは緩和モードのユニキャスト RPF を指定します。
		allow-default キーワードを指定すると、送信元アドレスのルックアップでデフォルト ルートと一致させることが可能であり、これを検証に使用できます。
		rx キーワードは厳格モードのユニキャスト RPF を指定します。

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

ステップ 6	**show ip interface 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。

	コマンドまたはアクション	目的
ステップ 7	**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 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ユニキャスト RPF の設定例

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

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

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

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

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

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

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

```
interface Ethernet2/4
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via rx
```

ユニキャスト RPF の設定の確認

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

コマンド	目的
show running-config interface 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

この章では、Cisco NX-OS デバイスでコントロール プレーン ポリシング（CoPP）を設定する手順を説明します。

この章は、次の内容で構成されています。

- CoPP の概要，168 ページ
- コントロール プレーンの保護，169 ページ
- CoPP ポリシー テンプレート，171 ページ
- CoPP のクラス マップ，174 ページ
- 1 秒間あたりのパケットのクレジット制限，175 ページ
- CoPP と管理インターフェイス，175 ページ
- CoPP のライセンス要件，175 ページ
- CoPP の注意事項と制約事項，175 ページ
- CoPP のアップグレードの注意事項，176 ページ
- CoPP の設定，176 ページ
- CoPP show コマンド，181 ページ
- CoPP 設定ステータスの表示，182 ページ
- CoPP のモニタ，182 ページ
- CoPP 統計情報のクリア，183 ページ
- CoPP の設定例，184 ページ
- CoPP の設定例，185 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，188 ページ
- CoPP に関する追加情報，189 ページ

• CoPP の機能の履歴，189 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。

コントロール プレーン

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

管理プレーン

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

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

プレーンは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

DoS 攻撃の例は次のとおりです。

- インターネット制御メッセージ プロトコル（ICMP）エコー要求
- IP フラグメント
- TCP SYN フラッディング

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

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

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

コントロール プレーンの保護

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

コントロール プレーンのパケット タイプ

コントロール プレーンには、次のような異なるタイプのパケットが到達します。

受信パケット

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

例外パケット

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

リダイレクト パケット

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

収集パケット

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

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

CoPP の分類

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

次のパラメータは、パケットの分類に使用できます。

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

- Default：スイッチド トラフィックとルーテッド トラフィック間の、CPU にバインドされているポリシングの適切なバランスを提供するレイヤ 2 およびレイヤ 3 のポリシー。
- Layer 2：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るレイヤ 2 ポリシー
- Layer 3：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るレイヤ 3 ポリシー

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。 デフォルト ポリシーから開始して、必要に応じて後で 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 Access Control List（ACL; アクセス コントロール リスト）を追加する必要があります。

setup コマンドを使用して設定ユーティリティを再入力することで、default、Layer 2 および Layer 3 のテンプレートを切り替えることができます。

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、またはこれに関連付けられたクラス マップを変更することはできません。 また、このポリシーのクラス マップ設定も変更できません。

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy
  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 300
```

レイヤ 2 CoPP ポリシー

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy
  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 1200
  class copp-s-v6routingProto2
    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-bfd
    police pps 350
  class copp-s-bpdu
    police pps 12300
  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
```

レイヤ 3 CoPP ポリシー

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy
  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 4000
class copp-s-v6routingProto2
  police pps 1600
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-bfd
  police pps 350
class copp-s-bpdu
  police pps 6000
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
```

CoPP のクラス 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。 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。

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。
- CoPP のカスタマイズは継続的なプロセスです。 CoPP は、特定の環境で使用されているプロトコルや機能のほか、サーバ環境に必要なスーパーバイザ機能に従って設定する必要があります。 これらのプロトコルや機能が変更されたら、CoPP を変更する必要があります。

- CoPP を継続的にモニタすることを推奨します。 ドロップが発生した場合は、CoPP がトラフィックを誤ってドロップしたのか、または誤動作や攻撃に応答してドロップしたのかを判定してください。 いずれの場合も、状況を分析して、別の CoPP ポリシーを使用するか、またはカスタマイズされた CoPP ポリシーを変更する必要があるかどうかを評価します。
- 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。
- IPv6 と IPv4 の CoPP ACL エントリには、別々の TCAM リージョンを使用します。 IPv6 CoPP が動作するには、IPv6 ACL SUP TCAM リージョン（ipv6-sup）がゼロ以外のサイズに切り分けられている必要があります。 詳細については、ACL TCAM リージョン, （96 ページ）およびACL TCAM リージョン サイズの設定, （113 ページ）のトピックを参照してください。

CoPP のアップグレードの注意事項

CoPP 機能をサポートする Cisco NX-OS リリースに CoPP 機能をサポートしないリリースからアップグレードする場合は、アップグレード後にデバイスの CoPP をイネーブル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。 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がある 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。

たとえば、Cisco NX-OX Release 5.0(3)U2(2)（CoPP 機能をサポートする）から Cisco NX-OS Release 5.0(3)U3(1)（IPv6 サポートの CoPP クラスを追加する）にアップグレードする場合、デバイス上の IPv6 CoPP 機能をイネーブルにするためにセットアップ スクリプトを実行する必要があります。

セットアップ スクリプトが 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。

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 キーワードの permit および deny は、照合時には無視されます。

IPv4 または IPv6 パケットのポリシーを設定できます。

はじめる前に

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

手順の概要

1. **configure terminal**
2. **class-map type control-plane match-any** *class-map-name*
3. （任意） **match access-group name** *access-list-name*
4. **exit**
5. （任意） **show class-map type control-plane** [*class-map-name*]
6. （任意） **copy running-config startup-config**

手順の詳細

	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。 （注） ACL キーワードの **permit** および **deny** は、CoPP 照合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。

	コマンドまたはアクション	目的
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 または IPv6 パケットのポリシーを設定できます。

はじめる前に

コントロール プレーン クラス マップが設定してあることを確認します。

手順の概要

1. **configure terminal**
2. **policy-map type control-plane** *policy-map-name*
3. **class** {*class-map-name* [**insert-before** *class-map-name2*] | **class**}
4. **police** [**pps**] {*pps-value*}
5. **exit**
6. **exit**
7. （任意） **show policy-map type control-plane** [**expand**] [**name** *class-map-name*]
8. （任意） **copy running-config startup-config**

手順の詳細

	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	**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 マップ名は最大 64 文字で、大文字と小文字は区別されます。

	コマンドまたはアクション	目的

ステップ 3	**class** {*class-map-name* [**insert-before** *class-map-name2*] | **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*} 例： `switch(config-pmap-c)# police pps 100`	パケット/秒（PPS）の観点から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。

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。

手順の概要

1. **configure terminal**
2. **control-plane**
3. [**no**] **service-policy input** *policy-map-name*
4. **exit**
5. （任意） **show running-config copp** [**all**]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

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

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

ステップ 3	[**no**] **service-policy input** *policy-map-name* 例： `switch(config-cp)# service-policy input copp-system-policy`	入トラフィックのポリシー マップを指定します。

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

ステップ 5	**show running-config copp** [**all**] 例： `switch(config)# show running-config copp`	（任意） CoPP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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 ipv6 access-lists	CoPP IPv6 ACL を含め、デバイス上で設定されているすべての IPv6 ACL を表示します。
show arp access-lists	CoPP ARP ACL を含め、デバイス上で設定されているすべての ARP ACL を表示します。
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	コントロール プレーン ポリシー マップと関連するクラス マップおよびPPSの値を表示します。
show running-config copp [**all**]	実行コンフィギュレーション内の CoPP 設定を表示します。
show running-config aclmgr [**all**]	実行コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。 **all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show startup-config copp [**all**]	スタートアップ コンフィギュレーション内の CoPP 設定を表示します。

コマンド	目的
show startup-config aclmgr [**all**]	スタートアップ コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。 **all** オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

CoPP 設定ステータスの表示

手順の概要

1. switch# **show copp status**

手順の詳細

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

次に、CoPP 設定ステータスを表示する例を示します。

```
switch# show copp status
```

CoPP のモニタ

手順の概要

1. switch# **show policy-map interface control-plane**

手順の詳細

	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。

	コマンドまたはアクション	目的
		統計情報は、OutPackets（コントロールプレーンに対して許可されたパケット）と DropPackets（レート制限によってドロップされたパケット）に関して指定します。

次に、CoPP をモニタする例を示します。

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

service-policy input: copp-system-policy-default

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

CoPP 統計情報のクリア

手順の概要

1. （任意） switch#**show policy-map interface control-plane**
2. switch# **clear copp statistics**

手順の詳細

	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
```

関連する IP ACL を使用したサンプル CoPP クラスの作成

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

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

次に、CoPP ポリシーにクラスを追加する例を示します。

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

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

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

ダイナミック クラス（IPv6 ACL）の作成

次に、IPv6 ACL を作成する例を示します

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

次に、CoPP の既存または新規クラスと ACL を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
```

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 で使用できるようにする前に、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、およびプライオリティをこれらのいずれかに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]

IPv6 access list copp-system-acl-dhcpc6
        10 permit udp any any eq 546
IPv6 access list copp-system-acl-dhcps6
        10 permit udp any ff02::1:2/128 eq 547
        20 permit udp any ff05::1:3/128 eq 547
IPv6 access list copp-system-acl-eigrp6
        10 permit 88 any ff02::a/128
IPv6 access list copp-system-acl-v6routingProto2
        10 permit udp any ff02::66/128 eq 2029
        20 permit udp any ff02::fb/128 eq 5353
IPv6 access list copp-system-acl-v6routingproto1
        10 permit 89 any ff02::5/128
        20 permit 89 any ff02::6/128
        30 permit udp any ff02::9/128 eq 521

class-map type control-plane match-any copp-icmp
  match access-group name copp-system-acl-icmp
class-map type control-plane match-any copp-ntp
  match access-group name copp-system-acl-ntp
class-map type control-plane match-any copp-s-arp
class-map type control-plane match-any copp-s-bfd
class-map type control-plane match-any copp-s-bpdu
class-map type control-plane match-any copp-s-dai
class-map type control-plane match-any copp-s-default
class-map type control-plane match-any copp-s-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%
```

CoPP に関する追加情報

ここでは、CoPP の実装に関する追加情報について説明します。

関連資料

関連項目	参照先
ライセンス	*Cisco NX-OS* ライセンス ガイド
コマンド リファレンス	『*Cisco Nexus 3000 Series Command Reference*』

CoPP の機能の履歴

表 ***16*** : ***CoPP*** の機能の履歴

機能名	機能情報
CoPP	5.0(3)U2(1) で導入
IPv6	5.0(3)U3(1) で導入
複数の ACL を IPv4 および IPv6 アクセス リストを含む CoPP クラスに関連付けることができます。	5.0(3)U3(1) で導入

索 引

A

AAA 3, 7, 8, 10, 12, 18, 23, 24, 39
  MSCHAP 認証のイネーブル化 18
  RADIUS サーバの設定 39
  アカウンティング 7
  コンソール ログインの設定 12
  制約事項 12
  設定の確認 23
  設定例 23
  説明 3
  前提条件 12
  注意事項 12
  デフォルト設定 24
  認証 7
  ユーザ ログインのプロセス 10
  利点 8
AAA アカウンティング 19
  デフォルト方式の設定 19
AAA アカウンティング ログ 22
  クリア 22
  表示 22
AAA 許可 59
  TACACS+ サーバでの設定 59
AAA サーバ 19, 22
  SNMPv3 パラメータの指定 19, 22
  VSA のユーザ ロールの指定 19
  ユーザ ロールの指定 22
AAA サーバ グループ 9
  説明 9
AAA サービス 8, 9
  設定オプション 9
  リモート 8
AAA プロトコル 7
  RADIUS 7
  TACACS+ 7
AAA ログイン 15
  認証失敗メッセージのイネーブル化 15
ACL 98
  制限事項 98
ACL 92, 93, 94, 98, 109
  VLAN 109
  アプリケーション 92
  シーケンス番号 94
  処理順序 93
  前提条件 98
  タイプ 92
  注意事項 98
  プロトコルによるトラフィックの識別 93
  ライセンス 98
ACL TCAM リージョン 113, 116
  設定 113
  デフォルト サイズに戻す 116

B

BGP 160
  ユニキャスト RPF との使用 160

C

cisco-av-pair 19, 22
  AAA ユーザ パラメータの指定 19, 22
CoPP 168, 169, 170, 171, 174, 175, 176, 178, 179, 181, 182, 183, 184
  アップグレードに関する注意事項 176
  管理インターフェイスの制約事項 175
  クラス マップ 174
  クラス マップの設定 176
  コントロール プレーン サービス ポリシー、設定 179
  コントロール プレーンの保護 169
  コントロール プレーン保護、分類 170
  制限事項 175

CoPP *(続き)*
設定ステータス **182**
設定の確認 **181**
設定例 **184**
注意事項 **175**
デフォルト ポリシー **171**
統計情報のクリア **183**
に関する情報 **168**
ポリシー テンプレート **171**
ポリシー マップの設定 **178**
モニタリング **182**
ライセンス **175**
CoPP ポリシー **172**
レイヤ 2 **172**
CoPP ポリシー マップ **178**
設定 **178**

D

DAI **144, 145**
制約事項 **144**
注意事項 **144**
デフォルト設定 **145**
DHCP スヌーピング **121, 123, 125, 126**
概要 **121**
制約事項 **125**
説明 **121**
注意事項 **125**
デフォルト設定 **126**
バインディング データベース **123**
DHCP スヌーピング バインディング データベース **123**
関連項目：DHCP スヌーピング バインディング データベース
エントリ **123**
説明 **123**
関連項目：DHCP スヌーピング バインディング データベース
DHCP バインディング データベース。参照先： DHCP スヌーピング バインディング データベース
DHCP リレー エージェント **124, 133, 134**
VRF サポートのイネーブル化またはディセーブル化 **134**
VRF のサポート **124**
イネーブル化またはディセーブル化 **133**
DHCP リレー バインディング データベース **125**
説明 **125**
DoS 攻撃 **162**
ユニキャスト RPF、配置 **162**
Dynamic Host Configuration Protocol スヌーピング。参照先： DHCP スヌーピング

I

ID **21, 27**
シスコのベンダー ID **21, 27**
IP ACL 統計情報 **108**
クリア **108**
モニタリング **108**
IP ACL **5, 92, 95, 102, 103, 105, 106**
Logical Operation Unit：論理演算ユニット **95**
アプリケーション **92**
削除 **102**
シーケンス番号の変更 **103**
説明 **5**
タイプ **92**
ポート ACL として適用 **105**
ルータ ACL として適用 **106**
論理演算子 **95**

L

Logical Operation Unit：論理演算ユニット **95**
IP ACL **95**
LOU。参照先： Logical Operation Unit：論理演算ユニット

M

MSCHAP **18**
認証のイネーブル化 **18**

R

RADIUS **4, 25, 26, 27, 28, 36, 44, 45**
サーバの設定 **28**
設定例 **45**
説明 **4**
前提条件 **28**
操作 **26**
送信リトライ回数の設定 **36**
タイムアウト間隔の設定 **36**
デフォルト設定 **45**
統計情報、表示 **44**
ネットワーク環境 **25**

RADIUS *(続き)*
モニタリング 27
RADIUS サーバ 35, 37, 39, 42, 43, 45
AAA の設定 39
削除、ホストの 42
手動モニタリング 43
設定例 45
送信リトライ回数の設定 37
タイムアウト間隔の設定 37
統計情報の表示 43
ログイン時にユーザによる指定を許可 35
RADIUS サーバ グループ 34
グローバル発信元インターフェイス 34
RADIUS サーバの事前共有キー 32
RADIUS、サーバの定期的なモニタリング 40
RADIUS、サーバ ホスト 29
設定 29
RADIUS 統計情報 44
クリア 44
RADIUS のグローバルな事前共有キー 30

S

SNMPv3 19, 22
AAA サーバのパラメータの指定 22
AAA パラメータの指定 19
SSH 5
説明 5

T

TACACS+ 4, 47, 48, 49, 50, 51, 63, 67, 74, 75
RADIUS の利点 47
グローバルな事前共有キー 49
グローバルなタイムアウト間隔の設定 67
コマンド許可の検証 63
事前共有キー 49
制約事項 50
設定 51
設定の確認 74
設定例 75
説明 4, 47
前提条件 50
統計情報の表示 74
フィールドの説明 75
ユーザ ログインにおける動作 48
TACACS+ 許可の特権レベル サポート 64
設定 64
TACACS+ コマンドの許可 60, 62
設定 60
テスト 62
TACACS+ サーバ 51, 68, 69, 73, 74, 75
TCP ポートの設定 69
手動モニタリング 73
設定の確認 74
タイムアウト間隔の設定 68
統計情報の表示 74
フィールドの説明 75
ホストの設定 51
TACACS+ サーバ グループ 57
グローバル発信元インターフェイス 57
TCAM 113, 116
設定 113
デフォルト サイズに戻す 116
TCP ポート 69
TACACS+ サーバ 69
Telnet 5
説明 5

V

VLAN ACL 109
に関する情報 109
VSA 21
形式 21
サポートの説明 21
プロトコルのオプション 21

あ

アカウンティング 7
説明 7
アップグレード 176
CoPP の注意事項 176

か

管理インターフェイス 175
CoPP の制約事項 175

き

機能履歴 189
CoPP 189
許可 10, 63
コマンドの検証 63
ユーザ ログイン 10

く

クラス マップ 174, 176
CoPP 174
CoPP の設定 176

け

権限ロール 66
許可または拒否のコマンド 66

こ

コマンド 63
許可検証のイネーブル化 63
許可検証のディセーブル化 63
コントロール プレーン クラス マップ 181
設定の確認 181
コントロール プレーン サービス ポリシー、設定 179
CoPP 179
コントロール プレーンの保護 169
CoPP 169
パケット タイプ 169
コントロール プレーン保護、CoPP 171
レート制御メカニズム 171
コントロール プレーン保護、分類 170
コントロール プレーン ポリシー マップ 181
設定の確認 181

さ

サーバ 35
RADIUS 35
サーバ グループ 9
サービス拒絶攻撃 162
IP アドレス スプーフィング、軽減 162

し

シスコ 21, 27
ベンダー ID 21, 27
事前共有キー 49
TACACS+ 49
新機能に関する情報 1
説明 1

せ

制限事項 98, 175
ACL 98
CoPP 175
制約事項 125, 144
DAI 144
DHCP スヌーピング 125
設定ステータス 182
CoPP 182
設定例 184, 185
CoPP 184

た

ダイナミック ARP インスペクション 139, 140, 141, 143
ARP キャッシュ ポイズニング 140
ARP スプーフィング攻撃 140
ARP 要求 139
DHCP スヌーピング バインディング データベース 141
インターフェイスの信頼状態 141
機能 141
ドロップされたパケットのロギング 143
ネットワーク セキュリティの問題とインターフェイスの信頼状態 141

ち

注意事項 98, 125, 144, 175
ACL 98
CoPP 175
DAI 144
DHCP スヌーピング 125

て

デフォルト CoPP ポリシー 171
デフォルト設定 24, 145
　AAA 24
　DAI 145

と

統計情報 74, 108
　TACACS+ 74
　クリア 108
　モニタリング 108
統計情報のクリア 183
　CoPP 183

に

認証 7, 9, 10
　説明 7
　方式 9
　ユーザ ログイン 10
　リモート 7
　ローカル 7

は

発信元インターフェイス 34, 57
　RADIUS サーバ グループ 34
　TACACS+ サーバ グループ 57

へ

変更された機能に関する情報 1
　説明 1
ベンダー固有属性 21

ほ

ポート ACL 105
ポリシー テンプレート 171
　説明 171

も

モニタリング 27, 40, 182
　CoPP 182
　RADIUS 27
　RADIUS サーバ 40

ゆ

ユーザ ロール 19, 22
　AAA サーバでの指定 19, 22
ユーザ ログイン 10
　許可プロセス 10
　認証プロセス 10
ユニキャスト RPF 159, 160, 161, 162, 163, 165
　BGP 属性 160
　BOOTP 162
　DHCP 162
　FIB 159
　実装 160
　ストリクト モード 163
　制限事項 162
　設定の確認 165
　設定例 165
　説明 159
　注意事項 162
　デフォルト設定 163
　統計情報 161
　トンネリング 162
　配置 162
　ライセンス 161
　ルーズ モード 163

ら

ライセンス 98, 161, 175
　ACL 98
　CoPP 175
　ユニキャスト RPF 161

る

ルータ ACL 106

れ

例 24
AAA の設定 24
レイヤ 2 172
CoPP ポリシー 172
レート制御メカニズム 171
コントロール プレーン保護、CoPP 171

ろ

ログイン 35
RADIUS サーバ 35
論理演算子 95
IP ACL 95