Cisco Nexus 3550-T Configuration Guide, Release 10.1(x)

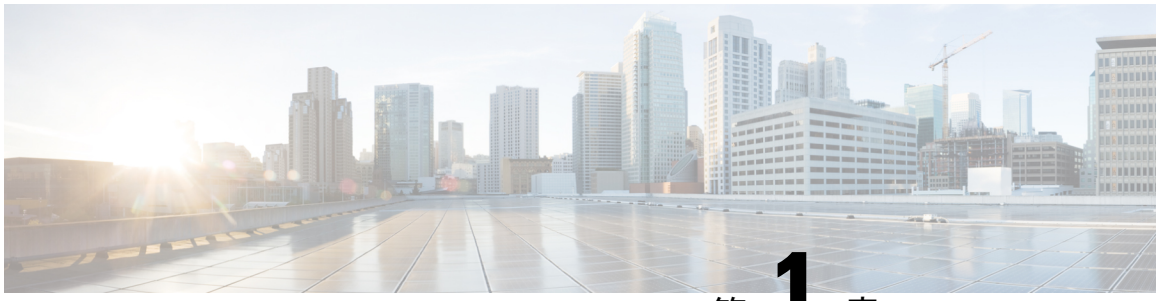
初版：2021 年 12 月 17 日

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/

目 次

第 I 部

Cisco Nexus 3550-T 構成ガイドの概要



第 1 章

序文

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

この前書きは、次の項で構成されています。

Full Cisco Trademarks with Software License

対象読者

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

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を指定する引数です。

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

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の `screen` フォント	ユーザが入力しなければならない情報は、太字の 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。

Cisco Nexus® 3550-T スイッチの関連資料

Cisco Nexus® 3550-T シリーズ スイッチ全体のマニュアル セットは、次の URL にあります。

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

マニュアルに関するフィードバック

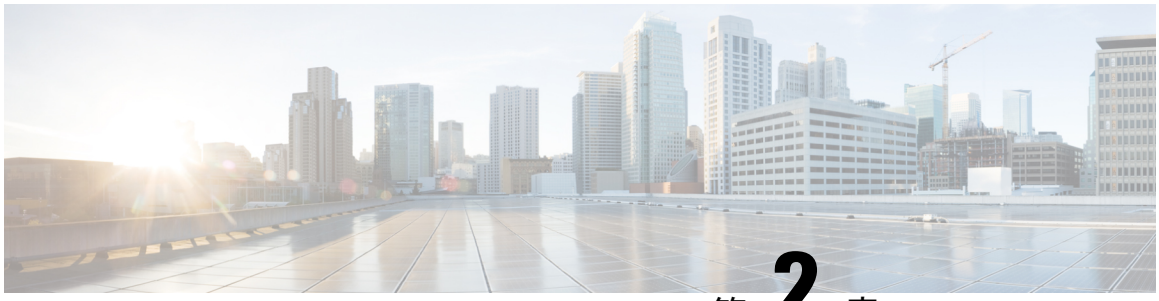
このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、nexus3550t-docfeedback@cisco.com にコメントをお送りください。ご協力をよろしくお願いいたします。

通信、サービス、およびその他の情報

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

Cisco バグ検索ツール

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



第 2 章

コンフィギュレーションの概要

Cisco Nexus® 3550-T スイッチの概要

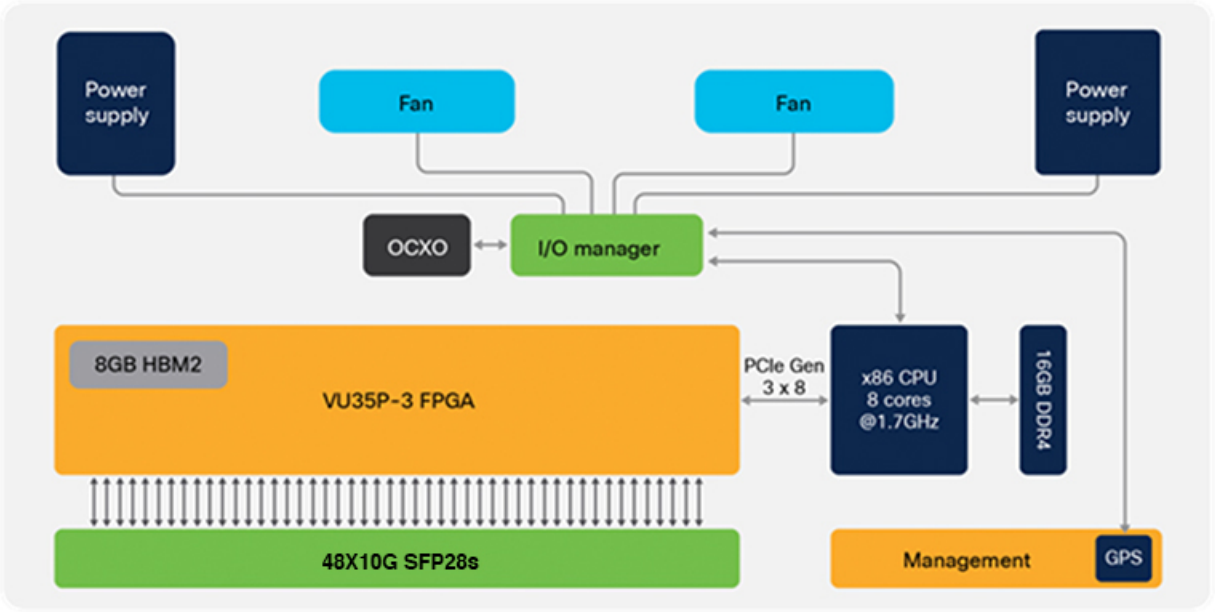
CiscoNexus® 3550-T プログラマブル ネットワーク プラットフォームは、独自の低遅延設計を備えた top-of-rack ソフトウェア アプリケーション プラットフォームです。

柔軟で低遅延のアプリケーション プラットフォーム

Cisco Nexus® 3550-T プラットフォームは、シングルラックユ ニットのフォーム ファクタで 10G イーサネット接続ポートを最大 48 個搭載できます。このプラットフォームは、強力なプログラマブル FPGA を中心に構築されており、カスタム アプリケーションおよび使用例に対応する完全なファームウェア開発環境を提供します。

Cisco Nexus® 3550-T プラットフォームのブロック図を以下に示します。

図 *1 :* データシート *Cisco Public*



Cisco Nexus® 3550-T プログラマブル ネットワーク プラットフォーム

利点

- Cisco Nexus® 3550-T の次世代超低遅延ネットワーク スイッチ プラットフォームは、データセンター ネットワーキング、高周波取引（HFT）、金融サービス、およびサービス プロバイダ ネットワークにおける遅延の影響を受けやすいアプリケーションのニーズに対応するように特別に設計されています。
- Cisco Nexus® 3550-T プラットフォームおよびスイッチ超低遅延スイッチ プラットフォーム、FPGA アプリケーションプログラミング、多重化および高精度のタイムスタンプにより、ミッション クリティカルなネットワーク アプリケーションを容易にします。

ULL ネットワーク ソリューションの価値を最大限に引き出します

Cisco Nexus® 3550-T の次世代の超低遅延ネットワーク スイッチ プラットフォームは、データセンター ネットワーキングおよびサービス プロバイダー ネットワークにおける遅延の影響を受けやすいアプリケーションのニーズに対応するように特別に設計されています。

Cisco Nexus 3550-T シリーズプラットフォームおよびスイッチ超低遅延スイッチプラットフォーム、FPGA アプリケーション プログラミング、多重化および正確なタイムスタンプにより、ミッション クリティカルなネットワーク アプリケーションを容易にします。

シスコの環境維持への取り組み

シスコの企業の社会的責任（CSR）レポートの「環境の持続性」セクションでは、製品、ソリューション、運用・拡張運用、サプライチェーンに対する、シスコの環境持続性ポリシーとイニシアチブを掲載しています。

次の表に、環境の持続可能性に関する主要なトピック（CSR レポートの「環境の持続性」セクションに記載）への参照リンクを示します。

持続性に関するトピック	参照先
製品の材料に関する法律および規制に関する情報	材料
製品、バッテリ、パッケージを含む電子廃棄物法規制に関する情報	WEEE 適合性

シスコでは、パッケージデータを情報共有目的でのみ提供しています。これらの情報は最新の法規制を反映していない可能性があります。シスコは、情報が完全、正確、または最新のものであることを表明、保証、または確約しません。これらの情報は予告なしに変更されることがあります。

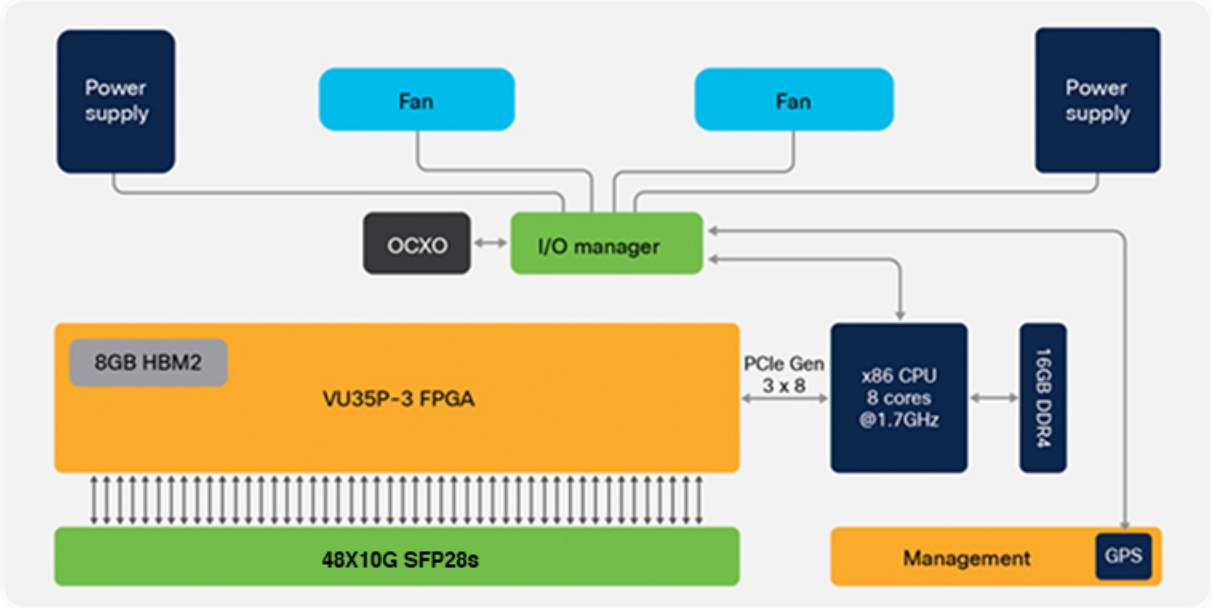
目的達成に役立つ柔軟な支払いソリューション

Cisco Capital® により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。シスコの柔軟な支払いソリューションは 100 ヵ国以上で利用可能であり、ハードウェア、ソフトウェア、サービス、およびサードパーティ製の補完的な機器を、利用しやすい計画的な支払い方法で購入できます。詳細はこちらをご覧ください。

Cisco Nexus® 3550-T スイッチのハードウェア アーキテクチャ

Cisco Nexus® 3550-T プログラマブル ネットワーク プラットフォームは、動的に再構成可能な FPGA（Field Programmable Gate Array）を中心に構築された固定フォーム ファクタを持ち、10G 対応で x86（Intel® Atom® プロセッサ、8 コア、 最大 1.7 GHz）管理 CPU と連動する 48 個のポートを提供します。48 個のポートはすべて、「-3」スピードグレードの Xilinx Virtex UltraScale Plus VU35P FPGA に直接接続されています。FPGA には、8 GB の高帯域幅メモリ（HBM）が搭載されています。Cisco Nexus® 3550-T のハードウェア アーキテクチャを次の図 2 に示します。

図 *2 : Cisco Nexus 3550-T* プログラマブル ネットワーク プラットフォーム データ シート



Cisco Nexus® 3550-T プログラマブル ネットワーク プラットフォーム ハードウェア アーキテクチャ

容易な管理

Cisco Nexus® 3550-T プログラマブル ネットワーク プラットフォームは、コンソール ポート、マイクロ USB ポート、1 G RJ45 ポート、および 10G SFP+ ポートを備え、これらは管理インターフェイスとして使用できます。

Cisco Nexus® 3550-T プログラマブル ネットワーク プラットフォームには、標準のエンタープライズ管理機能と展開機能が含まれています。

プログラマビリティ

Cisco Nexus® 3550-T プログラマブル ネットワーク プラットフォームは、Cisco Nexus® 3550-T FPGA モジュールにアプリケーション固有のインテリジェンスを追加するための強力な開発フレームワークを提供します。ネットワーク

スイッチ プラットフォームの機能

Cisco Nexus® 3550-T プログラマブル ネットワーク プラットフォームは、パケット対応の統計情報をサポートしています。Cisco Nexus® 3550-Tファームウェアには、送受信されたパケット数/バイト数、送受信エラー数などの重要なパケット統計情報、および光レベル、動作温度、トランシーバ機能などの詳細な診断を監視する機能があります。

これらの統計情報はすべて、クリティカルパスで遅延なしに利用できます。使用可能な統計情報の一部を次に示します。

接続性

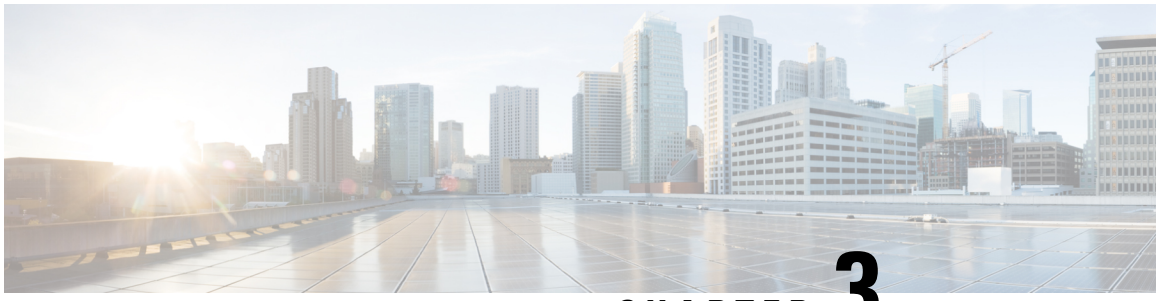
- 48 X SFP28（Small Form-Factor Pluggable）構成（SFP +およびSFPとの下位互換性）
- SFP+ 光ファイバ（10GBASE-SR、10GBASE-LR、10GBASE-LRM、1000BASE-SX、1000BASE-LX）
- SFP+ 銅線直接接続
- RJ45 管理ポート
- SMA for PPS in/out*（3.3 V、50 Ohm 信号インターフェイス）
- GPS* 入力用 SMA
- RJ45 管理ポート
- RJ45 業界標準シリアル ポート（デフォルト速度：115200 N81）
- USB（ファームウェア アップグレード用）

全般

- 19 インチ 1RU、ラック マウント
- 重量：10 kg（22ポンド）
- ホットスワップ可能なデュアル電源
- 標準：AC 90 ～ 264V、47 ～ 64 Hz（IEC C13-C14 ケーブル同梱）
- オプション：DC 40 ～ 72V
- 最大消費電力：150W
- ホットスワップ可能デュアル ファン モジュール
- オプションのエアーフロー方向
- 動作温度：-5 °C ～ 45°C
- 保管温度：-40 ～ 70 °C（-40 ～ 158 °F）
- 動作時相対湿度：5 ～ 90 %（結露しないこと）
- 保管相対湿度：5 ～ 95 %（結露しないこと）

第 II 部

Cisco Nexus 3550-T セキュリティの設定ガイド



CHAPTER 3

セキュリティの概要

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。

この章は、次の項で構成されています。

ライセンス要件

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

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

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

認証

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

許可

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

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

アカウンティング

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

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

詳細については、AAA の設定, on page 17の章を参照してください。

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 サーバーがネットワーク アクセス サーバーとして動作している場合は、ネットワーク アクセス サーバーと RADIUS セキュリティ サーバーとの間の通信を確立する手段に、AAA が使用されます。

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

RADIUS

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

TACACS+

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

詳細については、RADIUS の設定, on page 55の章を参照してください。

SSH および Telnet

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

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

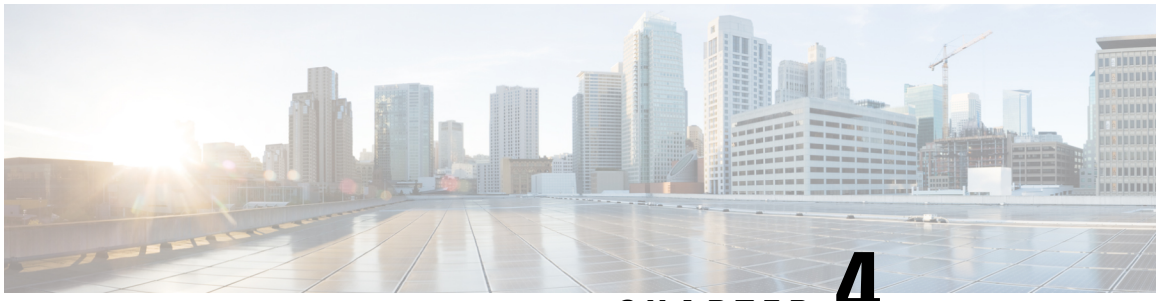
Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。Telnet を使用すると、あるサイトのユーザが別のサイトのログイン サーバと TCP 接続を確立し、キーストロークをデバイス間でやり取りできます。Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

詳細については、SSH および Telnet の設定, on page 105の章を参照してください。

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。

詳細については、IP ACL の設定, on page 85の章を参照してください。



CHAPTER 4

AAA の設定

この章では、Cisco NX-OS デバイスで認証、許可、アカウンティング（AAA）を設定する手順について説明します。

この章は、次の項で構成されています。

AAA について

ここでは、Cisco NX-OS デバイスの AAA について説明します。

AAA セキュリティ サービス

AAA 機能を使用すると、Cisco NX-OS デバイスを管理するユーザの ID を確認し、ユーザにアクセスを許可し、ユーザの実行するアクションを追跡できます。Cisco NX-OS デバイスは、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control System Plus（TACACS+）プロトコルをサポートします。

Cisco NX-OS は入力されたユーザ ID およびパスワードの組み合わせに基づいて、ローカルデータベースによるローカル認証または許可、あるいは 1 つまたは複数の AAA サーバによるリモート認証または許可を実行します。Cisco NX-OS デバイスと AAA サーバの間の通信は、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

ログインとパスワードのダイアログ、チャレンジとレスポンス、メッセージング サポート、および選択したセキュリティ プロトコルに応じた暗号化などを使用してユーザを識別します。

認証は、デバイスにアクセスする人物またはデバイスの ID を確認するプロセスです。この ID の確認は、Cisco NX-OS デバイスにアクセスするエンティティから提供されるユーザ ID とパスワードの組み合わせに基づいて行われます。Cisco NX-OS デバイスでは、ローカル認証（ローカル ルックアップ データベースを使用）またはリモート認証（1 台または複数の RADIUS サーバまたは TACACS+ サーバを使用）を実行できます。

許可

アクセス コントロールを提供します。AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てるプロセスです。Cisco NX-OS ソフトウェアでは、AAA サーバからダウンロードされる属性を使用して権限付与が行われます。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

情報を収集する、情報をローカルのログに記録する、情報を AAA サーバに送信して課金、監査、レポート作成などを行う方法を提供します。

アカウンティング機能では、Cisco NX-OS デバイスへのアクセスに使用されるすべての管理セッションを追跡し、ログに記録して管理します。この情報を使用して、トラブルシューティングや監査のためのレポートを生成できます。アカウンティング ログは、ローカルに保存することもできれば、リモート AAA サーバに送信することもできます。

Note Cisco NX-OS ソフトウェアでは、認証、許可、およびアカウンティングを個別にサポートしています。たとえば、アカウンティングは設定せずに、認証と許可を設定したりできます。

AAA を使用する利点

AAA は、次のような利点を提供します。

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

リモート AAA サービス

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

- ファブリック内の各 Cisco NX-OS デバイスのユーザ パスワード リストの管理が容易になります。
- 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 Cisco NX-OS デバイスのアカウンティング ログを中央で管理できます。
- ファブリック内の各 Cisco NX-OS デバイスについてユーザ属性を管理する方が、デバイスのローカル データベースを使用するより簡単です。

AAA サーバグループ

認証、許可、アカウンティングのためのリモート AAA サーバは、サーバ グループを使用して指定できます。サーバ グループとは、同じ AAA プロトコルを実装した一連のリモート AAA サーバです。サーバ グループの目的は、リモート AAA サーバが応答できなくなったときにフェールオーバー サーバを提供することです。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。Cisco NX-OS デバイスは、最初のグループ内のサーバからエラーを受け取った場合、次のサーバ グループ内のサーバで試行します。

AAA サービス設定オプション

Cisco NX-OS デバイスの AAA 設定は、サービス ベースです。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
- Network Admission Control（NAC）の Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）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ごとに CLI（コマンドライン インターフェイス）の関連コマンドを示します。

***Table 1: AAA* サービス コンフィギュレーション コマンド**

AAA サービス コンフィギュレーション オプション	関連コマンド
Telnet または SSH ログイン	**aaa authentication login default**
コンソール ログイン	**aaa authentication login console**
	aaa authentication eou default
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。

すべての RADIUS サーバ

RADIUS サーバのグローバル プールを使用して認証を行います。

指定サーバ グループ

設定した特定の RADIUS、TACACS+、または LDAP サーバ グループを使用して認証を行います。

ローカル

ローカルのユーザ名またはパスワード データベースを使用して認証を行います。

なし

AAA 認証が使用されないように指定します。

Note 「指定サーバ グループ」方式でなく、「すべての RADIUS サーバ」方式を指定した場合、Cisco NX-OS デバイスは、設定された RADIUS サーバのグローバル プールから設定の順に RADIUS サーバを選択します。このグローバル プールからのサーバは、Cisco NX-OS デバイス上の RADIUS サーバ グループ内で選択的に設定できるサーバです。

次の表に、AAA サービスに対応して設定できる AAA 認証方式を示します。

***Table 2: AAA* サービスの *AAA* 認証方式**

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

Note 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 アカウンティングについて、Cisco NX-OS デバイスは各オプションを指定された順序で試行します。その他の設定済みオプションが失敗した場合、ローカル オプションがデフォルト方式です。コンソールまたはデフォルトログインのローカルオプションを無効にするには、**no aaa authentication login** {**console** | **default**} **fallback error local** コマンドを使用します。

ユーザ ログインの認証および許可プロセス

次に、このプロセスについて順番に説明します。

- Cisco NX-OS デバイスへのログイン時に、Telnet、SSH、またはコンソール ログイン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 グループを設定している場合は、Cisco NX-OS デバイスが次のように、グループ内の最初の AAA サーバに認証要求を送信します。
  - 特定の AAA サーバが応答しなかった場合は、その次の AAA サーバ、さらにその次へと、各サーバが順に試行されます。この処理は、リモート サーバが認証要求に応答するまで続けられます。
  - 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。
  - コンソール ログインでローカルへのフォールバックがディセーブルでないかぎり、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 NX-OS デバイスがリモート AAA サーバ経由で正常に認証を実行した場合は、次の可能性があります。
  - 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 NX-OS デバイスにログインでき、ローカル データベース内で設定されているロールが割り当てられます。

Note 「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。

AES パスワード暗号化およびプライマリ暗号キー

強力で、反転可能な 128 ビットの高度暗号化規格（AES）パスワード暗号化（タイプ 6 暗号化ともいう）を有効にすることができます。タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能を有効にし、パスワード暗号化および復号化に使用されるプライマリ暗号キーを設定する必要があります。

AES パスワード暗号化をイネーブルにしてプライマリ キーを設定すると、タイプ 6 パスワード暗号化を無効にしない限り、サポートされているアプリケーション（現在は RADIUS と TACACS+）の既存および新規作成されたクリア テキスト パスワードがすべて、タイプ 6 暗号化の形式で保存されます。また、既存の弱いすべての暗号化パスワードをタイプ 6暗号化パスワードに変換するように Cisco NX-OS を設定することもできます。

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、TACACS+ サーバ、または LDAP サーバが IP を使用して到達可能であることを確認します。
- Cisco NX-OS デバイスが、AAA サーバのクライアントとして設定されていること。
- 秘密キーが、Cisco NX-OS デバイスおよびリモート AAA サーバに設定されていることを確認します。
- リモート サーバが Cisco NX-OS デバイスからの AAA 要求に応答することを確認します。

AAA の注意事項と制約事項

AAA に関する注意事項と制約事項は次のとおりです。

- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- Cisco Nexus® 3550-T スイッチは、TACACS +でのみ **aaa authentication login ascii-authentication** コマンドをサポートします（RADIUS ではサポートしません）。
- デフォルトのログイン認証方式を（**local** キーワードを使用せずに）変更すると、コンソール ログイン認証方式が設定によって上書きされます。コンソール認証方式を明示的に設定するには、**aaa authentication login console** {**group** *group-list* [**none**] | **local** | **none**} コマンドを使用します。
- **login block-for** および **login quiet-mode** コンフィギュレーション モード コマンドは、それぞれ **system login block-for** および **system login quiet-mode** に名前が変更されました。

- **system login quiet-mode access-class QUIET_LIST** コマンドを使用する場合は、指定したトラフィックのみをブロックするようにアクセスリストが正しく定義されていることを確認する必要があります。たとえば、信頼できないホストからのユーザログインのみをブロックする必要がある場合、アクセス リストは、それらのホストからのSSH、Telnet、およびHTTP ベースのアクセスに対応するポート22、23、80、および 443 を指定する必要があります。

AAA のデフォルト設定

次の表に、AAA パラメータのデフォルト設定を示します。

***Table 3: AAA* パラメータのデフォルト設定**

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

AAA の設定

ここでは、Cisco NX-OS デバイスで AAA 機能を設定する手順について説明します。

Note 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。

Note Cisco Nexus® 3550-T シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド aaa authentication login ascii-authentication をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、aaa authentication login ascii-authentication スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されます。

AAA の設定プロセス

AAA 認証およびアカウンティングを設定するには、次の作業を行います。

1. 認証にリモート RADIUS、TACACS+、または LDAP サーバを使用する場合は、Cisco NX-OS デバイス上でホストを設定します。
2. コンソール ログイン認証方式を設定します。
3. ユーザ ログインのためのデフォルトのログイン認証方式を設定します。
4. デフォルト AAA アカウンティングのデフォルト方式を設定します。

コンソール ログイン認証方式の設定

ここでは、コンソール ログインの認証方式を設定する方法を説明します。

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、TACACS+、または LDAP サーバの指定サブセット
- Cisco NX-OS デバイスのローカル データベース
- ユーザ名のみ（none）

デフォルトの方式はローカルですが、無効にするオプションがあります。

Note **aaa authentication** コマンドの **group radius** および **group***server-name* 形式は、以前に定義された RADIUS サーバのセットを参照します。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。

Note リモート認証がイネーブルになっているときにパスワード回復を実行すると、パスワード回復の実行後すぐにコンソール ログインのローカル認証がイネーブルになります。そのため、新しいパスワードを使用して、コンソール ポート経由で Cisco NX-OS デバイスにログインできます。ログイン後は、引き続きローカル認証を使用するか、または AAA サーバで設定された管理者パスワードのリセット後にリモート認証をイネーブルにすることができます。パスワード回復プロセスに関する詳細情報については、『*Cisco Nexus*® シリーズ *NX-OS* トラブルシューティング ガイド』を参照してください。

Before you begin

必要に応じて RADIUS、TACACS+、または LDAP サーバ グループを設定します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa authentication login console** {**group** *group-list* [**none**] | **local** | **none**} **Example:** `switch(config)# aaa authentication login console group radius`	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 プールを使用して認証を行います。 ***named-group*** RADIUS、TACACS+、またはLDAPサーバの指定サブセットを使用して認証を行います。 **local** 方式は、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。 デフォルトのコンソール ログイン方式は **local** です。これは、方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られない場合に、コンソール ログインに対してローカルへのフォール バックが無効でない限り、使用されます。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	コンソール ログイン認証方式の設定を表示します。

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

デフォルトの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、TACACS+、または LDAP サーバの指定サブセット
- Cisco NX-OS デバイスのローカル データベース
- ユーザ名だけ

デフォルトの方式はローカルですが、無効にするオプションがあります。

Before you begin

必要に応じて RADIUS、TACACS+、または LDAP サーバ グループを設定します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa authentication login default** {**group** *group-list* [**none**] | **local** | **none**} **Example:** `switch(config)# aaa authentication login default group radius`	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 プールを使用して認証を行います。 • *named-group*：認証に RADIUS、TACACS+ または LDAP サーバの名前付きサブセットを使用します。 **local** 方式は、ローカル データベースを認証に使用します。**none** 方式では、

	Command or Action	Purpose
		AAA 認証が使用されないように指定します。デフォルトのログイン方式は**local**です。これは、方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られない場合に、コンソール ログインに対してローカルへのフォール バックがディセーブルでない限り、使用されます。 次のいずれかを設定できます。 • AAA 認証グループ • 認証なしの AAA 認証グループ • ローカル認証 • 認証なし **Note** **local** キーワードは、AAA 認証グループを設定するときはサポートされません（必須ではありません）。これは、ローカル認証は、リモート サーバが到達不能の場合のデフォルトであるためです。たとえば、**aaa authentication login default group g1** を設定した場合、AAA グループ g1 を使用して認証を行うことができなければ、ローカル認証が試行されます。これに対し、**aaa authentication login default group g1 none** を設定した場合、AAA グループ g1 を使用して認証を行うことができなければ、認証は実行されません。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show aaa authentication** **Example:**	デフォルトのログイン認証方式の設定を表示します。

	Command or Action	Purpose
	`switch# show aaa authentication`	
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ローカル認証へのフォールバックの無効化

デフォルトでは、コンソール ログインまたはデフォルト ログインのリモート認証が設定されている場合、どの AAA サーバにも到達不能なときに（認証エラーになります）、ユーザが Cisco NX-OS デバイスからロックアウトされないように、ローカル認証にフォールバックされます。ただし、セキュリティを向上させるために、ローカル認証へのフォールバックを無効にできます。

⚠

Caution ローカル認証へのフォールバックを無効にすると、Cisco NX-OS デバイスがロックされ、パスワード回復を実行しないとアクセスできなくなることがあります。デバイスからロックアウトされないようにするために、ローカル認証へのフォールバックを無効にする対象は、デフォルト ログインとコンソール ログインの両方ではなく、いずれかだけにすることを推奨します。

Before you begin

コンソール ログインまたはデフォルト ログインのリモート認証を設定します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**no aaa authentication login** {**console** | **default**} **fallback error local** **Example:** `switch(config)# no aaa authentication login console fallback error local`	コンソール ログインまたはデフォルト ログインについて、リモート認証が設定されている場合にどの AAA サーバにも到達不能なときに実行されるローカル認証へのフォールバックを無効にします。 ローカル認証へのフォールバックを無効にすると、次のメッセージが表示されます。

	Command or Action	Purpose
		`"WARNING!!! Disabling fallback can lock your switch."`

ステップ 3	(Optional) **exit**
	Example:
	`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	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	コンソール ログインおよびデフォルト ログイン認証方式の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

AAA 認証のデフォルト ユーザ ロールのイネーブル化

ユーザ ロールを持たないリモート ユーザに、デフォルトのユーザ ロールを使用して、RADIUS または TACACS+ リモート認証による Cisco NX-OS デバイスへのログインを許可できます。AAA のデフォルトのユーザ ロール機能をディセーブルにすると、ユーザ ロールを持たないリモート ユーザはデバイスにログインできなくなります。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa user default-role** **Example:** `switch(config)# aaa user default-role`	AAA 認証のためのデフォルト ユーザ ロールをイネーブルにします。デフォルトではイネーブルになっています。 デフォルト ユーザ ロールの機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

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

	Command or Action	Purpose
ステップ 4	(Optional) **show aaa user default-role** **Example:** `switch# show aaa user default-role`	AAA デフォルト ユーザ ロールの設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ 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有効化

ログイン時にリモート AAA サーバが応答しない場合、そのログインは、ローカル ユーザ データベースにロール オーバーして処理されます。このような場合に、ログイン失敗メッセージが有効になっていると、次のメッセージがユーザの端末に表示されます。

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

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa authentication login error-enable** **Example:** `switch(config)# aaa authentication login error-enable`	ログイン認証失敗メッセージを有効にします。デフォルトではディセーブルになっています。

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

ステップ 4	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	ログイン失敗メッセージの設定を表示します。

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

成功したログイン試行と失敗したログイン試行

成功したログイン試行と失敗したログイン試行をすべて、設定されたsyslogサーバに記録するようにスイッチを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル設定モードを開始します。
ステップ 2	必須: [**no**] **login on-failure log** 例： `switch(config)# login on-failure log`	ロギング レベルが 6 に設定されている場合のみ、失敗した認証に関するすべてのメッセージを設定済みの syslog サーバに記録します。この設定では、ログイン失敗後に次のsyslogメッセージが表示されます。 AUTHPRIV-3-SYSTEM_MSG：pam_aaa：Authentication failed for user admin from 172.22.00.00 （注） ロギング レベル authpriv が 6 の場合、追加の Linux カーネル認証メッセージが以前のメッセージとともに表示されます。これらの追加のメッセージを無視する必要がある場合、authpriv 値を 3 に設定する必要があります。

ステップ 3	必須: [**no**] **login on-success log**
	例：
	`switch(config)# login on-success log`
	`switch(config)# logging level authpriv 6`
		ロギング レベルが 6 に設定されている場合のみ、成功した認証に関するすべてのメッセージを設定済みの syslog サーバに記録します。この設定では、ログインに成功すると次のsyslogメッセージが表示されます。

	コマンドまたはアクション	目的
	`switch(config)# logging level daemon 6`	AUTHPRIV-6-SYSTEM_MSG：pam_aaa：Authentication success for user admin from 172.22.00.00 （注） ロギング レベル authpriv が 6 の場合、追加の Linux カーネル認証メッセージが以前のメッセージとともに表示されます。これらの追加のメッセージを無視する必要がある場合、authpriv 値を 3 に設定する必要があります。
ステップ 4	（任意） **show login on-failure log** 例： `switch(config)# show login on-failure log`	失敗した認証メッセージをsyslogサーバに記録するようにスイッチが設定されているかどうかを表示します。
ステップ 5	（任意） **show login on-successful log** 例： `switch(config)# show login on-successful log`	成功した認証メッセージをsyslogサーバに記録するようにスイッチが設定されているかどうかを表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザごとのログイン ブロックの設定

スイッチがグローバル コンフィギュレーション モードになっていることを確認します。

ユーザごとのログイン ブロック機能を使用すると、Denial of Service（DoS）攻撃の疑いを検出して、辞書攻撃の影響を緩和することができます。この機能はローカルおよびリモート ユーザに適用されます。ログインに失敗したユーザをブロックするようにログイン パラメータを設定するには、ここに示す手順を実行します。

（注） リモート ユーザのログイン ブロックを構成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**aaa authentication rejected** *attempts* **in** *seconds* **ban** *seconds* 例： `switch(config)# aaa authentication rejected 3 in 20 ban 300`	ユーザをブロックするようにログイン パラメータを設定します。 （注） デフォルトのログイン パラメータに戻すには **no aaa authentication rejected** コマンドを使用します。
ステップ 3	**exit** 例： `switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 4	（任意） **show running config** 例： `switch# show running config`	ログイン パラメータを表示します。
ステップ 5	**show aaa local user blocked** 例： `switch# show aaa local user blocked`	ブロックされたローカル ユーザを表示します。
ステップ 6	**clear aaa local user blocked {username user| all}** 例： `switch(config)# switch# clear aaa local user blocked username testuser`	ブロックされたローカル ユーザをクリアします。 all：ブロックされたすべてのローカル ユーザをクリアします。
ステップ 7	**show aaa user blocked** 例： `switch(config)# show aaa user blocked`	ブロックされたすべてのローカル ユーザとリモート ユーザを表示します。
ステップ 8	（任意） **clear aaa user blocked{username user| all}** 例： `switch# clear aaa user blocked username testuser`	ブロックされたすべてのローカル ユーザとリモート ユーザをクリアします。 all：ブロックされたすべてのローカル ユーザとリモート ユーザをクリアします。

例

（注） network-admin だけが show および clear コマンドを実行できます。

次に、20 秒の間に 3 回のログイン試行が失敗した場合に、300 秒間ユーザをブロックするログイン パラメータを設定する例を示します。

```
switch(config)# aaa authentication rejected 3 in 20 ban 300
switch# show run | i rejected
aaa authentication rejected 3 in 20 ban 300
switch# show aaa local user blocked
Local-user                  State
testuser                    Watched (till 11:34:42 IST Nov 12 2020)
switch# clear aaa local user blocked username testuser
switch# show aaa user blocked
Local-user                  State
testuser                    Watched (till 11:34:42 IST Nov 12 2020)
switch# clear aaa user blocked username testuser
```

CHAP 認証の有効化

Cisco NX-OS ソフトウェアは、チャレンジ ハンドシェーク認証プロトコル（CHAP）をサポートしています。このプロトコルは、業界標準の Message Digest（MD5）ハッシュ方式を使用して応答を暗号化する、チャレンジ レスポンス認証方式のプロトコルです。リモート認証サーバ（RADIUS または TACACS+）を通じて、Cisco NX-OS スイッチへのユーザ ログインに CHAP を使用できます。

デフォルトでは、Cisco NX-OS デバイスは、Cisco NX-OS デバイスとリモート サーバの間でパスワード認証プロトコル（PAP）認証を使用します。CHAP が有効の場合は、CHAP ベンダー固有属性（VSA）を認識するように RADIUS サーバまたは TACACS+ サーバを設定する必要があります。

Note Cisco Nexus® 3550-T switches スイッチは、TACAAS+ に対してのみ CLI コマンド aaa authentication login ascii-authentication をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、aaa authentication login ascii-authentication スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されます。

次の表に、CHAP に必要な RADIUS および TACACS+ VSA を示します。

Table 4: CHAP RADIUS* および *TACACS+ VSA

ベンダー ID 番号	ベンダータイプ番号	VSA	説明
311	11	CHAP-Challenge	AAA サーバから CHAP 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	CHAP-Response	チャレンジに対する応答として CHAP ユーザが入力した値を保持します。Access-Request パケットだけで使用します。

Before you begin

ログイン用の AAA ASCII 認証を無効にします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**no aaa authentication login ascii-authentication** **Example:** `switch(config)# no aaa authentication login ascii-authentication`	ASCII 認証を無効にします。
ステップ 3	**aaa authentication login chap enable** **Example:** `switch(config)# aaa authentication login chap enable`	CHAP 認証を有効にします。デフォルトでは無効になっています。 **Note** Cisco NX-OS デバイスで、CHAP と MSCHAP（または MSCHAP V2）の両方を有効にすることはできません。

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

	Command or Action	Purpose
ステップ 5	(Optional) **show aaa authentication login chap** **Example:** `switch# show aaa authentication login chap`	CHAP の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MSCHAP または MSCHAP V2 認証の有効化

マイクロソフト チャレンジ ハンドシェーク認証プロトコル（MSCHAP）は、マイクロソフト版の CHAP です。Cisco NX-OS ソフトウェアは、MSCHAP Version 2（MSCHAP V2）にも対応しています。リモート認証サーバ（RADIUS または TACACS+）を通じて、Cisco NX-OS スイッチへのユーザ ログインに MSCHAP を使用できます。MSCHAP V2 では、リモート認証 RADIUS サーバを介した Cisco NX-OS デバイスへのユーザ ログインだけがサポートされます。MSCHAP V2 の場合に TACACS+ グループを設定すると、デフォルトの AAA ログイン認証では、次に設定されている方式が使用されます。他のサーバ グループが設定されていない場合は、ローカル方式が使用されます。

Note Cisco NX-OS ソフトウェアは、次のメッセージを表示する場合があります。

「Warning: MSCHAP V2 is supported only with Radius.」

この警告メッセージは単なる情報メッセージであり、RADIUS での MSCHAP V2 の動作には影響しません。

デフォルトでは、Cisco NX-OS デバイスは、Cisco NX-OS デバイスとリモート サーバの間でパスワード認証プロトコル（PAP）認証を使用します。MSCHAP または MSCHAP V2 を有効にする場合は、MSCHAP および MSCHAP V2 ベンダー固有属性（VSA）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。

Table 5: MSCHAP および MSCHAP V2 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 または MSCHAP V2 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 または MSCHAP V2 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。

Before you begin

ログイン用の AAA ASCII 認証を無効にします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**no aaa authentication login ascii-authentication** **Example:** `switch(config)# no aaa authentication login ascii-authentication`	ASCII 認証を無効にします。
ステップ 3	**aaa authentication login** {**mschap** | **mschapv2**} **enable** **Example:** `switch(config)# aaa authentication login mschap enable`	MSCHAP または MSCHAP V2 認証を有効にします。デフォルトでは無効になっています。 **Note** Cisco NX-OS デバイスで、MSCHAP と MSCHAP V2 の両方を有効にすることはできません。
ステップ 4	**exit** **Example:**	コンフィギュレーション モードを終了します。

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
ステップ 5	(Optional) **show aaa authentication login** {**mschap** | **mschapv2**} **Example:** `switch# show aaa authentication login mschap`	MSCHAP または MSCHAP V2 の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの AAA アカウンティング方式の設定

Cisco NX-OS ソフトウェアは、アカウンティングに TACACS+ 方式と RADIUS 方式をサポートします。Cisco NX-OS デバイスは、ユーザーのアクティビティを、アカウンティング レコードの形式で TACACS+ または RADIUS セキュリティ サーバーにレポートします。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 NX-OS デバイスは、これらの属性をアカウンティング レコードとして報告します。そのアカウンティング レコードは、セキュリティ サーバ上のアカウンティング ログに格納されます。

特定のアカウンティング方式を定義するデフォルト方式リストを作成できます。次の方式を含めることができます。

RADIUS サーバ グループ
RADIUS サーバのグローバル プールを使用してアカウンティングを行います。

指定されたサーバ グループ
指定された RADIUS または TACACS+ サーバ グループを使用してアカウンティングを行います。

ローカル
ローカルのユーザ名またはパスワードデータベースを使用してアカウンティングを行います。

Note 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。

Before you begin

必要に応じて RADIUS または TACACS+ サーバ グループを設定します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa accounting default** {**group** *group-list* | **local**} **Example:** `switch(config)# aaa accounting default group radius`	デフォルトのアカウンティング方式を設定します。 *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 プールを使用してアカウンティングを行います。 • *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** 方式はローカル データベースを使用してアカウンティングを行います。 デフォルトのアカウンティング方式は、**local** です。これはサーバ グループが何も設定されていない場合、または設定されたすべてのサーバ グループから応答が得られなかった場合に使用されます。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show aaa accounting** **Example:** `switch# show aaa accounting`	デフォルトの AAA アカウンティング方式の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco NX-OS デバイスによる AAA サーバの VSA の使用

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

VSA の概要

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

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

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

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

VSA の形式

次の VSA プロトコル オプションが、Cisco NX-OS ソフトウェア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るプロトコル。

Accounting
accounting-request パケットで使用されるプロトコル。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 NX-OS ソフトウェアでサポートされています。

roles

ユーザに割り当てられたすべてのロールの一覧です。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。たとえば、ユーザが network-operator および network-admin のロールに属している場合、値フィールドは network-operator network-admin となります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、RADIUS サーバから送信されます。この属性は shell プロトコル値とだけ併用できます。次に、ロール属性を使用する例を示します。

```
shell:roles=network-operator network-admin
```

```
shell:roles*network-operator network-admin
```

次に、FreeRADIUS でサポートされるロール属性の例を示します。

```
Cisco-AVPair = shell:roles=\network-operator network-admin\
Cisco-AVPair = shell:roles*\network-operator network-admin\
```

Note VSA を、shell:roles*"network-operator network-admin" または "shell:roles*\"network-operator network-admin\"" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

accountinginfo
標準の RADIUS アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。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 Cisco NX-OS のユーザ ロールおよび 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 NX-OS デバイスのユーザ ロール マッピングを指定できます。

```
shell:roles="roleA roleB …"
```

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

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。

セキュア ログイン機能の設定

ログイン パラメータの設定

可能性のあるサービス妨害（DoS）攻撃が検出された場合に、それ以降のログイン試行を自動的にブロックし、複数回の接続試行の失敗が検出された場合に待機期間を適用することでディクショナリ攻撃を遅らせるように、ログインパラメータを設定できます。

（注） この機能は、システム スイッチオーバーが発生した場合、または AAA プロセスが再起動した場合に再起動します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コ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**] **login block-for** *seconds* **attempts** *tries* **within** *seconds* 例： `switch(config)# login block-for 100 attempts 2 within 60`	待機モード期間を設定します。すべての引数の範囲は 1 ～ 65535 です。 60 秒以内に 2 回ログイン要求が失敗した場合に 100 秒の待機モードに入るようにスイッチを設定する例を示します。 このコマンドを入力すると、TelnetまたはSSHを介したすべてのログイン試行は、待機期間中に拒否されます。アクセス コントロール リスト (ACL) も、コマンドが入力されます。 （注） 他のログインコマンドを使用する前に、このコマンドを入力する必要があります。
ステップ 3	（任意） [**no**] **login quiet-mode access-class** *acl-name* 例： `switch(config)# login quiet-mode access-class myacl`	待機モードに切り替わるときに、スイッチに適用される ACL を指定します。スイッチが待機モードになっている間は、すべてのログイン要求が拒否され、使用できる接続はコンソール経由の接続のみになります。
ステップ 4	（任意） **show login** [**failures**] 例： `switch(config)# show login`	ログイン パラメータを表示します。**failures** オプションは、失敗したログイン試行に関連する情報のみを表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ ログイン セッションの制限

ユーザ1人あたりのあたりの同時ログインセッションの最大数を制限することができます。これにより、ユーザが複数の不要なセッションを持つことを防止し、有効なSSHまたはTelnetセッションにアクセスする不正ユーザの潜在的なセキュリティ問題を解決します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コ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**] **user max-logins** *max-logins* 例： `switch(config)# user max-logins 1`	ユーザ 1 人あたりの最大同ログイン 時セッション数を制限します。指定できる範囲は1～7です。最大ログイン制限を 1 に設定すると、ユーザ 1 人あたりの Telnet または SSH セッションが 1 に制限されます。 （注） 設定されたログイン制限は、すべてのユーザに適用されます。個々のユーザに異なる制限を設定することはできません。
ステップ 3	（任意） **show running-config all | i max-login** 例： `switch(config)# show running-config all | i max-login`	ユーザ1人あたりの最大同時セッション数を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

パスワードの長さの制限

ユーザパスワードの最小長と最大長を制限できます。この機能を使用すると、ユーザに強力なパスワードの入力を強制することで、システムのセキュリティを強化できます。

始める前に

パスワードの強度の確認を有効にするには、**password strength-check** コマンドを使用する必要があります。パスワードの長さを制限したが、パスワード強度チェックを有効にせず、ユーザが制限された長さの範囲内にないパスワードを入力すると、エラーが表示されますが、ユーザアカウントが作成されます。パスワードの長さを適用し、ユーザアカウントが作成されないようにするには、パスワード強度チェックを有効にし、パスワードの長さを制限する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コ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**] **userpassphrase** {**min-length** *min-length* | **max-length** *max-length*} 例： `switch(config)# userpassphrase min-length 8 max-length 80`	ユーザ パスワードの最小長または最大長を制限します。パスワードの最小長は 4 ～ 127 文字にすることができます。パスワードの最大長は 80 ～ 127 文字です。
ステップ 3	（任意） **show userpassphrase** {**length** | **max-length** | **min-length**} 例： `switch(config)# show userpassphrase length`	ユーザ パスワードの最小長と最大長を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ名のパスワード プロンプトのイネーブル化

ユーザによるユーザ名入力後にパスワード入力を要求するように、スイッチを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**password prompt username**
	例：
	`switch(config)# password prompt username`
	`Password prompt username is enabled. After providing the required options in the username command, press enter. User will be prompted for the username password and password will be hidden. Note: Choosing password key in the same`
		password オプションを付けずに **username** コマンドまたは **snmp-server user** コマンドが入力された後に、ユーザに対してパスワード入力要求のプロンプトを表示するようスイッチを設定します。ユーザが入力したパスワードは非表示にされます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
	line while configuring user account, password will not be hidden.	
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

RADIUS または TACACS+ の共有秘密の設定

スイッチとRADIUSまたはTACACS +サーバ間のリモート認証およびアカウンティング用に設定する共有秘密は、機密情報であるため非表示にする必要があります。これらの暗号化された共有秘密の生成には、 **radius-server** [**host**] **key** および **tacacs-server** [**host**] **key** コマンドをそれぞれ使用します。SHA256ハッシュ方式は、暗号化された共有秘密を保存するために使用されます。

手順

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

ステップ 2	**generate type7_encrypted_secret**
	例：
	`switch(config)# generate type7_encrypted_secret`
	`Type-7 (Vigenere) Encryption,`
	` Use this encrypted secret to configure`
	` radius and tacacs shared secret with`
	` key type 7.`
	` Copy complete secret with double quotes.`
	
	`Enter plain text secret:`
	`Confirm plain text secret:`
	`Type 7 Encrypted secret is : "fewhg"`
		キー タイプ 7 で RADIUS または TACACS+ の共有秘密を設定します。共有秘密の入力を 2 回平文で求められます。秘密は、入力すると非表示になります。次に、暗号化されたバージョンの秘密が表示されます。
		（注） プレーン テキストの秘密情報の暗号化バージョンを別途生成しておき、その後で暗号化された共有秘密を設定することができます。その際には、 **radius-server** [**host**] **key** および **tacacs-server** [**host**] **key** を使用します コマンドを発行します。

ステップ 3	（任意） **copy running-config startup-config** 例：	実行コンフィギュレーションを、スタートアップ 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
	`switch(config)# copy running-config startup-config`	

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 NX-OS デバイスは、AAA アカウンティング アクティビティのローカル ログを保持しています。このログはモニタリングしたりクリアしたりできます。

Procedure

	Command or Action	Purpose
ステップ 1	**show accounting log** [*size* | **last-index** | **start-seqnum** *number* | **start-time** *year month day hh*:*mm*:*ss*] **Example:** `switch# show accounting log`	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。コマンドの出力を制限する場合は、*size* 引数を使用します。指定できる範囲は 0 ～ 250000 バイトです。また、ログ出力の開始シーケンス番号または開始時間を指定できます。開始インデックスの範囲は、1 ～ 1000000 です。アカウンティング ログ ファイルにある最後のインデックス番号の値を表示するには、**last-index** キーワードを使用します。
ステップ 2	(Optional) **clear accounting log** [**logflash**] **Example:** `switch# clear aaa accounting log`	アカウンティング ログの内容をクリアします。**logflash** キーワードはログ フラッシュに保存されているアカウンティング ログをクリアします。

AAA 設定の確認

AAA の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show aaa accounting	AAA アカウンティングの設定を表示します。

コマンド	目的
show aaa authentication [**login** {**ascii-authentication** | **chap** | **error-enable** | **mschap** | **mschapv2**}]	AAA 認証ログイン設定情報を表示します。
show aaa groups	AAA サーバ グループの設定を表示します。
show login [**failures**]	ログイン パラメータを表示します。**failures** オプションは、失敗したログイン試行に関連する情報のみを表示します。 **Note** **clear login failures** コマンドは、現在の監視期間内のログイン失敗をクリアします。
show login on-failure log	syslog サーバに対して認証失敗メッセージをログ記録するようにスイッチが設定されているか表示します。
show login on-successful log	syslog サーバに対して認証成功メッセージをログ記録するようにスイッチが設定されているか表示します。
show running-config aaa [**all**]	実行コンフィギュレーションの AAA 設定を表示します。
show running-config all | i max-login	ユーザ 1 人あたりの最大同時セッション数を表示します。
show startup-config aaa	スタートアップ コンフィギュレーションの AAA 設定を表示します。
show userpassphrase {**length** | **max-length** | **min-length**}	ユーザ パスワードの最小長と最大長を表示します。

AAA の設定例

次に、AAA を設定する例を示します。

```
aaa authentication login default group radius
aaa authentication login console group radius
aaa accounting default group radius
```

ログイン パラメータの設定例

次に、60秒以内に3回ログイン要求が失敗した場合に100秒の待機モードに入るようにスイッチを設定する例を示します。この例は、ログインの失敗を示しません。

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within 60
switch(config)# show login

No Quiet-Mode access list has been configured, default ACL will be applied.

 Switch is enabled to watch for login Attacks.
 If more than 3 login failures occur in 60 seconds or less,
 logins will be disabled for 100 seconds.

 Switch presently in Normal-Mode.
 Current Watch Window remaining time 45 seconds.
 Present login failure count 0.

switch(config)# show login failures
*** No logged failed login attempts with the device.***
```

以下に、待機モードACLの設定例を示します。待機時間中、myaclのACLからのホスト以外、すべてのログイン要求が拒否されます。この例は、ログインの失敗も示します。

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within 60
switch(config)# login quiet-mode access-class myacl

switch(config)# show login

 Switch is enabled to watch for login Attacks.
 If more than 3 login failures occur in 60 seconds or less,
 logins will be disabled for 100 seconds.

 Switch presently in Quiet-Mode.
 Will remain in Quiet-Mode for 98 seconds.
 Denying logins from all sources.

switch(config)# show login failures
Information about last 20 login failure's with the device.
--------------------------------------------------------------------------------
Username      Line          SourceIPAddr    Appname    TimeStamp
--------------------------------------------------------------------------------
asd           /dev/pts/0    171.70.55.158   login      Mon Aug  3 18:18:54 2015
qweq          /dev/pts/0    171.70.55.158   login      Mon Aug  3 18:19:02 2015
qwe           /dev/pts/0    171.70.55.158   login      Mon Aug  3 18:19:08 2015
--------------------------------------------------------------------------------
```

パスワード プロンプト機能の設定例

次の例では、**username** コマンド入力後にユーザ パスワード入力要求のプロンプトを表示し、パスワードが入力されなかった場合にはエラー メッセージを表示するようスイッチを設定する方法を示します。

```
switch# configure terminal
switch(config)# password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password
will not be hidden.


switch(config)# username user1
Enter password:
Confirm password:
warning: password for user:user1 not set. S/he may not be able to login
```

次の例では、**snmp-server user** コマンド入力後にユーザ パスワード入力要求のプロンプトを表示し、その後、ユーザに提示するプロンプトを表示するようにスイッチを設定する方法を示します。

```
switch# configure terminal
switch(config)# password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password
will not be hidden.


N3550-T(config)# snmp-server user user1
Enter auth md5 password (Press Enter to Skip):
Enter auth sha password (Press Enter to Skip):
```

AAA に関する追加情報

ここでは、AAA の実装に関する追加情報について説明します。

関連資料

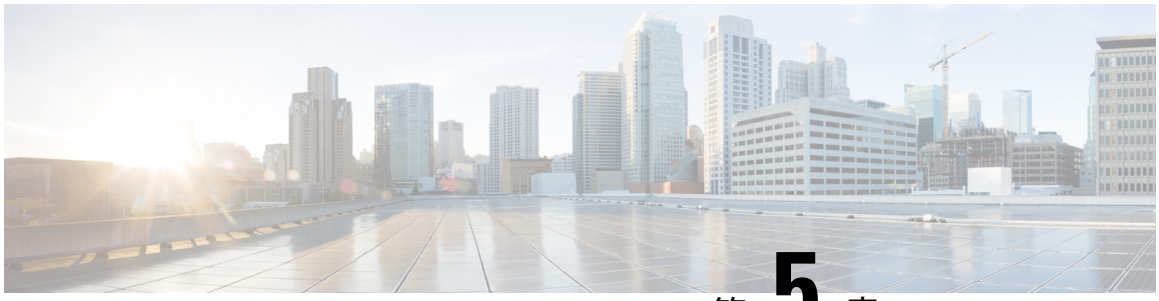
関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	*Cisco NX-OS* ライセンス ガイド

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
AAA に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 5 章

トラフィック ストーム制御の設定

この章では、Cisco NX-OS デバイスに、トラフィック ストーム制御機能を設定する手順について説明します。

Cisco Nexus® 3550-T スイッチ ハードウェアには、コントロール プレーン ポリシング（CoPP）が導入されていません。Storm-Control を使用して、各ポートから CPU へのトラフィックの量を制御できます。Cisco Nexus® 3550-T スイッチのストーム制御機能は、トラフィック分類を提供しません。

トラフィック ストーム制御のライセンス要件

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	トラフィック ストーム制御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 nx-os イメージにバンドルされており、無料で提供されます。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。

トラフィック ストーム制御のガイドラインと制約事項

トラフィック ストーム制御には、次の設定時のガイドラインおよび制約事項があります。

- Cisco Nexus® 3550-T スイッチは、インターフェイスごとの最大許容トラフィック フレーム レートの設定をサポートしています。

  これは、次のコマンドを介して CLI を介して提供されます。

```
storm-control-cpu all <rate>
```

- pps の範囲は 0 ー 250000000 です。
- デフォルト値は 2000 です。
- ストーム制御は、L2 と L3 の両方の物理インターフェイスに適用できます。
- ポートチャネルでサポートされます。

Cisco Nexus® 3550-T スイッチには次の制限が適用されます。

- このレート制限は、すべてのトラフィック タイプに適用されます。つまり、プロトコル/pkt タイプ ベースのスロットリングはありません。
  - 上記の制限により、ソフトウェアで転送されたデータ パケット、キャッシュ ミス、または mac-learn 通知が多数ある場合、CDP、LACP、ARP、OSPF などの制御パケットが失われる可能性があります。

トラフィック ストーム制御の設定例

次に、トラフィック ストーム制御の設定例を示します。

```
module-1# show hardware internal exbl hw port_dump 46
port 46:
  unknown mcast      : false   l3 mcast           : false
  dst nat            : false   src nat            : false
  in meta            : false   out meta           : false
  mux mode           : false   access mode        : true
  default route      : false   forwarding         : true
  bridge (l2)        : true    ucast fail to sw   : false
  dst acl            : false   src acl            : false
  vrrp               : false

  rate burst size    : 255
  rate delay (cycles): 125000
<snip>
```

```
switch(config)# sh run int e1/47
!Command: show running-config interface Ethernet1/47
!Running configuration last done at: Thu Jan 31 01:10:45 2008
!Time: Thu Jan 31 19:01:15 2008

version 10.1(2t)E1(0) Bios:version 3.2

interface Ethernet1/47
  switchport
  no shutdown
```

```
module-1# show hardware internal exbl hw port_dump 46
port 46:
  unknown mcast      : false   l3 mcast           : false
  dst nat            : false   src nat            : false
  in meta            : false   out meta           : false
  mux mode           : false   access mode        : true
  default route      : false   forwarding         : true
  bridge (l2)        : true    ucast fail to sw   : false
  dst acl            : false   src acl            : false
```

```
  vrrp               : false

  rate burst size    : 255
  rate delay (cycles): 50000
<snip>
```

```
switch(config)# sh run int e1/47
!Command: show running-config interface Ethernet1/47
!Running configuration last done at: Thu Jan 31 01:10:45 2008
!Time: Thu Jan 31 19:01:15 2008

version 10.1(2t)E1(0) Bios:version 3.2

interface Ethernet1/47
  switchport
  storm-control-cpu all 5000
  no shutdown
```

```
module-1# show hardware internal exbl hw port_dump 46
port 46:
  unknown mcast      : false   l3 mcast           : false
  dst nat            : false   src nat            : false
  in meta            : false   out meta           : false
  mux mode           : false   access mode        : true
  default route      : false   forwarding         : true
  bridge (l2)        : true    ucast fail to sw   : false
  dst acl            : false   src acl            : false
  vrrp               : false

  rate burst size    : 255
  rate delay (cycles): 1
<snip>
```

```
switch(config)# sh run int e1/47
!Command: show running-config interface Ethernet1/47
!Running configuration last done at: Thu Jan 31 01:10:45 2008
!Time: Thu Jan 31 19:01:15 2008

version 10.1(2t)E1(0) Bios:version 3.2

interface Ethernet1/47
  switchport
  storm-control-cpu all 250000000
  no shutdown
```

```
module-1# show hardware internal exbl hw port_dump 46
port 46:
  unknown mcast      : false   l3 mcast           : false
  dst nat            : false   src nat            : false
  in meta            : false   out meta           : false
  mux mode           : false   access mode        : true
  default route      : false   forwarding         : true
  bridge (l2)        : true    ucast fail to sw   : false
  dst acl            : false   src acl            : false
  vrrp               : false

  rate burst size    : 255
  rate delay (cycles): 0  --□ Drops all packtes to host/CPU from this port
<snip>
```

```
switch(config)# sh run int e1/47
!Command: show running-config interface Ethernet1/47
!Running configuration last done at: Thu Jan 31 01:10:45 2008
!Time: Thu Jan 31 19:01:15 2008

version 10.1(2t)E1(0) Bios:version 3.2
```

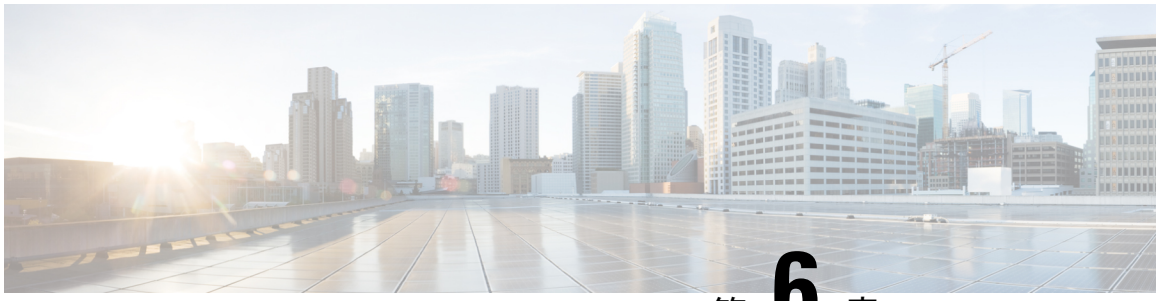
```
interface Ethernet1/47
  switchport
  storm-control-cpu all 0
  no shutdown

module-1# show hardware internal exbl hw port_dump 46
port 46:
  unknown mcast      : false   l3 mcast           : false
  dst nat            : false   src nat            : false
  in meta            : false   out meta           : false
  mux mode           : false   access mode        : true
  default route      : false   forwarding         : true
  bridge (l2)        : true    ucast fail to sw   : false
  dst acl            : false   src acl            : false
  vrrp               : false

  rate burst size    : 255
  rate delay (cycles): 0  --□ Drops all packtes to host/CPU from this port
<snip>

switch(config)# sh run int e1/47
!Command: show running-config interface Ethernet1/47
!Running configuration last done at: Thu Jan 31 01:10:45 2008
!Time: Thu Jan 31 19:01:15 2008

version 10.1(2t)E1(0) Bios:version 3.2

interface Ethernet1/47
  switchport
  storm-control-cpu all 0
  no shutdown
```

トラフィック ストーム制御に関する追加情報

ここでは、トラフィック ストーム制御の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	*Cisco NX-OS* ライセンス ガイド



第 6 章

RADIUS の設定

この章では、Cisco NX-OS デバイスで Remote Access Dial-In User Service（RADIUS）プロトコルを設定する手順について説明します。

この章は、次の項で構成されています。

RADIUS について

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 NX-OS デバイスで稼働し、すべてのユーザ認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウンティング要求を送信します。

RADIUS ネットワーク環境

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

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

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク。たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバ ベースのセキュリティ データベースを使用できます。
- すでに RADIUS を使用中のネットワーク。RADIUS を使用した Cisco NX-OS デバイスをネットワークに追加できます。この作業は、AAA サーバに移行するときの最初の手順になります。
- リソースアカウンティングが必要なネットワーク。RADIUSアカウンティングは、RADIUS認証またはRADIUS認可とは個別に使用できます。RADIUSアカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネット サービス プロバイダー（ISP）は、RADIUSアクセスコントロールおよびアカウンティング用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。
- 認証プロファイルをサポートするネットワーク。ネットワークでRADIUSサーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルをセットアップできます。ユーザごとのプロファイルにより、Cisco NX-OS デバイスは、既存の RADIUS ソリューションを使用してポートを容易に管理できると同時に、共有リソースを効率的に管理してさまざまなサービス レベル契約（SLA）を提供できます。

RADIUS の動作

ユーザが RADIUS を使用して Cisco NX-OS デバイスへのログインおよび認証を試行すると、次のプロセスが実行されます。

- 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。
- 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。
- 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
  ユーザが認証されました。
  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、新しいパスワードを選択するよう要求が発行されます。

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

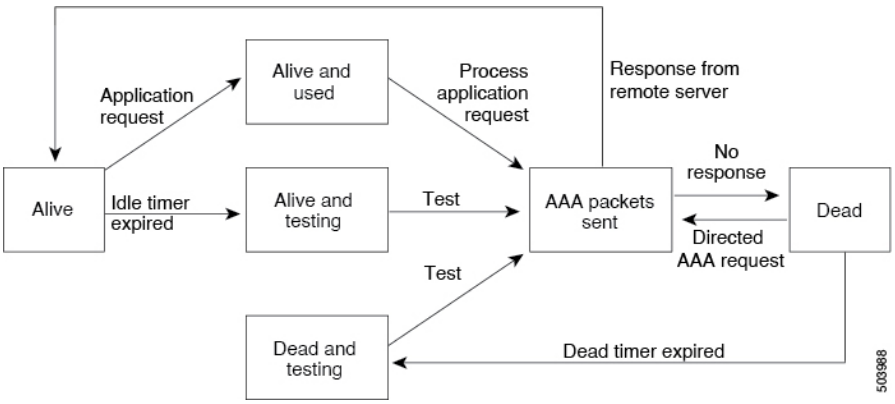
- ユーザがアクセス可能なサービス（Telnet、rlogin、またはローカルエリア トランスポート（LAT）接続、ポイントツーポイント プロトコル（PPP）、シリアル ラインインターネット プロトコル（SLIP）、EXEC サービスなど）
- ホストまたはクライアントの IPv4 アドレス、アクセス リスト、ユーザー タイムアウトなどの接続パラメータ

RADIUS サーバのモニタリング

応答しない RADIUS サーバがあると、AAA 要求の処理が遅れることがあります。AAA 要求の処理時間を節約するために、定期的に RADIUS サーバをモニタリングし、RADIUS サーバが応答を返す（アライブ）かどうかを調べるよう、Cisco NX-OS デバイスを設定できます。Cisco NX-OS デバイスは、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。Cisco NX-OS デバイスは定期的にデッド 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。このモニタリング プロセスでは、実際の AAA 要求が送信される前に、RADIUS サーバが稼働状態であることを確認します。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、Cisco NX-OS デバイスによって、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。

***Figure 3: RADIUS* サーバの状態**

次の図に、RADIUS サーバ モニタリングの状態を示します。



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

ベンダー固有属性

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

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

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

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

次の VSA プロトコル オプションが、Cisco NX-OS ソフトウェア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るプロトコル。

Accounting
accounting-request パケットで使用されるプロトコル。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 NX-OS ソフトウェアでは、次の属性がサポートされています。

roles
ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。たとえば、ユーザが network-operator および network-admin のロールに属している場合、値フィールドは network-operator network-admin となります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、RADIUS サーバから送信されます。この属性はシェル プロトコル値とだけ併用できます。次に、Cisco Access Control Server（ACS）でサポートされるロール属性の例を示します。

```
shell:roles=network-operator network-admin

shell:roles*"network-operator network-admin
```

次に、FreeRADIUS でサポートされるロール属性の例を示します。

```
Cisco-AVPair = shell:roles=\network-operator network-admin\

Cisco-AVPair = shell:roles*\network-operator network-admin\
```

Note VSA を、shell:roles*"network-operator network-admin" または "shell:roles*\"network-operator network-admin\"" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

accountinginfo
標準の RADIUS アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。この属性は、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分だけに送信されます。この属性と共に使用できるのは、アカウンティングのプロトコル データ ユニット（PDU）だけです。

RADIUS 認可変更について

標準RADIUSインターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリが送信されたサーバが応答するプル モデルで使用されます。Cisco NX-OS ソフトウェアは、プッシュ モデルで使用される RFC 5176 で定義された RADIUS Change of Authorization（CoA）要求をサポートしています。このモデルでは、要求は外部サーバからネットワークに接続されたデバイスへ発信され、外部の認証、認可、およびアカウンティング（AAA）またはポリシー サーバからの動的なセッション再設定が可能になります。

Dot1x が有効の場合、ネットワーク デバイスはオーセンティケータとして機能し、セッションごとのダイナミック COA を処理します。

次の要求がサポートされています。

- セッション再認証
- セッションの終了

セッション再認証

セッションの再認証を開始するには、認証、認可、およびアカウンティング（AAA）サーバは、Cisco VSA および 1 個以上のセッションの ID 属性を含む標準 CoA 要求メッセージを送信します。Cisco VSA は Cisco:Avpair=“subscriber:command=reauthenticate” の形式です。

次のシナリオでは、現在のセッション状態によって、メッセージに対するデバイスの応答が決まります。

- セッションが現在、IEEE 802.1x によって認証されている場合、デバイスは Extensible Authentication Protocol over LAN（EAPoL）-RequestId メッセージをサーバに送信することで応答します。
- 現在、セッションが MAC 認証バイパス（MAB）で認証されている場合は、デバイスはサーバにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

- デバイスがコマンドを受信する際にセッションの認証が行われている場合、デバイスはプロセスを終了し、認証シーケンスを再起動して、最初に試行されるように設定された方式を開始します。

セッションの終了

CoA 接続解除要求は、ホスト ポートを無効にせずにセッションを終了します。CoA 接続解除：終了の要求によって、指定したホストのオーセンティケータ ステート マシンが再初期化されますが、ホストのネットワークへのアクセスは制限されません。

セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して Disconnect-NAK メッセージを返します。

セッションが見つかったが、何らかの内部エラーのために NAS がセッションを削除できなかった場合、デバイスは「Session Context Not Removable」エラー コード属性を持つ Disconnect-NAK メッセージを返します。

セッションが見つかった場合、デバイスはセッションを終了します。セッションが完全に削除されると、デバイスは Disconnect-ACK メッセージを返します。

RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバーの IPv4 アドレスまたはホスト名を取得していること。
- RADIUS サーバからキーを取得すること。
- Cisco NX-OS デバイスが、AAA サーバの RADIUS クライアントとして設定されていること。

RADIUS の注意事項と制約事項

RADIUS には次のガイドラインおよび制限事項があります。

- Cisco NX-OS デバイスに設定できる RADIUS サーバの最大数は 64 です。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- ワンタイム パスワードをサポートするのは RADIUS プロトコルだけです。
- Cisco Nexus® 3550-T switches スイッチは、TACAAS+ に対してのみ CLI コマンド aaa authentication login ascii-authentication をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、aaa authentication login

ascii-authentication スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されます。

RADIUS のデフォルト設定

次の表に、RADIUS パラメータのデフォルト設定を示します。

***Table 6: RADIUS* パラメータのデフォルト設定**

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
認証ポート	1812
アカウンティング ポート	1813
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	テスト

RADIUS サーバの設定

ここでは、Cisco NX-OS デバイスで RADIUS サーバを設定する手順を説明します。

Note Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

Note Cisco Nexus® 3550-T switches スイッチは、TACAAS+ に対してのみ CLI コマンド aaa authentication login ascii-authentication をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、aaa authentication login ascii-authentication スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されます。

RADIUS サーバの設定プロセス

1. Cisco NX-OS デバイスと RADIUS サーバとの接続を確立します。
2. RADIUS サーバの RADIUS 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。
   - デッドタイム間隔
   - ユーザ ログイン時の RADIUS サーバの指定の許可
   - タイムアウト間隔
   - TCP ポート
5. （任意）RADIUS 設定の配布がイネーブルになっている場合は、ファブリックに対して RADIUS 設定をコミットします。

Related Topics

RADIUS サーバ ホストの設定 （62 ページ）
グローバル RADIUS キーの設定 （63 ページ）

RADIUS サーバ ホストの設定

リモートの RADIUS サーバにアクセスするには、RADIUS サーバの IP アドレスまたはホスト名を設定する必要があります。最大 64 の RADIUS サーバを設定できます。

Note RADIUS サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスに設定するとき、デフォルトでは RADIUS サーバはデフォルトの RADIUS サーバ グループに追加されます。RADIUS サーバを別の RADIUS サーバ グループに追加することもできます。

Before you begin

サーバがすでにサーバ グループのメンバーとして設定されていることを確認します。

サーバが RADIUS トラフィックを認証するよう設定されていることを確認します。

Cisco NX-OS デバイスが、AAA サーバの RADIUS クライアントとして設定されていること。

Procedure

	Command or Action	Purpose

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

ステップ 2	**radius-server host** {*ipv4-address* | *hostname*} **Example:** `switch(config)# radius-server host 10.10.1.1`	認証に使用する RADIUS サーバの IPv4 アドレスまたはホスト名を指定します。
ステップ 3	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 4	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用します。

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

ステップ 6	(Optional) **show radius-server** **Example:** `switch# show radius-server`	RADIUS サーバの設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

特定の RADIUS サーバ用のキーの設定 （65 ページ）

グローバル RADIUS キーの設定

Cisco NX-OS デバイスで使用するすべてのサーバの RADIUS キーを設定できます。RADIUS キーとは、Cisco NX-OS デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

Before you begin

リモート RADIUS サーバの RADIUS キーの値を取得します。

リモート RADIUS サーバに RADIUS キーを設定します。

Procedure

	Command or Action	Purpose

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

ステップ 2	**radius-server key** [**0** | **6** | **7**] *key-value* **Example:** `switch(config)# radius-server key 0 QsEfThUkO`	すべての RADIUS サーバ用の RADIUS キーを指定します。*key-value* がクリア テキスト形式（**0**）か、タイプ 6 暗号化形式（**6**）か、タイプ 7 暗号化形式（**7**）かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存する前にクリアテキストのキーを暗号化します。デフォルトの形式はクリア テキストです。最大で 63 文字です。 デフォルトでは、RADIUS キーは設定されません。

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

ステップ 4	(Optional) **show radius-server** **Example:** `switch# show radius-server`	RADIUS サーバの設定を表示します。 **Note** RADIUS キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された RADIUS キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

RADIUS サーバ グループの設定 （66 ページ）

特定の RADIUS サーバ用のキーの設定

Cisco NX-OS デバイスで、特定の RADIUS サーバ用のキーを設定できます。RADIUS キーは、Cisco NX-OS デバイスと特定の RADIUS サーバとの間で共有する秘密テキスト ストリングです。

Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

リモート RADIUS サーバのキーの値を取得します。

RADIUS サーバにキーを設定します。

Procedure

	Command or Action	Purpose

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

ステップ 2	**radius-server host** {*ipv4-address* | *hostname*} **key** [**0** | **6** | **7**] *key-value* **Example:** `switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg`	特定の RADIUS サーバ用の RADIUS キーを指定します。*key-value* がクリア テキスト形式（**0**）か、タイプ 6 暗号化形式（**6**）か、タイプ 7 暗号化形式（**7**）かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存する前にクリアテキストのキーを暗号化します。デフォルトの形式はクリア テキストです。最大で 63 文字です。 この RADIUS キーが グローバル RADIUS キーの代わりに使用されます。

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

ステップ 4	(Optional) **show radius-server** **Example:**	RADIUS サーバの設定を表示します。

	Command or Action	Purpose
	`switch# show radius-server`	**Note** RADIUS キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された RADIUS キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

RADIUS サーバ ホストの設定 （62 ページ）

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。

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

Before you begin

グループ内のすべてのサーバが RADIUS サーバであることを確認します。

Procedure

	Command or Action	Purpose

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

ステップ 2	**aaa group server radius** *group-name*
	Example:
	`switch(config)# aaa group server radius RadServer`
	`switch(config-radius)#`
		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 文字の長さの英数字のストリングで、大文字小文字が区別されます。

	Command or Action	Purpose
		RADIUS サーバ グループを削除するには、このコマンドの **no** 形式を使用します。 **Note** デフォルトのシステム生成デフォルト グループ（RADIUS）は削除できません。
ステップ 3	**server** {*ipv4-address* | *hostname*} **Example:** `switch(config-radius)# server 10.10.1.1`	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** コマンドを実行し、このコマンドを再試行します。
ステップ 4	(Optional) **deadtime** *minutes* **Example:** `switch(config-radius)# deadtime 30`	モニタリング デッド タイムを設定します。デフォルト値は0分です。指定できる範囲は 1 ～ 1440 です。 **Note** RADIUS サーバ グループのデッド タイム間隔が 0 より大きい場合は、この値がグローバルなデッド タイム値より優先されます。
ステップ 5	(Optional) **server** {*ipv4-address* | *hostname*} **Example:** `switch(config-radius)# server 10.10.1.1`	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。 **Tip** 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 6	(Optional) **use-vrf** *vrf-name* **Example:** `switch(config-radius)# use-vrf default`	サーバ グループ内のサーバとの接続に使用する VRF を指定します。

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

	Command or Action	Purpose
ステップ 8	(Optional) **show radius-server groups** [*group-name*] **Example:** `switch(config)# show radius-server groups`	RADIUS サーバ グループの設定を表示します。
ステップ 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

RADIUS デッド タイム間隔の設定 （78 ページ）

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。デフォルトでは、Cisco NX-OS ソフトウェアは、使用可能なあらゆるインターフェイスを使用します。

Procedure

	Command or Action	Purpose

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

ステップ 2	**ip radius source-interface** *interface* **Example:** `switch(config)# ip radius source-interface mgmt 0`	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。

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

ステップ 4	(Optional) **show radius-server** **Example:** `switch# show radius-server`	RADIUS サーバの設定情報を表示します。

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

Related Topics

RADIUS サーバ グループの設定 （66 ページ）

ログイン時にユーザによる RADIUS サーバの指定を許可

デフォルトでは、Cisco NX-OS デバイスはデフォルトの AAA 認証方式に基づいて認証要求を転送します。認証要求送信先 RADIUS サーバーをユーザーが指定できるように Cisco NX-OS デバイスを設定するには、directed-request オプションを有効にします。このオプションを有効にした場合、ユーザーは *username***@vrfname***hostname* としてログインできます。ここで、**hostname** は使用する VRF、**hostname**は設定された RADIUS サーバーの名前です。

Note directed-request オプションを有効にすると、Cisco NX-OS デバイスでは認証に RADIUS 方式だけを使用し、デフォルトのローカル方式は使用しないようになります。

Note ユーザ指定のログインは Telnet セッションに限りサポートされます。

Procedure

	Command or Action	Purpose

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

ステップ 2	**radius-server directed-request** **Example:** `switch(config)# radius-server directed-request`	ログイン時にユーザが認証要求の送信先となる RADIUS サーバを指定できるようにします。デフォルトでは無効になっています。
ステップ 3	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	配布するために保留状態になっている RADIUS 設定を表示します。

	Command or Action	Purpose
ステップ 4	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用します。

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

ステップ 6	(Optional) **show radius-server directed-request** **Example:** `switch# show radius-server directed-request`	directed request の設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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、Cisco NX-OS デバイス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。タイムアウト間隔には、Cisco NX-OS デバイスが RADIUS 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。

Procedure

	Command or Action	Purpose

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

ステップ 2	**radius-server retransmit** *count* **Example:** `switch(config)# radius-server retransmit 3`	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	**radius-server timeout** *seconds* **Example:**	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

	Command or Action	Purpose
	`switch(config)# radius-server timeout 10`	ト間隔は 5 秒で、範囲は 1 ～ 60 秒です。
ステップ 4	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 5	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用します。

ステップ 6	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 7	(Optional) **show radius-server** **Example:** `switch# show radius-server`	RADIUS サーバの設定を表示します。
ステップ 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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 NX-OS デバイス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。Cisco NX-OS デバイスが、タイムアウト エラーを宣言する前に、RADIUS サーバからの応答を待機するタイムアウト間隔も設定できます。

Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose
ステップ 2	**radius-server host** {*ipv4-address* | *hostname*} **retransmit** *count* **Example:** `switch(config)# radius-server host server1 retransmit 3`	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。 **Note** 特定の RADIUS サーバに指定した再送信回数は、すべての RADIUS サーバに指定した再送信回数より優先されます。
ステップ 3	**radius-server host** {*ipv4-address* | *hostname*} **timeout** *seconds* **Example:** `switch(config)# radius-server host server1 timeout 10`	特定のサーバの送信タイムアウト間隔を指定します。デフォルトはグローバル値です。 **Note** 特定の RADIUS サーバに指定したタイムアウト間隔は、すべての RADIUS サーバに指定したタイムアウト間隔より優先されます。
ステップ 4	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 5	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用し、CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 6	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 7	(Optional) **show radius-server** **Example:** `switch# show radius-server`	RADIUS サーバの設定を表示します。
ステップ 8	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

RADIUS サーバ ホストの設定 （62 ページ）

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。また、デフォルトのポートとの競合が発生する場合は、RADIUS アカウンティング メッセージと認証メッセージの送信先である宛先 UDP ポート番号を指定することもできます。

Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

Procedure

	Command or Action	Purpose

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

ステップ 2	(Optional) **radius-server host** {*ipv4-address* | *hostname*} **acct-port** *udp-port* **Example:** `switch(config)# radius-server host 10.10.1.1 acct-port 2004`	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 1813 です。範囲は 0 ～ 65535 です。
ステップ 3	(Optional) **radius-server host** {*ipv4-address* | *hostname*} **accounting** **Example:** `switch(config)# radius-server host 10.10.1.1 accounting`	RADIUS サーバをアカウンティングだけに使用することを指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	(Optional) **radius-server host** {*ipv4-address* | *hostname*} **auth-port** *udp-port* **Example:** `switch(config)# radius-server host 10.10.2.2 auth-port 2005`	RADIUS 認証メッセージ用の UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。範囲は 0 ～ 65535 です。
ステップ 5	(Optional) **radius-server host** {*ipv4-address* | *hostname*} **authentication** **Example:** `switch(config)# radius-server host 10.10.2.2 authentication`	RADIUS サーバを認証だけに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。

	Command or Action	Purpose
ステップ 6	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 7	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用します。

ステップ 8	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 9	(Optional) **show radius-server** **Example:** `switch(config)# show radius-server`	RADIUS サーバの設定を表示します。
ステップ 10	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

Related Topics

RADIUS サーバ ホストの設定 （62 ページ）

RADIUS サーバのグローバルな定期モニタリングの設定

各サーバに個別にテスト パラメータを設定しなくても、すべての RADIUS サーバの可用性をモニタリングできます。テスト パラメータが設定されていないサーバは、グローバル レベルのパラメータを使用してモニタリングされます。

Note 各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。

グローバル コンフィギュレーション パラメータには、サーバで使用するユーザ名とパスワード、およびアイドル タイマーなどがあります。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、Cisco NX-OS デバイスがテスト パケットを送信するかを指定します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。

Note ネットワークのセキュリティを保護するために、RADIUSデータベースの既存のユーザ名と同じものを使用しないことを推奨します。

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

Before you begin

RADIUS をイネーブルにします。

Procedure

	Command or Action	Purpose

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

ステップ 2	**radius-server test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3`	グローバルなサーバ 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。 **Note** 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	**radius-server deadtime** *minutes* **Example:** `switch(config)# radius-server deadtime 5`	Cisco NX-OS デバイスが、前回応答しなかった RADIUS サーバをチェックするまでの時間（分）を指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。

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

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

Related Topics

各 RADIUS サーバの定期モニタリングの設定 （76 ページ）

各 RADIUS サーバの定期モニタリングの設定

各 RADIUS サーバの可用性をモニタリングできます。コンフィギュレーション パラメータには、サーバで使用するユーザ名とパスワード、およびアイドル タイマーなどがあります。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 Cisco NX-OS 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定期的にサーバをテストしたり、1 回だけテストを実行したりできます。

Note 各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。

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

Note デフォルトのアイドル タイマー値は 0 分です。アイドル時間間隔が 0 分の場合、Cisco NX-OS デバイスは、RADIUS サーバの定期的なモニタリングを実行しません。

Before you begin

RADIUS を有効にします。

1 つまたは複数の RADIUS サーバ ホストを追加します。

Procedure

	Command or Action	Purpose

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

ステップ 2	**radius-server host** {*ipv4-address* | *hostname*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3`	サーバ モニタリング用のパラメータを個別に指定します。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。 **Note** 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	**radius-server deadtime** *minutes* **Example:** `switch(config)# radius-server deadtime 5`	Cisco NX-OS デバイスが、前回応答しなかった RADIUS サーバをチェックするまでの時間（分）を指定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。

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

ステップ 5	(Optional) **show radius-server** **Example:** `switch# show radius-server`	RADIUS サーバの設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

RADIUS サーバ ホストの設定 （62 ページ）
RADIUS サーバのグローバルな定期モニタリングの設定 （74 ページ）

RADIUS 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 NX-OS デバイスが、RADIUS サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを確認するためにテスト パケットを送信するまでの間隔を指定します。デフォルト値は 0 分です。

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

Procedure

	Command or Action	Purpose

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

ステップ 2	**radius-server deadtime** *minutes* **Example:** `switch(config)# radius-server deadtime 5`	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	(Optional) **show radius** {**pending** | **pending-diff**} **Example:** `switch(config)# show radius pending`	配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 4	(Optional) **radius commit** **Example:** `switch(config)# radius commit`	一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用します。

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

ステップ 6	(Optional) **show radius-server** **Example:** `switch# show radius-server`	RADIUS サーバの設定を表示します。

	Command or Action	Purpose
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

RADIUS サーバ グループの設定 （66 ページ）

ワンタイム パスワードの設定

RSA SecurID トークン サーバを使用することで、Cisco NX-OS デバイスでワンタイム パスワード（OTP）をサポートできます。この機能を使用すると、ユーザは、暗証番号（ワンタイム パスワード）とその時点で RSA SecurID トークンに表示されるトークン コードの両方を入力することで、Cisco NX-OS デバイスに対する認証を実行できます。

Note Cisco NX-OS デバイスにログインするために使用されるトークン コードは、60 秒ごとに変更されます。デバイス検出に関する問題を防ぐために、Cisco Secure ACS 内部データベースに存在する異なるユーザ名を使用することを推奨します。

Before you begin

Cisco NX-OS デバイスで、RADIUS サーバ ホストとデフォルトのリモート ログイン認証を設定します。

次のものがインストールされていることを確認します。

- Cisco Secure Access Control Server（ACS）Version 4.2
- RSA Authentication Manager Version 7.1（RSA SecurID トークン サーバ）
- RSA ACE Agent/Client

ワンタイム パスワードをサポートするために、Cisco NX-OS デバイスで（RADIUS サーバ ホストとリモート認証以外の）設定を行う必要はありません。ただし、Cisco Secure ACS を次のように設定する必要があります。

1. RSA SecurID トークン サーバ認証をイネーブルにします。
2. RSA SecurID トークン サーバを不明ユーザ ポリシー データベースに追加します。

RADIUS サーバまたはサーバ グループの手動モニタリング

RADIUS サーバまたはサーバ グループに対し手動でテスト メッセージを送信できます。

Procedure

	Command or Action	Purpose
ステップ 1	**test aaa server radius** {*ipv4-address* | *hostname*} *username password* **Example:** `switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH`	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	**test aaa group** *group-name username password* **Example:** `switch# test aaa group RadGroup user2 As3He3CI`	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。

Dynamic Author Server の有効化または無効化

手順

	コマンドまたはアクション	目的

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

ステップ 2	**aaa server radius dynamic-author** 例： `switch(config)# aaa server radius dynamic-author`	RADIUS dynamic author server を有効にします。このコマンドのno形式を使用すれば、RADIUS dynamic author server を無効にできます。

RADIUS 認可変更の設定

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定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**] **aaa server radius dynamic-author** 例： `switch(config)# aaa server radius dynamic-author`	スイッチを AAA サーバとして設定し、外部ポリシー サーバとの連携を促進します。このコマンドの no 形式を使用して、RADIUS ダイナミック オーサーと、関連付けられたクライアントを無効にできます。
ステップ 3	[**no**] **client** {*ip-address* | **hostname** } [**server-key** [**0** | **7**] *string*] 例： `switch(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1`	AAA サーバ クライアントの IP アドレスまたはホスト名を設定します。オプションの server-key キーワードと string 引数を使用して、「クライアント」レベルでサーバ キーを設定します。クライアント サーバを削除するには、このコマンドの no 形式を使用します。 （注） クライアント レベルでサーバ キーを設定すると、グローバル レベルで設定されたサーバ キーが上書きされます。
ステップ 4	[**no**] **port** *port-number* 例： `switch(config-locsvr-da-radius)# port 3799`	設定された RADIUS クライアントからの RADIUS 要求をデバイスが受信するポートを指定します。ポート範囲は 1 ～ 65535 です。デフォルトのポートに戻すには、このコマンドの no 形式を使用します。 （注） パケット オブ ディスコネクトのデフォルト ポートは 1700 です。
ステップ 5	[**no**] **server-key** [**0** | **7**] *string*	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。サーバ キーを削除するには、このコマンドの no 形式を使用します。

RADIUS 設定の確認

RADIUS 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 radius {**status** | **pending** | **pending-diff**}	Cisco Fabric Services の RADIUS 設定の配布状況と他の詳細事項を表示します。

コマンド	目的
show running-config radius [**all**]	実行コンフィギュレーションの RADIUS 設定を表示します。
show startup-config radius	スタートアップコンフィギュレーションの RADIUS 設定を表示します。
show radius-server [*hostname* | *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 認可変更の設定の検証

RADIUS 認可変更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 dot1x	実行コンフィギュレーションの dot1x 設定を表示します。
show running-config aaa	実行コンフィギュレーションの AAA 設定を表示します。
show running-config radius	実行コンフィギュレーションの RADIUS 設定を表示します。
show aaa server radius statistics	ローカルの RADIUS サーバ統計情報を表示します。
show aaa client radius statistics {*ip address* | *hostname* }	ローカルの RADIUS クライアント統計情報を表示します。
clear aaa server radius statistics	ローカルの RADIUS サーバ統計情報をクリアします。
clear aaa client radius statistics {*ip address* | *hostname* }	ローカルの RADIUS クライアント統計情報をクリアします。

RADIUS サーバのモニタリング

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モニタします。

Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	**show radius-server statistics** {*hostname* | *ipv4-address*} **Example:** `switch# show radius-server statistics 10.10.1.1`	RADIUS 統計情報を表示します。

Related Topics

RADIUS サーバ ホストの設定 （62 ページ）
RADIUS サーバ統計情報のクリア （83 ページ）

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。

Before you begin

Cisco NX-OS デバイスの RADIUS サーバを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	(Optional) **show radius-server statistics** {*hostname* | *ipv4-address*} **Example:** `switch# show radius-server statistics 10.10.1.1`	Cisco NX-OS デバイスの RADIUS サーバ統計情報を表示します。
ステップ 2	**clear radius-server statistics** {*hostname* | *ipv4-address*} **Example:** `switch# clear radius-server statistics 10.10.1.1`	RADIUS サーバ統計情報をクリアします。

Related Topics

RADIUS サーバ ホストの設定 （62 ページ）

RADIUS の設定例

次に、RADIUS を設定する例を示します。

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
```

RADIUS 認可変更の設定例

次に、RADIUS の認可変更を設定する方法の例を示します。

```
radius-server host 10.77.143.170 key 7 "fewhg123" authentication accounting
aaa server radius dynamic-author
    client 10.77.143.170 vrf management server-key 7 "fewhg123"
```

RADIUS に関する追加情報

ここでは、RADIUS の実装に関する追加情報について説明します。

関連資料

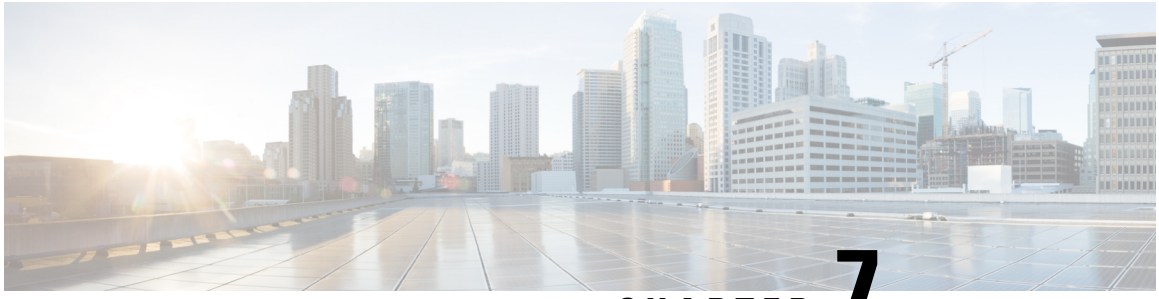
関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
VRF コンフィギュレーション	*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成ガイド

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
RADIUS に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



CHAPTER 7

IP ACL の設定

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

特に指定がなければ、IP ACL は IPv4 の ACL を意味します。

この章は、次の項で構成されています。

ACL について

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。デバイスは、ある ACL がパケットに適用されると判断すると、そのすべてのルールの条件にパケットを照合し、テストします。最初に一致したルールで、そのパケットが許可されるか拒否されるかが決定されます。一致するものがなければ、デバイスは適用可能な暗黙のルールを適用します。デバイスは、許可されたパケットの処理を続行し、拒否されたパケットはドロップします。

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

ACL のタイプと適用

セキュリティ トラフィック フィルタリングには次のタイプの ACL を使用できます。

IPv4 ACL
Cisco Nexus® 3550-T デバイスは、IPv4 ACL を IPv4 TCP および UDP トラフィックだけに適用します。

IP には次の種類のアプリケーションがあります。

ルータ ACL
レイヤ 3 トラフィックのフィルタリング

VTY ACL
仮想テレタイプ（VTY）トラフィックのフィルタリング

Note Cisco Nexus® 3550-T では、ルータおよび VTY ACL IP アプリケーションのみがサポートされています。

Note 次のインターフェイスの ACL で指定された条件に基づいて入力トラフィックをフィルタリングするために、入力ポリシーのみを Cisco Nexus® 3550-T スイッチで構成できます。

- 物理層 3 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

次の表に、セキュリティ ACL の適用例の概要を示します。

Table 7: セキュリティ ***ACL*** の適用

適用	サポートするインターフェイス	サポートする ACL のタイプ
ルータ ACL	• 物理層 3 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 • 管理インターフェイス	• IPv4 ACL **Note** 出力ルータ ACL は、Cisco Nexus® 3550-T スイッチのアップリンクポートでは**サポートされません。**

ACL の適用順序

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 Ingress ルータ ACL のみを適用します。

ルールについて

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

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。デバイスは、許可ルール内の基準と一致するトラフィックを許可し、拒否ルール内の基準と一致するトラフィックをブロックします。ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

ここでは、ルールを設定する際に使用できるオプションをいくつか紹介します。

送信元と宛先

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

IP ACL の暗黙ルール

IP 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デバイス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
```

この暗黙ルールによって、デバイスは不一致 IP トラフィックを確実に拒否します。

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

その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。これらのオプションは、ACLのタイプによって異なります。次のリストには、ほとんどの追加フィルタリング オプションが含まれていますが、すべてを網羅しているわけではありません。

- 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

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

既存のルールの間に新しいルールを追加

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。

ルールの削除

シーケンス番号を使用しない場合は、ルールを削除するために、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
```

ルールの移動

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、Cisco NX-OS 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。Cisco NX-OS では、入力方向でのみ論理演算子をサポートします。

このデバイスは、論理演算ユニット（LOU）というレジスタに、演算子とオペランドの組み合わせを格納します。各タイプの演算子は、次のように LOU を使用します。

eq
LOU には格納されません。
gt
1 LOU を使用します。
lt
1 LOU を使用します。
range
1 LOU を使用します。

時間範囲

時間範囲を使用して、ACLルールが有効になる時期を制御できます。たとえば、インターフェイスに着信するトラフィックに特定の ACL を適用するとデバイスが判断し、その ACL のあるルールの時間範囲が有効になっていない場合、デバイスは、トラフィックをそのルールと照合しません。デバイスは、そのデバイスのクロックに基づいて時間範囲を評価します。

時間範囲を使用する ACL を適用すると、デバイスはその ACL で参照される時間範囲の開始時または終了時に影響する I/O モジュール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。

IPv4 の ACL は時間範囲をサポートしています。デバイスがトラフィックに ACL を適用する場合、有効なルールは次のとおりです。

- 時間範囲が指定されていないすべてのルール
- デバイスがその ACL をトラフィックに適用した時点（秒）が時間範囲に含まれているルール

名前が付けられた時間範囲は再利用できます。多くの ACL ルールを設定する場合は、時間範囲を名前で一度設定すれば済みます。時間範囲の名前は最大 64 の英文字で指定します。

時間範囲には、1 つまたは複数のルールで構成されます。これらのルールは次の 2 種類に分類できます。

絶対

特定の開始日時、終了日時、その両方を持つルール、またはそのどちらも持たないルール。絶対時間範囲のルールがアクティブかどうかは、開始日時または終了日時の有無によって、次のように決まります。

- 開始日時と終了日時が両方指定されている：この時間範囲ルールは、現在の時刻が開始日時よりも後で終了日時よりも前の場合にアクティブになります。
- 開始日時が指定され、終了日時は指定されていない：この時間範囲ルールは、現在の時刻が開始日時よりも後である場合にアクティブになります。
- 開始日時は指定されず、終了日時が指定されている：この時間範囲ルールは、現在の時刻が終了日時よりも前である場合にアクティブになります。

- 開始日時も終了日時も指定されていない：この時間範囲ルールは常にアクティブです。

たとえば、新しいサブネットへのアクセスを許可するようにネットワークを設定する場合、そのサブネットをオンラインにする予定日の真夜中からアクセスを許可するような時間範囲を指定し、この時間範囲をそのサブネットに適用する ACL ルールに使用します。デバイスはこのルールを含む ACL を適用する場合、開始日時が過ぎると、この時間範囲を使用するルールの適用を自動的に開始します。

定期

毎週 1 回以上アクティブになるルール。たとえば、定期時間範囲を使用すると、平日の営業時間中だけ、研究室のサブネットにアクセスできるようにすることができます。デバイスは、そのルールを含む ACL が適用されていて、時間範囲がアクティブな場合にだけ、この時間範囲を使用する ACL ルールを自動的に適用します。

Note デバイスは、時間範囲内のルールの順序に関係なく、時間範囲がアクティブかどうかを判断します。Cisco NX-OS は、時間範囲を編集できるように時間範囲内にシーケンス番号を入れます。

時間範囲には備考を含めることもできます。備考を使用すると、時間範囲にコメントを挿入できます。備考は、最大 100 文字の英数字で指定します。

デバイスは次の方法で時間範囲がアクティブかどうかを判断します。

- 時間範囲に絶対ルールが 1 つまたは複数含まれている：現在の時刻が 1 つまたは複数の絶対ルールの範囲内であれば、その時間範囲はアクティブです。
- 時間範囲に定期ルールが 1 つまたは複数含まれている：現在の時刻が 1 つまたは複数の定期ルールの範囲内であれば、その時間範囲はアクティブです。
- 時間範囲に絶対ルールと定期ルールが両方含まれている：現在の時刻が 1 つまたは複数の絶対ルールと 1 つ以上の定期ルールの範囲内にある場合に、その時間範囲はアクティブです。

時間範囲に絶対ルールと定期ルールが両方含まれている場合、定期ルールがアクティブになるのは、最低 1 つの絶対ルールがアクティブな場合だけです。

IP 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。

IP ACL の注意事項と制約事項

IP ACL の設定に関する注意事項と制約事項は次のとおりです。

- 異なるシーケンス番号を持つ重複した ACL エントリは、設定で許可されます。ただし、これらの重複エントリはハードウェア アクセス リストにプログラムされません。
- 通常、IP パケットに対する ACL 処理は I/O モジュール上で実行されます。これには、ACL 処理を加速化するハードウェアを使用します。場合によっては、スーパーバイザ モジュールで処理が実行されることもあります。この場合、特に多数のルールが設定されている ACL を処理する際には、処理速度が遅くなることがあります。管理インターフェイス トラフィックは、常にスーパーバイザ モジュールで処理されます。次のカテゴリのいずれかに属する IP パケットがレイヤ 3 インターフェイスから出る場合、これらのパケットはスーパーバイザ モジュールに送られて処理されます。
  - IP オプションがある IPv4 パケット（他の 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）

  Cisco Nexus® 3550-T スイッチでは、リダイレクトされたパケットによってスーパーバイザ モジュールが過負荷になるのを防ぐために、ストーム制御設定が使用されます。

  ストーム制御については、トラフィック ストーム制御の設定 （51 ページ） を参照してください。

  。
- 時間範囲を使用する ACL を適用すると、デバイスは、その ACL エントリで参照される時間範囲の開始時または終了時に ACL エントリを更新します。時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。
- VTY ACL 機能はすべての VTY 回線のすべてのトラフィックを制限します。異なる VTY 回線に異なるトラフィックの制限を指定できません。どのルータの ACL も VTY ACL として設定できます。
- 出力 VTY ACL（アウトバウンド方向の VTY 回線に適用される IP ACL）は、ファイル転送プロトコル（TFTP、FTP、SCP、SFTPなど）が出力 VTY ACL 内で明示的に許可されていない限り、スイッチがファイル転送プロトコルによってファイルをコピーするのを禁止します。
- 未定義の ACL をインターフェイスに適用すると、システムは空の ACL と見なし、すべてのトラフィックを許可します。
- IP トンネルは、ACLまたはQoSポリシーをサポートしません。
- 出力方向の IPv4 ACL ロギングはサポートされていません。
- ACL ロギングは、**ip port access-group** コマンドで設定されたポート ACL と、**ip access-group** コマンドで設定されたルータ ACL にのみ適用されます。

- DoS 攻撃を防ぐため、IPv4 ACL フローの総数はユーザ定義の最大値に制限されます。この制限に到達すると、新しいログは既存のフローが終了するまで作成されません。
- IPv4 ACL ロギングによって生成される syslog エントリ数は、ACL ロギング プロセスで設定されたログ レベルによって制限されています。Syslogエントリの数がこの制限を超えると、ロギング機能が一部のロギング メッセージをドロップする場合があります。したがって、IPv4 ACL ロギングは課金ツールやACLとの一致数を正確に把握するための情報源として使用しないでください。
- レイヤ 3 の物理または論理インターフェイスに適用されるルータ ACL がマルチキャスト トラフィックとマッチしません。この動作は、Cisco Nexus® 3550-T スイッチに適用されます。
- 複数のインターフェイスに同じ QoS ポリシーと ACL が適用された場合、ラベルが共有されるのは、QoS ポリシーが no-stats オプションで適用されたときだけです。
- HTTP メソッドに基づくアクセス リストは、Cisco Nexus® 3550-T プラットフォーム スイッチおよび Cisco Nexus® 3550-T スイッチではサポートされていません。
- Cisco Nexus® 3550-T スイッチには次の注意事項と制限事項が適用されます。
  - RACLは、マルチキャスト MAC 宛先アドレスを持つパケットでは照合できません。

IP ACL のデフォルト設定

次の表に、IP ACL パラメータのデフォルト設定を示します。

***Table 8: IP ACL* パラメータのデフォルト値**

パラメータ	デフォルト
IP ACL	デフォルトでは IP ACL は存在しません。
IP ACL エントリ	1024
ACL ルール	すべての ACL に暗黙のルールが適用されます。
オブジェクト グループ	デフォルトではオブジェクト グループは存在しません。
時間範囲	デフォルトでは時間範囲は存在しません。

IP ACL の設定

IP ACL の作成

デバイスに IPv4 ACL を作成し、これにルールを追加できます。

Before you begin

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

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。
		Note ACL が有効な場合、TCP および UDP パケットのみが Cisco Nexus® 3550-T ハードウェアで処理されます。

ステップ 2	次のコマンドを入力します。 **ip access-list** *name*
	Example:
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		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	[*sequence-number*] {**permit** | **deny**} *protocol* {*source-ip-prefix* | *source-ip-mask*} {*destination-ip-prefix* | *destination-ip-mask*}	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。 IPv4 アクセス リストの場合、送信元と接続先の IPv4 プレフィックスを指定できます。これは、最初の連続するビットでのみ一致します。または、アドレスのいずれかのビットに一致する送信元と接続先の IPv4 ワイルドカード マスクを指定できます。

	Command or Action	Purpose
ステップ 4	(Optional) 次のコマンドを入力します。 **show ip access-lists***name* **Example:** `switch(config-acl)# show ip access-lists acl-01`	IP ACL の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-acl)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL の変更

既存の IPv4 ACL のルールの追加と削除は実行できますが、既存のルールを変更することはできません。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。

Before you begin

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。

Procedure

	Command or Action	Purpose

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

ステップ 2	次のコマンドを入力します。 **ip access-list** *name*
	Example:
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		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	(Optional) [*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:**	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

	Command or Action	Purpose
	`switch(config-acl)# 100 permit ip 192.168.2.0/24 any`	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。
ステップ 4	(Optional) **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*} **Example:** `switch(config-acl)# no 80`	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。
ステップ 5	(Optional) 次のコマンドを入力します。**show ip access-lists***name* **Example:** `switch(config-acl)# show ip access-lists acl-01`	IP ACL の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-acl)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

Before you begin

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。

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose
ステップ 2	**resequence** {**ip** | **ipv4**} **access-list** *name starting-sequence-number increment* **Example:** `switch(config)# resequence access-list ip acl-01 100 10`	ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。*starting-sequence-number* 引数と *increment* 引数は、1 ～ 4294967295 の整数で指定します。
ステップ 3	(Optional) **show ip access-lists** *name* **Example:** `switch(config)# show ip access-lists acl-01`	IP ACL の設定を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL の削除

IP ACL をデバイスから削除できます。

Before you begin

その 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ます。削除できるのは、現在適用されている ACL 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。デバイスは削除された ACL を空であると見なします。MAC ACL が構成されているインターフェイスを探すには、summary キーワードを指定して **show ip access-lists** コマンドを使用します。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	次のコマンドを入力します。 **no ip access-list** *name* **Example:**	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。

	Command or Action	Purpose
	`switch(config)# no ip access-list acl-01`	
ステップ 3	(Optional) 次のコマンドを入力します。 **show ip access-lists** *name* **summary** **Example:** `switch(config)# show ip access-lists acl-01 summary`	IP ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ルータ ACL としての IP ACL の適用

IPv4 ACL は、次のタイプのインターフェイスに適用できます。

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

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。

Before you begin

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

Procedure

	Command or Action	Purpose

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

ステップ 2	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*
	• **interface port-channel** *channel-number*
	Example:
	`switch(config)# interface ethernet 1/3`
	`switch(config-if)#`
		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。

	Command or Action	Purpose
ステップ 3	次のコマンドを入力します。 **ip access-group** *access-list* **Example:** `switch(config-if)# ip access-group acl1 in`	IPv4 ACL を、指定方向のトラフィックのレイヤ3インターフェイスに適用します。各方向にルータ ACL を 1 つ適用できます。
ステップ 4	(Optional) **show running-config aclmgr** **Example:** `switch(config-if)# show running-config aclmgr`	ACL の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ 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 の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip access-lists	IPv4 ACL の設定を表示します。
show running-config aclmgr [**all**]	IP ACL の設定および IP ACL が適用されるインターフェイスを含めて、ACL の実行コンフィギュレーションを表示します。

コマンド	目的
show startup-config aclmgr [**all**]	ACL のスタートアップ コンフィギュレーションを表示します。 **Note** このコマンドは、スタートアップ コンフィギュレーションのユーザ設定 ACL を表示します。**all** オプションを使用すると、スタートアップ構成のデフォルトとユーザー定義による ACL の両方が表示されます。

IP ACL の設定例

次に、acl-01 という名前の IPv4 ACL を作成して、これを RACL としてイーサネット インターフェイス 1/1（レイヤ 3 インターフェイス）に適用する例を示します。

```
ip access-list acl-01
  permit ip 192.168.2.0/24 any
interface ethernet 1/1
  ip port access-group acl-01 in
```

時間範囲の設定

時間範囲の作成

デバイス上で時間範囲を作成し、これにルールを追加できます。

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose

ステップ 2	**time-range** *name*
	Example:
	`switch(config)# time-range workday-daytime`
	`switch(config-time-range)#`
		時間範囲を作成し、時間範囲コンフィギュレーション モードを開始します。

ステップ 3	(Optional) [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time* **Example:** `switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59`	指定開始日時と終了日時の間（両端を含める）の 1 日以上の連続した曜日だけ有効になるような定期ルールを作成します。
ステップ 4	(Optional) [*sequence-number*] **periodic** *list-of-weekdays time* **to** *time* **Example:** `switch(config-time-range)# periodic weekdays 06:00:00 to 20:00:00`	*list-of-weekdays* 引数で指定された曜日の、指定開始時刻と終了時刻の間（両端を含む）だけ有効になるような定期ルールを作成します。*list-of-weekdays* 引数の値には次のキーワードも使用できます。 • **daily** ：1 週間のすべての曜日 • **weekdays** ：月曜日から金曜日まで • **weekend** ：土曜日から日曜日まで
ステップ 5	(Optional) [*sequence-number*] **absolute start** *time date* [**end** *time date*] **Example:** `switch(config-time-range)# absolute start 1:00 15 march 2013`	**start** キーワードの後ろに指定した日時から有効になる絶対基準でのルールを作成します。**end** キーワードを省略した場合、そのルールは開始日時を過ぎると常に有効になります。
ステップ 6	(Optional) [*sequence-number*] **absolute** [start *time date*] **end** *time date* **Example:** `switch(config-time-range)# absolute end 23:59:59 31 may 2013`	**end** キーワードの後ろに指定した日時まで有効になる絶対基準でのルールを作成します。**start** キーワードを省略すると、そのルールは終了日時を過ぎるまでずっと有効です。
ステップ 7	(Optional) **show time-range** *name* **Example:** `switch(config-time-range)# show time-range workday-daytime`	時間範囲の設定を表示します。
ステップ 8	(Optional) **copy running-config startup-config** **Example:** `switch(config-time-range)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲の変更

既存の時間範囲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。

Procedure

	Command or Action	Purpose

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

ステップ 2	**time-range** *name*
	Example:
	`switch(config)# time-range workday-daytime`
	`switch(config-time-range)#`
		特定の時間範囲の時間範囲コンフィギュレーション モードを開始します。

ステップ 3	(Optional) [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time* **Example:** `switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59`	指定開始日時と終了日時の間（両端を含める）の 1 日以上の連続した曜日だけ有効になるような定期ルールを作成します。
ステップ 4	(Optional) [*sequence-number*] **periodic** *list-of-weekdays time* **to** *time* **Example:** `switch(config-time-range)# 100 periodic weekdays 05:00:00 to 22:00:00`	*list-of-weekdays* 引数で指定された曜日の、指定開始時刻と終了時刻の間（両端を含む）だけ有効になるような定期ルールを作成します。*list-of-weekdays* 引数の値には次のキーワードも使用できます。 • **daily** ：1 週間のすべての曜日 • **weekdays** ：月曜日から金曜日まで • **weekend** ：土曜日から日曜日まで
ステップ 5	(Optional) [*sequence-number*] **absolute start** *time date* [**end** *time date*] **Example:** `switch(config-time-range)# absolute start 1:00 15 march 2013`	**start** キーワードの後ろに指定した日時から有効になる絶対基準でのルールを作成します。**end** キーワードを省略した場合、そのルールは開始日時を過ぎると常に有効になります。

	Command or Action	Purpose
ステップ 6	(Optional) [*sequence-number*] **absolute** [**start** *time date*] **end** *time date* **Example:** `switch(config-time-range)# absolute end 23:59:59 31 may 2013`	**end** キーワードの後ろに指定した日時まで有効になる絶対基準でのルールを作成します。**start** キーワードを省略すると、そのルールは終了日時を過ぎるまでずっと有効です。
ステップ 7	(Optional) **no** {*sequence-number* | **periodic** *arguments* . . . | **absolute** *arguments*. . . } **Example:** `switch(config-time-range)# no 80`	時間範囲から特定のルールを削除します。
ステップ 8	(Optional) **show time-range** *name* **Example:** `switch(config-time-range)# show time-range workday-daytime`	時間範囲の設定を表示します。
ステップ 9	(Optional) **copy running-config startup-config** **Example:** `switch(config-time-range)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲の削除

デバイスから時間範囲を削除できます。

Before you begin

その時間範囲が ACL ルールのいずれかに使用されているかどうかを確認します。削除できるのは、ACL ルールに使用されている時間範囲です。ACL ルールに使用されている時間範囲を削除しても、その ACL が適用されているインターフェイスの設定には影響しません。デバイスは削除された時間範囲を使用する ACL ルールを空であると見なします。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no time-range** *name* **Example:** `switch(config)# no time-range daily-workhours`	名前を指定した時間範囲を削除します。

	Command or Action	Purpose
ステップ 3	(Optional) **show time-range** **Example:** `switch(config-time-range)# show time-range`	すべての時間範囲の設定を表示します。削除された時間範囲は表示されません。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲のシーケンス番号の変更

時間範囲のルールに割り当てられているすべてのシーケンス番号を変更できます。

Procedure

	Command or Action	Purpose

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

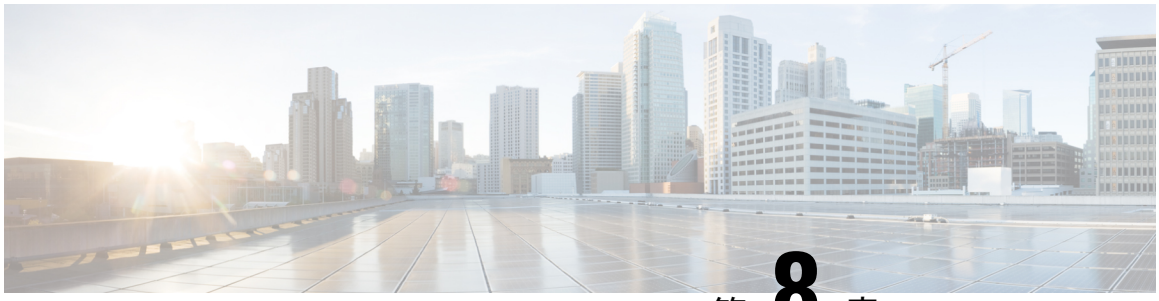
ステップ 2	**resequence time-range** *name starting-sequence-number increment*
	Example:
	`switch(config)# resequence time-range daily-workhours 100 10`
	`switch(config)#`
		時間範囲のルールにシーケンス番号を割り当てます。指定した開始シーケンス番号は最初のルールに割り当てられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。

ステップ 3	(Optional) **show time-range** *name* **Example:** `switch(config)# show time-range daily-workhours`	時間範囲の設定を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲設定の確認

時間範囲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 time-range	時間範囲の設定を表示します。
show running-config aclmgr	すべての時間範囲を含めて、ACLの設定を表示します。



第 8 章

SSH および Telnet の設定

この章では、Cisco NX-OS デバイス上でセキュア シェル（SSH）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。

この章は、次の項で構成されています。

SSH および Telnet について

ここでは、SSH および Telnet について説明します。

SSH サーバー

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

SSH がサポートするユーザ認証メカニズムには、Remote Authentication Dial-In User Service（RADIUS）、TACACS+、LDAP、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 クライアントは、SSH プロトコルで稼働しデバイス認証および暗号化を提供するアプリケーションです。Cisco NX-OS デバイスは、SSH クライアントを使用して、別の Cisco NX-OS デバイスまたは SSH サーバの稼働する他のデバイスとの間で暗号化された安全な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 NX-OS ソフトウェアの 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 NX-OS 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 サーバ 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 に対応する以下の 2 通りのキー ペアを使用できます。

- **dsa** オプションでは、SSH バージョン 2 プロトコル用の DSA キー ペアを作成します。
- **rsa** オプションでは、SSH バージョン 2 プロトコル用の RSA キー ペアを作成します。

デフォルトでは、Cisco NX-OS ソフトウェアは 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）
- Privacy-Enhanced Mail（PEM）の公開キー証明書

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

デジタル証明書を使用した SSH 認証

Cisco NX-OS デバイスでの SSH 認証では、ホスト認証用に X.509 デジタル証明書をサポートしています。X.509 デジタル証明書は、メッセージの出所と整合性を保証するデータ項目です。これには安全な通信のための暗号化されたキーが含まれています。また、発信者のアイデン

ティティを証明するために信頼できる認証局（CA）によって署名されています。X.509デジタル証明書のサポートにより、認証に DSA と RSA のいずれかのアルゴリズムを使用します。

証明書のインフラストラクチャでは、Secure Socket Layer（SSL）に対応し、セキュリティインフラストラクチャによってクエリーまたは通知を通じて最初に返される証明書が使用されます。証明書が信頼できる CA のいずれかで設定されており、無効にされたり期限が切れたりしていなければ、証明書の検証は成功します。

X.509 証明書を使用する SSH 認証用にデバイスを設定できます。認証に失敗した場合は、パスワードの入力が求められます。

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。

デフォルトでは、Telnet サーバが Cisco NX-OS デバイス上でディセーブルになっています。

SSH および Telnet の前提条件

レイヤ 3 インターフェイス上で IP、mgmt 0 インターフェイス上でアウトバンド、またはイーサネット インターフェイス上でインバンドを設定していることを確認します。

SSH と Telnet の注意事項と制約事項

SSH および Telnet に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS ソフトウェアは、SSH バージョン 2（SSHv2）だけをサポートしています。
- **no feature ssh feature** コマンドを使用すると、ポート 22 はディセーブルになりません。ポート 22 は常にオープンで、すべての着信外部接続を拒否する拒否ルールがプッシュされます。
- Poodle の脆弱性により、SSLv3 はサポートされなくなりました。
- IPSG は、次のものではサポートされません。
  - Cisco Nexus® 3550-T スイッチの最後の 6 個の 40 Gb 物理ポート
  - Cisco Nexus® 3550-T スイッチのすべての 40 Gb 物理ポート
- X.509 証明書を使用する SSH 認証用にデバイスを設定できます。認証に失敗した場合は、パスワードの入力が求められます。
- SFTP サーバ機能では、通常の SFTP の **chown** および **chgrp** コマンドを発行します。

- SFTP サーバが有効になっている場合は、admin ユーザだけが SFTP を使用してデバイスにアクセスできます。
- SSH パスワードレス ファイル コピーを目的として AAA プロトコル（RADIUS や TACACS+ など）を介してリモート認証されたユーザ アカウントにインポートされた SSH 公開キーと秘密キーは、同じ名前のローカル ユーザ アカウントでない限り、Nexus デバイスがリロードされると保持されません。リモート ユーザ アカウントは、SSH キーがインポートされる前にデバイスで設定されます。
- SSH のタイムアウト時間は、tac-pac の生成時間よりも長くする必要があります。そうでないと、VSH ログに %VSHD-2-VSHD_SYSLOG_EOL_ERR エラーが記録されることがあります。理想的には、tac-pac または showtech を収集する前に 0（無限）に設定します。

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

SSH および Telnet のデフォルト設定

次の表に、SSH および Telnet パラメータのデフォルト設定を示します。

Table 9: デフォルトの ***SSH*** および ***Telnet*** 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	ディセーブル
Telnet ポート番号	23
SSH ログインの最大試行回数	3
SCP サーバ	ディセーブル
SFTP サーバ	ディセーブル

SSH の設定

ここでは、SSH の設定方法について説明します。

SSH サーバ キーの生成

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

Procedure

	Command or Action	Purpose

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

ステップ 2	**no feature ssh** **Example:** `switch(config)# no feature ssh`	SSH を無効にします。
ステップ 3	**feature ssh** **Example:** `switch(config)# feature ssh`	SSH を有効にします。

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

ステップ 5	(Optional) **show ssh key** [**dsa** | **rsa** |] [] **Example:** `switch# show ssh key`	SSH サーバ キーを表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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、次のいずれかの形式で指定できます。

- OpenSSH 形式
- Internet Engineering Task Force（IETF）SECSH 形式

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。

Before you begin

IETF SCHSH 形式の SSH 公開キーを作成します。

Procedure

	Command or Action	Purpose
ステップ 1	**copy** *server-file* **bootflash:***filename* **Example:** `switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub`	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。サーバは FTP、Secure Copy（SCP）、Secure FTP（SFTP）、または TFTP のいずれかを使用できます。
ステップ 2	**configure terminal** **Example:** `switch# configure terminal switch(config)#`	グローバル コンフィギュレーション モードを開始します
ステップ 3	**username** *username* **sshkey file bootflash:***filename* **Example:** `switch(config)# username User1 sshkey file bootflash:secsh_file.pub`	IETF SECSH 形式の SSH 公開キーを設定します。
ステップ 4	**exit** **Example:** `switch(config)# exit switch#`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	(Optional) **show user-account** **Example:** `switch# show user-account`	ユーザアカウントの設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

OpenSSH 形式の SSH 公開キーの指定

ユーザ アカウントに OpenSSH 形式の SSH 公開キーを指定できます。

Before you begin

OpenSSH 形式の SSH 公開キーを作成します。

Procedure

	Command or Action	Purpose

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

ステップ 2	**username** *username* **sshkey** *ssh-key*
	Example:
	`switch(config)# username User1 sshkey ssh-rsa`
	`AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPj`
	`hOBYmsi6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+`
	`XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5S4Tplx8=`
		OpenSSH 形式の SSH 公開キーを設定します。

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

ステップ 4	(Optional) **show user-account** **Example:** `switch# show user-account`	ユーザアカウントの設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH ログイン試行の最大回数の設定

SSH ログイン試行の最大回数を設定できます。許可される試行の最大回数を超えると、セッションが切断されます。

Note ログイン試行の合計回数には、公開キー認証、証明書ベースの認証、およびパスワードベースの認証を使用した試行が含まれます。イネーブルにされている場合は、公開キー認証が優先されます。証明書ベースとパスワード ベースの認証だけがイネーブルにされている場合は、証明書ベースの認証が優先されます。これらすべての方法で、ログイン試行の設定された数を超えると、認証失敗回数を超過したことを示すメッセージが表示されます。

Procedure

	Command or Action	Purpose

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

ステップ 2	**ssh login-attempts** *number* **Example:** `switch(config)# ssh login-attempts 5`	ユーザが SSH セッションへのログインを試行できる最大回数を設定します。ログイン試行のデフォルトの最大回数は3です。値の範囲は 1 ～ 10 です。 **Note** このコマンドの **no** 形式を使用すると、以前のログイン試行の値が削除され、ログイン試行の最大回数がデフォルト値の 3 に設定されます。
ステップ 3	(Optional) **show running-config security all** **Example:** `switch(config)# show running-config security all`	SSH ログイン試行の設定された最大回数を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SSH セッションの開始

Cisco NX-OS デバイスから IPv4 を使用して SSH セッションを開始し、リモート デバイスと接続します。

Before you begin

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。

リモート デバイスの SSH サーバを有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	**ssh** [*username@*]{*ipv4-address* | *hostname*} **Example:** `switch# ssh 10.10.1.1`	IPv4 を使用してリモート デバイスとの SSH IPv4 セッションを作成します。

ブート モードからの SSH セッションの開始

SSH セッションは、リモート デバイスに接続する Cisco NX-OS デバイスのブート モードから開始できます。

Before you begin

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。

リモート デバイスの SSH サーバを有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	**ssh** [*username@*]*hostname* **Example:** `switch(boot)# ssh user1@10.10.1.1`	リモート デバイスへの SSH セッションを、Cisco NX-OS デバイスのブート モードから作成します。
ステップ 2	**exit** **Example:** `switch(boot)# exit`	ブート モードを終了します。
ステップ 3	**copy scp:**//[*username@*]*hostname*/*filepath directory* **Example:** `switch# copy scp://user1@10.10.1.1/users abc`	セキュア コピー プロトコル（SCP）を使用して、ファイルを Cisco NX-OS デバイスからリモート デバイスへコピーします。

SSH のパスワードが不要なファイル コピーの設定

Cisco NX-OS デバイスから Secure Copy（SCP）サーバまたは Secure FTP（SFTP）サーバに、パスワードなしでファイルをコピーすることができます。これを行うには、SSH による認証用の公開キーと秘密キーで構成される RSA または DSA のアイデンティティを作成する必要があります。

Procedure

	Command or Action	Purpose

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

ステップ 2	[**no**] **username** *username* **keypair generate** {**rsa** [*bits* [**force**]] | **dsa** [**force**]} **Example:** `switch(config)# username user1 keypair generate rsa 2048 force`	SSH の公開キーと秘密キーを生成し、指定したユーザの Cisco NX-OS デバイスのホーム ディレクトリ（$HOME/.ssh）に格納します。Cisco NX-OS デバイスでは、これらのキーを使用してリモート マシンの SSH サーバと通信します。 *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、**force** キーワードを使用します。**force** キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーは生成されません。
ステップ 3	(Optional) **show username** *username* **keypair** **Example:** `switch(config)# show username user1 keypair`	指定したユーザの公開キーを表示します。 **Note** セキュリティ上の理由から、このコマンドで秘密キーは表示されません。
ステップ 4	Required: **username** *username* **keypair export** {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**] **Example:** `switch(config)# username user1 keypair export bootflash:key_rsa rsa`	Cisco NX-OS デバイスのホーム ディレクトリから、指定したブートフラッシュ ディレクトリまたは一時ディレクトリに、公開キーと秘密キーをエクスポートします。

	Command or Action	Purpose
		既存のキーを置き換える場合は、**force** キーワードを使用します。**force** キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーはエクスポートされません。 生成したキー ペアをエクスポートするとき、秘密キーを暗号化するパスフレーズを入力するように求められます。秘密キーは、指定したファイルとしてエクスポートされ、公開キーは、同じファイル名に .pub 拡張子を付けてエクスポートされます。これで、このキー ペアを任意の Cisco NX-OS デバイスにコピーし、SCP または SFTP を使用してサーバのホーム ディレクトリに公開キー ファイル（*.pub）をコピーできるようになります。 **Note** セキュリティ上の理由から、このコマンドはグローバル コンフィギュレーション モードでしか実行できません。
ステップ 5	Required: **username** *username* **keypair import** {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**] **Example:** `switch(config)# username user1 keypair import bootflash:key_rsa rsa`	指定したブートフラッシュ ディレクトリまたは一時ディレクトリから、Cisco NX-OS デバイスのホーム ディレクトリに、エクスポートした公開キーと秘密キーをインポートします。 既存のキーを置き換える場合は、**force** キーワードを使用します。**force** キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーはインポートされません。 生成したキー ペアをインポートするとき、秘密キーを復号化するパスフレーズを入力するように求められます。秘密キーは指定したファイルとしてインポートされ、公開キーは同じファイル名に .pub 拡張子を付けてインポートされます。

	Command or Action	Purpose
		Note セキュリティ上の理由から、このコマンドはグローバル コンフィギュレーション モードでしか実行できません。 **Note** パスワードなしでサーバにアクセスできるのは、サーバでキーが設定されているユーザのみです。

What to do next

SCP サーバまたは SFTP サーバで、次のコマンドを使用して、*.pub ファイル（たとえば、key_rsa.pub）に格納された公開キーを authorized_keys ファイルに追加します。

$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys

これで、標準の SSH コマンドおよび SCP コマンドを使用してパスワードを指定しなくても、Cisco NX-OS デバイスからサーバにファイルをコピーできます。

SCP サーバと SFTP サーバの設定

リモートデバイスとの間でファイルをコピーできるように、Cisco NX-OS デバイスで SCP サーバまたは SFTP サーバを設定できます。SCP サーバまたは SFTP サーバをイネーブルにした後、Cisco NX-OS デバイスとの間でファイルをコピーするために、リモート デバイスで SCP または SFTP コマンドを実行できます。

Note arcfour および blowfish cipher オプションは SCP サーバではサポートされません。

Procedure

	Command or Action	Purpose

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

ステップ 2	**[no] feature scp-server** **Example:** `switch(config)# feature scp-server`	Cisco NX-OS デバイス上で SCP サーバをイネーブルまたはディセーブルにします。

	Command or Action	Purpose
ステップ 3	Required: [**no**] **feature sftp-server** **Example:** `switch(config)# feature sftp-server`	Cisco NX-OS デバイス上で SFTP サーバをイネーブルまたはディセーブルにします。

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

ステップ 5	(Optional) **show running-config security** **Example:** `switch# show running-config security`	SCP サーバと SFTP サーバの設定ステータスを表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

X.509v3 証明書ベースの SSH 認証の設定

X.509v3 証明書を使用する SSH 認証を設定できます。

始める前に

リモート デバイスの SSH サーバをイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**username** *user-id* [**password** [**0** | **5**] *password*] 例： `switch(config)# username jsmith password 4Ty18Rnt`	ユーザ アカウントを設定します。*user-id* 引数は、最大 28 文字の英数字で、大文字と小文字が区別されます。指定できる文字は、A ～ Z の英大文字、a ～ z の英小文字、0 ～ 9 の数字、ハイフン（-）、ピリオド（.）、アンダースコア（_）、プラス符号（+）、および等号（=）です。アット マーク（@）はリモート ユーザ名では使用で

	コマンドまたはアクション	目的
		きますが、ローカルユーザ名では使用できません。 ユーザ名の先頭は英数字で始まる必要があります。 デフォルトパスワードは定義されていません。オプションの **0** は、パスワードがクリア テキストであり、**5** はパスワードが暗号化されていることを意味します。デフォルトは **0**（クリア テキスト）です。 （注） パスワードを指定しなかった場合、ユーザは Cisco NX-OS デバイスにログインできません。 （注） 暗号化パスワードオプションを使用してユーザアカウントを作成する場合、対応する SNMP ユーザは作成されません。
ステップ 3	**username** *user-id* **ssh-cert-dn** *dn-name* {**dsa** | **rsa**} 例： `switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa`	既存のユーザアカウント認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。識別名は最大 512 文字で、例に示す形式に従う必要があります。電子メールアドレスと状態がそれぞれ emailAddress と ST に設定されていることを確認します。

ステップ 4	[**no**] **crypto ca trustpoint** *trustpoint*
	例：
	`switch(config)# crypto ca trustpoint winca`
	`switch(config-trustpoint)#`
		トラストポイントを設定します。
		（注） このコマンドの **no** 形式を使用してトラストポイントを削除する前に、まず **delete crl** および **delete ca-certificate** コマンドを使用して、CRL および CA 証明書を削除する必要があります。

ステップ 5	**crypto ca authenticate** *trustpoint* 例：	トラストポイントの CA 証明書を設定します。

	コマンドまたはアクション	目的
	`switch(config-trustpoint)# crypto ca authenticate winca`	（注） CA 証明書を削除するには、トラストポイント コンフィギュレーション モードで **delete ca-certificate** コマンドを入力します。
ステップ 6	（任意） **crypto ca crl request** *trustpoint* **bootflash:***static-crl***.crl** 例： `switch(config-trustpoint)# crypto ca crl request winca bootflash:crllist.crl`	この項はオプションですが、強く推奨されます。トラストポイントの証明書失効リスト（CRL）を設定します。CRL ファイルは、トラストポイントによって失効した証明書のリストのスナップショットです。このスタティック CRL リストは、認証局（CA）からデバイスに手動でコピーされます。 （注） スタティック CRL は、サポートされている唯一の失効チェック方式です。 （注） CRL を削除するには、**delete crl** コマンドを入力します。
ステップ 7	（任意） **show crypto ca certificates** 例： `switch(config-trustpoint)# show crypto ca certificates`	設定されている証明書またはチェーンと、関連付けられているトラストポイントを表示します。
ステップ 8	（任意） **show crypto ca crl** *trustpoint* 例： `switch(config-trustpoint)# show crypto ca crl winca`	指定したトラストポイントの CRL リストの内容を表示します。
ステップ 9	（任意） **show user-account** 例： `switch(config-trustpoint)# show user-account`	設定されたユーザアカウントの詳細を表示します。
ステップ 10	（任意） **show users** 例： `switch(config-trustpoint)# show users`	デバイスにログオンしているユーザが表示されます。
ステップ 11	（任意） **copy running-config startup-config** 例：	実行コンフィギュレーションを、スタートアップ 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
	`switch(config-trustpoint)# copy running-config startup-config`	

レガシー SSH アルゴリズム サポートの設定

レガシーSSHセキュリティアルゴリズム、メッセージ認証コード（MAC）、キータイプ、および暗号のサポートを設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	（任意） **ssh kexalgos** [**all**] 例： `switch(config)# ssh kexalgos all`	接続ごとのキーの生成に使用されるキー交換方式である、サポートされているすべての KexAlgorithms を有効にするには、 **all** キーワードを使用します。 サポートされる KexAlgorithmn は次のとおりです。 • curve25519-sha256 • diffie-hellman-group-exchange-sha256 • diffie-hellman-group1-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group1-sha1 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384
ステップ 3	（任意） **ssh macs all** 例： `switch(config)# ssh macs all`	トラフィック変更の検出に使用されるメッセージ認証コードである、サポートされているすべてのMACを有効にします。 サポートされる MAC は次のとおりです。 • hmac-sha1

	コマンドまたはアクション	目的
ステップ 4	（任意） **ssh ciphers** [**all**] 例： `switch(config)# ssh ciphers all`	サポートされているすべての暗号を有効にして接続を暗号化するには、 **all** キーワードを使用します。 サポート対象の暗号方式： • aes128-cbc • aes192-cbc • aes256-cbc • aes128-ctr • aes192-ctr • aes256-ctr • aes256-gcm@openssh.com • aes128-gcm@openssh.com
ステップ 5	（任意） **ssh keytypes all** 例： `switch(config)# ssh keytypes all`	サーバがクライアントに対して自身を認証するために使用できる公開キー アルゴリズムである、サポートされているすべての PubkeyAcceptedKeyType を有効にします。 サポートされるキー タイプは次のとおりです。 • ssh-dss • ssh-rsa

サポートされるアルゴリズム：FIPモードが有効の場合

FIP モードが有効な場合にサポートされるアルゴリズムのリストは次のとおりです。

表 *10*：サポートされるアルゴリズム：*FIP*モードが有効の場合

アルゴリズム	サポート対象	サポート対象外
ciphers	• aes128-ctr • aes256-ctr • aes256-gcm@openssh.com • aes128-gcm@openssh.com	• aes192-ctr • aes128-cbc • aes192-cbc • aes256-cbc

アルゴリズム	サポート対象	サポート対象外
hmac	• hmac-sha2-256 • hmac-sha2-512 • hmac-sha1	• hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • hmac-sha1-etm@openssh.com
kexalgo	• ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group16-sha512 • diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256	• curve25519-sha256 • curve25519-sha256@libssh.org
keytypes	• rsa-sha2-256 • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521	ssh-rsa

デフォルトの SSH サーバ ポートの変更

SSHv2 のポート番号をデフォルトのポート番号 22 から変更できます。。デフォルトの SSH ポートの変更時に使用される暗号化により、より強力なプライバシーとセッション整合性をサポートする接続が実現します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**no feature ssh** 例： `switch(config)# no feature ssh`	SSH を無効にします。
ステップ 3	**show sockets** *local-port-range* 例：	使用可能なポート範囲を表示します。

	コマンドまたはアクション	目的
	`switch(config)# show sockets local port range (15001 - 58000)` `switch(config)# local port range (58001 - 63535) and nat port range (63536 - 65535)`	
ステップ 4	**ssh port** *local-port* 例： `switch(config)# ssh port 58003`	ポートを設定します。
ステップ 5	**feature ssh** 例： `switch(config)# feature ssh`	SSH を有効にします。

ステップ 6	**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 7	（任意） **show running-config security all** 例： `switch# ssh port 58003`	セキュリティの設定を表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH ホストのクリア

サーバから SCP または SFTP を使用してファイルをダウンロードする場合、またはこのデバイスからリモート ホストに SSH セッションを開始する場合には、そのサーバと信頼できる SSH 関係が確立されます。ユーザ アカウントの、信頼できる SSH サーバのリストはクリアすることができます。

Procedure

	Command or Action	Purpose
ステップ 1	**clear ssh hosts** **Example:** `switch# clear ssh hosts`	SSH ホスト セッションおよび既知のホスト ファイルをクリアします。

SSH サーバのディセーブル化

Cisco NX-OS 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。SSH サーバをディセーブルにすると、SSH でスイッチにアクセスすることを防止できます。

Procedure

	Command or Action	Purpose

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

ステップ 2	**no feature ssh** **Example:** `switch(config)# no feature ssh`	SSH を無効にします。

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

ステップ 4	(Optional) **show ssh server** **Example:** `switch# show ssh server`	SSH サーバの設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ 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、Cisco NX-OS デバイス上の SSH サーバ キーを削除できます。

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

Procedure

	Command or Action	Purpose

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

ステップ 2	**no feature ssh** **Example:** `switch(config)# no feature ssh`	SSH を無効にします。

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

ステップ 4	(Optional) **show ssh key** **Example:** `switch# show ssh key`	SSH サーバ キーの設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

SSH サーバ キーの生成 （109 ページ）

SSH セッションのクリア

Cisco NX-OS デバイスから SSH セッションをクリアできます。

Procedure

	Command or Action	Purpose
ステップ 1	**show users** **Example:** `switch# show users`	ユーザ セッション情報を表示します。
ステップ 2	**clear line** *vty-line* **Example:** `switch(config)# clear line pts/12`	ユーザSSHセッションをクリアします。

Telnet の設定

ここでは、Cisco NX-OS デバイスで Telnet を設定する手順を説明します。

Telnet サーバのイネーブル化

Cisco NX-OS デバイス上で Telnet サーバをイネーブルにできます。デフォルトでは、Telnet はディセーブルです。

Procedure

	Command or Action	Purpose

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

ステップ 2	**feature telnet** **Example:** `switch(config)# feature telnet`	Telnet サーバをイネーブルにします。デフォルトではディセーブルになっています。

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

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

リモート デバイスとの Telnet セッションの開始

Cisco NX-OS デバイスから SSH セッションを開始して、リモート デバイスと接続できます。IPv4 のいずれかを使用して Telnet セッションを開始できます。

Before you begin

リモート デバイスのホスト名または IP アドレスと、必要な場合はリモート デバイスのユーザ名を取得します。

Cisco NX-OS デバイス上で Telnet サーバを有効にします。

リモート デバイス上で Telnet サーバを有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	**telnet** {*ipv4-address* | *host-name*} [*port-number*] **Example:** `switch# telnet 10.10.1.1`	IPv4 を使用してリモート デバイスとの Telnet セッションを開始します。デフォルトのポート番号は 23 です。値の範囲は 1 ～ 65535 です。

Related Topics

Telnet サーバのイネーブル化 （126 ページ）

Telnet セッションのクリア

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

Before you begin

Cisco NX-OS デバイス上で Telnet サーバをイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	**show users** **Example:** `switch# show users`	ユーザ セッション情報を表示します。
ステップ 2	**clear line** *vty-line* **Example:** `switch(config)# clear line pts/12`	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 および Telnet 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 ssh key [**dsa** | **rsa**] []	SSH サーバ キーを表示します。

コマンド	目的
show running-config security [**all**]	実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。**all** キーワードを指定すると、SSH およびユーザアカウントのデフォルト値が表示されます。
show ssh server	SSH サーバの設定を表示します。
show telnet server	Telnet サーバの設定を表示します。
show username *username* **keypair**	指定したユーザの公開キーを表示します。
show user-account	設定されたユーザ アカウントの詳細を表示します。
show users	デバイスにログオンしているユーザが表示されます。

SSH の設定例

次の例は、OpenSSH キーを使用して SSH を設定する方法を示しています。

Procedure

ステップ 1 SSH サーバをディセーブルにします。

Example:

```
switch# configure terminal
switch(config)# no feature ssh
```

ステップ 2 SSH サーバ キーを生成します。

Example:

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

ステップ 3 SSH サーバをイネーブルにします。

Example:

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

ステップ 4 SSH サーバ キーを表示します。

Example:

ステップ 5 OpenSSH 形式の SSH 公開キーを指定します。

Example:

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50r
v7gsEPjhOBYmsi6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5
4Tplx8=
```

ステップ 6 設定を保存します。

Example:

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

SSH のパスワードが不要なファイル コピーの設定例

次に、Cisco NX-OS デバイスから Secure Copy（SCP）サーバまたは Secure FTP（SFTP）サーバに、パスワードなしでファイルをコピーする例を示します。

Procedure

ステップ 1 SSH の公開キーと秘密キーを生成し、指定したユーザの Cisco NX-OS デバイスのホーム ディレクトリに格納します。

Example:

```
switch# configure terminal
switch(config)# username admin keypair generate rsa
generating rsa key(1024 bits)......
generated rsa key
```

ステップ 2 指定したユーザの公開キーを表示します。

Example:

```
switch(config)# show username admin keypair

**************************************

rsa Keys generated: Thu Jul  9 11:10:29 2013

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************

could not retrieve dsa key information
**************************************
```

ステップ 3 Cisco NX-OS デバイスのホーム ディレクトリから、指定したブートフラッシュ ディレクトリに、公開キーと秘密キーをエクスポートします。

Example:

```
switch(config)# username admin keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
.
.
        951     Jul 09 11:13:59 2013  key_rsa
        221     Jul 09 11:14:00 2013  key_rsa.pub
.
.
```

ステップ 4 これら 2 つのファイルを他の Cisco NX-OS デバイスへコピーした後、**copy scp** または **copy sftp** コマンドを使用して、Cisco NX-OS デバイスのホーム ディレクトリにインポートします。

Example:

```
switch(config)# username admin keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# show username admin keypair
**************************************

rsa Keys generated: Thu Jul  9 11:10:29 2013

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************

could not retrieve dsa key information
**************************************
switch(config)#
```

ステップ 5 SCP サーバまたは SFTP サーバで、key_rsa.pub に格納されている公開キーを authorized_keys ファイルに追加します。

Example:

```
$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys
```

これで、標準の SSH コマンドおよび SCP コマンドを使用してパスワードを指定しなくても、Cisco NX-OS デバイスからサーバにファイルをコピーできます。

ステップ 6 (Optional) DSA キーについてこの手順を繰り返します。

X.509v3 証明書ベースの SSH 認証の設定例

次の例は、X.509v3 証明書を使用する SSH 認証の設定方法を示しています。

```
configure terminal
username jsmith password 4Ty18Rnt
username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith"
 rsa
crypto ca trustpoint tp1
crypto ca authenticate tp1
crypto ca crl request tp1 bootflash:crl1.crl

show crypto ca certificates
Trustpoint: tp1
CA certificate 0:
subject= /CN=SecDevCA
issuer= /CN=SecDevCA
serial=01AB02CD03EF04GH05IJ06KL07MN
notBefore=Jun 29 12:36:26 2016 GMT
notAfter=Jun 29 12:46:23 2021 GMT
SHA1 Fingerprint=47:29:E3:00:C1:C1:47:F2:56:8B:AC:B2:1C:64:48:FC:F4:8D:53:AF
purposes: sslserver sslclient

show crypto ca crl tp1
Trustpoint: tp1 CRL: Certificate Revocation List (CRL):
    Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: /CN=SecDevCA
    Last Update: Aug 8 20:03:15 2016 GMT
    Next Update: Aug 16 08:23:15 2016 GMT
    CRL extensions:
        X509v3 Authority Key Identifier:
            keyid:30:43:AA:80:10:FE:72:00:DE:2F:A2:17:E4:61:61:44:CE:78:FF:2A

show user-account
user:user1
        this user account has no expiry date
        roles:network-operator
        ssh cert DN : /C = US, ST = New York, L = Metropolis, O = cisco , OU = csg, CN
= user1; Algo: x509v3-sign-rsa

show users
NAME      LINE        TIME          IDLE      PID         COMMENT
user1     pts/1       Jul 27 18:43  00:03     18796      (10.10.10.1)   session=ssh
```

SSH および Telnet に関する追加情報

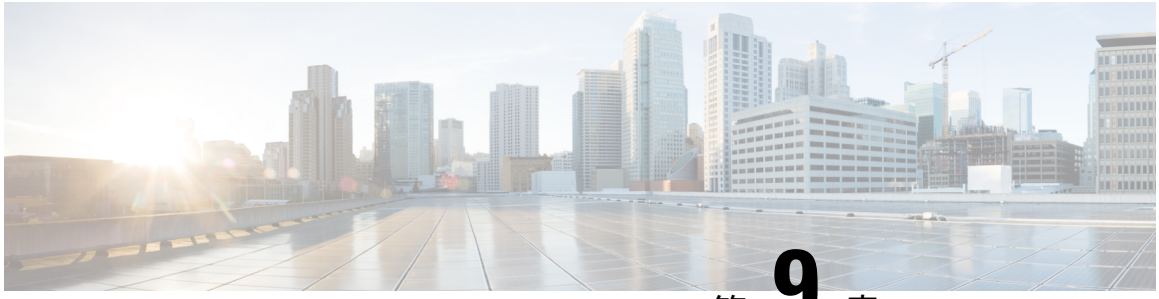
ここでは、SSH および Telnet の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	*Cisco NX-OS* ライセンス ガイド
VRF コンフィギュレーション	*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成ガイド

MIB

MIB	MIB のリンク
SSH および Telnet に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 9 章

DHCP の設定

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

この章は、次の項で構成されています。

DHCP クライアントについて

DHCP クライアント機能によって、インターフェイスに IPv4 アドレスを構成できます。インターフェイスには、管理ポート、およびスイッチ仮想インターフェイス（SVI）が含まれます。

DHCP の注意事項と制約事項

DHCP 設定時の注意事項と制約事項は次のとおりです。

- POAP の安全性を確保するために、DHCP スヌーピングが有効であることを確認し、ファイアウォール ルールを設定して意図しない、または悪意のある DHCP サーバをブロックしてください。

（注） 安全な POAP を構成するには、ファイアウォール ルールを正しく設定する必要があります。

（注） DHCP 構成制限については、『*Cisco Nexus 3550-T* 検証済み拡張性ガイド』を参照してください。

DHCP の設定

DHCP クライアントの有効化

DHCP クライアント機能によって、管理インターフェイスに IPv4 アドレスを構成できます。

（注） DHCP クライアントは DHCP リレー プロセスに依存しないため、**feature dhcp** コマンドを有効にする必要はありません。

手順

	コマンドまたはアクション	目的

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

ステップ 2	次のどちらかを選択します。
	• **interface mgmt 0**
	例：
	`switch(config)# interface mgmt. 0`
	`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、DHCPクライアント機能を有効にするインターフェイスとして管理インターフェイスを指定します。

ステップ 3	**[no] {ip } address dhcp** 例： `switch(config-if)# ip address dhcp`	インターフェイスに IPv4 アドレスを割り当てます。 IP を削除するには、このコマンドの **no** 形式を使用します。
ステップ 4	（任意） 次の手順を実行します。 • **show running-config interface mgmt 0** 例： `switch(config-if)# show running-config interface mgmt. 0`	実行コンフィギュレーションのインターフェイスに割り当てられた IPv4 アドレスを表示します。

	コマンドまたはアクション	目的
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 {**ip**} **address dhcp** コマンドだけが保持されます。割り当てられたIPアドレスは、実行コンフィギュレーションに表示されても保存されません。

DHCP クライアントの設定例

次に、DHCP クライアント機能を使用して VLAN インターフェイスに IPv4 アドレスを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# no shutdown
switch(config-if)# ip address dhcp
switch(config-if)# show running-config interface vlan 7
interface Vlan7
no shutdown
ip address dhcp
```

DHCP に関する追加情報

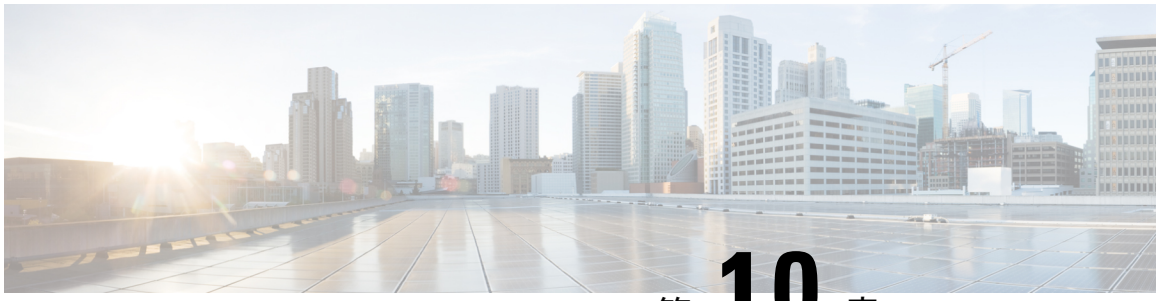
関連資料

関連項目	マニュアル タイトル
レイヤ 3 仮想化	『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』

標準

第 III 部

Cisco Nexus 3550-T システム管理の構成ガイド



第 10 章

システム管理の概要

ソフトウェア イメージ

Cisco NX-OS ソフトウェアは、1 つの NXOS ソフトウェア イメージで構成されています。このイメージは、すべての Cisco Nexus 3550-T スイッチで実行されます。

ライセンス要件

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

Cisco Discovery Protocol

Cisco Discovery Protocol（CDP）を使用して、デバイスに直接接続されているすべてのシスコ製機器を検出し、情報を表示できます。CDP は、ルータ、ブリッジ、アクセス サーバ、コミュニケーション サーバ、スイッチを含む、シスコ製のあらゆる機器で動作します。CDP は、メディアにもプロトコルにも依存せず、ネイバー デバイスのプロトコル アドレスを収集し、各デバイスのプラットフォームを検出します。CDP の動作はデータリンク層上に限定されます。異なるレイヤ 3 プロトコルをサポートする 2 つのシステムで相互学習が可能です。

LLDP

リンク層検出プロトコル（LLDP）はベンダーに依存しない、単一方向のデバイス ディスカバリ プロトコルです。このプロトコルでは、ネットワーク上の他のデバイスにネットワーク デ

バイスから固有の情報をアドバタイズできます。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する2つのシステムで互いの情報を学習できます。LLDPはグローバルに、またはインターフェイスごとにイネーブルにすることができます。

第 11 章

CDP の設定

この章では、Cisco NX-OS デバイス上で Cisco Discovery Protocol（CDP）を設定する方法について説明します。

この章は、次の項で構成されています。

CDP について

Cisco Discovery Protocol（CDP）は、ルータ、ブリッジ、アクセス サーバ、コミュニケーション サーバ、スイッチを含め、シスコ製のあらゆる機器で動作する、メディアにもプロトコルにも依存しないプロトコルです。CDP を使用すると、デバイスに直接接続されているすべてのシスコ デバイスの情報を検出して表示できます。

CDP はネイバー デバイスのプロトコル アドレスを収集し、各デバイスのプラットフォームを検出します。CDP の動作はデータリンク層上に限定されます。異なるレイヤ 3 プロトコルをサポートする 2 つのシステムで相互学習が可能です。

CDP が設定された各デバイスは、マルチキャスト アドレスに定期的にアドバタイズメントを送信します。各デバイスは、SNMP メッセージを受信できるアドレスを少なくとも 1 つアドバタイズします。アドバタイズメントには保持時間情報も含まれます。保持時間は、受信デバイスが CDP 情報を削除するまでに保持する時間の長さを表します。アドバタイズメントまたはリフレッシュ タイマーおよびホールド タイマーを設定できます。

CDP Version-2（CDPv2）では、接続デバイスとの間でネイティブ VLAN ID またはポート デュプレックス ステートが一致していないインスタンスを追跡できます。

CDP では、次の Type-Length-Value（TLV）フィールドがアドバタイズされます。

- デバイス ID

- アドレス
- ポート ID
- 機能
- バージョン
- プラットフォーム
- ネイティブ VLAN
- 全二重/半二重
- SysName
- SysObjectID
- 管理アドレス
- Physical Location

すべての CDP パケットに VLAN ID が含まれます。レイヤ 2 アクセス ポート上で CDP を設定した場合、そのアクセス ポートから送信される CDP パケットには、アクセス ポートの VLAN ID が含まれます。レイヤ 2 トランク ポート上で CDP を設定した場合は、そのトランク ポートから送信される CDP パケットに、トランク ポート上で許可設定されている最小の VLAN ID が含まれます。トランク ポートは、そのトランク ポートの許可 VLAN リストに指定されている VLAN ID であれば、どの VLAN ID が含まれている CDP パケットでも受信できます。VLAN については、「*Cisco Nexus® 3550-T Layer 2 Switching* 構成」のセクションを参照してください。

高可用性

Cisco NX-OS は、CDP のステートフルおよびステートレス両方のリスタートをサポートします。

CDP の注意事項と制約事項

CDP に関する設定時の注意事項および制約事項は、次のとおりです。

- 接続数が 256 のハブにポートを接続した場合、CDP はポートあたり最大 256 のネイバーを検出できます。
- デバイス上で CDP をイネーブルにする必要があります。イネーブルにしておかないと、インターフェイス上で CDP をイネーブルにできません。
- CDP を設定できるのは、物理インターフェイスおよびポート チャネル上に限られます。

CDP のデフォルト設定

次の表に、CDP パラメータのデフォルト設定を示します。

パラメータ	デフォルト
CDP	グローバルおよびすべてのインターフェイスでイネーブル
CDP version	バージョン 2
CDP device ID	シリアル番号
CDP timer	60 秒
CDP hold timer	180 秒

CDP の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があります。

CDP のグローバルな有効化または無効化

CDP はデフォルトで有効になっています。CDP をディセーブルにしてから、もう一度イネーブルにできます。

インターフェイス上で CDP をイネーブルにするには、先にデバイス上で CDP をイネーブルにしておく必要があります。CDP がグローバルなディセーブルになっているときに、特定のインターフェイス上で CDP をイネーブルにしても、これらのインターフェイス上で CDP がアクティブになることはなく、エラー メッセージが戻ります。

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **cdp enable** 例： `switch(config)# cdp enable`	デバイス全体で CDP 機能を有効または無効にします。デフォルトでは有効。

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

インターフェイス上での CDP の有効化または無効化

CDP はデフォルトで、インターフェイス上でイネーブルです。インターフェイス上で CDP をディセーブルにできます。

CDP がグローバルなディセーブルになっているときに、特定のインターフェイス上で CDP をイネーブルにしても、これらのインターフェイス上で CDP がアクティブになることはなく、エラー メッセージが戻ります。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface slot/port*
	例：
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	[**no**] **cdp enable** 例： `switch(config-if)# cdp enable`	このインターフェイスで CDP を有効または無効にします。デフォルトでは有効。 （注） CDP がデバイス上でグローバルに有効になっていることを確認します。
ステップ 4	（任意） **show cdp interface** *interface slot/port* 例： `switch(config-if)# show cdp interface ethernet 1/2`	インターフェイスの CDP 情報を表示します。

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

CDP オプション パラメータの設定

この手順でオプションのコマンドを使用して CDP を変更できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	（任意） **cdp advertise** {**v1** | **v2**} 例： `switch(config)# cdp advertise v1`	デバイスがサポートする CDP のバージョンを設定します。デフォルトは v2 です。
ステップ 3	（任意） **cdp format device-id** {**mac-address** | **serial-number** | **system-name**} 例： `switch(config)# cdp format device-id mac-address`	CDP デバイス ID を設定します。オプションは次のとおりです。 • **mac-address**：シャーシの MAC アドレスを指定します。 • **serial-number**：シャーシのシリアル番号/組織固有識別子（OUI） • **system-name**：システム名または完全修飾ドメイン名 デフォルトは **system-name** です。
ステップ 4	（任意） **cdp holdtime** *seconds* 例： `switch(config)# cdp holdtime 150`	CDP ネイバー情報を削除するまでに保持する時間を設定します。範囲は 10 ～ 255 秒です。デフォルト値は 180 秒です。
ステップ 5	（任意） **cdp timer** *seconds* 例： `switch(config)# cdp timer 50`	CDP がネイバーにアドバタイズメントを送信するリフレッシュ タイムを設定します。範囲は 5 ～ 254 秒です。デフォルトは 60 秒です。

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

CDP コンフィギュレーションの確認

CDP 設定を表示するには、次のタスクのうちのいずれかを実行します。

コマンド	目的
show cdp all	CDP がイネーブルになっているすべてのインターフェイスを表示します。
show cdp entry {**all** | **name** *entry-name*}	CDP データベース エントリを表示します。
show cdp global	CDP グローバル パラメータを表示します。
show cdp interface *interface slot*/*port*	CDP インターフェイスのステータスを表示します。
show cdp neighbors {**device-id** | **interface** *interface slot*/*port*} [**detail**]	CDP ネイバーのステータスを表示します。
show cdp interface *interface slot*/*port*	インターフェイスの CDP トラフィック統計を表示します。

インターフェイスの CDP 統計情報を消去するには、**clear cdp counters** コマンドを使用します。

1 つまたはすべてのインターフェイスの CDP キャッシュを消去するには、**clear cdp table** コマンドを使用します。

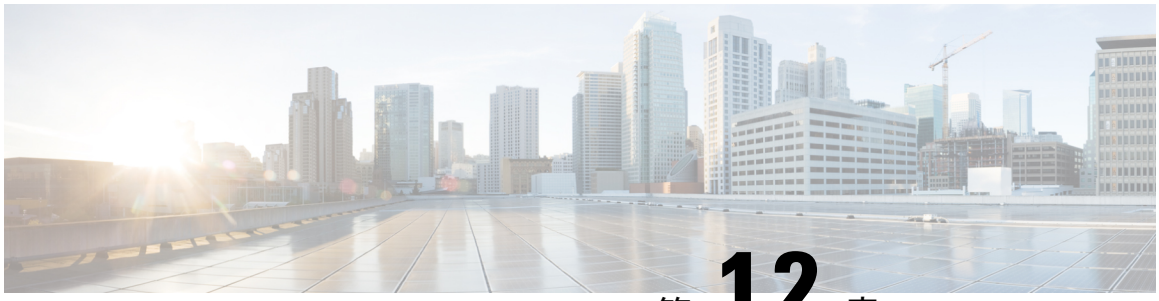
show cdp neighbors detail コマンドを（**show cdp neighbors** コマンドの代わりに）使用することを推奨します。**show cdp neighbors** コマンドが表示するのは、プラットフォーム名の 13 文字だけです。完全なプラットフォーム名を表示するには、**show cdp neighbors detail** コマンドを使用します。

CDP のコンフィギュレーション例

CDP 機能を有効にして、リフレッシュ タイマーおよびホールド タイマーを設定する例を示します。

```
configure terminal
cdp enable
cdp timer 50
```

```
cdp holdtime 100
```



第 12 章

LLDP の設定

この章では、ローカル ネットワーク上の他のデバイスを検出するために、Link Layer Discovery Protocol（LLDP）を設定する方法について説明します。

（注） この章で使用するコマンドのシンタックスおよび使用方法の詳細については、このリリースに対応するコマンド リファレンスおよび *Cisco IOS Configuration Fundamentals* コマンド リファレンス、リリース *12.2* の「システム管理コマンド」セクションを参照してください。

この章は、次の内容で構成されています。

LLDP について

Cisco Discovery Protocol（CDP）は、ネットワークに接続された他のシスコ デバイスを自動的に検出し学習することをネットワーク管理アプリケーションによって可能にするデバイス検出プロトコルです。Cisco Discovery Protocol（CDP）は、ネットワークに接続された他のシスコ デバイスを自動的に検出し学習することをネットワーク管理アプリケーションによって可能にするデバイス検出プロトコルです。

他社製デバイスのディスカバリを許可するために、スイッチは、IEEE 802.1ab 規格で定義されているベンダー ニュートラルなデバイス ディスカバリ プロトコルである Link Layer Discovery Protocol（LLDP）もサポートしています。LLDP を使用すると、ネットワーク デバイスはそれ自体のデバイスに関する情報を、ネットワーク上の他のデバイスにアドバタイズできます。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する 2 つのシステムで互いの情報を学習できます。

LLDP は、デバイスおよびそのインターフェイスの機能と現在のステータスに関する情報を送信する単一方向のプロトコルです。LLDP デバイスはこのプロトコルを使用して、他の LLDP デバイスからだけ情報を要求します。

LLDP は一連の属性をサポートしており、これを使用して他のデバイスを検出します。これらの属性には、タイプ、長さ、および値（TLV）の説明が含まれています。LLDP デバイスは TLV を使用して、ネットワーク上の他のデバイスと情報を送受信できます。設定情報、デバイスの機能、デバイス ID などの詳細情報は、このプロトコルを使用してアドバタイズできます。

LLDP は、デフォルトで次の TLV をアドバタイズします。

- 管理用アドレス
- ポートの説明
- ポートVLAN
- システム機能
- システムの説明
- システム名

高可用性

LLDP 機能はステートレス リスタートおよびステートフル リスタートをサポートします。リブートまたはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションを適用します。

高可用性の詳細については、『*Cisco Nexus* シリーズ *NX-OS* 高可用性および冗長性ガイド』を参照してください。

仮想化のサポート

Cisco Nexus® 3550-T スイッチでサポートされる LLDP のインスタンスは 1 つだけです。

LLDP に関する注意事項および制約事項

LLDP の設定のガイドラインおよび制限事項は、次のとおりです。

- インターフェイス上でLLDPをイネーブルまたはディセーブルにするには、事前にデバイス上で LLDP をイネーブルにしておく必要があります。
- LLDP は物理インターフェイスだけでサポートされています。
- LLDP は 1 つのポートにつき 1 つのデバイスを検出できます。

LLDP のデフォルト設定

この表は、LLDP のデフォルト設定を示します。

パラメータ	デフォルト
グローバル LLDP	無効
インターフェイス上の LLDP	イネーブル（LLDPがグローバルにイネーブルになった後）
LLDP 保持時間（ディセーブルになる前）	120 秒
LLDP 再初期化遅延	2 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP 受信	イネーブル（LLDPがグローバルにイネーブルになった後）
LLDP 転送	イネーブル（LLDPがグローバルにイネーブルになった後）

LLDP の設定

この章では、Cisco Nexus® 3550-T スイッチに Link Layer Discovery Protocol（LLDP）を構成する方法について説明します。

LLDP をグローバルに有効化または無効化する

デバイスでLLDPをグローバルにイネーブルまたはディセーブルにできます。デバイスでLLDPパケットの送信および受信を可能にするには、LLDP をグローバルにイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **feature lldp** **例：** `switch(config)# feature lldp`	デバイス上でLLDPをイネーブルまたはディセーブルにします。LLDPはデフォルトでディセーブルです。

	コマンドまたはアクション	目的
ステップ 3	（任意） **show running-config lldp** 例： `switch(config)# show running-config lldp`	LLDP のグローバル コンフィギュレーションを表示します。LLDP が有効の場合、「feature lldp」と表示されます。LLDP が無効の場合、「Invalid command」エラーが表示されます。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイス上での LLDP の有効化または無効化

LLDP をグローバルに有効にすると、LLDP は、デフォルトで、サポートされているすべてのインターフェイスで有効になります。ただし、LLDP パケットの送信だけ、または受信だけを実行するために、個々のインターフェイスでの LLDP のイネーブルまたはディセーブル、あるいはインターフェイスの選択的な設定を実行できます。

始める前に

デバイスで LLDP をグローバルにイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		LLDP をイネーブルにする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	[**no**] **lldp transmit** 例： `switch(config-if)# lldp transmit`	インターフェイス上で LLDP パケットの送信をイネーブルまたはディセーブルにします。LLDP をグローバルに有効にすると、LLDP は、デフォルトで、サポートされているすべてのインターフェイスで有効になります。

	コマンドまたはアクション	目的
ステップ 4	[**no**] **lldp receive** 例： `switch(config-if)# lldp receive`	インターフェイス上でLLDPパケットの受信をイネーブルまたはディセーブルにします。LLDPをグローバルに有効にすると、LLDPは、デフォルトで、サポートされているすべてのインターフェイスで有効になります。
ステップ 5	（任意） **show lldp interface** *interface slot/port* 例： `switch(config-if)# show lldp interface ethernet 1/1`	インターフェイス上でLLDPの設定を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

物理インターフェイスごとの複数の LLDP ネイバー

多くの場合、ネットワーク デバイスは複数のLLDPパケットを送信しますが、そのうちの1つは実際のホストからのものです。Cisco Nexusスイッチがデバイスと通信しているが、インターフェイスごとに1つのLLDPネイバーしか管理できない場合は、実際に必要なホストとのネイバーになることが失敗する可能性があります。これを最小限に抑えるために、Cisco Nexus スイッチ インターフェイスは複数の LLDP ネイバーをサポートできるため、正しいデバイスで LLDP ネイバーになる可能性が高くなります。

同じインターフェイスで複数のLLDPネイバーをサポートするには、LLDPマルチネイバー サポートをグローバルに設定する必要があります。

LLDP マルチネイバー サポートのイネーブル化またはディセーブル化

始める前に

インターフェイスでLLDPマルチネイバーサポートを有効にする前に、次の点を考慮してください。

- デバイスでLLDPをグローバルにイネーブルにしていることを確認します（グローバル設定コマンド **feature lldp**）。

（注） LLDP をグローバルに有効にすると、LLDP は、デフォルトで、サポートされているすべてのインターフェイスで有効になります。

- 1 つのインターフェイスで最大 3 つのネイバーがサポートされます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	必須: [**no**] **lldp multi-neighbor**
	例：
	`switch(config)# lldp multi-neighbor`
	`switch(config)#`
		すべてのインターフェイスのLLDPマルチネイバーサポートをグローバルに有効または無効にします。

ステップ 3	**interface** *port* / *slot*
	例：
	`switch(config)# interface 1/1`
	`switch(config-if)#`
		LLDP をイネーブルにする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 4	（任意） [**no**] **lldp transmit** 例： `switch(config-if)# lldp transmit`	インターフェイスでの LLDP パケットの送信をディセーブル（またはイネーブル）にします。 （注） このインターフェイスでの LLDP パケットの送信は、グローバル **feature lldp** コマンドを使用してイネーブルにされました。このオプションは、この特定のインターフェイスの機能を無効にします。
ステップ 5	（任意） [**no**] **lldp receive** 例： `switch(config-if)# lldp receive`	インターフェイスでの LLDP パケットの受信をディセーブル（またはイネーブル）にします。

	コマンドまたはアクション	目的
		（注） このインターフェイスでの LLDP パケットの受信は、グローバル **feature lldp** コマンドを使用してイネーブルになりました。このオプションは、この特定のインターフェイスの機能を無効にします。
ステップ 6	（任意） **show lldp interface**l *port* / *slot* 例： `switch(config-if)# show lldp interface 1/1`	インターフェイス上でLLDPの設定を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ポート チャネル インターフェイスでの LLDP サポートの有効化または無効化

始める前に

ポート チャネルで LLDP サポートを有効にする前に、次の点を考慮してください。

- デバイスでLLDPをグローバルにイネーブルにしていることを確認します（グローバル設定コマンド **feature lldp**）。

（注） LLDP をグローバルに有効にすると、LLDP は、デフォルトで、サポートされているすべてのインターフェイスで有効になります。

- ポート チャネルに **lldp transmit** および **lldp receive** コンフィギュレーション コマンドを適用しても、ポート チャネルのメンバーの設定には影響しません。
- LLDP ネイバーは、LLDP 送受信がポート チャネルの両側で設定されている場合にのみ、ポート チャネル間で形成されます。

（注） LLDP の送受信コマンドは、MCT、VPC、FEX ファブリック、FEX ポート チャネル、およびポート チャネル サブ インターフェイスでは機能しません。

LLDP ポート チャネル機能をグローバルに有効にすると、LLDP 設定はこれらのポート タイプのいずれにも適用されません。ポート チャネルから設定が削除された場合、またはポート タイプ機能がグローバルに無効になった場合は、**lldp port-channel** コマンドを使用して新しくサポートされたポート チャネルで有効にすることはできません。コマンドはすでに発行されています。問題のポート チャネルで LLDP ポート チャネルを有効にするには、**lldp transmit** および **lldp receive** を各ポート チャネルに対して設定します（次の手順のステップ 4、5、および 6 を参照）。

手順

	コマンドまたはアクション	目的

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

ステップ 2	必須: [**no**] **lldp port-channel**
	例：
	`switch(config)# lldp port-channel`
	`switch(config)#`
		すべてのポート チャネルの LLDP 送受信をグローバルに有効または無効にします。

ステップ 3	**interface port-channel** [*port-channel-number* | *port-channel-range*]
	例：
	`switch(config)# interface port-channel 3`
	`switch(config-if)#`
	例：
	複数のポート チャネルで LLDP を設定する場合は、ポート チャネル番号の範囲を入力します。
	`switch(config)# interface port-channel 1-3`
	`switch(config-if-range)#`
		LLDP を有効にするインターフェイス ポートチャネルを指定し、インターフェイス設定モードを開始します。
		LLDP を有効にするインターフェイス ポートチャネル範囲を指定し、インターフェイス範囲設定モードを開始します。

ステップ 4	（任意） [**no**] **lldp transmit** 例： `switch(config-if)# lldp transmit`	ポート チャネルまたはポート チャネルの範囲で LLDP パケットの送信を無効（または有効）にします。

	コマンドまたはアクション	目的
		（注） このポート チャネルでの LLDP パケットの送信は、ステップ 3 の **lldp port-channel** コマンドを使用して有効になりました。このオプションは、この特定のポート チャネルの機能を無効にします。
ステップ 5	（任意） [**no**] **lldp receive** 例： `switch(config-if)# lldp receive`	ポート チャネルまたはポート チャネルの範囲での LLDP パケットの受信を無効（または有効）にします。 （注） このポート チャネルでの LLDP パケットの受信は、ステップ 3 の **lldp port-channel** コマンドを使用して有効になりました。このオプションは、この特定のポート チャネルの機能を無効にします。
ステップ 6	（任意） **show lldp interface port-channel** *port-channel-number* 例： `switch(config-if)# show lldp interface port-channel 3`	ポートチャネル上の LLDP 設定を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

LLDP オプション パラメータの設定

LLDP の更新頻度、受信デバイスが情報を破棄するまでに保持している時間、および初期化の遅延時間を設定できます。

手順

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

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	
ステップ 2	（任意）[**no**] **lldp holdtime** *seconds* 例： `switch(config)# lldp holdtime 200`	ユーザのデバイスから送信された情報が、受信側デバイスで廃棄されるまでに保持される時間を秒単位で指定します。 値の範囲は 10 ～ 255 秒で、デフォルト値は 120 秒です。
ステップ 3	（任意）[**no**] **lldp reinit** *seconds* 例： `switch(config)# lldp reinit 5`	任意のインターフェイス上でLLDPを初期化する際の遅延時間を秒単位で指定します。 指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。
ステップ 4	（任意）[**no**] **lldp timer** *seconds* 例： `switch(config)# lldp timer 50`	LLDPアップデートの送信頻度を秒単位で設定します。 値の範囲は5～254秒で、デフォルト値は 30 秒です。
ステップ 5	（任意）**show lldp timers** 例： `switch(config)# show lldp timers`	LLDPの保持時間、遅延時間、更新頻度の設定を表示します。
ステップ 6	（任意）**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

LLDP 設定の確認

LLDP 設定を表示するには、次のタスクのうちのいずれかを実行します。

コマンド	目的
show running-config lldp	LLDP のグローバル コンフィギュレーションを表示します。
show lldp interface *interface slot/port*	LLDP のインターフェイス コンフィギュレーションを表示します。
show lldp timers	LLDPの保持時間、遅延時間、更新頻度の設定を表示します。

コマンド	目的
show lldp neighbors {**detail** | **interface** *interface slot*/*port*}	LLDP ネイバーのデバイス ステータスを表示します。
show lldp traffic interface *interface slot*/*port*	インターフェイス上で送信および受信された LLDP パケットの数を表示します。

LLDP の統計を消去するには、**clear lldp counters** コマンドを使用します。

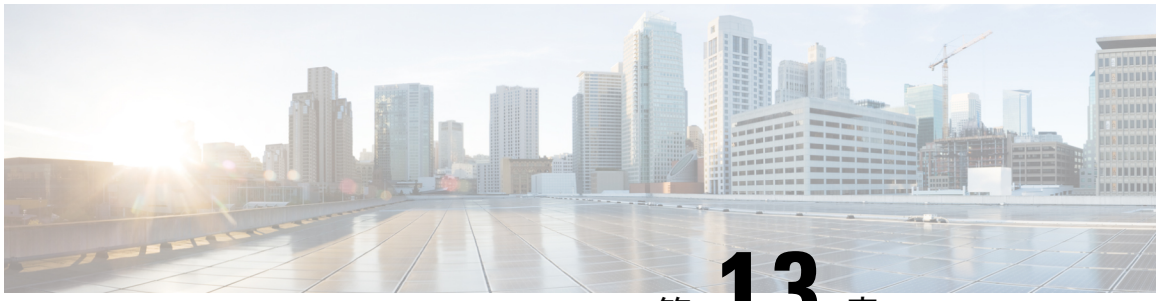
LLDP の設定例

次に、1 つのデバイス上での LLDP の有効化、一部のインターフェイス上での LLDP の無効化の方法、オプションパラメータ（ホールド時間、遅延時間、更新頻度など）の構成方法の例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature lldp
switch(config)# interface ethernet 1/9
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# interface ethernet 1/10
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# lldp holdtime 200
switch(config)# lldp reinit 5
switch(config)# lldp timer 50
```

第 IV 部

Cisco Nexus 3550-T Multicast Routing 構成ガイド



第 13 章

マルチキャスト構成の概要

ライセンス要件

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

マルチキャストについて

IP マルチキャストは、同一セットの IP パケットをネットワーク上の複数のホストに転送する手法です。IPv4 ネットワークで、マルチキャストを使用して、複数の受信者に効率的にデータを送信できます。

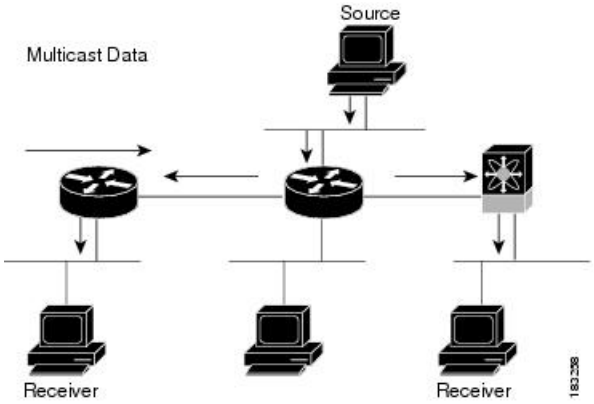
マルチキャストには、グループと呼ばれる IP マルチキャスト アドレスに送信されたマルチキャスト データの送信側と受信側の配信と検出の両方の手法が含まれます。グループと送信元 IP アドレスが入ったマルチキャスト アドレスは、しばしばチャネルと呼ばれます。Internet Assigned Number Authority（IANA）では、IPv4 マルチキャスト アドレスとして、224.0.0.0 ～ 239.255.255.255 を割り当てています。詳細については、次の URL を参照してください。 http://www.iana.org/assignments/multicast-addresses

（注） マルチキャストに関連する RFC の完全なリストについては、「*IP* マルチキャストに関する *IETF RFC*」の章を参照してください。

ネットワーク上のルータは、受信者からのアドバタイズメントを検出して、マルチキャストデータの要求対象となるグループを特定します。その後、ルータは送信元からのデータを複製して、対象の受信者へと転送します。グループ宛のマルチキャストデータが送信されるのは、そのデータを要求する受信者を含んだ LAN セグメントだけです。

次の図に、1 つの送信元から 2 つの受信者へと、マルチキャスト データを送信する場合の例を示します。この図で、中央のホストが属する LAN セグメントにはマルチキャスト データを要求する受信者が存在しないため、このホストは受信者にデータを転送しません。

図 *4: 1* つの送信元から *2* つの受信者へのマルチキャスト トラフィック



Cisco NX-OS PIM

Cisco NX-OS は Protocol Independent Multicast（PIM）スパース モードを使用したマルチキャストをサポートしています。PIM は IP ルーティング プロトコルに依存せず、使用されているすべてのユニキャスト ルーティング プロトコルが提供するユニキャスト ルーティング テーブルを利用できます。PIM スパース モードでは、ネットワーク上の要求元だけにマルチキャストトラフィックが伝送されます。PIM デンス モードは Cisco NX-OS ではサポートされていません。

（注） このマニュアルで、「PIM」という用語は PIM スパース モード バージョン 2 を表します。

マルチキャスト コマンドにアクセスするには、PIM機能をイネーブルにする必要があります。ドメイン内の各ルータのインターフェイス上で、PIM をイネーブルにしないかぎり、マルチキャスト機能はイネーブルになりません。PIM はIPv4 ネットワーク用に設定できます。デフォルトでは、IGMP がシステムで稼働しています。

マルチキャスト対応ルータ間で使用される PIM は、マルチキャスト配信ツリーを構築して、ルーティング ドメイン内にグループ メンバーシップをアドバタイズします。PIM は、複数の送信元からのパケットが転送される共有配信ツリーと、単一の送信元からのパケットが転送される送信元配信ツリーを構築します。

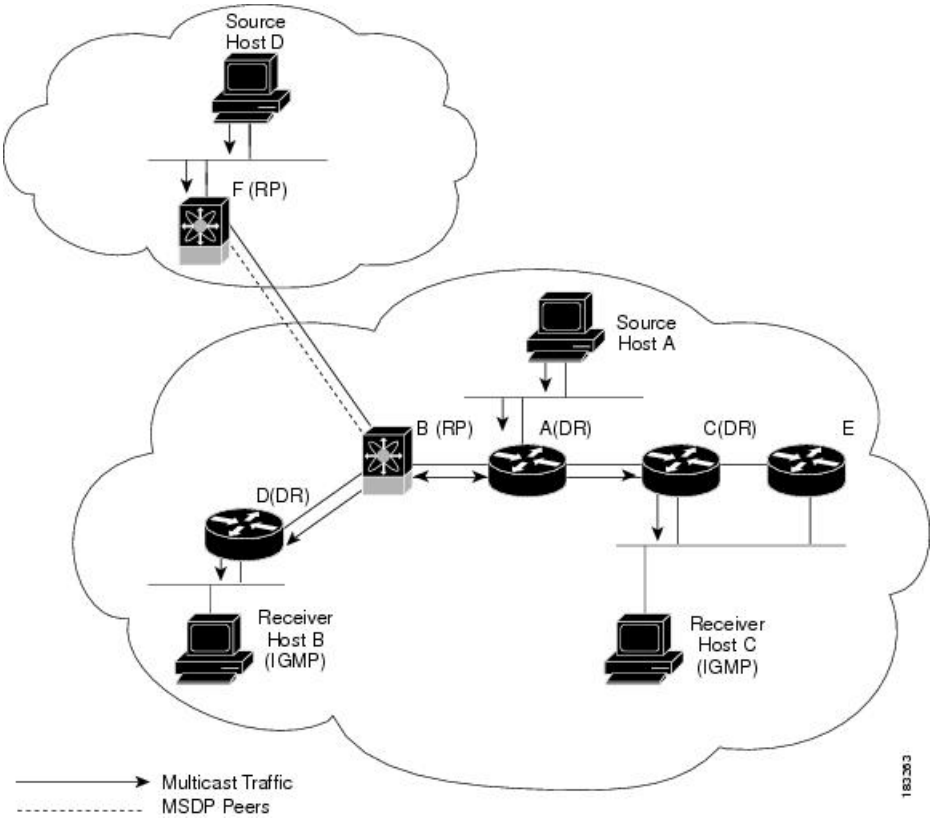
配信ツリーは、リンク障害またはルータ障害のためにトポロジが変更されると、トポロジを反映して自動的に変更されます。PIMは、マルチキャスト対応の送信元と受信者の両方を動的に追跡します。

ルータはユニキャスト ルーティング テーブルおよびRPF ルートを使用して、マルチキャスト ルーティング情報を生成します。

（注） このマニュアルでは、「IPv4用のPIM」という表現は、Cisco NX-OSにおけるPIMスパース モードの導入を表します。

次の図に、IPv4 ネットワーク内の 2 つの PIM ドメインを示します。

図 *5 : IPv4* ネットワーク内の *PIM* ドメイン



- 矢印の付いた直線は、ネットワークで伝送されるマルチキャスト データのパスを表します。マルチキャスト データは送信元ホストの A および D から発信されます。
- 点線でつながれているルータ B および Fは、Multicast Source Discovery Protocol（MSDP）ピアです。MSDP を使用すると、他の PIM ドメイン内にあるマルチキャスト送信元を検出できます。

- ホスト B およびホスト C ではマルチキャスト データを受信するため、インターネット グループ管理プロトコル（IGMP）プロトコルを使用して、マルチキャスト グループへの加入要求をアドバタイズします。
- ルータ A、C、および D は指定ルータ（DR）です。LAN セグメントに複数のルータが接続されている場合は（C や E など）、PIM ソフトウェアによって DR となるルータが 1 つ選択されます。これにより、マルチキャストデータの窓口として、1 つのルータだけが使用されます。

ルータ B とルータ F は、それぞれ異なる PIM ドメインのランデブー ポイント（RP）です。RP は、複数の送信元と受信者を接続するため、PIM ドメイン内の共通ポイントとして機能します。

PIM は送信元と受信者間の接続に関して、送信元マルチキャスト（ASM）モードをサポートしています。

アーキテクチャ セールス マネージャ（ASM）

Any Source Multicast（ASM）は PIM ツリー構築モードの 1 つです。新しい送信元および受信者を検出する場合には共有ツリーを、受信者から送信元への最短パスを形成する場合は送信元ツリーを使用します。共有ツリーでは、ランデブーポイント（RP）と呼ばれるネットワーク ノードをルートとして使用します。送信元ツリーは第 1 ホップ ルータをルートとし、アクティブな発信元である各送信元に直接接続されています。ASM モードでは、グループ範囲に対応する RP が必要です。RP は静的に構成できます。RP が学習されている場合、グループは ASM モードで動作します。

RP を設定する場合、デフォルト モードは ASM モードです。

IGMP

デフォルトでは、PIM のインターネット グループ管理プロトコル（IGMP）が、システムで実行されています。

IGMP は、マルチキャスト グループのメンバーシップを要求するため、マルチキャストデータを受信する必要があるホストで使用されます。グループ メンバーシップが確立されると、対象のグループのマルチキャスト データが要求元ホストの LAN セグメントに転送されます。

インターフェイスには IGMPv2 を設定できます。デフォルトでは IGMPv2 がイネーブルになっています。

（注） PIM が無効になっているレイヤ 2 ポートで IGMPv2 を使用するには制限があります。機能を使用する前にIGMP スヌーピングに関する注意事項と制限事項（186ページ）セクションを参照してください。

マルチキャストに関する注意事項と制限事項

- Cisco Nexus® 3550-T プラットフォームは FHR をサポートできません。
- トランクを介したマルチキャストは、Cisco Nexus® 3550-T プラットフォームではサポートされていません。
- 不明なマルチキャストトラフィックによるトラフィック ストーム制御はサポートされていません。
- 双方向モードは、Cisco Nexus® 3550-T プラットフォーム スイッチではサポートされていません。
- Cisco Nexus® 3550-T は、マルチキャスト RPF チェックを行いません。RPF 機能不全のパケットは、学習済みの受信者にフラッディングされます。

マルチキャストのハイ アベイラビリティ要件

マルチキャスト ルーティング プロトコルを再起動すると、MRIB プロセスによってステートが回復されます。スーパーバイザのスイッチオーバーが発生した場合、MRIB はハードウェアからステートを回復し、マルチキャスト プロトコルは定期的なメッセージ アクティビティからステートを回復します。

SW と HW マルチキャスト ルート間の不一致のトラブルシューティング

症状

このセクションでは、アクティブなフローで MRIB に表示されるが、MFIB でプログラムされていない *、G、エントリに関連した症状、考えられる原因、および推奨されるアクションについて説明します。

考えられる原因

この問題は、ハードウェアの容量を超えて多数のアクティブ フローを受信した場合に発生します。これにより、空きハードウェア インデックスがなくなって、一部のエントリがハードウェアでプログラムされなくなります。

ハードウェア リソースを解放するためにアクティブなフローの数が大幅に削減された場合、ハードウェア テーブルがいっぱいであったときに以前影響されていたフローについては、エントリ、タイムアウト、再入力が生じ、プログラミングがトリガーされるまで、MRIB と MFIB の間で不整合が見られることがあります。

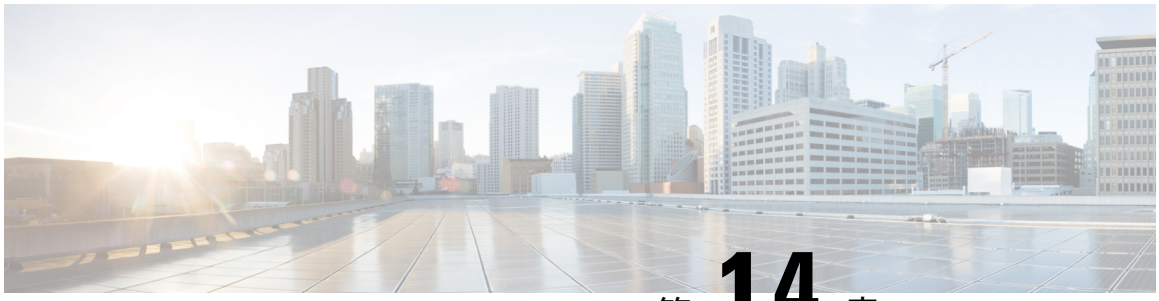
現在、ハードウェア リソースが解放された後に、MRIBテーブルを調べて、ハードウェアの欠落しているエントリを再プログラムするメカニズムはありません。

改善処置

エントリを確実に再プログラミングするには、**clear ip mroute *** コマンドを使用します。

シスコのテクニカル サポート

説明	リンク
Technical Assistance Center（TAC）ホーム ページ：多数の技術関連の記事と、製品、テクノロジー、ソリューション、テクニカル ティップス、ツールへのリンクを提供する Web サイトです。必要な記事は検索して見つけることができます。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/public/support/tac/home.shtml



第 14 章

IGMP の設定

この章では、IPv4 ネットワークの Cisco NX-OS デバイスに対するインターネット グループ管理プロトコル（IGMP）の設定方法を説明します。

IGMP について

IGMP は、ホストが特定のグループにマルチキャスト データを要求するために使用する IPv4 プロトコルです。ソフトウェアは、IGMP を介して取得した情報を使用し、マルチキャスト グループまたはチャネル メンバーシップのリストをインターフェイス単位で保持します。これらの IGMP パケットを受信したシステムは、既知の受信者が含まれるネットワーク セグメントに、要求されたグループまたはチャネルに関する受信データをマルチキャスト送信します。

IGMP プロセスはデフォルトで実行されています。インターフェイスでは IGMP を手動でイネーブルにできません。IGMP は、インターフェイスで次のいずれかの設定作業を行うと、自動的にイネーブルになります。

- Protocol-Independent Multicast（PIM）のイネーブル化
- ローカル マルチキャスト グループの静的なバインディング

IGMP のバージョン

デバイスでは、IGMPv2 と IGMPv3、および IGMPv1 のレポート受信がサポートされています。

デフォルトでは、ソフトウェアが IGMP プロセスを起動する際に、IGMPv2 がイネーブルになります。必要に応じて、各インターフェイスでは IGMPv3 をイネーブルにできます。

IGMPv3 には、次に示す IGMPv2 からの重要な変更点があります。

- ホストによるレポート抑制が行われなくなり、IGMP クエリー メッセージを受信するたびに IGMP メンバーシップ レポートが送信されるようになりました。

（注） Cisco Nexus® 3550-T スイッチは SSM をサポートしていません。

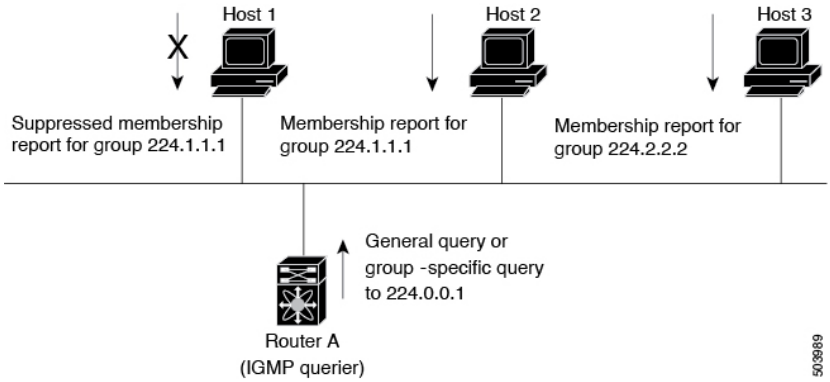
IGMPv2 の詳細については、RFC 2236 を参照してください。

IGMPv3 の詳細については、RFC 5790 を参照してください。

IGMP の基礎

次の図に、ルータが IGMP を使用し、マルチキャスト ホストを検出する基本的なプロセスを示します。ホスト 1、2、および 3 は要求外の IGMP メンバーシップ レポート メッセージを送信して、グループまたはチャネルに関するマルチキャスト データの受信を開始します。

図 *6 : IGMPv1* および *IGMPv2* クエリ応答プロセス



下の図では、ルータ A（サブネットの代表 IGMP クエリア）は、すべてのホストが含まれる 224.0.0.1 ホスト マルチキャスト グループに定期的にクエリ メッセージを送信して、マルチキャスト データを受信するホストを検出します。グループ メンバーシップ タイムアウト値を設定できます。指定したタイムアウト値が経過すると、ルータはサブネット上にグループのメンバーまたは送信元が存在しないと見なします。

IP アドレスが最小のルータが、サブネットの IGMP クエリアとして選出されます。ルータは、自身よりも下位の IP アドレスを持つルータからクエリー メッセージを継続的に受信している間、クエリア タイムアウト値をカウントするタイマーをリセットします。ルータのクエリア タイマーが期限切れになると、そのルータは代表クエリアになります。そのあとで、このルータが、自身よりも下位の IP アドレスを持つルータからのホスト クエリー メッセージを受信すると、ルータは代表クエリアとしての役割をドロップしてクエリア タイマーを再度設定します。

この図では、ホスト1からのメンバーシップ レポートの送出が止められており、最初にホスト2からグループ 224.1.1.1 に関するメンバーシップ レポートが送信されます。ホスト1はホスト2からレポートを受信します。ルータに送信する必要があるメンバーシップ レポートは、グループにつき 1 つだけであるため、その他のホストではレポートの送出が止められ、ネットワーク トラフィックが軽減されます。レポートの同時送信を防ぐため、各ホストではランダムな時間だけレポート送信が保留されます。クエリの最大応答時間パラメータを設定すると、ホストが応答をランダム化する間隔を制御できます。

（注） IGMPv1 および IGMPv2 メンバーシップ レポートが抑制されるのは、同じポートに複数のホストが接続されている場合だけです。

（注） IGMPv3 ホストでは、IGMP メンバーシップ レポートの抑制が行われません。

代表クエリアから送信されるメッセージの存続可能時間（TTL）値は 1 です。つまり、サブネット上の直接接続されたルータからメッセージが転送されることはありません。IGMP の起動時に送信されるクエリ メッセージの頻度および回数を個別に設定したり、スタートアップ クエリ インターバルを短く設定したりすることで、グループ ステートの確立時間を最小限に抑えることができます。通常は不要ですが、起動後のクエリーインターバルをチューニングすることで、ホスト グループ メンバーシップ メッセージへの応答性と、ネットワーク上のトラフィック量のバランスを調整できます。

注意 クエリー インターバルを変更すると、マルチキャスト転送能力が著しく低下することがあります。

マルチキャスト ホストがグループを脱退する場合、IGMPv2 以上を実行するホストでは、IGMP Leave メッセージを送信します。このホストがグループを脱退する最後のホストであるかどうかを確認するために、IGMP クエリ メッセージが送信されます。そして、最終メンバーのクエリ応答インターバルと呼ばれる、ユーザーが設定可能なタイマーが起動されます。タイマーが切れる前にレポートが受信されない場合は、ソフトウェアによってグループ ステートが解除されます。ルータはグループ ステートが解除されないかぎり、このグループにマルチキャスト トラフィックを送信し続けます。

輻輳ネットワークでのパケット損失を補正するには、ロバストネス値を設定します。ロバストネス値は、IGMP ソフトウェアがメッセージ送信回数を確認するために使用されます。

224.0.0.0/24 内に含まれるリンク ローカル アドレスは、インターネット割り当て番号局（IANA）によって予約されています。ローカル ネットワーク セグメント上のネットワーク プロトコルでは、これらのアドレスが使用されます。これらのアドレスは TTL が 1 であるため、ルータからは転送されません。IGMP プロセスを実行すると、デフォルトでは、非リンク ローカル アドレスにだけメンバーシップ レポートが送信されます。ただし、リンク ローカル アドレスにレポートが送信されるよう、ソフトウェアの設定を変更することができます。

IGMP の前提条件

IGMP の前提条件は、次のとおりです。

- デバイスにログインしている。
- グローバル構成コマンド。この章の例で示すデフォルトのコンフィギュレーションモードは、デフォルト VRF に適用されます。

IGMP に関する注意事項と制限事項

IGMP に関する注意事項および制限事項は次のとおりです。

- 低遅延のために、Cisco Nexus® 3550-T スイッチは L2 ポートの {Vlan,MAC} ルックアップのみをサポートします。IP ベースの {VLAN,G} または {VLAN,G,S} ルックアップはありません。
- 最適化された {Vlan,MAC} ルックアップ用にルートがインストールされるため、Route-Aliasing が予想されます。
- すべての不明なマルチキャスト パケット ミスは、同じ L2 ドメイン内の他のルータへのフラッドの代わりにドロップされます。
- Cisco Nexus® 3550-T スイッチを使用したマルチアクセス ネットワークは機能しません。PIM 対応ルータの 1 つが Cisco Nexus® 3550-T スイッチの場合、同じ VLAN セグメントに 2 つの PIM ルータを配置できません。Cisco Nexus® 3550-T スイッチは、非 DR として機能できません。
- multicast-lookup ミス パケットが VLAN でフラッディングされないため、L2 トランジット ノードで PIM を有効にすることはできません。
- Cisco Nexus® 3550-T スイッチは、SVI の L3 トランジット ボックスとして使用しないでください。ただし、L2 受信者は SVI のトランジット ボックスに存在する場合があります。L3 物理ポートで L3 トランジットとして使用できます。
- FHR サポートなし – これにより、L3 マルチキャスト ルーティングが必要な VLAN に送信元が直接接続されることは想定されません。
- {Vlan,Mac} ルックアップにより、IGMPv2 のレポートはすでにアタッチされている受信者にフラッドされ、この結果は report-suppression に表示されます。IGMPv3 として構成済みのホストを保持することが推奨されます。
- IGMPv3（RFC 5790）に従って送信元のリストを除外またはブロックすることはサポートされていません。

IGMP のデフォルト設定

次の表に、IGMP パラメータのデフォルト設定を示します。

表 *11 : IGMP* パラメータのデフォルト設定

パラメータ	デフォルト
IGMP のバージョン	2
スタートアップ クエリー インターバル	30 秒
スタートアップ クエリーの回数	2
ロバストネス値	2
クエリア タイムアウト	255 秒
クエリー タイムアウト	255 秒
クエリーの最大応答時間	10 秒
クエリー インターバル	125 秒
最終メンバーのクエリー応答インターバル	1 秒
最終メンバーのクエリー回数	2
グループ メンバーシップ タイムアウト	260 秒
リンク ローカルマルチキャスト グループのレポート	無効
ルータ アラートの実施	無効
即時離脱	ディセーブル

IGMP パラメータの設定

IGMP グローバル パラメータおよびインターフェイス パラメータを設定すると、IGMP プロセスの動作を変更できます。

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

IGMP インターフェイス パラメータの設定

次の表に、設定可能なオプションの IGMP インターフェイス パラメータを示します。

表 *12 : IGMP* インターフェイス パラメータ

パラメータ	説明
IGMP のバージョン	インターフェイスでイネーブルにする IGMP のバージョン。有効な IGMP バージョンは 2 または 3 です。デフォルトは 2 です。
スタティック マルチキャスト グループ	インターフェイスに静的にバインドされるマルチキャスト グループ。(*, G) というステートでインターフェイスの加入先グループを構成します。**match ip multicast** コマンドで、使用するグループ プレフィックスおよびグループ範囲を示すルートマップ ポリシー名を指定できます。 （注） （*, G）ステートで構成しても、送信元ツリーが構築されるのはIGMPv3を有効化している場合だけです。 ネットワーク上の全マルチキャスト対応ルータを含むマルチキャスト グループを設定すると、このグループに ping 要求を送信することで、すべてのルータから応答を受け取ることができます。
発信インターフェイス（OIF）上のスタティック マルチキャスト グループ	発信インターフェイスに静的にバインドされるマルチキャスト グループ。（*, G）というステートで出力インターフェイスの加入先グループを構成するか、（*, , G）というステートでグループに加入するソース IP を指定します。**match ip multicast** コマンドで、使用するグループ プレフィックス、グループ範囲、および送信元プレフィックスを示すルートマップ ポリシー名を指定できます。 （注） （*, G）ステートで構成しても、送信元ツリーが構築されるのはIGMPv3を有効化している場合だけです。

パラメータ	説明
スタートアップ クエリー インターバル	スタートアップ クエリー インターバル。デフォルトでは、ソフトウェアができるだけ迅速にグループ ステートを確立できるように、このインターバルはクエリー インターバルより短く設定されています。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 31 秒です。
スタートアップ クエリーの回数	スタートアップ クエリーインターバル中に送信される起動時のクエリー数。有効範囲は 1 ～ 10 です。デフォルトは 2 です。
ロバストネス値	輻輳ネットワークでのパケット損失を許容範囲内に抑えるために使用される、調整可能なロバストネス変数。ロバストネス変数を大きくすれば、パケットの再送信回数を増やすことができます。有効範囲は1～7です。デフォルトは 2 です。
クエリア タイムアウト	前クエリアがクエリーを停止してから、自身がクエリアとして処理を引き継ぐまで、ソフトウェアが待機する秒数。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。
クエリーの最大応答時間	IGMPクエリーでアドバタイズされる最大応答時間。大きな値を設定すると、ホストの応答時間が延長されるため、ネットワークのIGMPメッセージを調整できます。この値は、クエリー インターバルよりも短く設定する必要があります。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
クエリー インターバル	IGMPホストクエリーメッセージの送信頻度。大きな値を設定すると、ソフトウェアによるIGMP クエリーの送信頻度が低くなるため、ネットワーク上の IGMP メッセージ数を調整できます。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。

パラメータ	説明
最終メンバーのクエリー応答インターバル	サブネット上の既知のアクティブ ホストから最後にホスト Leave メッセージを受信したあと、ソフトウェアが IGMP クエリーへの応答を送信するインターバル。このインターバル中に応答が受信されない場合、グループ ステートは解除されます。この値を使用すると、サブネット上でソフトウェアがトラフィックの送信を停止するタイミングを調整できます。この値を小さく設定すると、グループの最終メンバーまたは送信元が脱退したことを、より短時間で検出できます。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
最終メンバーのクエリー回数	サブネット上の既知のアクティブ ホストから最後にホスト Leave メッセージを受信したあと、最終メンバーのクエリー応答インターバル中に、ソフトウェアが IGMP クエリーを送信する回数。有効範囲は 1 ～ 5 です。デフォルトは 2 です。 この値を 1 に設定すると、いずれかの方向でパケットが検出されなくなると、クエリー対象のグループまたはチャネルのマルチキャスト ステートが解除されます。次のクエリー インターバルが開始されるまでは、グループを再度関連付けることができます。
グループ メンバーシップ タイムアウト	ルータによって、ネットワーク上にグループのメンバーまたは送信元が存在しないと見なされるまでのグループ メンバーシップ インターバル。有効範囲は 3 ～ 65,535 秒です。デフォルト値は 260 秒です。
リンク ローカル マルチキャスト グループのレポート	224.0.0.0/24 内のグループにレポートを送信できるようにするためのオプション。リンク ローカル アドレスは、ローカル ネットワーク プロトコルだけで使用されます。非リンク ローカル グループには、常にレポートが送信されます。デフォルトではディセーブルになっています。

パラメータ	説明
即時離脱	デバイスからグループ固有のクエリーが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間を最小限にできるオプション。即時脱退をイネーブルにすると、デバイスではグループに関する Leave メッセージの受信後、ただちにマルチキャスト ルーティング テーブルからグループ エントリが削除されます。デフォルトではディセーブルになっています。 （注） このコマンドは、所定のグループに対するインターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。

手順

	コマンドまたはアクション	目的

ステップ 1	**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** *interface*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。
		（注） ステップ 3 でリストされているコマンドを使用して、IGMP インターフェイス パラメータを設定します。

ステップ 3	**ip igmp version** *value* 例： `switch(config-if)# ip igmp version 3`	IGMP バージョンを指定値に設定します。有効な値は 2 または 3 です。デフォルトは 2 です。 このコマンドの **no** 形式を使用すると、バージョンは 2 に設定されます。
ステップ 4	**ip igmp join-group** {*group* [**source** *source*] } 例： `switch(config-if)# ip igmp join-group 230.0.0.0`	指定したグループまたはチャネルに参加するようにデバイス上のインターフェイスを設定します。デバイスは CPU 消費用のマルチキャスト パケットのみを受け入れます。

	コマンドまたはアクション	目的
		注意 このコマンドを使用して生成されたトラフィックは、デバイス CPU で処理可能である必要があります。CPUの負荷制約のため、このコマンドを使用することは（特に形式を問わずスケーリングで使用することは）推奨されません。代わりに **ip igmp static-oif** コマンドの使用を検討してください。
ステップ 5	**ip igmp static-oif** {*group* [**source** *source*]} 例： `switch(config-if)# ip igmp static-oif 230.0.0.0`	マルチキャスト グループを発信インターフェイスに静的にバインドし、デバイス ハードウェアで処理します。グループ アドレスのみを指定した場合は、（*,G）ステートが作成されます。送信元アドレスを指定した場合は、（*, G）ステートが作成されます。 （注） （*, G）ステートで送信元ツリーを構築するには、IGMPv3 を有効化する必要があります。
ステップ 6	**ip igmp startup-query-interval** *seconds* 例： `switch(config-if)# ip igmp startup-query-interval 25`	ソフトウェアの起動時に使用されるクエリーインターバルを設定します。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 31 秒です。
ステップ 7	**ip igmp startup-query-count** *count* 例： `switch(config-if)# ip igmp startup-query-count 3`	ソフトウェアの起動時に使用されるクエリー数を設定します。有効範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 8	**ip igmp robustness-variable** *value* 例： `switch(config-if)# ip igmp robustness-variable 3`	ロバストネス変数を設定します。有効値の範囲は、1 ～ 7 です。デフォルトは 2 です。
ステップ 9	**ip igmp querier-timeout** *seconds* 例： `switch(config-if)# ip igmp querier-timeout 300`	クエリアとして処理を引き継ぐかどうかをソフトウェアが判断するための、クエリア タイムアウト値を設定します。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。

	コマンドまたはアクション	目的
ステップ 10	**ip igmp query-timeout** *seconds* 例： `switch(config-if)# ip igmp query-timeout 300`	クエリアとして処理を引き継ぐかどうかをソフトウェアが判断するための、クエリー タイムアウト値を設定します。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。 （注） このコマンドの機能は、**ip igmp querier-timeout** コマンドと同じです。
ステップ 11	**ip igmp query-max-response-time** *seconds* 例： `switch(config-if)# ip igmp query-max-response-time 15`	IGMP クエリーでアドバタイズされる応答時間を設定します。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
ステップ 12	**ip igmp query-interval** *interval* 例： `switch(config-if)# ip igmp query-interval 100`	IGMP ホスト クエリー メッセージの送信頻度を設定します。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。
ステップ 13	**ip igmp last-member-query-response-time** *seconds* 例： `switch(config-if)# ip igmp last-member-query-response-time 3`	メンバーシップ レポートを送信してから、ソフトウェアがグループ ステートを解除するまでのクエリーインターバルを設定します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
ステップ 14	**ip igmp last-member-query-count** *count* 例： `switch(config-if)# ip igmp last-member-query-count 3`	ホストの Leave メッセージを受信してから、IGMP クエリーが送信される回数を設定します。有効範囲は 1 ～ 5 です。デフォルトは 2 です。
ステップ 15	**ip igmp group-timeout** *seconds* 例： `switch(config-if)# ip igmp group-timeout 300`	IGMPv2 のグループ メンバーシップ タイムアウトを設定します。有効範囲は 3 ～ 65,535 秒です。デフォルト値は 260 秒です。
ステップ 16	**ip igmp report-link-local-groups** 例： `switch(config-if)# ip igmp report-link-local-groups`	224.0.0.0/24 に含まれるグループに対して、レポート送信をイネーブルにします。非リンク ローカル グループには、常にレポートが送信されます。デフォルトでは、リンク ローカル グループにレポートは送信されません。

	コマンドまたはアクション	目的
ステップ 17	**ip igmp report-policy** ポリシー 例： `switch(config-if)# ip igmp report-policy my_report_policy`	ルートマップポリシーに基づく、IGMP レポートのアクセスポリシーを設定します。
ステップ 18	**ip igmp access-group** ポリシー 例： `switch(config-if)# ip igmp access-group my_access_policy`	インターフェイスが接続されたサブネット上のホストについて、加入可能なマルチキャストグループを制御するためのルートマップポリシーを設定します。 （注） **match ip multicast group** コマンドだけがこのルートマップポリシーでサポートされます。ACL を照合するための **match ip address** コマンドはサポートされていません。
ステップ 19	**ip igmp immediate-leave** 例： `switch(config-if)# ip igmp immediate-leave`	デバイスが、グループに関する Leave メッセージの受信後、ただちにマルチキャストルーティングテーブルからグループエントリを削除できるようにします。このコマンドを使用すると、デバイスからグループ固有のクエリが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間が最小限になります。デフォルトではディセーブルになっています。 （注） このコマンドは、所定のグループに対するインターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。
ステップ 20	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

IGMP プロセスの再起動

IGMP プロセスを再起動し、オプションとして、すべてのルートをフラッシュすることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**restart igmp** 例： `switch# restart igmp`	IGMP プロセスを再起動します。

ステップ 2	**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 3	**ip igmp flush-routes** 例： `switch(config)# ip igmp flush-routes`	IGMP プロセスの再起動時に、ルートを削除します。デフォルトでは、ルートはフラッシュされません。
ステップ 4	（任意） **show running-configuration igmp** 例： `switch(config)# show running-configuration igmp`	実行コンフィギュレーション情報を表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IGMP 構成の確認

IGMP の設定情報を表示するには、次の作業のいずれかを行います。

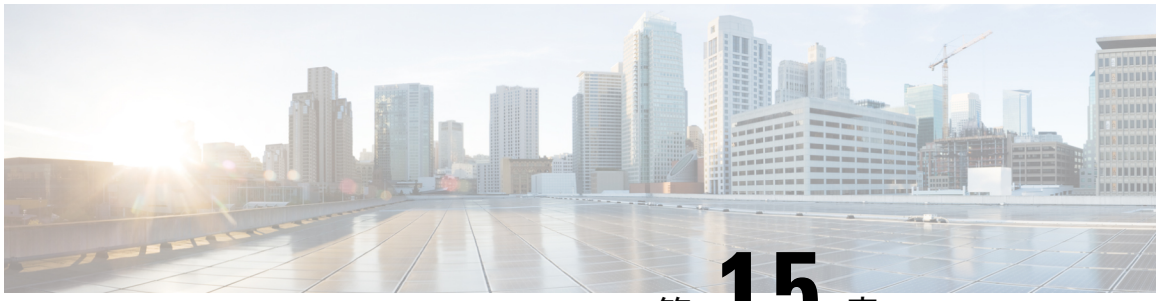
コマンド	説明
show ip igmp interface [*interface*] [**brief**]	すべてのインターフェイスまたは選択されたインターフェイスについて、IGMP 情報を表示します。

コマンド	説明
show ip igmp groups [{**source** [*group*]}] | {**group** [*source*]}] [**interface**] [**summary**]	グループまたはインターフェイスについて、IGMP で接続されたグループのメンバーシップを表示します。
show ip igmp route [{**source** [*group*]}] | {**group** [*source*]}] [**interface**] [**summary**]	グループまたはインターフェイスについて、IGMP で接続されたグループのメンバーシップを表示します。
show ip igmp local-groups	IGMP ローカル グループ メンバーシップを表示します。
show running-configuration igmp	IGMP 実行コンフィギュレーション情報を表示します。
show startup-configuration igmp	IGMP スタートアップ コンフィギュレーション情報を表示します。

IGMP の設定例

次に、IGMP パラメータの設定例を示します。

```
configure terminal

  interface ethernet 1/1
    ip igmp version 3
    ip igmp join-group 230.0.0.0
    ip igmp startup-query-interval 25
    ip igmp startup-query-count 3
    ip igmp robustness-variable 3
    ip igmp querier-timeout 300
    ip igmp query-timeout 300
    ip igmp query-max-response-time 15
    ip igmp query-interval 100
    ip igmp last-member-query-response-time 3
    ip igmp last-member-query-count 3
    ip igmp group-timeout 300
    ip igmp report-link-local-groups
```



第 15 章

IGMP スヌーピングの設定

この章では、IPv4 ネットワークの Cisco NX-OS デバイスに対するインターネット グループ管理プロトコル（IGMP）スヌーピングの構成方法を説明します。

IGMP スヌーピングについて

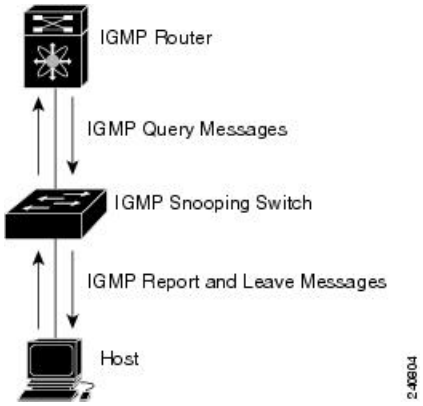
（注） デバイスの IGMP スヌーピングはディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、デバイス内で誤ったフラッディングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

IGMP スヌーピング ソフトウェアは、VLAN 内のレイヤ 2 IP マルチキャスト トラフィックを調べて、該当する受信側が入っているポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセス LAN 環境における帯域幅消費量を削減し、VLAN 全体へのフラッディングを回避します。IGMP スヌーピングは、マルチキャスト対応ルータに接続されたポートを追跡して、ルータによる IGMP メンバーシップ レポートの転送機能を強化します。トポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。デバイスでは、IGMP スヌーピングがデフォルトでイネーブルになっています。

この図に、ホストと IGMP ルータ間に設置された IGMP スヌーピング スイッチを示します。IGMP スヌーピング スイッチは、IGMP メンバーシップ レポートおよび Leave メッセージをスヌーピングして、必要な場合にだけ接続された IGMP ルータに転送します。

（注） {Vlan,Mac} ルックアップにより、IGMPv2 のレポートはすでにアタッチされている受信者にフラッド/転送され、この結果は report-suppression に表示されます。これは、Cisco Nexus 3550-T 10.1(2t) リリースのみに固有のものです。

図 *7: IGMP* スヌーピング スイッチ



IGMP スヌーピング ソフトウェアは、IGMPv1、IGMPv2、および IGMPv3 コントロール プレーン パケットの処理に関与し、レイヤ 3 コントロール プレーン パケットを代行受信して、レイヤ 2 の転送処理を操作します。

Cisco NX-OS IGMP スヌーピング ソフトウェアには、次のような独自機能があります。

- MAC アドレスに基づいたマルチキャスト転送

IGMP スヌーピングの詳細については、「RFC4541」を参照してください。

IGMPv1 および IGMPv2

IGMPv1 と IGMPv2 は両方とも、メンバーシップ レポート抑制をサポートします。つまり、同一サブネット上の 2 つのホストが同一グループのマルチキャスト データを受信する場合、他方のホストからメンバー レポートを受信するホストは、そのレポートを送信しません。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各 VLAN スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバーのクエリー メッセージがホストに送信されません。ソフトウェアは IGMP Leave メッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP Leave メッセージが存在しないため、特定のグループについてマルチキャスト データを要求するホストが存続しないことを示すために、メンバーシップ メッセージ タイムアウトが利用されます。

（注） 高速脱退機能がイネーブルになっている場合、他のホストの存在は確認されないため、最終メンバーのクエリー インターバル設定が無視されます。

IGMPスヌーピングクエリア

マルチキャスト トラフィックをルーティングする必要がないために、Protocol-Independent Multicast（PIM）がインターフェイス上でディセーブルになっている場合は、メンバーシップ クエリーを送信するようにIGMP スヌーピング クエリアを設定する必要があります。このクエリアは、マルチキャスト送信元と受信者を含み、その他のアクティブ クエリアを含まない VLAN で定義します。

VLAN で任意の IP アドレスを使用するようにクエリアを設定できます。

ベスト プラクティスとして、簡単にクエリアを参照できるようにするには、一意の IP アドレス（スイッチ インターフェイスまたはホット スタンバイ ルータ プロトコル（HSRP）仮想 IP アドレスでまだ使用されていないもの）を設定するべきです。

（注） クエリアのIPアドレスは、ブロードキャストIPアドレス、マルチキャストIPアドレス、または 0（0.0.0.0）にしないでください。

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信されます。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

IGMP スヌーピング クエリアは、RFC 2236 に記述されているようにクエリア選択を実行します。クエリア選択は、次の構成で発生します。

- 異なるスイッチ上の同じ VLAN に同じサブネットに複数のスイッチ クエリアが設定されている場合。
- 設定されたスイッチ クエリアが他のレイヤ 3 SVI クエリアと同じサブネットにある場合。

IGMP スヌーピングの前提条件

IGMP スヌーピングには、次の前提条件が適用されます。

- デバイスにログインしている。
- この章の例で示すデフォルトのコンフィギュレーション モードは、デフォルト VRF に適用されます。

IGMP スヌーピングに関する注意事項と制限事項

IGMP スヌーピングに関する注意事項および制約事項は次のとおりです。

- Cisco Nexus® 3550-T スイッチは、遅延を減らすために PIM が無効になっている着信ポートのパケットのマルチキャスト DestMAC に基づいて、既知のマルチキャスト パケットを転送します。したがって、Cisco Nexus® 3550-T スイッチの IGMPv1/v2 着信レポートは、既知のマルチキャストの受信者に転送されます。
- 低遅延のために、Cisco Nexus® 3550-T スイッチは L2 ポートの {Vlan,MAC} ルックアップのみをサポートします。IP ベースの {VLAN,G} または {VLAN,G,S} ルックアップはありません。
- {Vlan,Mac} ルックアップにより、IGMPv2 のレポートはすでにアタッチされている受信者にフラッドされ、この結果は report-suppression に表示されます。IGMPv3 として構成済みのホストを保持することが推奨されます。
- **ip igmp snooping group-timeout** を有効にする必要があります **ip igmp snooping proxy general-queries** を使用する場合のコマンド を参照してください。これを「never」に設定することをお勧めします。そのように設定しないと、マルチキャストパケットが損失する場合があります。
- Cisco Nexus® 3550-T スイッチは、IPv4 の IGMP スヌーピングをサポートしていますが、IPv6 の MLD スヌーピングはサポートしていません。
- レイヤ 3 IPv6 マルチキャスト ルーティングはサポートされていません。

デフォルト設定

パラメータ	デフォルト
IGMP スヌーピング	有効
明示的な追跡	有効
高速脱退	無効
最終メンバー クエリ間隔	1 秒
スヌーピング クエリア	無効
レポート抑制	有効
リンクローカル グループ抑制	有効
Optimise-multicast-flood	無効

パラメータ	デフォルト
デバイス全体での IGMPv3 レポート抑制	無効
VLAN ごとの IGMPv3 レポート抑制	有効（Enabled）

IGMP スヌーピング パラメータの設定

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

（注） 他のコマンドを有効にする前に、IGMP スヌーピングをグローバルにイネーブルにする必要があります。

グローバル IGMP スヌーピング パラメータの設定

グローバルに IGMP スヌーピング プロセスの動作を変更するには、オプションの IGMP スヌーピング パラメータを設定します。

IGMP スヌーピング パラメータの注記

- IGMP スヌーピング プロキシ パラメータ

  IGMP 一般クエリー（GQ）の各インターバルでスヌーピング スイッチにかかる負担を減らすために、Cisco NX-OS ソフトウェアには、マルチキャスト ルータに設定されたクエリーインターバルから、IGMP スヌーピング スイッチの定期的な一般クエリー動作を分離する方法が用意されています。

  IGMP 一般クエリーをすべてのスイッチ ポートにフラッディングする代わりに、マルチキャスト ルータからの一般クエリーを消費するようにデバイスを設定できます。デバイスが一般クエリーを受信すると、現在アクティブなすべてのグループに対してプロキシ レポートを生成し、ルータのクエリーで指定された MRT で指定されている期間でプロキシ レポートを配布します。同時に、マルチキャスト ルータの定期的な一般クエリーのアクティビティに関係なく、デバイスは、ラウンドロビン方式で VLAN の各ポート上に IGMP 一般クエリーを送信します。これは、次の式によって算出されるレートで VLAN のすべてのインターフェイスを順に処理します。

  レート = {VLAN 内のインターフェイスの数} * {設定された MRT} * {VLAN の数}

  このモードでクエリーを実行する場合、デフォルト MRT 値は 5,000 ミリ秒（5 秒）です。VLAN にスイッチポートが 500 個あるデバイスの場合、システムのすべてのインターフェ

イスを一巡するには2,500秒（40分）かかります。これは、デバイス自体がクエリアの場合でも同様です。

この動作は、随時 1 台のホストだけが一般クエリーに応答し、デバイスのパケット/秒 IGMP 機能を下回るレートによる同時レポート レートが保持されることを確実にします（約 3,000 ～ 4,000 pps）。

（注） このオプションを使用する場合は、**ip igmp snooping group-timeout** を変更する必要があります。 パラメータを高い値に設定するか、タイムアウトしないようにします。

ip igmp snooping プロキシの一般的なクエリ mrt コマンドを使用すると、スヌーピング機能はマルチキャストルータからの一般クエリーにプロキシ応答するようになる一方で、指定された MRT 値を持つ各スイッチポートに対するラウンドロビン式の一般クエリーの送信も行われます。（デフォルトの MRT 値は 5 秒です）。

- IGMP スヌーピング グループ タイムアウト パラメータ

  グループ タイムアウトパラメータを設定すると3回連続で一般クエリーの処理できなかった場合のメンバーシップの期限切れ動作がディセーブルになります。グループ メンバーシップは、デバイスがそのポートで明示的なIGMP脱退を受信するまで、特定のスイッチポートに残ります。

  The **ip igmp snooping group-timeout** {*timeout* | **never**} コマンドは 3 回連続で一般クエリーを受信しなかったときの IGMP スヌーピング グループ メンバーシップの期限切れ動作を変更するか、ディセーブルにします。

手順

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 次のコマンドを使用して、グローバル IGMP スヌーピング パラメータを設定します。

オプション	説明
ip igmp snooping `switch(config)# ip igmp snooping`	デバイスの IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。

オプション	説明
	（注） このコマンドの **no** 形式により、グローバル設定がディセーブルになっている場合は、個々の VLAN で IGMP スヌーピングがイネーブルであるかどうかに関係なく、すべての VLAN で IGMP スヌーピングがディセーブルになります。 IGMP スヌーピングを無効にすると、Cisco Nexus® 3550-Tswitch は IGMP スヌーピング パケット処理のみを無効にします。したがって、このコマンドの **no** 形式を使用しても、マルチキャスト パケットを含む IGMP パケットはハードウェアで転送されません。
ip igmp snooping event-history `switch(config)# ip igmp snooping event-history`	イベント履歴バッファのサイズを設定します。デフォルトは small です。
ip igmp snooping group-timeout {*minutes* | **never**} `switch(config)# ip igmp snooping group-timeout never`	デバイス上のすべての VLAN のグループ メンバーシップ タイムアウト値を設定します。
ip igmp snooping link-local-groups-suppression `switch(config)# ip igmp snooping link-local-groups-suppression`	デバイス全体のリンクローカル グループ抑制を構成します。デフォルトではイネーブルになっています。
ip igmp snooping proxy general-inquiries [**mrt** *seconds*] `switch(config)# ip igmp snooping proxy general-inquiries`	デバイスの IGMP スヌーピング プロキシを設定します。デフォルトは 5 秒です。
ip igmp snooping v3-report-suppression `switch(config)# ip igmp snooping v3-report-suppression`	マルチキャスト対応ルータに送信されるメンバシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。

オプション	説明
ip igmp snooping report-suppression `switch(config)# ip igmp snooping report-suppression`	IGMPv3 レポート抑制およびプロキシ レポートを設定します。デフォルトではディセーブルになっています。

ステップ 3 **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 ごとの IGMP スヌーピング パラメータの設定

VLAN ごとに IGMP スヌーピング プロセスの動作を変更するには、オプションの IGMP スヌーピング パラメータを設定します。

（注） このコンフィギュレーション モードを使用して目的の IGMP スヌーピング パラメータを設定します。ただし、この設定は指定した VLAN を明示的に作成した後にのみ適用されます。VLAN の作成については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

手順

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 igmp snooping**

例：

```
switch(config)# ip igmp snooping
```

IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。

（注） このコマンドの**no**形式により、グローバル設定がディセーブルになっている場合は、個々の VLAN で IGMP スヌーピングがイネーブルであるかどうかに関係なく、すべての VLAN で IGMP スヌーピングがディセーブルになります。 IGMP スヌーピングをディセーブルにすると、レイヤ2マルチキャストフレームがすべてのモジュールにフラッディングします。

ステップ 3 **vlan configuration** *vlan-id*

例：

```
switch(config)# vlan configuration 2
switch(config-vlan-config)#
```

VLAN に対して目的の IGMP スヌーピング パラメータを設定します。これらの設定は、指定した VLAN を作成するまで適用されません。

ステップ 4 次のコマンドを使用して、VLAN ごとに IGMP スヌーピング パラメータを設定します。

オプション	説明
ip igmp snooping `switch(config-vlan-config)# ip igmp snooping`	現在の VLAN に対して IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。
ip igmp snooping access-group {**prefix-list** | **route-map**} *policy-name* **interface** *interface slot/port* `switch(config-vlan-config)# ip igmp snooping access-group prefix-list plist interface ethernet 1/2`	プレフィックスリストまたはルートマップポリシーに基づいて、IGMP スヌーピング レポートにフィルタを設定します。デフォルトではディセーブルになっています。
ip igmp snooping explicit-tracking `switch(config-vlan-config)# ip igmp snooping explicit-tracking`	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトは、すべての VLAN でイネーブルです。
ip igmp snooping fast-leave `switch(config-vlan-config)# ip igmp snooping fast-leave`	IGMPv2 プロトコルのホスト レポート抑制メカニズムのために、明示的に追跡できない IGMPv2 ホストをサポートします。高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。デフォルトは、すべての VLAN でディセーブルです。
ip igmp snooping group-timeout {*minutes* | **never**}	指定した VLAN のグループ メンバーシップ タイムアウトを設定します。

オプション	説明
`switch(config-vlan-config)# ip igmp snooping group-timeout never`	
ip igmp snooping last-member-query-interval 秒 `switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3`	いずれのホストからもIGMPクエリーメッセージへの応答がないまま、最終メンバのクエリーインターバルの期限が切れた場合に、関連するVLANポートからグループを削除します。有効範囲は1～25秒です。デフォルト値は1秒です。
ip igmp snooping proxy general-queries [**mrt** *seconds*] `switch(config-vlan-config)# ip igmp snooping proxy general-queries`	指定したVLANのIGMPスヌーピング プロキシを設定します。デフォルトは5秒です。
ip igmp snooping querier *ip-address* `switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106`	マルチキャストトラフィックをルーティングする必要がないため、PIMをイネーブルにしていない場合に、スヌーピングクエリアを設定します。IPアドレスは、メッセージの送信元として使用します。
ip igmp snooping querier-timeout 秒 `switch(config-vlan-config)# ip igmp snooping querier-timeout 300`	マルチキャストトラフィックをルーティングする必要がないため、PIMをイネーブルにしていない場合の、IGMPv2のスヌーピング クエリア タイムアウト値を設定します。デフォルト値は255秒です。
ip igmp snooping query-interval 秒 `switch(config-vlan-config)# ip igmp snooping query-interval 120`	マルチキャストトラフィックをルーティングする必要がないため、PIMをイネーブルにしていない場合に、スヌーピングクエリーインターバルを設定します。デフォルト値は125秒です。
ip igmp snooping query-max-response-time 秒 `switch(config-vlan-config)# ip igmp snooping query-max-response-time 12`	マルチキャストトラフィックをルーティングする必要がないため、PIMをイネーブルにしていない場合に、クエリー メッセージのスヌーピング MRTを設定します。デフォルト値は10秒です。
ip igmp snooping report-policy {**prefix-list** | **route-map**} *policy-name* **interface** *interface slot/port*	プレフィックスリストまたはルートマップポリシーに基づいて、IGMP スヌーピング レポートにフィルタを設定します。デフォルトではディセーブルになっています。

オプション	説明
`switch(config-vlan-config)# ip igmp snooping report-policy route-map rmap interface ethernet 1/4`	
ip igmp snooping startup-query-count *value* `switch(config-vlan-config)# ip igmp snooping startup-query-count 5`	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時に送信されるクエリー数に対してスヌーピングを設定します。
ip igmp snooping startup-query-interval 秒 `switch(config-vlan-config)# ip igmp snooping startup-query-interval 15000`	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時のスヌーピング クエリー インターバルを設定します。
ip igmp snooping robustness-variable *value* `switch(config-vlan-config)# ip igmp snooping robustness-variable 5`	指定した VLAN のロバストネス値を設定します。デフォルト値は 2 です。
ip igmp snooping report-suppression `switch(config-vlan-config)# ip igmp snooping report-suppression`	マルチキャスト対応ルータに送信されるメンバシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。
ip igmp snooping mrouter interface *interface* `switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 1/1`	マルチキャスト ルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。**ethernet** *slot*/*port* のように、インターフェイスはタイプおよび番号で指定できます。
ip igmp snooping static-group *group-ip-addr* [**source** *source-ip-addr*] **interface** *interface* `switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 1/1`	VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メンバーとして設定します。**ethernet** *slot*/*port* のように、インターフェイスはタイプおよび番号で指定できます。
ip igmp snooping link-local-groups-suppression	指定した VLAN のリンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。

オプション	説明
`switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression`	
ip igmp snooping v3-report-suppression `switch(config-vlan-config)# ip igmp snooping v3-report-suppression`	指定したVLANのIGMPv3レポート抑制およびプロキシレポートを設定します。デフォルトではVLANごとに有効になっています。
ip igmp snooping version *value* `switch(config-vlan-config)# ip igmp snooping version 2`	指定したVLANのIGMPバージョン番号を設定します。

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。

IGMP スヌーピング設定の確認

コマンド	説明
show ip igmp snooping [**vlan** *vlan-id*]	IGMP スヌーピング設定を VLAN 別に表示します。
show ip igmp snooping groups [*source* [*group*] | *group* [*source*]] [**vlan** *vlan-id*] [**detail**]	グループに関する IGMP スヌーピング情報を VLAN 別に表示します。
show ip igmp snooping querier [**vlan** *vlan-id*]	IGMP スヌーピング クエリアを VLAN 別に表示します。
show ip igmp snooping mroute [**vlan** *vlan-id*]	マルチキャストルータポートをVLAN別に表示します。
show ip igmp snooping explicit-tracking [**vlan** *vlan-id*] [**detail**]	IGMP スヌーピングの明示的な追跡情報を VLAN 別に表示します。

IGMP スヌーピング統計情報の表示

次のコマンドを使用して、IGMP スヌーピング統計情報を表示できます。

コマンド	説明
show ip igmp snooping statistics vlan	IGMP スヌーピング統計情報を表示します。この出力で、仮想ポート チャネル（vPC）の統計情報を確認できます。
show ip igmp snooping {**report-policy** | **access-group**} **statistics** [**vlan** *vlan*]	IGMP スヌーピングのフィルタが設定されている場合、VLAN ごとに詳細な統計情報を表示します。

IGMP スヌーピング統計情報のクリア

次のコマンドを使用して、IGMP スヌーピング統計情報をクリアできます。

コマンド	説明
clear ip igmp snooping statistics vlan	IGMP スヌーピングの統計情報をクリアします。
clear ip igmp snooping {**report-policy** | **access-group**} **statistics** [**vlan** *vlan*]	IGMP スヌーピング フィルタの統計情報をクリアします。

IGMP スヌーピングの設定例

（注） このセクションでの設定は、指定された VLAN を作成した後にのみ適用されます。VLAN の作成については、「*Cisco Nexus 3550-T Layer 2 Switching* 構成ガイド」のセクションを参照してください。

次に、IGMP スヌーピング パラメータを設定する例を示します。

```
config t
  ip igmp snooping
  vlan configuration 2
    ip igmp snooping
    ip igmp snooping explicit-tracking
    ip igmp snooping fast-leave
    ip igmp snooping last-member-query-interval 3
    ip igmp snooping querier 172.20.52.106
    ip igmp snooping report-suppression
```

```
    ip igmp snooping mrouter interface ethernet 1/1
    ip igmp snooping static-group 230.0.0.1 interface ethernet 1/1
    ip igmp snooping link-local-groups-suppression
    ip igmp snooping v3-report-suppression
```

次に、プレフィックス リストを設定し、これらを使用して IGMP スヌーピング レポートをフィルタ処理する例を示します。

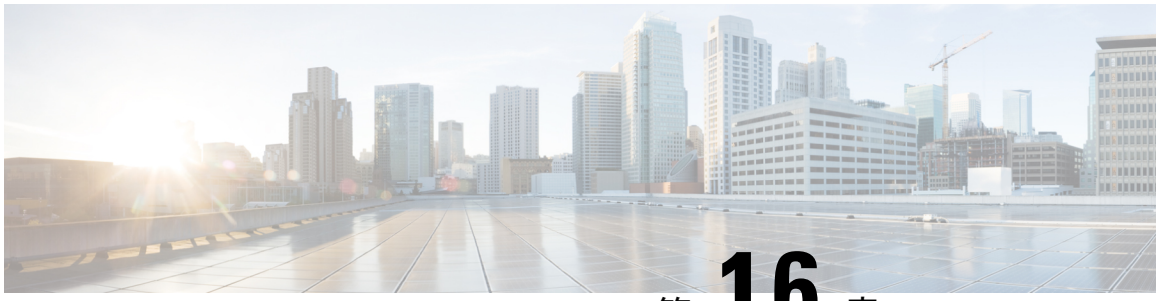
```
ip prefix-list plist seq 5 permit 224.1.1.1/32
ip prefix-list plist seq 10 permit 224.1.1.2/32
ip prefix-list plist seq 15 deny 224.1.1.3/32
ip prefix-list plist seq 20 deny 225.0.0.0/8 eq 32

vlan configuration 2
  ip igmp snooping report-policy prefix-list plist interface Ethernet 1/2
  ip igmp snooping report-policy prefix-list plist interface Ethernet 1/3
```

上記の例では、プレフィックス リストは 224.1.1.1 と 224.1.1.2 を許可していますが、224.1.1.3 と 225.0.0.0/8 範囲のすべてのグループを拒否しています。プレフィックス リストは、一致がない場合は暗黙的な「拒否」になります。その他すべてを許可する場合、**ip prefix-list plist seq 30 permit 224.0.0.0/4 eq 32** を追加します。

次に、ルート マップを設定し、これらを使用して IGMP スヌーピング レポートをフィルタ処理する例を示します。

```
route-map rmap permit 10
  match ip multicast group 224.1.1.1/32
route-map rmap permit 20
  match ip multicast group 224.1.1.2/32
route-map rmap deny 30
  match ip multicast group 224.1.1.3/32
route-map rmap deny 40
  match ip multicast group 225.0.0.0/8

vlan configuration 2
  ip igmp snooping report-policy route-map rmap interface Ethernet 1/4
  ip igmp snooping report-policy route-map rmap interface Ethernet 1/5
```

上記の例では、ルートマップは 224.1.1.1 と 224.1.1.2 を許可していますが、224.1.1.3 と 225.0.0.0/8 範囲のすべてのグループを拒否しています。ルートマップは、一致がない場合は暗黙的な「拒否」になります。その他すべてを許可する場合、**route-map rmap permit 50 match ip multicast group 224.0.0.0/4** を追加します。



第 16 章

PIM の設定

この章では、IPv4 ネットワークの Cisco NX-OS デバイスに Protocol Independent Multicast（PIM）機能を構成する方法を説明します。

PIM について

マルチキャスト対応ルータ間で使用される PIM は、マルチキャスト配信ツリーを構築して、ルーティング ドメイン内にグループ メンバーシップをアドバタイズします。PIM は、複数の送信元からのパケットが転送される共有配信ツリーと、単一の送信元からのパケットが転送される送信元配信ツリーを構築します。

Cisco NX-OS は、IPv4 ネットワーク（PIM）対応の PIM スパース モードをサポートします。PIM スパース モードでは、ネットワーク上の要求元だけにマルチキャスト トラフィックが伝送されます。ルータ上で同時に実行するように PIM を構成できます。PIM グローバル パラメータを使用すると、ランデブー ポイント（RP）、メッセージ パケット フィルタリング、および統計情報を設定できます。PIM インターフェイス パラメータを使用すると、マルチキャスト機能のイネーブル化、PIM の境界の識別、PIM hello メッセージ インターバルの設定、および指定ルータ（DR）のプライオリティ設定を実行できます。

（注） Cisco NX-OS は、PIM デンス モードをサポートしていません。

Cisco NX-OS でマルチキャスト機能を有効化するには、各ルータで PIM 機能を有効化してから、マルチキャストに参加する各インターフェイスで、PIM スパース モードを有効化する必要があります。PIM は IPv4 ネットワーク用に構成できます。IPv4 ネットワーク上のルータで IGMP がイネーブルになっていない場合は、PIM によって自動的にイネーブルにされます。

PIM グローバル構成パラメータを使用すると、マルチキャスト グループ アドレスの範囲を構成して、次に示す配信モードで利用できます。

- Any Source Multicast（ASM）：マルチキャスト送信元の検出機能を提供します。ASM では、マルチキャスト グループの送信元と受信者間に共有ツリーを構築し、新しい受信者がグループに追加された場合は、送信元ツリーに切り替えることができます。ASM モードを利用するには、RP を設定する必要があります。

ASM モードで使用される PIM スパース モードと共有配信ツリーの詳細については、「RFC 4601」を参照してください。

（注） Cisco Nexus® 3550-T は、次をサポートしていません。

- Cisco Nexus® 3550-T は、マルチキャスト FHR デバイスとして動作できません。
- Cisco Nexus® 3550-T は、ソース ツリー（SG-Tree）の形成をサポートしていません。

Hello メッセージ

ルータがマルチキャスト IPv4 アドレス 224.0.0.13 に PIM hello メッセージを送信して、PIM ネイバー ルータとの隣接関係を確立すると、PIM プロセスが開始されます。hello メッセージは 30 秒間隔で定期的に送信されます。PIM ソフトウェアはすべてのネイバーからの応答を確認すると、各 LAN セグメント内で優先順位が最大のルータを代表ルータ（DR）として選択します。DR 優先順位は、PIM hello メッセージの DR 優先順位値に基づいて決まります。全ルータの DR プライオリティ値が不明、またはプライオリティが等しい場合は、IP アドレスが最上位のルータが DR として選定されます。

hello メッセージには保持時間の値も含まれています。通常、この値は hello インターバルの 3.5 倍です。ネイバーから後続の hello メッセージがないまま保留時間を経過すると、デバイスはそのリンクで PIM エラーが生じたと判断します。

設定された保留時間の変更は、インターフェイスで PIM を有効または無効にした後に送信される最初の 2 つの hello には反映されない場合があります。その後、インターフェイスで送信される最初の 2 つの hello については、設定された保留時間が使用されます。これにより、正しい保留時間の hello を受信するまで、PIM ネイバーは、初期ネイバー セットアップについて、誤ったネイバー タイムアウト値を設定する可能性があります。

PIM ソフトウェアで、PIM ネイバーとの PIM hello メッセージの認証に MD5 ハッシュ値を使用するよう設定すると、セキュリティを高めることができます。

Join-Prune メッセージ

DR が新しいグループの受信者または送信元から IGMP メンバーシップ レポート メッセージを受信すると、DR は、ランデブー ポイント（ASM モード）に面しているインターフェイスから PIM Join メッセージを送信することにより、受信者を送信元に接続するためのツリーを作成します。ランデブー ポイント（RP）とは、ASM モードで PIM ドメイン内のすべての送信元およびホストにより使用される、共有ツリーのルートです。

DR はグループまたは送信元から最後のホストが脱退したことを認識すると、PIM Prune メッセージを送信して、配信ツリーから該当するパスを削除します。

各ルータは、マルチキャスト配信ツリーの上流方向のホップに Join または Prune アクションを次々と転送し、パスを作成（Join）または削除（Prune）します。

（注） このマニュアル内の「PIM join メッセージ」および「PIM prune メッセージ」という用語は、PIM join-prune メッセージに関して、Join または Prune アクションのうち実行されるアクションのみをわかりやすく示すために使用しています。

Join/Prune メッセージは、ソフトウェアからできるだけ短時間で送信されます。join-prune メッセージをフィルタリングするには、ルーティング ポリシーを定義します。

ステートのリフレッシュ

PIM では、3.5 分のタイムアウト間隔でマルチキャスト エントリをリフレッシュする必要があります。ステートをリフレッシュすると、トラフィックがアクティブなリスナーだけに配信されるため、ルータで不要なリソースが使用されなくなります。

PIM ステートを維持するために、最終ホップである DR は、Join/Prune メッセージを 1 分に 1 回送信します。次に、（*, G）ステートの構築例を示します。

- （*, G）ステートの構築例：IGMP（*, G）レポートを受信すると、DR は （*, G）PIM Join メッセージを RP 方向に送信します。

ステートがリフレッシュされていない場合、PIM ソフトウェアは、上流ルータのマルチキャスト発信インターフェイス リストから転送パスを削除し、配信ツリーを再構築します。

ランデブー ポイント

ランデブー ポイント（RP）は、マルチキャスト ネットワーク ドメイン内にあるユーザが指定したルータで、マルチキャスト共有ツリーの共有ルートとして動作します。必要に応じて複数の RP を設定し、さまざまなグループ範囲をカバーすることができます。

スタティック RP

マルチキャスト グループ範囲の RP は静的に設定できます。この場合、ドメイン内のすべてのルータに RP のアドレスを設定する必要があります。

スタティック RP を定義するのは、次のような場合です。

- ルータに Anycast RP アドレスを設定する場合
- デバイスに RP を手動で設定する場合

（注） Cisco Nexus® 3550-T は、Static-RP のみをサポートおよび検証します。

PIM 登録メッセージ

PIM Register メッセージは、マルチキャスト送信元に直接接続された指定ルータ（DR）から RP にユニキャストされます。PIM Register メッセージには次の機能があります。

- マルチキャスト グループに対する送信元からの送信がアクティブであることを RP に通知する
- 送信元から送られたマルチキャスト パケットを RP に配信し、共有ツリーの下流に転送する

DR は RP から Register-Stop メッセージを受信するまで、PIM Register メッセージを RP 宛に送信し続けます。RP が Register-Stop メッセージを送信するのは、次のいずれかの場合です。

- RP が送信中のマルチキャスト グループに、受信者が存在しない場合
- RP が送信元への SPT に加入しているにもかかわらず、送信元からのトラフィックの受信が開始されていない場合

PIM トリガー レジスタはデフォルトで有効になっています。

ip pim register-source を使用できます コマンドは、登録メッセージの送信元 IP アドレスが、RP がパケットを送信できる一意のルーテッド アドレスではない場合に、登録メッセージの送信元 IP アドレスを設定するために使用します。このような状況は、受信したパケットが転送されないように送信元アドレスがフィルタリングされる場合、または送信元アドレスがネットワークに対して一意でない場合に発生します。このような場合、RP から送信元アドレスへ送信される応答は DR に到達せず、Protocol Independent Multicast Sparse Mode（PIM-SM）プロトコル障害が発生します。

次に、登録メッセージの IP 送信元アドレスを DR のループバック 3 インターフェイスに設定する例を示します。

```
ip pim register-source loopback 3
```

（注） Cisco Nexus 3550-T ハードウェアにインストールされているすべてのマルチキャスト ルートに対して実行される RPF チェックはありません。エントリに到達したパケットは、着信インターフェイスに関係なく、プログラムされたすべての受信者にフラッディングされます。

（注） Cisco NX-OS では RP の処理の停滞を防ぐため、PIM Register メッセージのレート制限が行われます。

指定ルータ

PIM の ASM モードでは、各ネットワーク セグメント上のルータの中から指定ルータ（DR）が選択されます。DR は、セグメント上の指定グループおよび送信元にマルチキャスト データを転送します。

LAN セグメントごとの DR は、「Hello メッセージ」に記載された手順で決定されます。

ASM モードの場合、DR は RP に PIM Register パケットをユニキャストします。DR が、直接接続された受信者からの IGMP メンバーシップ レポートを受信すると、DR を経由するかどうかに関係なく、RP への最短パスが形成されます。これにより、同じマルチキャスト グループ上で送信を行うすべての送信元と、そのグループのすべての受信者を接続する共有ツリーが作成されます。

（注） Cisco Nexus 3550-T ハードウェアに接続された直接の受信者がない場合、Cisco Nexus 3550-T は指定されたルータにマルチキャスト パケットを転送しません。

（注） PIM-BIDIR モードは、Cisco Nexus 3550-T ではサポートされていません。

（注） 共有ツリーから送信元ツリーへの ASM スイッチオーバーは、Cisco Nexus 3550-T 10.1(2t) リリースではサポートされていません。

PIM の前提条件

- デバイスにログインしている。

- 現在の仮想ルーティングおよびフォワーディング（VRF）モードが正しい（グローバル コマンドの場合）。この章の例で示すデフォルトのコンフィギュレーション モードは、デフォルト VRF に適用されます。

（注） Cisco Nexus 3550-T - 10.1(2t) リリースはデフォルトの VRF のみをサポートします。

PIM の注意事項と制約事項

PIM には、次の注意事項と制限事項があります。

（注） ***Cisco Nexus 3550-T - 10.1(2t)* リリース** では、PIM はデフォルトの VRF のみがサポートされています。

- Cisco Nexus® 3550-T スイッチでは、PIM-ASM モードのみがサポートされています。
- ***Cisco Nexus 3550-T - 10.1(2t)* リリース** は、AutoRP または BSR 構成をサポートしていません。
- {Vrf,S,G} ルートがサポートされていないため、以下の構成が推奨されます：
  - **ip pim spt-threshold infinity** の構成
  - PIM-SSM を無効にします。
  - IGMPv3 スヌーピングが有効になっていても、IGMPv3 から受信した {S,G} は Cisco Nexus 3550-T - 10.1(2t) リリースにはインストールされません。
- RPF チェックはハードウェアに導入されていないため、受信した RPF 失敗パケットは、インストールされた {*,G} ルート oiflist に転送されます。ただし、着信 L3 ポートでパケットを転送しないようにハードウェア チェックが導入されています。
- Cisco Nexus® 3550-T スイッチはカットスルー転送を行います。したがって、MTU チェックは導入されていません。ハードウェア バッファリングはジャンボ パケット用に設計されておらず、通常の MTU サイズ 1516 を超えるパケットはサポートされていません。
- L3 マルチキャスト ルックアップは、トランク ポートでは有効化されていません。
- L3 マルチキャストには、次のスケール番号があります。
  - L2MCAST - MAC テーブルと共有される 768 システム全体 - {vlan,MAC}
  - EntriesL3MCAST - 384 システム全体の {vrf,G,*} エントリのみ

- L3 マルチキャストの結果には、トランク ポートを OIF として含めることはできません。トランク ポート OIF でインストールするように計算されたエントリは、ハードウェアにインストールされていません。
- L3 マルチキャスト ルックアップ ミス パケットは SUP にパントされません。したがって、Cisco Nexus® 3550-T スイッチは FHR として機能できません。ただし、{*,G} ツリーがすでにインストールされている場合は、そのパスに沿ってマルチキャストを転送します。
- L3 ルックアップが完了したとき。L2 ドメイン マルチキャストの受信者でさえ、減分された TTL でパケットを受信します。
- Cisco Nexus® 3550-T プラットフォーム スイッチは、MSDP をサポートしていません。
- ほとんどの Cisco Nexus デバイスでは、RPF 障害トラフィックはドロップされ、PIM アサートをトリガーするために非常に低レートで CPU に送信されます。Cisco Nexus® 3550-T スイッチは、RPF 障害をチェックせず、すべてのトラフィックはインストールされたルートに従って転送されます。
- ほとんどの Cisco Nexus デバイスのファーストホップ送信元検出では、ファースト ホップからのトラフィックは送信元サブネット チェックに基づいて検出され、マルチキャスト パケットは送信元がローカル サブネットに属する場合に限り、CPU にコピーされます。Cisco Nexus® 3550-T スイッチは FHR 機能をサポートしておらず、ファースト ホップ トラフィックを検出できないため、ローカル マルチキャスト送信元を学習するためにスーパーバイザにマルチキャスト パケットが送信されません。
- Cisco NX-OS の PIM は、いずれのバージョンの PIM デンス モードまたは PIM スパース モード バージョン 1 とも相互運用性がありません。

Hello メッセージに関する注意事項と制限事項

Hello メッセージには、次の注意事項および制約事項が適用されます。

- PIM hello 間隔はデフォルト値が推奨されます。この値は変更しないでください。

ランデブー ポイントの注意事項と制限事項

ランデブー ポイント (RP) には、次の注意事項と制限事項が適用されます。

- Cisco Nexus 3550-T - 10.1(2t) リリースは、静的 RP としてのみ動作できます。

デフォルト設定

次の表に、PIM パラメータのデフォルト設定を示します。

表 *13 : PIM* パラメータのデフォルト設定

パラメータ	デフォルト
共有ツリーだけを使用	無効
再起動時にルートをフラッシュ	無効
ログ ネイバーの変更	無効
Auto-RP メッセージ アクション	無効 （注） BSR は Cisco Nexus 3550-T - 10.1(2t) リリースでは使用できないため、Auto-RP メッセージ アクションを**有効にしないでください**。
BSR メッセージ アクション	無効 （注） BSR は Cisco Nexus 3550-T - 10.1(2t) リリースでは使用できないため、BSR メッセージアクションを**有効にしないでください**。
PIM スパース モード	無効
DR プライオリティ	1
hello 認証モード	無効
ドメイン境界	無効 （注） Cisco Nexus 3550-T - 10.1(2t) リリースではドメイン ボーダーが使用できないため、**有効にしないでください**。

（注） Cisco Nexus 3550-T - 10.1(2t) リリースはポリシー設定をサポートしていないため、無効になっています。

PIM の設定

（注） Cisco NX-OS は、PIM スパース モード バージョン 2 のみをサポートします。このマニュアルで「PIM」と記載されている場合は、PIM スパース モードのバージョン 2 を意味しています。

下の表で説明されているマルチキャスト配信モードを使用すると、PIM ドメインに、それぞれ独立したアドレス範囲を構成できます。

マルチキャスト配信モード	RP 設定の必要性	説明
アーキテクチャ セールス マネージャ（ASM）	はい	任意の送信元のマルチキャスト
マルチキャスト用 RPF ルート	いいえ	マルチキャスト用 RPF ルート

（注） RPF チェックは Cisco Nexus 3550-T - 10.1(2t) リリースではサポートされておらず、プログラムされた受信者への RPF 障害に関係なく、マルチキャスト パケットがフラッディングされます。

PIM の構成タスク

次の手順で PIM を構成します。

手順

	コマンドまたはアクション	目的
ステップ 1	各マルチキャスト配信モードで設定するマルチキャスト グループの範囲を選択します。	
ステップ 2	PIM をイネーブルにします。	
ステップ 3	ステップ 1 で選択したマルチキャスト配信モードについて、設定作業を行います。	
ステップ 4		

PIM 機能の有効化

PIM コマンドにアクセスするには、PIM 機能をイネーブルにしておく必要があります。

始める前に

Enterprise Services ライセンスがインストールされていることを確認してください。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**feature pim** 例： `switch(config)# feature pim`	PIM をイネーブルにします。デフォルトでは PIM はディセーブルになっています。
ステップ 3	（任意） **show running-configuration pim** 例： `switch(config)# show running-configuration pim`	PIM の実行コンフィギュレーション情報を示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

PIM6 スパース モード パラメータの設定

スパース モード ドメインに参加させる各デバイス インターフェイスで、PIM スパース モードを構成します。次の表に、構成可能なスパース モード パラメータを示します。

表 *14 : PIM* スパース モード パラメータ

パラメータ	説明
デバイスにグローバルに適用	
Register のレート制限	IPv4 Register のレート制限を毎秒のパケット数で設定します。指定できる範囲は 1 ～ 65,535 です。デフォルト設定は無制限です。

パラメータ	説明
初期ホールドダウン期間	IPv4 初期ホールドダウン期間を秒単位で設定します。このホールドダウン期間は、MRIB が最初に起動するのにかかる時間です。コンバージェンスを高速化するには、小さい値を入力します。指定できる範囲は 90 ～ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
デバイスの各インターフェイスに適用	
PIM スパース モード	インターフェイスに対して PIM をイネーブルにします。
DR プライオリティ	現在のインターフェイスに、PIM hello メッセージの一部としてアドバタイズされる指定ルータ（DR）プライオリティを設定します。複数の PIM 対応ルータが存在するマルチアクセス ネットワークでは、DR プライオリティの最も高いルータが DR ルータとして選定されます。プライオリティが等しい場合は、IP アドレスが最上位のルータが DR に選定されます。DR は、直接接続されたマルチキャスト送信元に PIM Register メッセージを送信するとともに、直接接続された受信者に代わって、ランデブーポイント（RP）方向に PIM Join メッセージを送信します。有効範囲は 1 ～ 4294967295 です。デフォルトは 1 です。
指定ルータの遅延	PIM hello メッセージでアドバタイズされる DR プライオリティを指定期間にわたり 0 に設定することで、指定ルータ（DR）の選定への参加を遅延させます。この遅延中、DR は変更されず、現在のスイッチにはそのインターフェイスでのすべてのマルチキャストの状態を把握する時間が与えられます。遅延期間が終了すると、DR 選出を再び開始するために、正しい DR プライオリティが hello パケットで送信されます。値の範囲は 3 ～ 0xffff 秒です。

パラメータ	説明
hello 認証モード	インターフェイスで、PIM hello メッセージ内の MD5 ハッシュ認証キー（パスワード）をイネーブルにして、直接接続されたネイバーによる相互認証を可能にします。PIM hello メッセージは、認証ヘッダー（AH）オプションを使用して符号化された IP セキュリティ です。暗号化されていない（クリアテキストの）キーか、または次に示す値のいずれかを入力したあと、スペースと MD5 認証キーを入力します。 • 0：暗号化されていない（クリアテキストの）キーを指定します。 • 3：3-DES 暗号化キーを指定します。 • 7：Cisco Type 7 暗号化キーを指定します。 認証キーの文字数は最大 16 文字です。デフォルトではディセーブルになっています。
hello 間隔	hello メッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1000 ～ 18724286 です。デフォルト値は 30000 です。 （注） このパラメータの検証済みの範囲および関連付けられた PIM ネイバー スケールについては、『*Cisco Nexus® 3550-T* 検証済みの拡張性ガイド』を参照してください。

PIM6 スパース モード パラメータの設定

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
ステップ 2	（任意） **ip pim register-rate-limit** *rate* 例： `switch(config)# ip pim register-rate-limit 1000`	レート制限を毎秒のパケット数で設定します。指定できる範囲は 1 ～ 65,535 です。デフォルト設定は無制限です。
ステップ 3	（任意） **ip pim spt-threshold infinity group-list** *route-map-name* 例： `switch(config)# ip pim spt-threshold infinity group-list my_route-map-name`	指定されたルートマップで定義されているグループ プレフィックスに対して、IPv4 PIM（*, G）状態のみを作成します。Cisco NX-OS リリース 3.1 は最大 1000 のルート マップ エントリを、リリース 3.1 より前の Cisco NX-OS は最大 500 のルートマップ エントリをサポートします。 （注） **ip pim use-shared-tree-only group-list** コマンドは、**ip pim spt-threshold infinity group-list** コマンドと同じ機能を実行します。いずれかのコマンドを使用してこの手順を実行できます。
ステップ 4	（任意） [**ip** | **ipv4**] **routing multicast holddown** *holddown-period* 例： `switch(config)# ip routing multicast holddown 100`	初期ホールドダウン期間を秒単位で設定します。指定できる範囲は 90 ～ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
ステップ 5	（任意） **show running-configuration pim** 例： `switch(config)# show running-configuration pim`	、PIM 実行コンフィギュレーション情報を表示します。

ステップ 6	**interface** *interface*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 7	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	現在のインターフェイスで PIM スパース モードをイネーブルにします。デフォルトではディセーブルになっています。

	コマンドまたはアクション	目的
ステップ 8	（任意） **ip pim dr-priority** *priority* 例： `switch(config-if)# ip pim dr-priority 192`	PIM hello メッセージの一部としてアドバタイズされる指定ルータ（DR）プライオリティを設定します。有効範囲は 1 ～ 4294967295 です。デフォルトは 1 です。
ステップ 9	（任意） **ip pim dr-delay** *delay* 例： `switch(config-if)# ip pim dr-delay 3`	PIM hello メッセージでアドバタイズされる DR プライオリティを指定期間にわたり 0 に設定することで、指定ルータ（DR）の選定への参加を遅延させます。この遅延中、DR は変更されず、現在のスイッチにはそのインターフェイスでのすべてのマルチキャストの状態を把握する時間が与えられます。遅延期間が終了すると、DR 選出を再び開始するために、正しい DR プライオリティが hello パケットで送信されます。値の範囲は 3 ～ 0xffff 秒です。 （注） このコマンドは、起動時、または IP アドレスかインターフェイスの状態が変更された後にのみ、DR 選定への参加を遅延させます。これは、マルチキャストアクセスのレイヤ 3 インターフェイス専用です。
ステップ 10	（任意） **ip pim hello-authentication ah-md5** *auth-key* 例： `switch(config-if)# ip pim hello-authentication ah-md5 my_key`	PIM hello メッセージ内の MD5 ハッシュ認証キーをイネーブルにします。暗号化されていない（クリアテキストの）キーか、または次に示す値のいずれかを入力したあと、スペースと MD5 認証キーを入力します。 • 0：暗号化されていない（クリアテキストの）キーを指定します。 • 3：3-DES 暗号化キーを指定します。 • 7：Cisco Type 7 暗号化キーを指定します。

	コマンドまたはアクション	目的
		キーの文字数は最大 16 文字です。デフォルトではディセーブルになっています。
ステップ 11	（任意） **ip pim hello-interval** *interval* 例： `switch(config-if)# ip pim hello-interval 25000`	hello メッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1000 ～ 18724286 です。デフォルト値は 30000 です。 （注） 最小値は 1 ミリ秒です。
ステップ 12	（任意） **show ip pim interface** [*interface* | **brief**] 例： `switch(config-if)# show ip pim interface`	PIM インターフェイスの情報を表示します。
ステップ 13	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ASM の構成

ASM モードを構成するには、スパース モードおよび RP の選択方式を構成します。RP の選択方式では、配信モードを指定して、マルチキャスト グループの範囲を割り当てます。

静的 RP の設定

RP を静的に設定するには、PIM ドメインに参加するルータのそれぞれに RP アドレスを設定します。

（注） RP アドレスがループバック インターフェイスを使用することをお勧めします。また、RP アドレスを持つインターフェイスで、**ip pim sparse-mode** が有効になっている必要があります。

静的 RP の設定

始める前に

Enterprise Services ライセンスがインストールされていること、および PIM がイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**ip pim rp-address** *rp-address* 例： `switch(config)# ip pim rp-address 192.0.2.33`	マルチキャスト グループに、PIM 静的 RP アドレスを構成します。 静的RPアドレスのプレフィックス リスト ポリシー名を指定できます。 モードは ASM です。
ステップ 3	（任意） **show ip pim group-range** *ip-prefix* 例： `switch(config)# show ip pim group-range`	PIM RP 情報を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ASM 専用の共有ツリーの設定

共有ツリーを構成できるのは、Any Source Multicast（ASM）グループの最終ホップ ルータだけです。この場合、受信者がアクティブ グループに加入しても、このルータでは共有ツリーから SPT へのスイッチオーバーは実行されません。

（注） Cisco Nexus® 3550-T は、共有ツリー機能のみをサポートします。

メッセージ フィルタリングの設定

以下の表に示す PIM メッセージのフィルタリングを構成できます。

表 *15 : PIM* メッセージのフィルタリング

メッセージの種類	説明
デバイスにグローバルに適用	

メッセージの種類	説明
ネイバーの変更の記録	ネイバーのステート変更を通知するSyslogメッセージをイネーブルにします。デフォルトではディセーブルになっています。

メッセージ フィルタリングの設定

始める前に

Enterprise Servicesライセンスがインストールされていること、およびPIMがイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的

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

ステップ2	（任意） **ip pim log-neighbor-changes** 例： `switch(config)# ip pim log-neighbor-changes`	ネイバーのステート変更を通知するSyslog メッセージをイネーブルにします。デフォルトではディセーブルになっています。
ステップ3	（任意） **show run pim** 例： `switch(config-if)# show run pim`	PIM 構成コマンドを表示します。
ステップ4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

PIM プロセスの再起動

フラッシュされたルートは、マルチキャスト ルーティング情報ベース（MRIB）、およびマルチキャスト転送情報ベース（MFIB）から削除されます。

PIM を再起動すると、次の処理が実行されます。

- PIM データベースが削除されます。
- MRIB および MFIB は影響を受けず、トラフィックは引き続き転送されます。

- マルチキャスト ルートの所有権が MRIB 経由で検証されます。
- ネイバーから定期的に送信される PIM Join メッセージおよび Prune メッセージを使用して、データベースにデータが再度読み込まれます。

PIM プロセスの再起動

始める前に

Enterprise Services ライセンスがインストールされていること、および PIM がイネーブルになっていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**restart pim** 例： `switch# restart pim`	PIM プロセスを再起動します。 （注） 再起動プロセス中にはトラフィック損失が発生する可能性があります。

ステップ 2	**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 3	**ip pim flush-routes** 例： `switch(config)# ip pim flush-routes`	PIM プロセスの再起動時に、ルートを削除します。デフォルトでは、ルートはフラッシュされません。
ステップ 4	（任意） **show running-configuration pim** 例： `switch(config)# show running-configuration pim`	**flush-routes** コマンドを含む、PIM 実行コンフィギュレーション情報を示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

PIM 設定の確認

PIM の構成情報を表示するには、次の作業のいずれかを行います。

コマンド	説明
show ip mroute [*ip-address*] [**detail** | **summary**]	IP マルチキャスト ルーティング テーブルを表示します。 **detail** オプションは、詳細なルート属性を表示します。 **summary** オプションは、ルート カウントとパケット レートを表示します。 （注） このコマンドは、マルチキャスト ヘビーテンプレートが有効になっている場合、Cisco Nexus® 3550-T スイッチのマルチキャスト カウンタも表示します。以下のサンプル出力を参照してください。
show ip pim group-range [*ip-prefix*]	学習済みまたは設定済みのグループ範囲およびモードを表示します。同様の情報については、**show ip pim rp** コマンドを参照してください。
show ip pim interface [*interface* | **brief**]	情報をインターフェイス別に表示します。
show ip pim neighbor [**interface** *interface* | *ip-prefix*]	ネイバーをインターフェイス別に表示します。
show ip pim oif-list *group* [*source*]	発信インターフェイス（OIF）リスト内のすべてのインターフェイスを表示します。
show ip pim route [*source* | *group* [*source*]]	各マルチキャスト ルートの情報を表示します。指定した（*, G）に対して、PIM Join メッセージを受信したインターフェイスなどを表示できます。
show ip pim rp [*ip-prefix*]	ソフトウェアの既知のランデブー ポイント（RP）およびその学習方法と、それらのグループ範囲を表示します。同様の情報については、**show ip pim group-range** コマンドを参照してください。
show running-config pim	実行コンフィギュレーション情報を表示します。
show startup-config pim	スタートアップ コンフィギュレーション情報を表示します。

コマンド	説明
show ip pim [**detail**]	PIM の詳細情報を表示します。

統計の表示

次に、PIM の統計情報を、表示およびクリアするコマンドについて説明します。

PIM 統計情報の表示

これらのコマンドを使用すると、PIM の統計とメモリ使用状況を表示できます。

コマンド	説明
show ip pim policy statistics	レジスタ、RP、および Join/Prune メッセージのポリシーについて、ポリシー統計情報を表示します。
show ip pim statistics	グローバル統計情報を表示します。

PIM 統計情報のクリア

これらのコマンドを使用すると、PIM 統計をクリアできます。

コマンド	説明
clear ippim interface statistics *interface*	指定したインターフェイスのカウンタをクリアします。
clear ip pim policy statistics	レジスタ、RP、および join-prune メッセージポリシーについて、ポリシー カウンタをクリアします。
clear ip pim statistics	PIM プロセスで使用されるグローバル カウンタをクリアします。

関連資料

関連項目	マニュアル タイトル

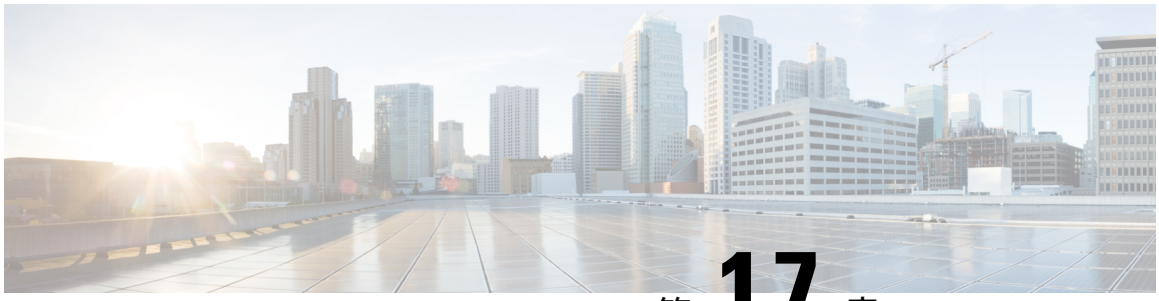
標準

MIB

MIB	MIB のリンク
PIM に関連した MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

第 V 部

Cisco Nexus 3550-T ユニキャスト ルーティングの構成ガイド



第 17 章

ユニキャスト ルーティングの概要

ライセンス要件

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

レイヤ 3 ユニキャスト ルーティングについて

レイヤ 3 ユニキャスト ルーティングには 2 つの基本的動作（最適なルーティング パスの決定およびパケットの交換）があります。ルーティング アルゴリズムを使用すると、ルータから宛先までの最適なパス（経路）を計算できます。この計算方法は、選択したアルゴリズム、ルート メトリック、そしてロード バランシングや代替パスの探索などの考慮事項により異なります。

ルーティングの基礎

ルーティング プロトコルは、メトリックを使用して、宛先までの最適なパスを調べます。メトリックとは、パス帯域幅などの、ルーティング アルゴリズムが宛先までの最適なパスを決定するために使用する測定基準です。パスを決定しやすいように、ルーティング アルゴリズムは、ルート情報（IP宛先アドレス、次のルータまたはネクストホップのアドレスなど）を含むルーティング テーブルを初期化して維持します。宛先とネクスト ホップの関連付けにより、ルータは、宛先までの途中にあるネクストホップとなる特定のルータにパケットを送信すると、最適なパスで IP 宛先まで届けられることを判定できます。ルータは、着信パケットを受信する

と、宛先アドレスをチェックし、このアドレスをネクスト ホップと関連付けようとします。ルート テーブルの詳細については、「ユニキャスト *RIB*」の項を参照してください。

ルーティング テーブルには、パスの優先度に関するデータなど、その他の情報が含まれていることもあります。ルータは、メトリックを比較して最適なルートを決定します。これらのメトリックは、使用しているルーティング アルゴリズムの設計によって異なります。「ルーティング メトリック」の項を参照してください。

各ルータは互いに通信し、さまざまなメッセージを送信して、そのルーティング テーブルを維持します。ルーティング更新メッセージは、ルーティング テーブルの全部または一部で構成されるメッセージです。ルータは、他のすべてのルータからのルーティング更新情報を分析して、ネットワーク トポロジの詳細な図を構築できます。ルータ間で送信されるメッセージのもう 1 つの例であるリンクステート アドバタイズメントは、送信ルータのリンク状態を他のルータに通知します。リンク情報を使用して、ルータが、ネットワーク宛先までの最適なルートを決定できるようにすることもできます。詳細については、「ルーティング アルゴリズム」の項を参照してください。

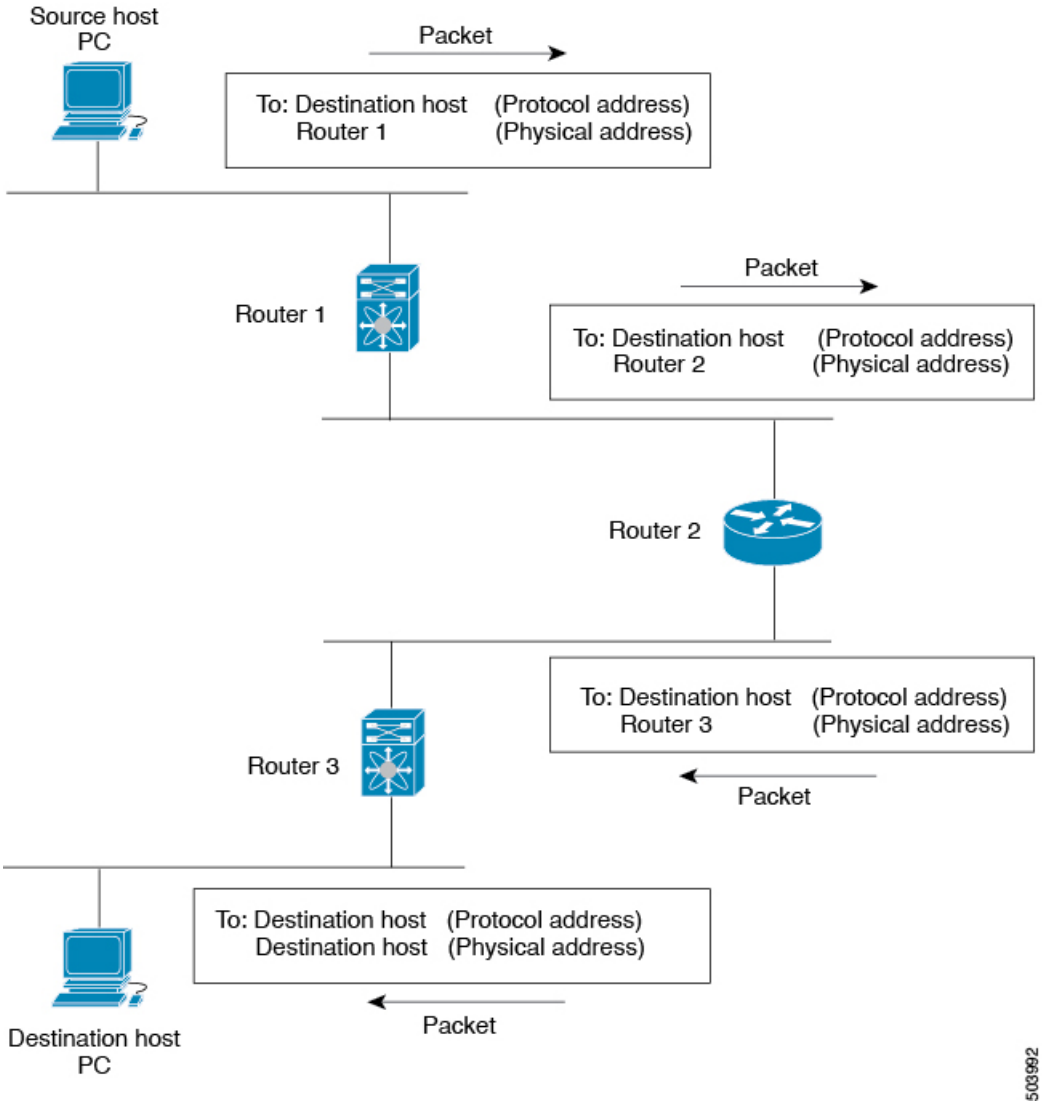
パケット交換

パケット交換では、ホストが、パケットを別のホストに送信する必要があることを決定します。何らかの手段でルータ アドレスを取得したら、送信元ホストは、明確にルータの物理（メディア アクセス コントロール（MAC）レイヤ）アドレスにアドレス指定されているが、宛先ホストの IP（ネットワーク層）アドレスを含むパケットを送信します。

ルータは宛先の IP アドレスを調べ、ルーティング テーブルでその IP アドレスを探します。ルータがパケットの転送方法を認識していない場合は、通常はパケットをドロップします。パケットの転送方法がわかった場合、ルータは、宛先の MAC アドレスをネクスト ホップ ルータの MAC アドレスに変更し、パケットを送信します。

ネクストホップが宛先のホストである場合や、同じ交換決定処理を行う別のルータである場合があります。パケットがインターネットワークを介して移動するにつれ、パケットの物理アドレスは変化しますが、プロトコル アドレスは一定のままです（次の図を参照）。

図 *8* : ネットワークを介したパケット ヘッダーの更新



ルーティング メトリック

ルーティング アルゴリズムは、多くの異なるメトリックを使用して最適なルートを決定します。高度なルーティングアルゴリズムは、複数のメトリックに基づいてルートを選択している場合があります。

パス長

パスの長さは、最も一般的なルーティング メトリックです。一部のルーティング プロトコルでは、各ネットワーク リンクに恣意的なコストの割り当てが可能です。この場合、パスの長さは、経由した各リンクに関連付けられたコストの合計となります。それ以外のルーティングプ

ロトコルでは、パケットが送信元から宛先までに経由する必要のある、ルータなどのネットワーク間製品の通過回数を指定するメトリックであるホップ数が定義されます。

Reliability

ルーティング アルゴリズムとの関連における信頼性は、各ネットワーク リンクの信頼性（ビット誤り率で示される）です。一部のネットワーク リンクは、他のネットワーク リンクよりダウンする頻度が高い場合があります。ネットワークがダウンした後、特定のネットワーク リンクが他のリンクより容易に、または短時間に修復される場合もあります。信頼性のランクを割り当てるときに考慮できる信頼性係数は、一般的にネットワーク リンクに割り当てる任意の数値です。

ルーティング遅延

ルーティング遅延は、送信元から宛先に、インターネットワークを通過してパケットを移動するために必要な時間の長さです。遅延は、中間のネットワーク リンクの帯域幅、経由する各ルータでのポート キュー、中間の全ネットワーク リンクでのネットワークの輻輳状況、パケットが移動する物理的な距離など、多くの要素に応じて異なります。ルーティング遅延はいくつかの重要な変数の組み合わせであるため、一般的で便利なメトリックです。

帯域幅

帯域幅は、リンクで使用可能なトラフィック容量です。たとえば、10 ギガビット イーサネット リンクは 1 ギガビット イーサネット リンクより優れています。帯域幅は、リンクで達成可能な最大スループットですが、帯域幅のより大きいリンクを経由するルートが、帯域幅のより小さいリンクを経由するルートより優れているとは限りません。たとえば、帯域幅の大きいリンクの方が混雑していると、実際には、パケットを宛先に送信するためにさらに長い時間がかかる場合があります。

負荷

負荷は、ルータなどのネットワーク リソースの使用状況の度合いです。負荷は、CPU 使用状況や処理される 1 秒あたりのパケット数など、さまざまな方法で計算できます。これらのパラメータを継続的にモニタすると、リソースに負担がかかる場合があります。

通信コスト

通信コストは、リンク上でルーティングするための稼働コストの測定単位です。通信コストは重要なメトリックの 1 つで、特にパフォーマンスより稼働コストの削減が優先される場合に使用されます。たとえば、専用回線での回線遅延が公衆回線より大きくても、使用時間に応じて課金される公衆回線上でなく、自身の専用回線上でパケットを送信できます。

ルータ ID

各ルーティング プロセスには、ルータ ID が関連付けられています。ルータ ID は、システムのあらゆるインターフェイスに設定できます。ルータ ID を設定しないと、Cisco NX-OS が次の基準に基づいて、ルータ ID を選択します。

- Cisco NX-OS は、他のあらゆるインターフェイス上で loopback0 を優先します。loopback0 が存在しない場合、Cisco NX-OS は、他のあらゆるインターフェイス タイプ上で最初のループバックを優先します。
- ループバック インターフェイスを設定しなかった場合、Cisco NX-OS はルータ ID としてコンフィギュレーション ファイルの最初のインターフェイスを使用します。Cisco NX-OS がルータ ID を選択した後にいずれかのループバック インターフェイスを設定した場合は、ループバック インターフェイスがルータ ID となります。ループバック インターフェイスが loopback0 ではなく、loopback0 を IP アドレスで設定した場合は、ルータ ID が loopback0 の IP アドレスに変更されます。
- ルータ ID の元であるインターフェイスが変更されると、新しい IP アドレスがルータ ID となります。他のどのインターフェイスの IP アドレスが変更されても、ルータ ID はまったく変更されません。

コンバージェンス

ルーティング アルゴリズム測定の鍵となる要素の 1 つは、ルータがネットワーク トポロジの変化に対応するために要する時間です。リンク障害など、なんらかの理由でネットワークの一部が変化すると、さまざまなルータのルーティング情報が一致しなくなる場合があります。変化したトポロジに関する情報が更新されているルータと、古い情報が残っているルータがあるためです。コンバージェンスとは、ネットワーク内のすべてのルータが更新され、ルーティング情報が一致するまでにかかる時間の長さです。コンバージェンス時間は、ルーティング アルゴリズムによって異なります。コンバージェンスが速い場合は、不正確なルーティング情報によるパッケージ損失の可能性が小さくなります。

ルートの再配布

ネットワークに複数のルーティング プロトコルが設定されている場合は、各プロトコルにルートの再配布を設定して、ルーティング情報を共有するように設定できます。たとえば、OSPF（Open Shortest Path First）プロトコルを設定して、ボーダー ゲートウェイ プロトコル（BGP）で検出したルートをアドバタイズできます。また、スタティック ルートを、どのダイナミック ルーティング プロトコルにも再配布できます。他のプロトコルからのルートを再配布するルータは、異なるルーティング プロトコル間で互換性のないルート メトリックを防ぐ再配布されたルータの固定ルートを設定します。たとえば、EIGRP から OSPF に再配布されたルートには、OSPF が認識できる固定リンク コスト メトリックが割り当てられます。

（注） ルーティング情報の再配布を設定する場合にルート マップを使用する必要があります。

ルート再配布では、アドミニストレーティブ ディスタンス（「アドミニストレーティブ ディスタンス」のセクションを参照してください）の使用によっても、2 つの異なるルーティング プロトコルで検出されたルートが区別されます。優先ルーティング プロトコルには、より低いアドミニストレーティブ ディスタンスが与えられており、そのルートが、より高いアドミニス

トレーティブディスタンスが割り当てられた他のプロトコルからのルートに優先して選択されます。

アドミニストレーティブ ディスタンス

アドミニストレーティブディスタンスは、ルーティング情報源の信頼性を示す評価基準です。値が高いほど信頼性の評価は低くなります。一般的にルートは、複数のプロトコルを通じて検出されます。アドミニストレーティブディスタンスは、複数のプロトコルから学習したルートを区別するために使用されます。最もアドミニストレーティブ ディスタンスが低いルートがIP ルーティング テーブルに組み込まれます。

スタブ ルーティング

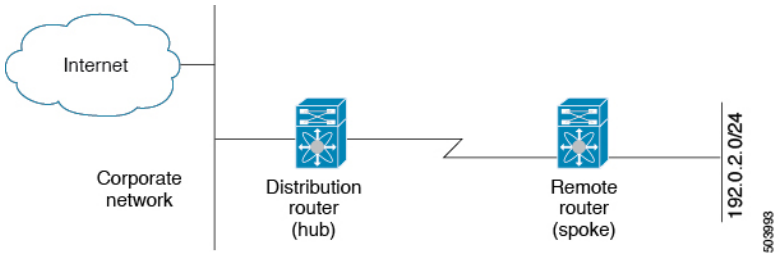
スタブ ルーティングはハブ アンド スポーク型ネットワーク トポロジで使用できます。このトポロジでは、1 つ以上の終端（スタブ）ネットワークが 1 台のリモートルータ（スポーク）に接続され、そのリモート ルータは 1 つ以上のディストリビューション ルータ（ハブ）に接続されています。リモートルータは、1つ以上のディストリビューション ルータにのみ隣接しています。リモート ルータへ流れる IP トラフィックのルートは、ディストリビューション ルータ経由のルートのみです。このタイプの設定は、ディストリビューション ルータが直接 WAN に接続されている WAN トポロジで使用されるのが一般的です。ディストリビューション ルータは、さらに多くのリモート ルータに接続できます。ディストリビューション ルータが 100 台以上のリモート ルータに接続されていることも、よくあります。ハブ アンド スポーク型トポロジでは、リモート ルータがすべての非ローカル トラフィックをディストリビューション ルータに転送する必要があります。これにより、リモート ルータが完全なルーティング テーブルを保持する必要はなくなります。通常、分散ルータは、デフォルトのルートのみをリモート ルータに送信します。

指定されたルートのみが、リモート（スタブ）ルータから伝播されます。スタブ ルータは、サマリー、接続されているルート、再配布されたスタティック ルート、外部ルート、および内部ルートに対するクエリーすべてに、応答として「inaccessible」というメッセージを返します。スタブとして設定されているルータは、自身のスタブ ルータとしてのステータスを報告するために、特殊なピア情報パケットがすべての隣接ルータに送信されます。

スタブ ルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブ ルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。スタブ ルータは、ディストリビューション ルータを使用して適切なアップデートをすべてのピアに送信します。

次の図は、単純なハブ アンド スポーク型のコンフィギュレーションを示しています。

図 *9* : 単純なハブ アンド スポーク ネットワーク



スタブ ルーティングを使用する場合でも、リモート ルータにルータをアドバタイズできます。この**単純なハブ アンド スポーク ネットワーク**の図は、リモート ルータが、分散ルータを介してのみ、企業ネットワークとインターネットにアクセスできることを示しています。この例では、企業ネットワークとインターネットへのパスが常に分散ルータを経由するため、リモート ルータ上の完全なルート テーブルの機能は無意味です。より大規模なルート テーブルを使用しても、リモート ルータに必要なメモリの量が削減されるだけです。使用される帯域幅とメモリは、分散ルータでルートを要約し、フィルタリングすると、削減できます。このネットワーク トポロジでリモート ルータは、他のネットワークから検出されたルートを受信する必要はありません。これは、宛先がどこであっても、リモート ルータは、すべての非ローカル トラフィックを分散ルータに送信する必要があるためです。真のスタブ ネットワークを設定するには、リモート ルータへのデフォルト ルートのみを送信するよう、分散ルータを設定する必要があります。

OSPF はスタブ エリアをサポートして、Enhanced Interior Gateway Routing Protocol（EIGRP）はスタブ ルータをサポートします。

（注） EIGRP スタブ ルーティング機能は、スタブ デバイスだけで使用します。スタブ デバイスは、コア中継トラフィックが通過しないネットワーク コアまたはディストリビューション レイヤに接続されたデバイスとして定義されます。リモート ルータへ流れる IP トラフィックのルートは、ディストリビューション ルータ経由のルートのみです。スタブ デバイスがディストリビューション デバイス以外の EIGRP ネイバーを持つことはできません。この制限を無視すると、望ましくない動作が発生します。

ルーティング アルゴリズム

ルーティング アルゴリズムによって、ルータが到達可能性情報を収集して報告する方法、トポロジの変化に対応する方法、宛先までの最適ルートを決定する方法が決まります。ルーティング アルゴリズムにはさまざまなタイプがあり、各アルゴリズムがネットワークやルータ リソースに与える影響もさまざまです。ルーティング アルゴリズムは、最適なルートの計算に影響するさまざまなメトリックを使用します。ルーティング アルゴリズムは、スタティックまたはダイナミック、内部または外部など、タイプで分類できます。

スタティック ルートおよびダイナミック ルーティング プロトコル

スタティック ルートは、手動で設定するルート テーブル エントリです。スタティック ルートは、手動で再設定しない限り、変更されません。スタティック ルートは設計が簡単で、ネットワーク トラフィックが比較的予想しやすい環境や、ネットワーク設計が比較的単純な環境での使用に適しています。

スタティック ルーティング システムはネットワークの変化に対応できないため、絶えず変化する大規模ネットワークには使用しないでください。今日のほとんどのルーティング プロトコルは、ダイナミック ルーティング アルゴリズムを使用しています。このアルゴリズムでは、着信ルーティング更新メッセージを分析して、ネットワーク状況の変化に合わせて調整します。メッセージがネットワークが変化したことを示している場合は、ルーティング ソフトウェアはルートを再計算し、新しいルーティング アップデート メッセージを送信します。これらのメッセージがネットワークを通過すると、ルータがそのアルゴリズムを再実行し、それに従ってルーティング テーブルを変更します。

適切であれば、ダイナミック ルーティング アルゴリズムをスタティック ルートで補完することができます。たとえば、各サブネットワークに IP デフォルト ゲートウェイまたは、ラスト リゾート ルータ（ルーティングできないすべてのパケットが送信されるルータ）へのスタティック ルートを設定する必要があります。

内部および外部ゲートウェイ プロトコル

ネットワークを、一意のルーティング ドメインまたは自律システムに分割できます。自律システムは、管理ガイドラインの特定のセットで規制された共通の管理機関の下の内部ネットワークの一部です。自律システム間でのルートを設定するルーティング プロトコルは、外部ゲートウェイ プロトコルまたはドメイン間プロトコルと呼ばれます。ボーダー ゲートウェイ プロトコル（BGP）は、外部ゲートウェイ プロトコルの例です。1 つの自律システム内で使用されるルーティング プロトコルは、内部ゲートウェイ プロトコルまたはドメイン内プロトコルと呼ばれます。EIGRP および OSPF は、内部ゲートウェイ プロトコルの例です。

ディスタンス ベクトル プロトコル

ディスタンス ベクトル プロトコルは、ディスタンス ベクトル アルゴリズム（Bellman-Ford アルゴリズムとも呼ばれます）を使用します。このアルゴリズムにより、各ルータは、そのルーティング テーブルの一部または全部を隣接ルータに送信します。ディスタンス ベクトル アルゴリズムでは、ルートが、ディスタンス（宛先までのホップ数など）および方向（ネクスト ホップ ルータなど）により定義されます。その後、これらのルートは、直接接続されたネイバー ルータにブロードキャストされます。各ルータは、これらの更新情報を使用して、ルーティング テーブルを確認し、更新します。

ルーティング ループを防ぐために、ほとんどのディスタンス ベクトル アルゴリズムはポイズン リバースを指定したスプリット ホライズンを使用します。これは、インターフェイスで検出されたルートを到達不能として設定し、それをそのインターフェイスで、次の定期更新中にアドバタイズするという意味です。このプロセスにより、ルータによるルート更新が、そのルータ自体に返信されなくなります。

ディスタンス ベクトル アルゴリズムは、一定の間隔で更新を送信しますが、ルート メトリックの値の変更に応じて、更新を送信することもできます。このように送信された更新により、ルート コンバージェンス時間の短縮が可能です。Routing Information Protocol（RIP）はディスタンス ベクトル プロトコルの 1 つです。

リンクステート プロトコル

リンク ステートプロトコルは、最短パス優先（SPF）とも呼ばれ、情報を隣接ルータと共有します。各ルータは、各リンクおよび直接接続されたネイバー ルータに関する情報を含むリンクステート アドバタイズメント（LSA）を構築します。

各 LSA にはシーケンス番号があります。ルータが LSA を受信し、そのリンクステート データベースを更新すると、その LSA はすべての隣接ネイバーにフラッディングされます。ルータが（同じルータから）同じシーケンス番号の 2 つの LSA を受信した場合、ルータは LSA アップデートのループを回避するため、ネイバーによって受信された最後の LSA をフラッディングしません。ルータは、受信直後に LSA をフラッディングするため、リンクステート プロトコルのコンバージェンス時間は最小となります。

ネイバー ルータの探索と隣接関係の確立は、リンクステート プロトコルの重要な部分です。ネイバー ルータは、特別な hello パケットを使用して探索されます。このパケットは、各ネイバー ルータのキープアライブ通知としても機能します。隣接関係は、ネイバー ルータ間のリンクステート プロトコルの一般的な動作パラメータ セットで確立されます。

ルータが受信した LSA は、そのルータのリンクステート データベースに追加されます。各エントリは、次のパラメータで構成されます。

- ルータ ID（LSA を構築したルータの）
- ネイバー ID
- リンク コスト
- LSA のシーケンス番号
- LSA エントリの作成時からの経過時間

ルータは、リンクステート データベース上で SPF アルゴリズムを実行し、そのルータの最短パス ツリーを構築します。この SPF ツリーを使用して、ルーティング テーブルにデータが入力されます。

リンクステートアルゴリズムでは、各ルータはネットワークの全体像をそのルーティングテーブルに構築します。リンクステートアルゴリズムが小さな更新を全体的に送信するのに対し、ディスタンスベクトルアルゴリズムは、より大きな更新をネイバールータのみに送信します。

リンクステート アルゴリズムは、より短時間でコンバージェンスするため、ディスタンス ベクトル アルゴリズムより、ルーティング ループがやや発生しにくくなっています。ただし、リンク ステートアルゴリズムは、ディスタンス ベクトル アルゴリズムより、より多くの CPU パワーとメモリを必要とし、実行とサポートをするにはよりコストが高くなります。一般的に、リンクステートプロトコルはディスタンスベクトルプロトコルよりもスケーラブルです。

OSPF は、リンクステート プロトコルの一例です。

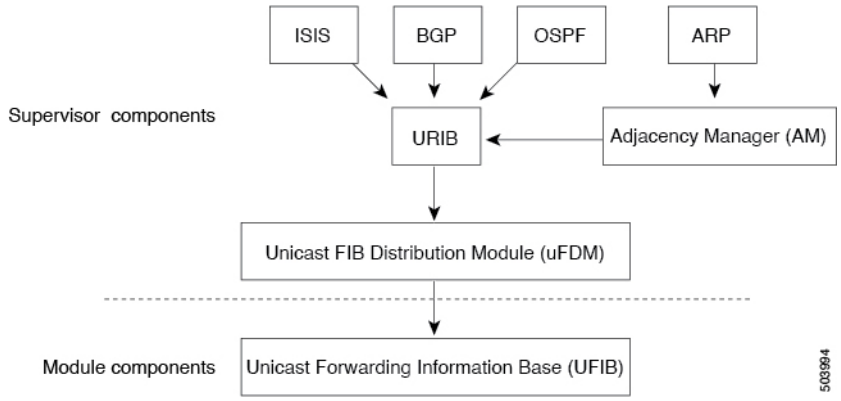
Cisco NX-OS フォワーディング アーキテクチャ

Cisco NX-OS では、転送アーキテクチャにより、すべてのルーティングの更新処理と、シャーシ内のすべてのモジュールへの転送情報の入力が行われます。

ユニキャスト RIB

Cisco NX-OS 転送アーキテクチャは、次の図に示すように、複数のコンポーネントから構成されています。

図 *10 : Cisco NX-OS* 転送アーキテクチャ



ユニキャスト RIB はアクティブなスーパーバイザ上にあります。ユニキャスト RIB は、直接接続のルート、スタティック ルート、ダイナミック ユニキャスト ルーティング プロトコルで検出されたルートを含むルーティング テーブルを維持しています。また、アドレス解決プロトコル（ARP）などの送信元から、隣接情報を収集します。ユニキャスト RIB は、特定のルートのための最適なネクスト ホップを決定し、ユニキャスト FIB 分散モジュール（FDM）のサービスを使用して、FIB にデータを入力します。

各ダイナミック ルーティング プロトコルは、タイム アウトしたあらゆるルートについて、ユニキャスト RIB を更新する必要があります。その後、ユニキャスト RIB はそのルートを削除し、そのルートに最適なネクスト ホップを再計算します（代わりに使用できるパスがある場合）。

隣接マネージャ

隣接マネージャはアクティブなスーパーバイザ上にあり、ARP、ネイバー探索プロトコル（NDP）、スタティック設定など、各種プロトコルの隣接情報を保持しています。最も基本的な隣接情報は、これらのプロトコルで探索されたレイヤ 3 からレイヤ 2 へのアドレス マッピングです。発信レイヤ 2 パケットは、隣接情報を使用して、レイヤ 2 ヘッダーの作成を終了します。

隣接マネージャは、ARP 要求による、レイヤ 3 からレイヤ 2 への特定のマッピングの探索をトリガーできます。新しいマッピングは、対応する ARP 返信を受信し、処理すると、使用できるようになります。

ユニキャスト転送分散モジュール

ユニキャスト転送分散モジュール（FDM）はアクティブなスーパーバイザ上に存在し、ユニキャスト RIB やその他の送信元からの転送パス情報を配布します。ユニキャスト RIB は、ユニキャスト FIB によってスタンバイ スーパーバイザおよびモジュール上のハードウェア転送テーブルにプログラミングされる転送情報を生成します。また、ユニキャスト FDM は、新規挿入されたモジュールへの FIB 情報のダウンロードも行います。

ユニキャスト FDM は隣接関係情報を収集し、ユニキャスト FIB でのルート更新時に、この情報およびその他のプラットフォーム依存の情報を書き直し（リライトし）ます。隣接情報およびリライト情報には、インターフェイス、ネクストホップ、およびレイヤ 3 からレイヤ 2 へのマッピング情報が含まれています。インターフェイスとネクストホップの情報は、ユニキャスト RIB からのルート更新情報で受信します。レイヤ 3 からレイヤ 2 へのマッピングは、隣接マネージャから受信します。

FIB

ユニキャスト FIB は、スーパーバイザ モジュールとスイッチング モジュール上にあり、ハードウェア転送エンジンで使用される情報を構築します。ユニキャスト FIB は、ユニキャスト FDM からルート更新情報を受信し、ハードウェア転送エンジンにプログラミングされるよう、この情報を送信します。ユニキャスト FIB は、ルート、パス、隣接関係の追加、削除、変更を管理します。

ルート更新メッセージに基づいて、ユニキャスト FIB は、VRF ごとのプレフィックスとネクストホップ隣接情報データベースを維持します。ネクストホップ隣接データ構造には、ネクストホップの IP アドレスとレイヤ 2 リライト情報が含まれます。同じネクストホップ隣接情報構造を複数のプレフィックスで使用できます。

ハードウェア フォワーディング

Cisco NX-OS は、分散パケット転送をサポートします。入力ポートは、パケット ヘッダーから該当する情報を取得し、その情報をローカル スイッチング エンジンに渡します。ローカル スイッチング エンジンはレイヤ 3 ルックアップを行い、この情報を使って、パケット ヘッダーをリライトします。入力モジュールは、パケットを出力ポートに転送します。出力ポートが別のモジュール上にある場合は、スイッチ ファブリックを使って、パケットが出力モジュールに転送されます。出力モジュールは、レイヤ 3 転送決定には関与しません。

また、 **show platform fib**、 または **show platform forwarding** コマンドを使用して、ハードウェア転送の詳細を表示することもできます。

ソフトウェア転送

Cisco NX-OS のソフトウェア転送パスは、主に、ハードウェアでサポートされない機能、またはハードウェア処理中に発生したエラーへの対処に使用されます。通常、IP オプション付きのパケットまたはフラグメンテーションの必要なパケットは、アクティブなスーパーバイザ上の CPU に渡されます。ソフトウェアでの切り替えが必要なパケットや終端される必要のあるパケットはすべて、スーパーバイザに渡されます。スーパーバイザは、ユニキャスト RIB および隣接マネージャから提供された情報を使用して、転送の決定を下します。モジュールは、ソフトウェア転送パスには関与しません。

ソフトウェア転送は、コントロール プレーン ポリシーおよびレート リミッタによって管理されます。詳細については、『Cisco NX-OS セキュリティの設定ガイド』を参照してください。

レイヤ 3 ユニキャスト ルーティング機能のまとめ

ここでは、Cisco NX-OS でサポートされるレイヤ 3 ユニキャスト機能およびプロトコルを簡単に説明します。

IPv4

レイヤ 3 は、IPv4 プロトコルを使用します。詳細については、「*IPV4* の構成」のセクションを参照してください。

Open Shortest Path First（OSPF）

Open Shortest Path First（OSPF）プロトコルは、AS 内のネットワーク到達可能性情報の交換に使用されるリンクステート ルーティング プロトコルです。各 OSPF ルータは、そのアクティブなリンクに関する情報をネイバー ルータにアドバタイズします。リンク情報には、リンク タイプ、リンク メトリック、およびリンクに接続された隣接ルータが含まれます。このリンク情報を含むアドバタイズメントは、リンクステートアドバタイズメントと呼ばれます。詳細については、「*OSPFv2* の構成」のセクションを参照してください。

BGP

BGP は自律システム間ルーティング プロトコルです。BGP ルータは、信頼性の高い転送メカニズムとして伝送制御プロトコル（TCP）を使用し、他の BGP ルータにネットワーク到達可能性情報をアドバタイズします。ネットワーク到達可能性情報には、宛先ネットワーク プレフィックス、宛先に到達するまでに通過する必要のある自律システムのリスト、およびネクストホップ ルータが含まれます。到達可能性情報には、ルートの優先度、ルートの始点、コミュニティなどの詳細なパス属性が含まれます。詳細については、「基本 *BGP* の構成」および「高度な *BGP* の構成」のセクションを参照してください。

スタティック ルーティング

スタティック ルーティングを使用して、宛先までの一定のルートを入力できます。この機能は、単純なトポロジの小規模ネットワークでは便利です。また、スタティック ルーティングは、他のルーティング プロトコルとともに、デフォルト ルートおよびルート配布の管理に使用されます。詳細については、「静的ルーティングの構成」のセクションを参照してください。

ファーストホップ冗長プロトコル（FHRP）

Virtual Router Redundancy Protocol（VRRP）などの First Hop Redundancy Protocol（FHRP）を使用すると、ホストで接続の冗長性を実現できます。アクティブなファーストホップ ルータがダウンした場合は、その機能を引き継ぐスタンバイ ルータが FHRP によって自動的に選択されます。アドレスは仮想のものであり、FHRP グループ内の各ルータ間で共有されているため、ホストを新しい IP アドレスで更新する必要はありません。VRRP の詳細については、「*VRRP* の構成」のセクションを参照してください。

オブジェクト トラッキング

オブジェクト トラッキングを使用すると、インターフェイス回線プロトコル状態、IP ルーティング、ルート到達可能性などの、ネットワーク上の特定のオブジェクトをトラッキングし、トラッキングしたオブジェクトの状態が変化したときに対処することができます。この機能により、ネットワークのアベイラビリティが向上し、オブジェクトがダウンした場合のリカバリ時間が短縮されます。

関連項目

機能名	機能情報
レイヤ 3 機能	「*Cisco Nexus® 3550-T* マルチキャスト ルーティング構成」セクション 『*Cisco Cisco NX-OS* シリーズ *NX-OS* 高可用性および冗長性ガイド』 自律システムの数を検索する:http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/autonomous_system_numbers.html

関連項目

第 18 章

IPv4 の設定

この章では、Cisco NX-OS デバイス上でのインターネット プロトコル バージョン 4（IPv4）（アドレス指定を含む）、アドレス解決プロトコル（ARP）および Internet Control Message Protocol（ICMP）の設定方法を説明します。

この章は、次の項で構成されています。

IPv4 の概要

デバイス上で IP を設定し、ネットワーク インターフェイスに IP アドレスを割り当てることができます。IP アドレスを割り当てると、インターフェイスがイネーブルになり、そのインターフェイス上のホストと通信できるようになります。

IP アドレスは、デバイス上でプライマリまたはセカンダリとして設定できます。インターフェイスには、1 つのプライマリ IP アドレスと複数のセカンダリ アドレスを設定できます。デバイスが生成したパケットは、常にプライマリ IPv4 アドレスを使用するため、インターフェイス上のすべてのネットワーキング デバイスは、同じプライマリ IP アドレスを共有する必要があります。各 IPv4 パケットは、送信元または宛先 IP アドレスからの情報に基づいています。詳細については、複数の IPv4 アドレス （236 ページ）を参照してください。

サブネットを使用して、IP アドレスをマスクできます。マスクは、IP アドレスがどのサブネットに属するかを決定するために使用されます。IP アドレスは、ネットワーク アドレスとホスト アドレスで構成されています。マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。マスクを使用してネットワークをサブネット化した場合、そのマスクはサブネット マスクと呼ばれます。サブネット マスクは 32 ビット値で、これにより IP パケットの受信者は、IP アドレスのネットワーク ID 部分とホスト ID 部分を区別できます。

IP 機能には、スーパーバイザ モジュールで終端する IPv4 パケットを取り扱い、また同様に、IPv4 ユニキャスト ルート ルックアップとソフトウェア アクセス コントロール リスト（ACL）の転送を含む IPv4 パケットの転送を行う役割があります。また、IP 機能は、ネットワーク インターフェイス IP アドレス設定、重複アドレス チェック、スタティック ルート、および IP クライアントのパケット送信/受信インターフェイスも管理します。

複数の IPv4 アドレス

Cisco NX-OS は、インターフェイスごとに複数の IP アドレスをサポートします。さまざまな状況に備え、いくつでもセカンダリ アドレスを指定できます。最も一般的な状況は次のとおりです。

- 特定のネットワーク インターフェイスのホスト IP アドレスの数が不足している場合。たとえば、サブネット化により、論理サブネットごとに 254 までのホストを使用できるが、物理サブネットの 1 つに 300 のホスト アドレスが必要な場合は、ルータ上またはアクセス サーバ上でセカンダリ IP アドレスを使用して、1 つの物理サブネットで 2 つの論理サブネットを使用できます。
- 1 つのネットワークの 2 つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。別のネットワークによって物理的に分離された複数のサブネットから、セカンダリ アドレスを使用して、1 つのネットワークを作成できます。このような場合、最初のネットワークは、2 番めのネットワークの上に拡張されます。つまり、上の階層となります。サブネットは、同時に複数のアクティブなインターフェイス上に表示できません。

（注） ネットワーク セグメント上のいずれかのデバイスがセカンダリ IPv4 アドレスを使用している場合は、同じネットワーク インターフェイス上の他のすべてのデバイスも、同じネットワークまたはサブネットからのセカンダリ アドレスを使用する必要があります。ネットワーク セグメント上で、一貫性のない方法でセカンダリ アドレスを使用すると、ただちにルーティング ループが発生する可能性があります。

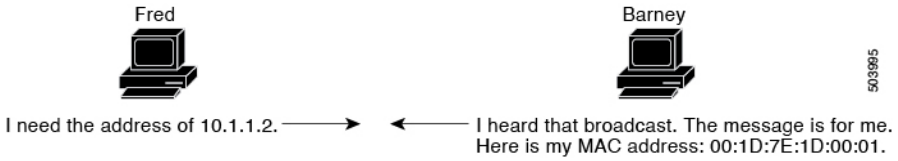
アドレス解決プロトコル

ネットワーキング デバイスおよびレイヤ 3 スイッチは ARP を使用して、IP（ネットワーク層）アドレスを物理（Media Access Control（MAC）レイヤ）アドレスにマッピングし、IP パケットがネットワーク上に送信されるようにします。デバイスは、他のデバイスにパケットを送信する前に自身の ARP キャッシュを調べて、MAC アドレスまたは対応する宛先デバイスの IP アドレスがないかを確認します。エントリがまったくない場合、送信元のデバイスは、ネットワーク上の全デバイスにブロードキャスト メッセージを送信します。

各デバイスは、問い合わせられた IP アドレスを自身のアドレスと比較します。一致する IP アドレスを持つデバイスだけが、デバイスの MAC アドレスを含むパケットとともにデータを送信したデバイスに返信します。送信元デバイスは、あとで参照できるよう、宛先デバイスの MAC アドレスをその ARP テーブルに追加し、データリンク ヘッダーおよびトレーラを作成し

てパケットをカプセル化し、データの転送へと進みます。次の図は、ARPブロードキャストと応答プロセスを示しています。

図 *11 : ARP* 処理



宛先デバイスが、別のデバイスを挟んだリモートネットワーク上にあるときは、同じ処理が行われますが、データを送信するデバイスが、デフォルト ゲートウェイのMACアドレスを求める ARP 要求を送信する点が異なります。アドレスが解決され、デフォルト ゲートウェイがパケットを受信した後に、デフォルトゲートウェイは、接続されているネットワーク上で宛先の IP アドレスをブロードキャストします。宛先デバイスのネットワーク上のデバイスは、ARP を使用して宛先デバイスのMACアドレスを取得し、パケットを配信します。ARP はデフォルトでイネーブルにされています。

ARP キャッシング

ARP キャッシングにより、ブロードキャストが最小になり、ネットワーク リソースの浪費が抑制されます。IP アドレスのMACアドレスへのマッピングは、ネットワーク間でパケットが送信されるたびに、ネットワーク上の各ホップ（デバイス）で行われるため、ネットワークのパフォーマンスに影響する場合があります。

ARP キャッシングでは、ネットワーク アドレスとそれに関連付けられたデータリンク アドレスが一定の期間メモリ内に保存されるため、パケットが送信されるたびに同じアドレスにブロードキャストするための貴重なネットワークリソースの使用が最小限に抑えられます。キャッシュエントリは、定期的に失効するよう設定されているため、保守が必要です。これは、古い情報が無効となる場合があるためです。ネットワーク上のすべてのデバイスは、アドレスのブロードキャストに従ってアドレス テーブルを更新します。

ARP キャッシュのスタティックおよびダイナミック エントリ

スタティック ルーティングは、手動で各デバイスの各インターフェイスに対応する IP アドレス、サブネットマスク、ゲートウェイ、および対応するMACアドレスを設定する必要があります。スタティック ルーティングでは、ルート テーブルを維持するために、より多くの処理が必要です。ルートを追加または変更するたびに、テーブルの更新が必要となるためです。

ダイナミック ルーティングは、ネットワーク上のデバイスが相互にルーティング テーブル情報を交換できるプロトコルを使用します。ダイナミック ルーティングは、キャッシュに制限時間を追加しない限り、ルート テーブルが自動更新されるため、スタティック ルーティングより効率的です。デフォルトの制限時間は 25 分ですが、キャッシュから追加および削除されるルートがネットワークに数多く存在する場合は、制限時間を変更します。

ARP を使用しないデバイス

ネットワークが2つのセグメントに分割されると、ブリッジによりセグメントが結合され、各セグメントへのトラフィックが MAC アドレスに基づいてフィルタリングされます。ブリッジは MAC アドレスだけを使用する独自のアドレス テーブルを作成します。デバイスが IP アドレスおよび対応する MAC アドレスの両方を含む ARP キャッシュを持っています。

パッシブ ハブは、ネットワーク内の他のデバイスを物理的に接続する集中接続デバイスです。パッシブ ハブはそのすべてのポートでデバイスにメッセージを送信し、レイヤ1で動作しますが、アドレス テーブルを保持しません。

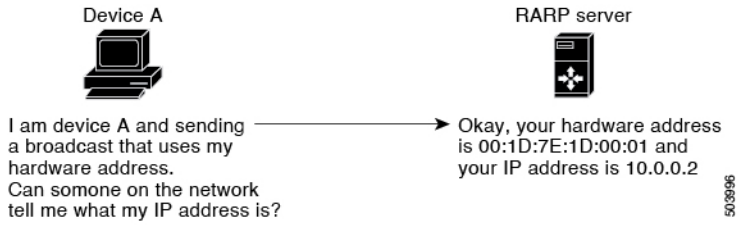
レイヤ2スイッチは、デバイス上のどのポートがそのポートだけに送信されたメッセージを受信するかを決定します。ただし、レイヤ3スイッチは、ARPキャッシュ（テーブル）を作成するデバイスです。

Reverse ARP

RFC 903 で定義された Reverse ARP（RARP）は、ARP と同じように動作しますが、RARP 要求パケットは MAC アドレスではなく IP アドレスを要求する点が異なります。RARP は多くの場合、ディスクレス ワークステーションで使用されます。これは、このタイプのデバイスには、起動時に使用する IP アドレスを格納する手段がないためです。認識できるアドレスは MAC アドレスだけで、これはハードウェアに焼き付けられているためです。

RARP を使用するには、ルータ インターフェイスとして、同じネットワーク セグメント上に RARP サーバが必要です。次の図に、RARP の仕組みを示します。

図 *12 : Reverse ARP*



RARP には、いくつかの制限があります。これらの制限により、ほとんどのビジネスでは、DHCP を使用してダイナミックに IP アドレスを割り当てています。DHCP は、RARP よりコスト効率が高く、必要な保守作業も少ないためです。最も重要な制限は次のとおりです。

- RARP はハードウェア アドレスを使用するため、多くの物理ネットワークを含む大規模なネットワークの場合は、各セグメント上に、冗長性のための追加サーバを備えた RARP サーバが必要です。各セグメントに 2 台のサーバを保持すると、コストがかかります。
- 各サーバは、ハードウェア アドレスと IP アドレスのスタティック マッピングのテーブルで設定する必要があります。IP アドレスの保守は困難です。
- RARP は、ホストの IP アドレスだけを提供し、サブネット マスクもデフォルト ゲートウェイも提供しません。

プロシキ ARP

プロキシ ARP を使用すると、物理的に 1 つのネットワーク上に存在するデバイスが、論理的に、同じデバイスまたはファイアウォールに接続された別の物理ネットワークの一部として表示されます。プロキシ ARP で、プライベート ネットワーク上のパブリック IP アドレスを持つデバイスをルータの背後に隠すと同時に、このデバイスを、ルータの前のパブリック ネットワーク上に表示できます。ルータはそのアイデンティティを隠すことにより、実際の宛先までパケットをルーティングする役割を担います。プロキシ ARP を使用すると、サブネット上のデバイスは、ルーティングもデフォルト ゲートウェイも設定せずにリモート サブネットまで到達できます。

複数のデバイスが同じデータリンク層のネットワークでなく、同じ IP ネットワーク内にある場合、これらのデバイスは相互に、ローカル ネットワーク上にあるかのようにデータを送信しようとします。ただし、これらのデバイスを隔てるルータは、ブロードキャスト メッセージを送信しません。これは、ルータがハードウェア レイヤのブロードキャストを渡さず、アドレスが解決されないためです。

デバイスでプロキシ ARP をイネーブルにし、ARP 要求を受信すると、プロキシ ARP はこれを、ローカル LAN 上にないシステムに対する要求と見なします。デバイスは、ブロードキャストの宛先であるリモートの宛先であるかのように、自身の MAC アドレスをリモートの宛先の IP アドレスに関連付ける ARP 応答で応答します。ローカル デバイスは、自身が宛先に直接、接続されていると認識していますが、実際には、そのパケットは、ローカルデバイスによりローカル サブネットワークから宛先のサブネットワークへと転送されています。デフォルトでは、プロキシ ARP はディセーブルになっています。

ローカル プロキシ ARP

ローカル プロキシ ARP を使用して、通常はルーティングが不要なサブネット内の IP アドレスを求める ARP 要求に対して、デバイスが応答できるようにすることができます。ローカル プロキシ ARP を有効にすると、ARP は、サブネット内の IP アドレスを求めるすべての ARP 要求に応答し、サブネット内のホスト間ですべてのトラフィックを転送します。この機能は、ホストが接続されているデバイスの設定により意図的に、ホストの直接通信が禁止されているサブネットだけで使用してください。

Gratuitous ARP

Gratuitous ARP は、送信元 IP アドレスと宛先 IP アドレスが同じである要求を送信し、重複する IP アドレスを検出します。Cisco NX-OSは Gratuitous ARP 要求または ARP キャッシュの更新の有効または無効をサポートします。

ICMP

Internet Control Message Protocol（ICMP）を使用して、IP 処理に関連するエラーおよびその他の情報を報告するメッセージパケットを提供できます。ICMP は、ICMP 宛先到達不能メッセージ、ICMP エコー要求（2 つのホスト間でパケットを往復送信する）、およびエコー返信メッ

セージなどのエラー メッセージを生成します。ICMP は多くの診断機能も備えており、ホストへのエラー パケットの送信およびリダイレクトが可能です。デフォルトでは、ICMP がイネーブルにされています。

次に示すのは、ICMP メッセージ タイプの一部です。

- ネットワーク エラー メッセージ
- ネットワーク輻輳メッセージ
- トラブルシューティング情報
- タイムアウト告知

（注） ICMP リダイレクトは、ローカル プロキシ ARP 機能がイネーブルになっているインターフェイスではディセーブルになります。

IPv4の前提条件

IPv4 には、次の前提条件があります。

- IPv4 はレイヤ 3 インターフェイス上だけで設定可能です。

IPv4 の注意事項および制約事項

IPv4 設定時の注意事項および制約事項は、次のとおりです。

- セカンダリ IP アドレスは、プライマリ IP アドレスの設定後にだけ設定できます。
- ***Cisco Nexus 3550-T - 10.1(2t)* リリース** スイッチは、IPv4 パス全体のハードウェア ロード バランシングをサポートせず、IPv4 ECMP からの最初のパスだけをハードウェアにインストールします。追加のパスはソフトウェア ルーティング テーブルでのみ使用でき、最初のパスがダウンすると、次のパスがハードウェアに更新されます。さらに、ハードウェアにインストールするために ECMP パスが計算されたときに生成される syslog があります。

パラメータ	スケール番号
IP-Host-Route	3072（最大）（クワッドあたり）
L3 ARP/隣接関係	386

パラメータ	スケール番号
IP-Routes	2304（最大）（クワッドあたり） （注） すべての IPv4 ルート配布が Cisco Nexus® 3550-T ハードウェアに適合するわけではありません。ルートがハードウェア テーブルに収まらない場合は、ソフトウェア転送を行います。

デフォルト設定

次の表に、IP パラメータのデフォルト設定値を示します。

パラメータ	デフォルト
ARP タイムアウト	1500 秒
『Proxy ARP』	ディセーブル

IPv4 の設定

（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。

IPv4 アドレス指定の設定

ネットワーク インターフェイスにプライマリ IP アドレスを割り当てることができます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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** *number* 例：	インターフェイス設定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 ethernet 1/3` `switch(config-if)#`	
ステップ 3	**ip address** *ip-address/length* [*secondary*] 例： `switch(config-if)# ip address 192.2.1.1 255.0.0.0`	インターフェイスに対するプライマリ IPv4 アドレスまたはセカンダリ IPv4 アドレスを指定します。 • 4 分割ドット付き 10 進表記のアドレスでネットワーク マスクを指定します。たとえば、255.0.0.0 は、1 に等しい各ビットが、ネットワーク アドレスに属した対応するアドレス ビットを意味することを示します。 • ネットワーク マスクは、スラッシュ（/）および数字、つまり、プレフィックス長として示される場合もあります。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。スラッシュは 10 進数値の前に置かれ、IP アドレスとスラッシュの間にスペースは入りません。
ステップ 4	（任意） **show ip interface** 例： `switch(config-if)# show ip interface`	IPv4 に設定されたインターフェイスを表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

複数の IP アドレスの設定

セカンダリ IP アドレスは、プライマリ IP アドレスの設定後にのみ追加できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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** *number*
	例：
	`switch(config)# interface ethernet 1/3`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**ip address** *ip-address/length* [*secondary*] 例： `switch(config-if)# ip address 192.168.1.1 255.0.0.0 secondary`	設定したアドレスをセカンダリ IPv4 アドレスとして指定します。
ステップ 4	（任意） **show ip interface** 例： `switch(config-if)# show ip interface`	IPv4 用に設定されたインターフェイスを表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。 （注） Cisco Nexus® 3550-T スイッチは、IPv4 パス全体のハードウェア ロードバランシングをサポートしておらず、IPv4 ECMP からの最初のパスだけをハードウェアにインストールします。追加のパスはソフトウェア ルーティング テーブルでのみ使用でき、最初のパスがダウンすると、次のパスがハードウェアに更新されます。

	コマンドまたはアクション	目的
		（注） Cisco Nexus® 3550-T スイッチは、インターフェイスで IP アドレスが設定されていない場合でも、ルート検索の結果に従って、MyMac を宛先として L3 パケットを転送します。SVI が作成されていない場合でも、MyMac パケットのルートテーブルルックアップが有効になっています。

スタティック ARP エントリの設定

デバイス上でスタティック ARP エントリを設定して、IP アドレスをスタティック マルチキャスト MAC アドレスを含む MAC ハードウェア アドレスにマッピングできます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet** *number*
	例：
	`switch(config)# interface ethernet 1/3`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**ip arp address** *ip-address mac-address* 例： `switch(config-if)# ip arp 192.168.1.1 0019.076c.1a78`	IP アドレスを MAC アドレスにスタティックエントリとして関連付けます。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。

プロキシ ARP の設定

デバイス上でプロキシ ARP を設定して、他のネットワークまたはサブネット上のホストのメディア アドレスを決定します。

手順

	コマンドまたはアクション	目的

ステップ 1	**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** *number*
	例：
	`switch(config)# interface ethernet 1/3`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**ip proxy-arp** 例： `switch(config-if)# ip proxy-arp`	インターフェイス上でプロキシ ARP を有効にします。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。

イーサネット インターフェイスでのローカル プロキシ ARP の設定

イーサネット インターフェイス上でローカル プロキシ ARP を設定することができます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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** *number*
	例：
	`switch(config)# interface ethernet 1/3`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**[no]ip local-proxy-arp** 例： `switch(config-if)# ip local-proxy-arp`	インターフェイス上でローカル プロキシ ARP をイネーブルにします。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。

SVI でのローカル プロキシ ARP の設定

SVI でのローカル プロキシ ARP を構成できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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 vlan vlan-id**
	例：
	`switch(config)# interface vlan 5`
	`switch(config-if)#`
		VLAN インターフェイスを作成し、SVI の設定モードを開始します。

ステップ 3	**[no] ip local-proxy-arp** 例： `switch(config-if)# ip local-proxy-arp`	SVI でローカル プロキシ ARP をイネーブルにします。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

無償 ARP の設定

インターフェイス上で Gratuitous ARP を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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** *number*
	例：
	`switch(config)# interface ethernet 1/3`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**ip arp gratuitous** {**request** | **update**] 例： `switch(config-if)# ip arp gratuitous request`	インターフェイス上で無償 ARP をイネーブルにします。無償 ARP はデフォルトで有効になっています。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。

ICMP 送信元 IP フィールドのインターフェイス IP アドレスの設定

ICMP エラー メッセージを処理するように ICMP ソース IP フィールドのインターフェイス IP アドレスを設定できます。

手順

	コマンドまたはアクション	目的

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

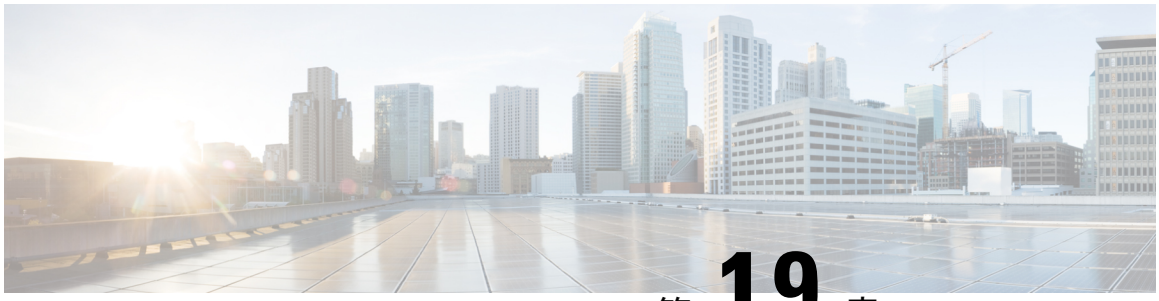
ステップ 2	[**no**] **ip source** {**ethernet** *slot/port* | **loopback** *number* | **port-channel** *number*} **icmp-errors** 例： `switch(config)# ip source loopback 0 icmp-errors`	ICMP 送信元 IP フィールドのインターフェイス IP アドレスを設定し、ICMP エラー メッセージをルーティングします。
ステップ 3	（任意） **copy running-config startup-config**	この設定変更を保存します。

	コマンドまたはアクション	目的
	例： `switch(config)# copy running-config startup-config`	

IPv4 設定の確認

IPv4 の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip adjacency	隣接関係テーブルを表示します。
show ip adjacency summary	スロットル隣接関係の数のサマリーを表示します。
show ip arp	ARP テーブルを表示します。
show ip arp summary	スロットル隣接関係の数のサマリーを表示します。
show ip interface	IP に関連するインターフェイス情報を表示します。
show ip arp statistics [**vrf** *default* | *management*]	ARP 統計情報を表示します。



第 19 章

OSPFv2 の設定

この章では、Cisco NX-OS デバイスで IPv4 ネットワーク用の Open Shortest Path First version 2（OSPFv2）を設定する方法について説明します。

この章は、次の項で構成されています。

OSPFv2 について

OSPFv2 は、IPv4 ネットワーク用 IETF リンクステート プロトコルです。OSPFv2 ルータは、helloパケットと呼ばれる特別なメッセージを各OSPF対応インターフェイスに送信して、ほかの OSPFv2 隣接ルータを探索します。ネイバー ルータが発見されると、この 2 台のルータはhelloパケットの情報を比較して、両者の設定に互換性のあるかどうかを判定します。これらの隣接ルータは隣接を確立しようとします。つまり、両者のリンクステートデータベースを同期させて、確実に同じOSPFv2ルーティング情報を持つようにします。隣接ルータは、各リンクの稼働状態に関する情報、リンクのコスト、およびその他のあらゆるネイバー情報を含むリンクステート アドバタイズメント（LSA）を共有します。これらのルータはその後、受信したLSAをすべてのOSPF対応インターフェイスにフラッディングします。これにより、すべてのOSPFv2ルータのリンクステート データベースが最終的に同じになります。すべての OSPFv2

ルータのリンクステートデータベースが同じになると、ネットワークは収束します。その後、各ルータは、ダイクストラの最短パス優先（SPF）アルゴリズムを使用して、自身のルートテーブルを構築します。

OSPFv2 ネットワークは、複数のエリアに分割できます。ルータは、ほとんどの LSA を 1 つのエリア内だけに送信するため、OSPF 対応ルータの CPU とメモリの要件が緩やかになります。

OSPFv2 は IPv4 をサポートしています。

（注） Cisco NX-OS 上の OSPFv2 は、RFC 2328 をサポートしています。この RFC では、ルートサマリー コストの計算に、RFC1583 で使用する計算と互換性がない別の方法が導入されました。また RFC 2328 では、AS-external パスに対して異なる選択基準が導入されました。すべてのルータが同じ RFC をサポートしていることを確認することが重要です。RFC。RFC1583 にのみ準拠しているルータがネットワークに含まれる場合は、**rfc1583compatibility** コマンドを使用します。デフォルトでサポートされている OSPFv2 用の RFC 標準は、Cisco NX-OS と Cisco IOS とで異なる場合があります。値が同じになるように設定するには、調整が必要です。詳細については、「OSPF RFC 互換モードの例」の項を参照してください。

Hello パケット

OSPFv2 ルータは、すべての OSPF 対応インターフェイスに hello パケットを定期的に送信します。ルータがこの hello パケットを送信する頻度は、インターフェイスごとに設定された hello 間隔により決定されます。OSPFv2 は、hello パケットを使用して、次のタスクを実行します。

- ネイバー探索
- キープアライブ
- 双方向通信
- 指定ルータの選定（「指定ルータ」セクションを参照してください）

hello パケットには、リンクの OSPFv2 コスト割り当て、hello 間隔、送信元ルータのオプション機能など、送信元の OSPFv2 インターフェイスとルータに関する情報が含まれます。これらの hello パケットを受信する OSPFv2 インターフェイスは、設定に受信インターフェイスの設定との互換性があるかどうかを判定します。互換性のあるインターフェイスはネイバーと見なされ、ネイバー テーブルに追加されます（「ネイバー情報」の項を参照してください）。

hello パケットには、送信元インターフェイスが通信したルータのルータ ID のリストも含まれます。受信インターフェイスが、このリストで自身の ID を見つけた場合は、2 つのインターフェイス間で双方向通信が確立されます。

OSPFv2 は、hello パケットをキープアライブ メッセージとして使用して、ネイバーが通信を継続中であるかどうかを判定します。ルータが設定されたデッド間隔（通常は hello 間隔の倍数）で hello パケットを受信しない場合、そのネイバーはローカル ネイバー テーブルから削除されます。

ネイバー情報

ネイバーであると見なされるようにするには、リモートインターフェイスと互換性があるように、OSPFv2 インターフェイスを設定しておく必要があります。この 2 つの OSPFv2 インターフェイスで、次の基準が一致している必要があります。

- hello 間隔
- デッド間隔
- エリア ID（エリア （253 ページ）セクションを参照してください）
- 認証
- オプション機能

一致する場合は、次の情報がネイバー テーブルに入力されます。

- ネイバー ID：ネイバーのルータ ID。
- プライオリティ：ネイバーのプライオリティ。プライオリティは、指定ルータの選定（指定ルータ （252 ページ）セクションを参照）に使用されます。
- 状態：ネイバーから通信があったか、双方向通信の確立処理中であるか、リンクステート情報を共有しているか、または完全な隣接関係が確立されたかを示します。
- デッド タイム：このネイバーから最後の hello パケットを受信した後に経過した時間を示します。
- IP アドレス：ネイバーの IP アドレス。
- 指定ルータ：ネイバーが指定ルータ、またはバックアップ指定ルータとして宣言されたかどうかを示します（指定ルータ （252 ページ）セクションを参照してください）。
- ローカル インターフェイス：このネイバーの hello パケットを受信したローカル インターフェイス。

隣接関係

すべてのネイバーが隣接関係を確立するわけではありません。ネットワーク タイプと確立された指定ルータに応じて、完全な隣接関係を確立して、すべてのネイバーと LSA を共有するものと、そうでないものがあります。詳細については、指定ルータ （252 ページ）を参照してください。

隣接関係は、OSPF のデータベース説明（DD）パケット、リンク状態要求（LSR）パケット、およびリンク状態更新（LSU）パケットを使用して確立されます。データベース説明パケットに含まれるのは、ネイバーのリンクステート データベースからの LSA ヘッダーだけです（リンクステート アドバタイズメント （254 ページ）セクションを参照してください）。ローカル ルータは、これらのヘッダーを自身のリンクステート データベースと比較して、新規の LSA か、更新された LSA かを判定します。ローカル ルータは、新規または更新の情報を必要とす

る各 LSA について、リンク状態要求（LSR）パケットを送信します。ネイバーは LSU パケットで応答します。このパケット交換は、両方のルータのリンクステート情報が同じになるまで継続します。

指定ルータ

複数のルータを含むネットワークは、OSPF 特有の状況です。すべてのルータがネットワークで LSA をフラッディングした場合は、同じリンクステート情報が複数の送信元から送信されます。ネットワークのタイプによっては、OSPFv2 は指定ルータ（DR）という 1 台のルータを使用して LSA のフラッディングを制御し、OSPFv2 の残りの部分に対してネットワークを代表する役割をさせる場合があります（「エリア」の項を参照）。DR がダウンした場合、OSPFv2 はバックアップ指定ルータ（BDR）を選択します。DR がダウンすると、OSPFv2 はこの BDR を使用します。

ネットワーク タイプは次のとおりです。

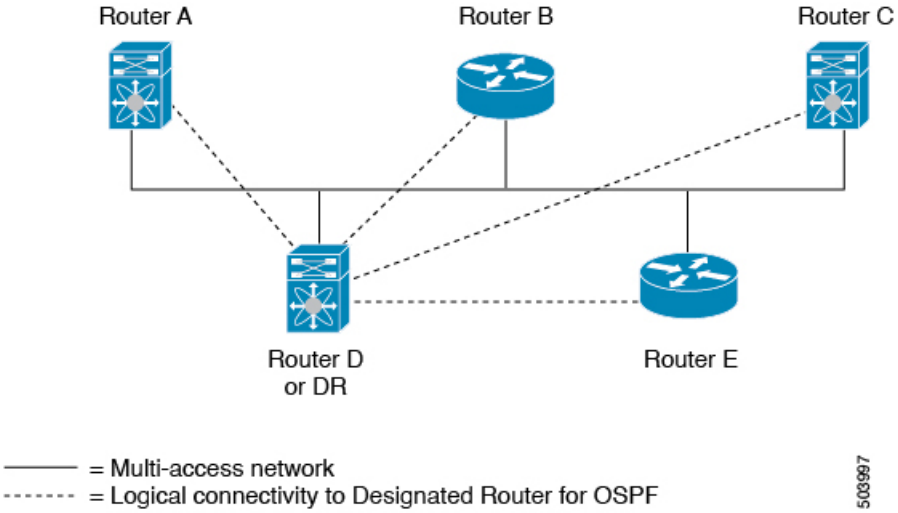
- ポイントツーポイント：2 台のルータ間にのみ存在するネットワーク。ポイントツーポイント ネットワーク上の全ネイバーは隣接関係を確立し、DR は存在しません。
- ブロードキャスト： ブロードキャスト トラフィックが可能なイーサネットなどの共有メディア上で通信できる複数のルータを持つネットワーク。OSPFv2 ルータは DR および BDR を確立し、これらにより、ネットワーク上の LSA フラッディングを制御します。OSPFv2 は、よく知られている IPv4 マルチキャスト アドレス 224.0.0.5 および MAC アドレス 0100.5300.0005 を使用して、ネイバーと通信します。

DR と BDR は、hello パケット内の情報に基づいて選択されます。インターフェイスは hello パケットの送信時に、どれが DR および BDR かわかっている場合は、優先フィールドと、DR および BDR フィールドを設定します。ルータは、hello パケットの DR および BDR フィールドで宣言されたルータと優先フィールドに基づいて、選定手順を実行します。最終的に OSPFv2 は、最も大きいルータ ID を DR および BDR として選択します。

他のルータはすべて DR および BDR と隣接関係を確立し、IPv4 マルチキャスト アドレス 224.0.0.6 を使用して、LSA 更新情報を DR と BDR に送信します。次の図は、すべてのルータと DR との隣接関係を示しています。

DR は、ルータ インターフェイスに基づいています。1 つのネットワークの DR であるルータは、別のインターフェイス上の他のネットワークの DR となることはできません。

図 *13* : マルチアクセス ネットワークの *DR*



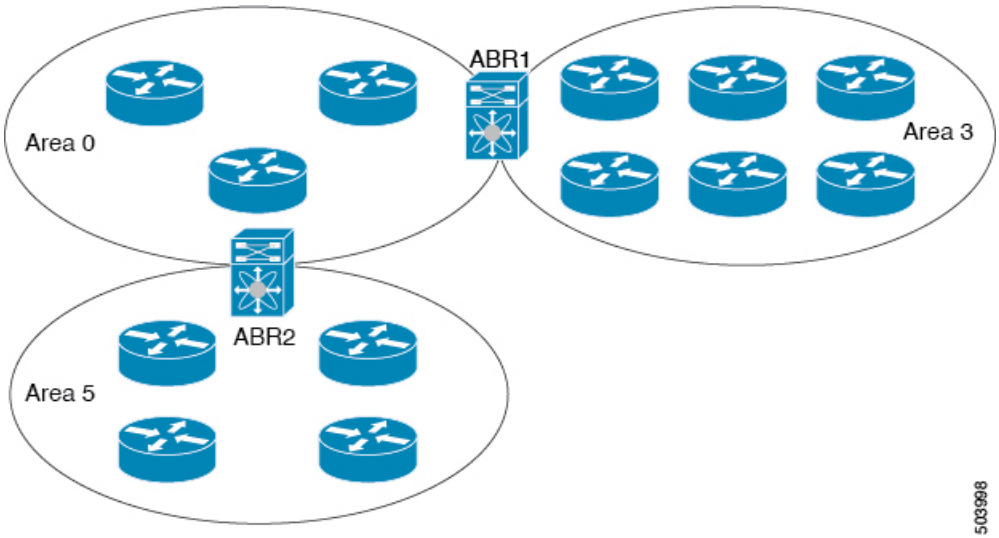
エリア

OSPFv2 ネットワークを複数のエリアに分割すると、ルータに要求される OSPFv2 の CPU とメモリに関する要件を制限できます。エリアとは、ルータの論理的な区分で、OSPFv2 ドメイン内にリンクして別のサブドメインを作成します。LSA フラッディングはエリア内でのみ発生し、リンクステートデータベースはエリア内のリンクにのみ制限されます。定義されたエリア内のインターフェイスには、エリア ID を割り当てることができます。エリア ID は、10.2.3.1 などの、数字またはドット付き 10 進表記で入力できる 32 ビット値です。

Cisco NX-OS は常にドット付き 10 進表記でエリアを表示します。

OSPFv2 ネットワーク内に複数のエリアを定義する場合は、0 という予約されたエリア ID を持つバックボーンエリアも定義する必要があります。エリアが複数ある場合は、1 台以上のルータがエリア境界ルータ（ABR）となります。図では、ABR がバックボーン エリアと他の 1 つ以上の定義済みエリアの両方に接続する方法を示します。

図 *14 : OSPFv2* エリア



ABR には、接続するエリアごとに個別のリンクステート データベースがあります。ABR は、接続したエリアの 1 つからバックボーン エリアにネットワーク集約（タイプ 3）LSA（「ルート集約」セクションを参照）を送信します。バックボーンエリアは、1 つのエリアに関する集約情報を別のエリアに送信します。OSPFv2 エリア図に、エリア 0 が、エリア 5 に関する集約情報をエリア 3 に送信しています。

OSPFv2 では、自律システム境界ルータ（ASBR）という、もう 1 つのルータ タイプも定義されています。このルータは、OSPFv2 エリアを別の自律システムに接続します。自律システムとは、単一の技術的管理エンティティにより制御されるネットワークです。OSPFv2 は、そのルーティング情報を別の自律システムに再配布したり、再配布されたルートを別の自律システムから受信したりできます。詳細については、「高度な機能」のセクションを参照してください。

リンクステート アドバタイズメント

OSPFv2 はリンクステート アドバタイズメント（LSA）を使用して、固有のルーティング テーブルを構築します。

リンクステート アドバタイズメント タイプ

OSPFv2 はリンクステート アドバタイズメント（LSA）を使用して、固有のルーティング テーブルを構築します。

次の表に、Cisco NX-OS でサポートされる LSA タイプを示します。

表 *16* : 表 *5-1 LSA* タイプ

タイプ	名前	説明
1	ルータ LSA	すべてのルータが送信する LSA。この LSA には、すべてのリンクの状態とコスト、およびリンク上のすべての OSPFv2 ネイバーの一覧が含まれます。ルータ LSA は SPF 再計算をトリガーします。ルータ LSA はローカル OSPFv2 エリアにフラッディングされます。
2	ネットワーク LSA	DR が送信する LSA。この LSA には、マルチアクセス ネットワーク内のすべてのルータの一覧が含まれます。ネットワーク LSA は SPF 再計算をトリガーします。「指定ルータ」のセクションを参照してください。
3	ネットワーク集約 LSA	エリア境界ルータが、ローカル エリア内の宛先ごとに外部エリアに送信する LSA。この LSA には、エリア境界ルータからローカルの宛先へのリンク コストが含まれます。「エリア」のセクションを参照してください。
4	ASBR 集約 LSA	エリア境界ルータが外部エリアに送信する LSA。この LSA は、リンク コストを ASBR のみにアドバタイズします。「エリア」の項を参照してください。
5	AS 外部 LSA	ASBR が生成する LSA。この LSA には、外部自律システム宛先へのリンク コストが含まれます。AS 外部 LSA は、自律システム全体にわたってフラッディングされます。「エリア」の項を参照してください。
7	NSSA 外部 LSA	ASBR が Not-So-Stubby Area（NSSA）内で生成する LSA。この LSA には、外部自律システム宛先へのリンク コストが含まれます。NSSA 外部 LSA は、ローカル NSSA 内のみでフラッディングされます。「エリア」のセクションを参照してください。
9–11	不透明 LSA	OSPF の拡張に使用される LSA。「不透明 LSA」のセクションを参照してください。

リンク コスト

各 OSPFv2 インターフェイスは、リンク コストを割り当てられています。このコストは任意の数字です。デフォルトでは、Cisco NX-OS が、設定された参照帯域幅をインターフェイス帯域幅で割った値をコストとして割り当てます。デフォルトでは、参照帯域幅は 40 Gbps です。リンク コストは各リンクに対して、LSA 更新情報で伝えられます。

フラッディングと LSA グループ ペーシング

OSPFv2 ルータは LSA を受信すると、その LSA をすべての OSPF 対応インターフェイスに転送し、この情報を使用して OSPFv2 エリアをフラッディングします。この LSA フラッディン

グにより、ネットワーク内のすべてのルータが同じルーティング情報を持つことが保証されます。LSA フラッディングは、OSPFv2 エリアの設定により異なります（「エリア」を参照）。LSA は、リンクステート リフレッシュ時間に基づいて（デフォルトでは 30 分ごとに）フラッディングされます。各 LSA には、リンクステート リフレッシュ時間が設定されています。

ネットワークの LSA 更新情報のフラッディング レートは、LSA グループ ペーシング機能を使用して制御できます。LSA グループ ペーシングにより、CPU またはバッファの高い使用率を低下させることができます。この機能により、同様のリンクステート リフレッシュ時間を持つ LSA がグループ化されるため、OSPFv2 で、複数の LSA を 1 つの OSPFv2 更新メッセージにまとめることが可能となります。

デフォルトでは、相互のリンクステート リフレッシュ時間が 10 秒以内の LSA が、同じグループに入れられます。この値は、大規模なリンクステート データベースでは低く、小規模のデータベースでは高くして、ネットワーク上の OSPFv2 負荷を最適化する必要があります。

リンクステート データベース

各ルータは、OSPFv2 ネットワーク用のリンクステート データベースを保持しています。このデータベースには、収集されたすべての LSA が含まれ、ネットワークを通過するすべてのルートに関する情報が格納されます。OSPFv2 は、この情報を使用して、各宛先への最適パスを計算し、この最適パスをルーティング テーブルに入力します。

MaxAge と呼ばれる設定済みの時間間隔で受信された LSA 更新情報がまったくない場合は、リンクステート データベースから LSA が削除されます。ルータは、LSA を 30 分ごとに繰り返してフラッディングし、正確なリンクステート情報が期限切れで削除されるのを防ぎます。Cisco NX-OS は、LSA グルーピング機能をサポートし、同時にすべての LSA が更新されないようにします。詳細については、「フラッディングと LSA グループ ペーシング」のセクションを参照してください。

不透明 LSA

不透明 LSA により、OSPF 機能の拡張が可能となります。不透明 LSA は、標準 LSA ヘッダーと、それに続くアプリケーション固有の情報で構成されます。この情報は、OSPFv2 または他のアプリケーションにより使用される場合があります。OSPFv2 は、OSPFv2 グレースフル リスタート機能をサポートするために Opaque LSA を使用します（「高可用性およびグレースフル リスタート」セクションを参照）。次のような 3 種類の不透明 LSA タイプが定義されています。

- LSA タイプ 9：ローカル ネットワークにフラッディングされます。
- LSA タイプ 10：ローカル エリアにフラッディングされます。
- LSA タイプ 11：ローカル自律システムにフラッディングされます。

OSPFv2およびユニキャストRIB

OSPFv2 は、リンクステート データベースでダイクストラの SPF アルゴリズムを実行します。このアルゴリズムにより、パス上の各リンクのリンク コストの合計に基づいて、各宛先への最適なパスが選択されます。そして、選択された各宛先への最短パスが OSPFv2 ルート テーブルに入力されます。OSPFv2 ネットワークが収束すると、このルート テーブルはユニキャスト RIB にデータを提供します。OSPFv2 はユニキャスト RIB と通信し、次の動作を行います。

- ルートの追加または削除
- 他のプロトコルからのルートの再配布への対応
- 変更されていない OSPFv2 ルートの削除およびスタブ ルータ アドバタイズメントを行うためのコンバージェンス更新情報の提供（OSPFv2 スタブ ルータ アドバタイズメント のセクションを参照してください）

さらに OSPFv2 は、変更済みダイクストラ アルゴリズムを実行して、集約および外部（タイプ 3、4、5、7）LSA の変更の高速再計算を行います。

認証

OSPFv2 メッセージに認証を設定して、ネットワークでの不正な、または無効なルーティング更新を防止できます。Cisco NX-OS は、次の 2 つの認証方式をサポートしています。

- 簡易パスワード認証
- MD5 認証ダイジェスト

OSPFv2 認証は、OSPFv2 エリアに対して、またはインターフェイスごとに設定できます。

簡易パスワード認証

簡易パスワード認証では、OSPFv2 メッセージの一部として送信された単純なクリア テキストのパスワードを使用します。受信 OSPFv2 ルータが OSPFv2 メッセージを有効なルート更新情報として受け入れるには、同じクリア テキスト パスワードで設定されている必要があります。パスワードがクリア テキストであるため、ネットワーク上のトラフィックをモニタできるあらゆるユーザがパスワードを入手できます。

暗号化認証

暗号化認証では、暗号化されたパスワードを OSPFv2認証に使用します。トランスミッタは、送信するパケットとキー文字列を使用してコードを計算し、そのコードとキー ID をパケットに挿入して、パケットを送信します。受信側は、受信したパケットとローカルに設定されたキーストリング（パケット内のキー ID に対応）を使用してコードをローカルに計算することにより、パケット内のコードを検証します。

メッセージダイジェスト 5（MD5）とハッシュベースのメッセージ認証コードセキュアハッシュアルゴリズム（HMAC-SHA）暗号化認証の両方がサポートされています。

MD5 認証

OSPFv2 メッセージを認証するには、MD5 認証を使用する必要があります。そのためには、ローカル ルータとすべてのリモート OSPFv2 ネイバーが共有するパスワードを設定します。Cisco NX-OS は各 OSPFv2 メッセージに対して、メッセージと暗号化されたパスワードに基づく MD5 一方向メッセージ ダイジェストを作成します。インターフェイスはこのダイジェストを OSPFv2 メッセージとともに送信します。受信する OSPFv2 ネイバーは、同じ暗号化パスワードを使用して、このダイジェストを確認します。メッセージが変更されていない場合はダイジェストの計算が同一であるため、OSPFv2 メッセージは有効と見なされます。

MD5 認証には、ネットワークでのメッセージの再送を防ぐための、各 OSPFv2 メッセージのシーケンス番号が含まれます。

HMAC-SHA 認証

OSPFv2 は RFC 5709 をサポートしており、MD5 よりも高いセキュリティを提供する HMAC-SHA アルゴリズムを使用できます。HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-384。および HMAC-SHA-512 アルゴリズムは、OSPFv2認証でサポートされます。

高度な機能

Cisco NX-OS は、ネットワークでの OSPFv2 の可用性やスケーラビリティを向上させる、高度な OSPFv3 機能をサポートしています。

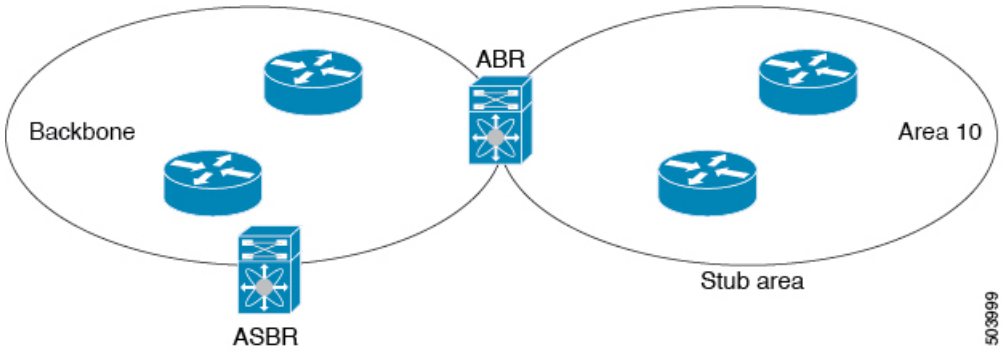
スタブ エリア

エリアをスタブエリアにすると、エリアでフラッディングされる外部ルーティング情報の量を制限できます。スタブ エリアとは、AS 外部（タイプ 5）LSA（「リンク ステート アドバタイズメント」のセクションを参照）が許可されないエリアです。これらの LSA は通常、外部ルーティング情報を伝播するためにローカル自律システム全体でフラッディングされます。スタブ エリアには、次の要件があります。

- スタブ エリア内のすべてのルータはスタブ ルータです。
- スタブ エリアには ASBR ルータは存在しません。
- スタブ エリアには仮想リンクを設定できません。

次の図には、外部 AS に到達するためにエリア 0.0.0.10 内のすべてのルータが ABR を通過する必要のある OSPFv2 AS の例を示します。エリア 0.0.0.10 は、スタブ エリアとして設定できます。

図 *15*：スタブ エリア



スタブ エリアは、外部自律システムへのバックボーン エリアを通過する必要のあるすべてのトラフィックにデフォルト ルートを使用します。IPv4 の場合のデフォルト ルートは 0.0.0.0 です。

Not-So-Stubby Area

Not-So-Stubby Area（NSSA）は、スタブ エリアに似ていますが、NSSA では、再配布を使用して NSSA 内で自律システム外部ルートをインポートできる点が異なります。NSSA ASBR はこれらのルートを再配布し、NSSA 外部（タイプ 7）LSA を生成して NSSA 全体でフラッディングします。または、NSSA を他のエリアに接続する ABR を設定することにより、この NSSA 外部 LSA を AS 外部（タイプ 5）LSA に変換することもできます。こうすると、ABR は、これらの AS 外部 LSA を OSPFv2 自律システム全体にフラッディングします。変換中は集約とフィルタリングがサポートされます。NSSA 外部 LSA に関する情報については、リンク ステート アドバタイズメント （254 ページ） セクションを参照してください。

たとえば、OSPFv2 を使用する中央サイトを、異なるルーティング プロトコルを使用するリモート サイトに接続するときに NSSA を使用すると、管理作業を簡素化できます。リモート サイトへのルートはスタブエリア内に再配布できないため、NSSA を使用する前に、企業サイトの境界ルータとリモート ルータの間の接続を OSPFv2 スタブエリアとして実行できません。NSSA が実装されたことで、企業ルータとリモートルータ間のエリアを NSSA として定義することにより、NSSA で OSPFv2 を拡張してリモート接続をカバーできます。

バックボーン エリア 0 を NSSA にできません。

（注） OSPF は、RFC 3101 セクション 2.5(3) に準拠しています。Not-so-Stubby Area に接続されたエリア境界ルータが P ビット クリアのデフォルト ルート LSA を受信した場合は、無視されます。OSPF は、これらの条件下で以前にデフォルト ルートを追加していました。

すでに RFC 非準拠の動作を使用するようにネットワークを設計しており、デフォルト ルートが NSSA ABR に追加されると想定している場合は、アップグレードするときに動作が変更されます。

古い動作を続行する場合は、**default-route nssa-abr pbit-clear** コマンドで有効にすることができます。

ルートの再配布

OSPFv2 は、ルート再配布を使用して、他のルーティング プロトコルからルートを学習できます。リンク コストをこれらの再配布されたルートに割り当てるか、またはデフォルト リンク コストを再配布されたすべてのルートに割り当てるように、OSPFv2 を設定します。

ルート再配布では、ルートマップを使用して、再配布する外部ルートを管理します。再配布を指定したルートマップを設定して、どのルートがOSPFv2に渡されるかを制御する必要があります。ルート マップを使用すると、宛先、送信元プロトコル、ルート タイプ、ルート タグなどの属性に基づいて、ルートをフィルタリングできます。ルートマップを使用して、これらの外部ルートがローカル OSPFv2 自律システムでアドバタイズされる前に AS 外部（タイプ 5）LSA および NSSA 外部（タイプ 7）LSA のパラメータを変更できます。ルート マップの構成については、「ルート ポリシー マネージャの構成」のセクションを参照してください。

ルート集約

OSPFv2 は、学習したすべてのルートを、すべての OSPF 対応ルータと共有するため、ルート集約を使用して、すべての OSPF 対応ルータにフラッディングされる一意のルートの数を削減した方がよい場合があります。ルート集約により、より具体的な複数のアドレスが、すべての具体的なアドレスを表す1つのアドレスに置き換えられるため、ルートテーブルが簡素化されます。たとえば、10.1.1.0/24、10.1.2.0/24、および10.1.3.0/24というアドレスを1つの集約アドレス 10.1.0.0/16 に置き換えることができます。

一般的には、エリア境界ルータ（ABR）の境界ごとに集約します。集約は2つのエリアの間でも設定できますが、バックボーンの方向に集約する方が適切です。こうすると、バックボーンがすべての集約アドレスを受信し、すでに集約されているそれらのアドレスを他のエリアに投入できるためです。集約には、次の 2 タイプがあります。

- エリア間ルート集約
- 外部ルート集約

エリア間ルート集約は ABR 上で設定し、自律システム内のエリア間のルートを集約します。集約の利点を生かすには、これらのアドレスを1つの範囲内にまとめることができるように、連続するネットワーク番号をエリア内で割り当てる必要があります。

外部ルート集約は、ルート再配布を使用してOSPFv2に投入される外部ルートに特有のルート集約です。集約する外部の範囲が連続していることを確認する必要があります。異なる2台のルータからの重複範囲を集約すると、誤った宛先にパケットが送信される原因となる場合があります。外部ルート集約は、ルートを OSPF に再配布している ASBR で設定してください。

集約アドレスの設定時に Cisco NX-OS は、ルーティング ブラック ホールおよびルート ループを防ぐために、集約アドレスの廃棄ルートを自動的に設定します。

高可用性およびグレースフル リスタート

Cisco NX-OS は、マルチレベルの高可用性 アーキテクチャを提供します。OSPFv2 は、ステートフル リスタートをサポートしています。これは、ノンストップ ルーティング（NSR）とも

呼ばれます。OSPFv2 で問題が発生した場合は、以前の実行時状態からの再起動を試みます。この場合、ネイバーはいずれのネイバーイベントも登録しません。最初の再起動が正常ではなく、別の問題が発生した場合、OSPFv2 はグレースフル リスタートを試みます。

グレースフル リスタート、つまり、Nonstop Forwarding（NSF）では、処理の再起動中も OSPFv2 がデータ転送パス上に存在し続けます。OSPFv2 はグレースフル リスタートを実行する必要がある場合、猶予 LSA と呼ばれるリンクローカル不透明（タイプ 9）LSA（「不透明 LSA」の項を参照）を送信します。この再起動中の OSPFv2 プラットフォームは NSF 対応と呼ばれます。

猶予 LSA には猶予期間が含まれます。猶予期間とは、ネイバー OSPFv2 インターフェイスが再起動中の OSPFv2 インターフェイスからの LSA を待つよう指定された時間です（通常、OSPFv2 は隣接関係を切断し、ダウン状態または再起動中の OSPFv2 インターフェイスからのすべての LSA を廃棄します）。参加するネイバーは、NSF ヘルパーと呼ばれ、再起動中の OSPFv2 インターフェイスから発信されたすべての LSA を、インターフェイスがまだ隣接しているかのように保持します。

再起動中の OSPFv2 インターフェイスが稼働を再開すると、ネイバーを再探索して隣接関係を確立し、LSA 更新情報の送信を再開します。この時点で、NSF ヘルパーは、グレースフル リスタートが完了したと認識します。

ステートフル リスタートは次のシナリオで使用されます。

- プロセスでの問題発生後の最初の回復試行

グレースフル リスタートは次のシナリオで使用されます。

- プロセスでの問題発生後の 2 回目の回復試行（4 分以内）
- **restart ospf** を使用したプロセスの手動再起動 コマンド

OSPFv2 スタブ ルータ アドバタイズメント

OSPFv2 スタブ ルータ アドバタイズメント機能を使用して、OSPFv2 インターフェイスをスタブ ルータとして機能するように設定できます。この機能は、ネットワークに新規ルータを機能制限付きで導入する場合や、過負荷になっているルータの負荷を制限する場合など、このルータ経由の OSPFv2 トラフィックを制限するときに使用します。また、この機能は、さまざまな管理上またはトラフィック エンジニアリング上の理由により使用する場合もあります。

OSPFv2 スタブ ルータ アドバタイズメントは、OSPFv2 ルータをネットワーク トポロジから削除しませんが、他の OSPFv2 ルータがこのルータを使用して、ネットワークの他の部分にトラフィックをルーティングできないようにします。このルータを宛先とするトラフィック、またはこのルータに直接接続されたトラフィックだけが送信されます。

OSPFv2 スタブ ルータ アドバタイズメントは、すべてのスタブ リンク（ローカル ルータに直接接続された）を、ローカル OSPFv2 インターフェイスのコストとしてマークします。すべてのリモート リンクは、最大のコスト（0xFFFF）としてマークされます。

複数の OSPFv2 インスタンス

Cisco Nexus® 3550-T スイッチは、同じノード上で動作する、OSPFv2 プロトコルの複数インスタンスをサポートしています。同一インターフェイスには複数のインスタンスを設定できません。デフォルトでは、すべてのインスタンスが同じシステム ルータ ID を使用します。複数のインスタンスが同じ OSPFv2 自律システムにある場合は、各インスタンスのルータ ID を手動で設定する必要があります。サポートされる OSPFv2 インスタンスの数については、『*Cisco Nexus® 3550-T* 検証済みの拡張性ガイド』を参照してください。

SPF 最適化

Cisco NX-OS は、次の方法で SPF アルゴリズムを最適化します。

- ネットワーク（タイプ 2）LSA、ネットワーク集約（タイプ 3）LSA、および AS 外部（タイプ 5）LSA 用の部分的 SPF：これらの LSA のいずれかが変更されると、Cisco NX-OS は、全体的な SPF 計算ではなく、高速部分計算を実行します。
- SPF タイマー：さまざまなタイマーを設定して、SPF 計算を制御できます。これらのタイマーには、後続の SPF 計算の幾何バックオフが含まれます。幾何バックオフにより、複数の SPF 計算による CPU 負荷が制限されます。

OSPFv2 の前提条件

OSPFv2 には、次の前提条件があります。

- OSPF を設定するための、ルーティングの基礎に関する詳しい知識がある。
- スイッチにログインしている。
- リモート OSPFv2 ネイバーと通信可能な IPv4 用インターフェイスが 1 つ以上設定されている。
- OSPFv2 ネットワーク戦略と、ネットワークのプランニングが完成している。たとえば、複数のエリアが必要かどうかを決定します。
- OSPF 機能がイネーブルにされている（「OSPFv2の有効化 」の項を参照）。

OSPFv2 の注意事項および制約事項

OSPFv2 設定時の注意事項および制約事項は、次のとおりです。

- **no graceful-restart planned only** コマンドを入力すると、グレースフル リスタートは無効になります。
- Cisco NX-OS は、ユーザがエリアを 10 進表記で入力するか、ドット付き 10 進表記で入力するかに関係なく、ドット付き 10 進表記でエリアを表示します。

- すべての OSPFv2 ルータが、同じ RFC 互換モードで動作する必要があります。Cisco Nexus® 3550-T の OSPFv2 は RFC 2328 に準拠しています。RFC 1583 にのみ対応しているルータがネットワークに含まれている場合は、ルータ設定モードで **rfc1583compatibility** コマンドを使用します。
- スケール シナリオでは、インターフェイスと OSPF プロセスのリンク ステート アドバタイズメントの数が大きい場合、OSPF MIB オブジェクトの SNMP エージェントのタイムアウト値が小さい SNMP ウォークは、タイムアウトになると予想されます。OSPF MIB オブジェクトのポーリング中に問い合わせる SNMP エージェントのタイムアウトを確認する場合は、ポーリングする SNMP エージェントのタイムアウト値を増加してください。
- アドミニストレーティブ ディスタンス機能には、次のガイドラインと制限事項が適用されます。
  - OSPF ルートに複数の等コスト パスがある場合、アドミニストレーティブ ディスタンスを設定しても **match ip route-source** コマンドに対しては決定性を持ちません。
  - アドミニストレーティブ ディスタンスの設定は、**match route-type**、**match ip address prefix-list**、および **match ip route-source prefix-list** コマンドでのみサポートされます。別の match 文は無視されます。
  - OSPF ルートのアドミニストレーティブ ディスタンスを設定する場合、**match route-type**、**match ip address**、および **match ip route-source** コマンドの間に優先順位はありません。このように、Cisco Nexus® 3550-T スイッチ OSPF のアドミニストレーティブ ディスタンスを設定するためのテーブル マップの動作は、Cisco IOS OSPF の場合と異なります。
  - 廃棄ルートには、アドミニストレーティブ ディスタンス 220 が常に割り当てられます。テーブル マップの設定は OSPF の廃棄ルートには適用されません。
- **show run ospf** コマンドの出力には、一部の OSPF コマンドのデフォルト値が表示される場合があります。
- Cisco Nexus® 3550-T スイッチは OSPF ネイバー探索パケットを転送しません。Cisco Nexus® 3550-T が中間スイッチの場合、OSPF ネイバーは探索されません。

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

（注） ***Cisco Nexus 3550-T - 10.1(2t)* リリース** は、デフォルトの VRF でのみ OSPFv2 をサポートすることに注意してください。

OSPFv2のデフォルト設定

次の表に、OSPFv2 パラメータのデフォルト設定値を示します。

表 *17 : OSPFv2* のデフォルト パラメータ

パラメータ	デフォルト
アドミニストレーティブ ディスタンス	110
hello 間隔	10 秒
デッド間隔	40 秒
廃棄ルート	イネーブル
グレースフル リスタートの猶予期間	60 秒
OSPFv2 機能	ディセーブル
スタブ ルータ アドバタイズメントの宣言期間	600 秒
リンク コスト計算の参照帯域幅	40 Gbps
LSA 最小到着時間	1000 ミリ秒
LSA グループ ペーシング	10 秒
SPF 計算初期遅延時間	200 ミリ秒
SPF の最小ホールド タイム	5000 ミリ秒
SPF 計算初期遅延時間	1000 ミリ秒

基本的な OSPFv2 の設定

OSPFv2 は、OSPFv2 ネットワークを設計した後に設定します。

OSPFv2の有効化

OSPFv2 を設定するには、その前に OSPFv2 機能を有効にする必要があります。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**feature ospf** 例： `switch(config)# feature ospf` 例：	OSPFv2 機能を有効にします。
ステップ 3	（任意） **show feature** 例： `switch(config)# show feature`	有効および無効にされた機能を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

OSPFv2機能をディセーブルにして、関連付けられている設定をすべて削除するには、グローバル設定モードで no feature ospf コマンドを使用します。

コマンド	目的
no feature ospf 例： `switch(config)# no feature ospf`	OSPFv2機能を無効にして、関連付けられた設定をすべて削除します。

OSPFv2インスタンスの作成

OSPFv2 を設定する最初のステップは、OSPFv2 インスタンスを作成することです。作成した OSPFv2インスタンスには、一意のインスタンス タグを割り当てます。インスタンス タグは任意の文字列です。

OSPFv2インスタンス パラメータの詳細については、高度なOSPFv2の設定（276ページ）の項を参照してください。

始める前に

OSPF 機能をイネーブルにしてあることを確認します（「OSPFv2の有効化」の項を参照）。

show ip ospf *instance-tag* コマンドを使用して、インスタンス タグが使用されていないことを確認します。

OSPFv2 がルータ ID（設定済みのループバック アドレスなど）を入手可能であるか、またはルータ ID オプションを設定する必要があります。

手順

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

ステップ 2	[**no**]**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)`
		新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	（任意） **router-id** *ip-address* **例：** `switch(config-router)# router-id 192.0.2.1`	OSPFv2 ルータ ID を設定します。この IP アドレスにより、この OSPFv2 インスタンスが識別されます。このアドレスは、システムの設定済みインターフェイス上に存在する必要があります。
ステップ 4	（任意） **show ip ospf** *instance-tag* **例：** `switch(config-router)# show ip ospf 201`	OSPF 情報を表示します。
ステップ 5	（任意） **copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

OSPFv2インスタンスと、関連付けられている設定をすべて削除するには、グローバル コンフィギュレーション モードで no feature ospf コマンドを使用します。

コマンド	目的
no router ospf *instance-tag* 例： `switch(config)# no router ospf 201`	OSPF インスタンスと、関連付けられた設定を削除します。

（注） このコマンドは、インターフェイス モードではOSPF設定を削除しません。インターフェイス モードで設定されたOSPFv2コマンドはいずれも、手動で削除する必要があります。

OSPFv2 インスタンスのオプション パラメータの設定

OSPF のオプション パラメータを設定できます。高度なOSPFv2の設定 （276 ページ） セクションを参照してください。

ルータ コンフィギュレーション モードで、次の OSPFv2 用オプション パラメータを設定できます。

始める前に

OSPF 機能を有効にしてあることを確認します（「OSPFv2の有効化」の項を参照）。

OSPFv2 がルータ ID（設定済みのループバック アドレスなど）を入手可能であるか、またはルータ ID オプションを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**distance** *number* 例： `switch(config-router)# distance 25`	このOSPFv2インスタンスのアドミニストレーティブ ディスタンスを設定します。範囲は1～255です。デフォルトは110です。
ステップ 2	**log-adjacency-changes [detail]** 例： `switch(config-router)# log-adjacency-changes`	ネイバーの状態が変化するたびに、システム メッセージを生成します。
ステップ 3	**maximum-paths** *path-number* 例： `switch(config-router)# maximum-paths 4`	ルート テーブル内の宛先への同じOSPFv2パスの最大数を設定します。このコマンドはロード バランシングに使用されます。指定できる範囲は 1 ～ 16 です。デフォルト値は 8 です。

	コマンドまたはアクション	目的
ステップ 4	**distance** *number* 例： `switch(config-router)# distance 25`	このOSPFv2インスタンスのアドミニストレーティブ ディスタンスを設定します。範囲は1～255です。デフォルトは110です。
ステップ 5	**log-adjacency-changes** [**detail**] 例： `switch(config-router)# log-adjacency-changes`	ネイバーの状態が変化するたびに、システム メッセージを生成します。
ステップ 6	**maximum-paths** *path-number* 例： `switch(config-router)# maximum-paths 4`	ルート テーブル内の宛先への同じOSPFv2パスの最大数を設定します。このコマンドはロード バランシングに使用されます。指定できる範囲は 1 ～ 16 です。デフォルト値は 8 です。 （注） Cisco Nexus® 3550-T ハードウェアは 1 つのパスのみインストールします。ECMP は Cisco Nexus® 3550-T ではサポートされていません。
ステップ 7	**passive-interface default** 例： `switch(config-router)# passive-interface default`	すべてのインターフェイス上でルーティングが更新されないようにします。このコマンドは、VRF またはインターフェイス コマンド モードの設定によって上書きされます。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config-router)# copy running-config startup-config`	この設定変更を保存します。

例

次の例は、OSPFv2 インスタンスを作成する方法を示しています。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# copy running-config startup-config
```

OSPFv2でのネットワークの設定

ルータがこのネットワークへの接続に使用するインターフェイスを介して、OSPFv2 へのネットワークを関連付けることで、このネットワークを設定できます（「ネイバー」セクションを参照）。すべてのネットワークをデフォルトバックボーンエリア（エリア 0）に追加したり、任意の 10 進数または IP アドレスを使用して新規エリアを作成したりできます。

（注） すべてのエリアは、バックボーン エリアに直接、または仮想リンク経由で接続する必要があります。

（注） インターフェイスに有効な IP アドレスを設定するまでは、OSPF はインターフェイス上でイネーブルにされません。

始める前に

OSPF 機能をイネーブルにしてあることを確認します（「OSPFv2の有効化」の項を参照）。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**ip address** *ip-prefix/length* 例： `switch(config-if)# ip address 192.0.2.1/16`	このインターフェイスにIPアドレスおよびサブネット マスクを割り当てます。
ステップ 4	**ip router ospf** *instance-tag* **area** *area-id* [**secondaries none**] 例： `switch(config-if)# ip router ospf 201 area 0.0.0.15`	OSPFv2 インスタンスおよびエリアにインターフェイスを追加します。

	コマンドまたはアクション	目的
ステップ 5	（任意） **show ip ospf** *instance-tag* **interface** *interface-type slot/port* 例： `switch(config-if)# show ip ospf 201 interface ethernet 1/2`	OSPF 情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	この設定変更を保存します。
ステップ 7	（任意） **ip ospf cost** *number* 例： `switch(config-if)# ip ospf cost 25`	このインターフェイスの OSPFv2 コストメトリックを設定します。デフォルトでは、参照帯域幅とインターフェイス帯域幅に基づいて、コストメトリックが計算されます。有効な範囲は 1 ～ 65535 です。
ステップ 8	（任意） **ip ospf dead-interval** *seconds* 例： `switch(config-if)# ip ospf dead-interval 50`	OSPFv2 デッド間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトでは、hello 間隔の秒数の 4 倍です。
ステップ 9	（任意） **ip ospf hello-interval** *seconds* 例： `switch(config-if)# ip ospf hello-interval 25`	OSPFv2 hello 間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 秒です。
ステップ 10	（任意） **[default | no] ip ospf passive-interface** 例： `switch(config-if)# ip ospf passive-interface`	インターフェイス上でルーティングが更新されないようにします。このコマンドによって、ルータまたはVRF コマンドモードの設定が上書きされます。**default** オプションは、このインターフェイスモードコマンドを削除して、ルータまたは VRF の設定に戻します（設定がある場合）。
ステップ 11	（任意） **ip ospf priority** *number* 例： `switch(config-if)# ip ospf priority 25`	エリアの DR の決定に使用される OSPFv2プライオリティを設定します。有効な範囲は 0 ～ 255 です。デフォルトは 1 です。「指定ルータ」の項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 12	（任意） **ip ospf shutdown** 例： `switch(config-if)# ip ospf shutdown`	このインターフェイス上の OSPFv2 インスタンスをシャットダウンします。

例

次に、OSPFv2 インスタンス 201 にネットワーク エリア 0.0.0.10 を追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0.0.0.10
switch(config-if)# copy running-config startup-config
```

show ip ospf interface コマンドを使用し、 すれば、インターフェイスの設定を確認できます。**show ip ospf neighbor** コマンドを使用し、 すれば、このインターフェイスの NAVERを確認できます。

エリアの認証の設定

エリア内のすべてのネットワーク、またはエリア内の個々のインターフェイスの認証を設定できます。インターフェイス認証設定を使用すると、エリア認証は無効になります。

始める前に

OSPF 機能が有効になっていることを確認するには、「OSPFv2の有効化」セクションを参照してください。

インターフェイス上のすべてのネイバーが、共有認証キーを含め、同じ認証設定を共有することを確認します。

この認証設定のためのキーチェーンを作成します。「*Cisco Nexus® 3550-T* のセキュリティの設定」セクションを参照してください。

（注） OSPFv2 の場合、**key** *key-id* にキー ID があります コマンドは、2ー255 の値のみをサポートします。

手順

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

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**area** *area-id* **authentication** [**message-digest**] 例： `switch(config-router)# area 0.0.0.10 authentication`	エリアの認証モードを設定します。

ステップ 4	**interface** *interface-type slot/port*
	例：
	`switch(config-router)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 5	（任意） **ip ospf authentication-key** [**0** | **3**] *key* 例： `switch(config-if)# ip ospf authentication-key 0 mypass`	このインターフェイスに簡易パスワード認証を設定します。認証が、キーチェーンにもメッセージ ダイジェストにも設定されていない場合は、このコマンドを使用します。0 の場合は、パスワードをクリアテキストで設定します。3 の場合は、パスワードを 3DES 暗号化として設定します。
ステップ 6	（任意） **ip ospf message-digest-key** *key-id* **md5** [**0** | **3**] *key* 例： `switch(config-if)# ip ospf message-digest-key 21 md5 0 mypass`	このインターフェイスにメッセージ ダイジェスト認証を設定します。認証がメッセージ ダイジェストに設定されている場合は、このコマンドを使用します。key-id の範囲は 1 ～ 255 です。MD5 オプションが 0 の場合はパスワードがクリアテキストで設定され、3 の場合はパス キーが 3DES 暗号化として設定されます。
ステップ 7	（任意） **show ip ospf** *instance-tag* **interface** *interface-type slot/port* 例： `switch(config-if)# show ip ospf 201 interface ethernet 1/2`	OSPF 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 8	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

インターフェイスの認証の設定

エリア内のすべてのネットワーク、またはエリア内の個々のインターフェイスの認証を設定できます。インターフェイス認証設定を使用すると、エリア認証は無効になります。

始める前に

OSPF 機能を有効化してあることを確認します（OSPFv2の有効化（264ページ）セクションを参照してください）。

インターフェイス上のすべてのネイバーが、共有認証キーを含め、同じ認証設定を共有することを確認します。

この認証設定のためのキーチェーンを作成します。「*Cisco Nexus® 3550-T* のセキュリティの設定」セクションを参照してください。

（注） OSPFv2 の場合、**key** *key-id* にキー ID があります コマンドは、2ー255 の値のみをサポートします。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**ip ospf authentication** [**message-digest**] 例： `switch(config-if)# ip ospf authentication`	OSPFv2 のインターフェイス認証モードをクリアテキスト タイプとメッセージ ダイジェスト タイプのどちらかでイネーブルにします。これにより、エリアに基

	コマンドまたはアクション	目的
		づくこのインターフェイスの認証が無効となります。すべてのネイバーが、この認証タイプを共有する必要があります。
ステップ 4	（任意） **ip ospf authentication key-chain** *key-id* 例： `switch(config-if)# ip ospf authentication key-chain Test1`	OSPFv2 のキーチェーンを使用するようにインターフェイス認証を設定します。キー チェーンの詳細については、『シスコ スタンドアロン*Cisco NX-OS* セキュリティ設定ガイド』を参照してください。
ステップ 5	（任意） **ip ospf authentication-key** [**0** | **3** | **7**] *key* 例： `switch(config-if)# ip ospf authentication-key 0 mypass`	このインターフェイスに簡易パスワード認証を設定します。認証が、キーチェーンにもメッセージ ダイジェストにも設定されていない場合は、このコマンドを使用します。 オプションは次のとおりです。 • 0：パスワードをクリアテキストで設定します。 • 3：パス キーを 3DES 暗号化として設定します。 • 7：パス キーを Cisco タイプ 7 暗号化として設定します。
ステップ 6	（任意） **ip ospf message-digest-key** *key-id* **md5** [**0** | **3** | **7**] *key* 例： `switch(config-if)# ip ospf message-digest-key 21 md5 0 mypass`	このインターフェイスにメッセージ ダイジェスト認証を設定します。認証がメッセージ ダイジェストに設定されている場合は、このコマンドを使用します。key-id の範囲は 1 ～ 255 です。MD5 オプションは次のとおりです。 • 0：パスワードをクリアテキストで設定します。 • 3：パス キーを 3DES 暗号化として設定します。 • 7：パス キーを Cisco タイプ 7 暗号化として設定します。
ステップ 7	（任意） **show ip ospf** *instance-tag* **interface** *interface-type slot/port* 例：	OSPF 情報を表示します。

	コマンドまたはアクション	目的
	`switch(config-if)# show ip ospf 201 interface ethernet 1/2`	
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、インターフェイスに暗号化されていない簡単なパスワードを設定し、イーサネット インターフェイス 1/2 のパスワードを設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# exit
switch(config)# interface ethernet 1/2
switch(config-if)# ip router ospf 201 area 0.0.0.10
switch(config-if)# ip ospf authentication
switch(config-if)# ip ospf authentication-key 0 mypass
switch(config-if)# copy running-config startup-config
```

次に、OSPFv2 HMAC-SHA-1 および MD5 暗号化認証を設定する例を示します。

```
switch# configure terminal
switch(config)# key chain chain1
switch(config-keychain)# key 1
switch(config-keychain-key)# key-string 7 070724404206
switch(config-keychain-key)# accept-lifetime 01:01:01 Jan 01 2015 infinite
switch(config-keychain-key)# send-lifetime 01:01:01 Jan 01 2015 infinite
switch(config-keychain-key)# cryptographic-algorithm HMAC-SHA-1
switch(config-keychain-key)# exit
switch(config-keychain)# key 2
switch(config-keychain-key)# key-string 7 070e234f1f5b4a
switch(config-keychain-key)# accept-lifetime 10:51:01 Jul 24 2015 infinite
switch(config-keychain-key)# send-lifetime 10:51:01 Jul 24 2015 infinite
switch(config-keychain-key)# cryptographic-algorithm MD5
switch(config-keychain-key)# exit
switch(config-keychain)# exit

switch(config)# interface ethernet 1/1
switch(config-if)# ip router ospf 1 area 0.0.0.0
switch(config-if)# ip ospf authentication message-digest
switch(config-if)# ip ospf authentication key-chain chain1

switch(config-if)# show key chain chain1
Key-Chain chain1
Key 1 -- text 7 "070724404206"
cryptographic-algorithm HMAC-SHA-1
accept lifetime UTC (01:01:01 Jan 01 2015)-(always valid) [active]
send lifetime UTC (01:01:01 Jan 01 2015)-(always valid) [active]
Key 2 -- text 7 "070e234f1f5b4a"
cryptographic-algorithm MD
accept lifetime UTC (10:51:00 Jul 24 2015)-(always valid) [active]
send lifetime UTC (10:51:00 Jul 24 2015)-(always valid) [active]
```

```
switch(config-if)# show ip ospf interface ethernet 1/1
Ethernet1/1 is up, line protocol is up
IP address 11.11.11.1/24
Process ID 1 VRF default, area 0.0.0.3
Enabled by interface configuration
State BDR, Network type BROADCAST, cost 40
Index 6, Transmit delay 1 sec, Router Priority 1
Designated Router ID: 33.33.33.33, address: 11.11.11.3
Backup Designated Router ID: 1.1.1.1, address: 11.11.11.1
2 Neighbors, flooding to 2, adjacent with 2
Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
Hello timer due in 00:00:08
Message-digest authentication, using keychain key1 (ready)
Sending SA: Key id 2, Algorithm MD5
Number of opaque link LSAs: 0, checksum sum 0
```

高度なOSPFv2の設定

OSPFv2 は、OSPFv2 ネットワークを設計した後に設定します。

境界ルータのフィルタ リストの設定

OSPFv2 ドメインを関連ネットワークを含む一連のエリアに分割できます。すべてのエリアは、エリア境界ルータ（ABR）経由でバックボーンエリアに接続している必要があります。OSPFv2 ドメインは、自律システム境界ルータ（ASBR）を介して、外部ドメインにも接続可能です。

ABR には、省略可能な次の設定パラメータがあります。

- Area range：エリア間のルート集約を設定します。「ルート集約の設定（287ページ）」の項を参照してください。
- Filter list：外部エリアから受信したネットワーク集約（タイプ 3）LSA をフィルタリングします。

ASBR もフィルタ リストをサポートしています。

始める前に

OSPF機能がイネーブルになっていることを確認します。OSPFv2の有効化（264ページ）のセクションを参照してください）

フィルタ リストが、着信または発信ネットワーク集約（タイプ 3）LSA の IP プレフィックスのフィルタリングに使用するルートマップを作成します。詳細については、「ルートポリシーマネージャの構成」のセクションを参照してください。「エリア（253ページ）」の項を参照してください。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規OSPFv2インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**area** *area-id* **filter-list route-map** *map-name* {**in** | **out**} 例： `switch(config-router)# area 0.0.0.10 filter-list route-map FilterLSAs in`	ABR 上で着信または発信ネットワーク集約（タイプ3）LSAをフィルタリングします。

ステップ 4	（任意） **show ip ospf policy statistics area** *id* **filter-list** {**in** | **out**}
	例：
	`switch(config-router)# show ip ospf policy`
	`statistics area 0.0.0.10 filter-list in`
		OSPF ポリシー情報を表示します。

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

例

次に、エリア 0.0.0.10 でフィルタ リストを設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 filter-list route-map FilterLSAs in
switch(config-router)# copy running-config startup-config
```

スタブ エリアの設定

OSPFv2 ドメインの外部トラフィックが不要な個所にスタブエリアを設定できます。スタブエリアは AS 外部（タイプ 5）LSA をブロックし、選択したネットワークへの往復の不要なルー

ティングを制限します。「スタブエリア」の項を参照してください。また、すべての集約ルートがスタブ エリアを経由しないようブロックすることもできます。

始める前に

OSPF機能がイネーブルになっていることを確認します。（「OSPFv2の有効化」の項を参照）。

設定されるスタブエリア内に、仮想リンクとASBRのいずれも含まれないことを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規OSPFv2インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**area** *area-id* **stub** 例： `switch(config-router)# area 0.0.0.10 stub`	このエリアをスタブ エリアとして作成します。
ステップ 4	（任意） **area** *area-id* **default-cost** *cost* 例： `switch(config-router)# area 0.0.0.10 default-cost 25`	このスタブ エリアに送信されるデフォルト サマリ ルートのコスト メトリックを設定します。指定できる範囲は 0 ～ 16777215 です。デフォルトは 1 です。
ステップ 5	（任意） **show ip ospf** *instance-tag* 例： `switch(config-router)# show ip ospf 201`	OSPF 情報を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

例

次に、スタブ エリアを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 stub
switch(config-router)# copy running-config startup-config
```

Totally Stubby エリアの設定

Totally Stubby エリアを作成して、すべての集約ルート更新がスタブ エリアに入るのを防ぐことができます。

Totally Stubby エリアを作成するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**area** *area-id* **stub no-summary** 例： `switch(config-router)# area 20 stub no-summary`	このエリアを Totally Stubby エリアとして作成します。

NSSA の設定

OSPFv2 ドメインの一部で一定限度の外部トラフィックが必要な場合は、その部分に NSSA を設定できます。また、この外部トラフィックを AS 外部（タイプ 5）LSA に変換して、このルーティング情報で OSPFv2 ドメインをフラッディングすることもできます。NSSA は、省略可能な次のパラメータで設定できます。

- No redistribution：再配布されたルートは、NSSA をバイパスして OSPFv2 自律システム内の他のエリアに再配布されます。このオプションは、NSSA ASBR が ABR も兼ねているときに使用します。
- Default information originate：外部自律システムへのデフォルト ルートの NSSA 外部（タイプ 7）LSA を生成します。このオプションは、ASBR のルーティング テーブルにデフォルト ルートが含まれる場合に NSSA ASBR 上で使用します。このオプションは、ASBR のルーティング テーブルにデフォルト ルートが含まれるかどうかに関係なく、NSSA ASBR 上で使用できます。
- Route map：目的のルートだけが NSSA および他のエリア全体でフラッディングされるように、外部ルートをフィルタリングします。
- No summary：すべての集約ルートが NSSA でフラッディングされないようにします。このオプションは NSSA ABR 上で使用します。
- Translate：NSSA 外のエリア向けに、NSSA 外部 LSA を AS 外部 LSA に変換します。再配布されたルートを OSPFv2 自律システム全体でフラッディングするには、このコマンドを NSSA ABR 上で使用します。また、これらの AS 外部 LSA の転送アドレスを無効にする

こともできます。このオプションを選択した場合は、転送アドレスが0.0.0.0に設定されます。

（注） 変換オプションでは、NSSA を作成し、他のオプションを設定する **area** *area-id* **nssa** コマンドの後に、別の **area** *area-id* **nssa** コマンドが必要です。

始める前に

OSPF機能を有効化してあることを確認します（OSPFv2の有効化（264ページ）セクションを参照してください）。

設定する NSSA 上に仮想リンクがないことと、この NSSA がバックボーン エリアでないことを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規OSPFv2インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**area** *area-id* **nssa [no-redistribution] [default-information-originate]originate** [**route-map** *map-name*]] [**no-summary**] 例： `switch(config-router)# area 0.0.0.10 nssa no-redistribution`	このエリアをNSSAとして作成します。
ステップ 4	（任意） **area** *area-id* **nssa translate type7** {**always** | **never**} [**suppress-fa**] 例： `switch(config-router)# area 0.0.0.10 nssa translate type7 always`	AS 外部（タイプ 7）LSA を NSSA 外部（タイプ 5）LSA に変換するように NSSA を設定します。
ステップ 5	（任意） **area** *area-id* **default-cost** *cost* 例： `switch(config-router)# area 0.0.0.10 default-cost 25`	この NSSA に送信されるデフォルト集約ルートのコスト メトリックを設定します。

	コマンドまたはアクション	目的
ステップ 6	（任意） **show ip ospf** *instance-tag* 例： `switch(config-router)# show ip ospf 201`	OSPF 情報を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、すべての集約ルート更新をブロックする NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa no-summary
switch(config-router)# copy running-config startup-config
```

次に、デフォルト ルートを生成する NSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa default-info-originate
switch(config-router)# copy running-config startup-config
```

次に、外部ルートをフィルタリングし、すべての集約ルート更新をブロックするNSSA を作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa route-map ExternalFilter no-summary
switch(config-router)# copy running-config startup-config
```

次に、常に NSSA 外部（タイプ 5）LSA を AS 外部（タイプ 7）LSA に変換する NSSA を作成し NSSA を設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa
switch(config-router)# area 0.0.0.10 nssa translate type 7 always
switch(config-router)# copy running-config startup-config
```

マルチエリアの隣接関係の設定

既存の OSPFv2 インターフェイスには複数のエリアを追加できます。追加の論理インターフェイスはマルチエリア隣接関係をサポートしています。

始める前に

OSPFv2 機能が有効にされている必要があります（OSPFv2の有効化 （264 ページ）のセクションを参照してください）。

インターフェイスにプライマリ エリアが構成されていることを確認します（OSPFv2でのネットワークの設定 （269 ページ）を参照してください）。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**ip router ospf** [*instance-tag*] **multi-area** *area-id* 例： `switch(config-if)# ip router ospf 201 multi-area 3`	別のエリアにインターフェイスを追加します。 （注） *instance-tag* 引数はオプションです。インスタンスを指定しない場合、マルチエリア設定は、そのインターフェイスのプライマリ エリアに設定されている同じインスタンスに適用されます。
ステップ 4	（任意） **show ip ospf** *instance-tag* **interface** *interface-type slot/port* 例： `switch(config-if)# show ip ospf 201 interface ethernet 1/2`	OSPFv2 情報を表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	この設定変更を保存します。

例

次に、OSPFv2 インターフェイスに別のエリアを追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0.0.0.10
switch(config-if)# ip router ospf 201 multi-area 20
switch(config-if)# copy running-config startup-config
```

再配布の設定

他のルーティング プロトコルから学習したルートを、ASBR 経由で OSPFv2 自律システムに再配布できます。

デフォルトルートを再配布するには、次のパラメータを指定する必要があります。

- Default information originate：外部自律システムへのデフォルト ルートのために、自律システム外部（タイプ 5）LSA を生成します。

（注） Default information originate は、オプションのルートマップ内の **match** 文を無視します。

デフォルト以外のルートの場合、OSPF でのルート再配布には、省略可能な次のパラメータを設定できます。

- Default metric：すべての再配布ルートに同じコスト メトリックを設定します。

（注） スタティック ルートを再配布する場合、デフォルトの スタティック ルートを正常に再配布するためには、Cisco NX-OS も **default-information originate** コマンドを必要とします。

始める前に

OSPF 機能をイネーブルにします。「OSPFv2の有効化」を参照してください。

再配布で使用する、必要なルート マップを作成します。

手順

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

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規OSPFv2インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**redistribute** {**bgp** *id* | **direct** | **eigrp** *id* | **isis** *id* | **ospf** *id* | **rip** *id* | **static**} **route-map** *map-name*
	例：
	`switch(config-router)# redistribute bgp`
	`route-map FilterExternalBGP`
		設定したルート マップ経由で、選択したプロトコルをOSPFに再配布します。
		（注） スタティック ルートを再配布する場合は、Cisco NX-OS でもデフォルト スタティック ルートが再配布されます。

ステップ 4	**default-information originate** [**always**] [**route-map** *map-name*] 例： `switch(config-router)# default-information-originate route-map DefaultRouteFilter`	デフォルト ルートがRIBに存在する場合は、このOSPFドメインにデフォルト ルートを作成します。次の省略可能なキーワードを使用します。 • **always**：常に0.0.0.のデフォルト ルートを生成します。ルートがRIBに存在しない場合でも。 • **route-map**：ルート マップがtrueを返す場合にデフォルト ルートを生成します。 （注） このコマンドは、ルート マップの **match** 文を無視します。
ステップ 5	**default-metric** [*cost*] 例： `switch(config-router)# default-metric 25`	再配布されたルートのコスト メトリックを設定します。このコマンドは、直接接続されたルートには適用されません。ルート マップを使用して、直接接続されたルートのデフォルトのメトリックを設定します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、ボーダー ゲートウェイ プロトコル（BGP）を OSPF に再配布する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# copy running-config startup-config
```

再配布されるルート数の制限

ルートの再配布によって、OSPFv2 ルート テーブルに多くのルートが追加される可能性があります。外部プロトコルから受け取るルートの数の上限を設定できます。OSPFv2 には、再配布ルートの制限を設定するために次のオプションが用意されています。

- 上限固定：設定された最大値に OSPFv2 が達すると、メッセージをログに記録します。OSPFv2 は以降の再配布ルートを受け取りません。任意で、最大値のしきい値パーセンテージを設定して、OSPFv2 がこのしきい値を超えたときに警告を記録するようにすることもできます。
- 警告のみ：OSPFv2 が最大値に達したときのみ、警告のログを記録します。OSPFv2 は、再配布されたルートを受け入れ続けます。
- 取り消し：OSPFv2 が最大値に達したときにタイムアウト期間を開始します。このタイムアウト期間後、現在の再配布されたルート数が最大制限より少なければ、OSPFv2 はすべての再配布されたルートを要求します。再配布されたルートの現在数が最大数に達した場合、OSPFv2 はすべての再配布されたルートを取り消します。OSPFv2 が追加の再配布されたルートを受け付ける前に、この状況を解消する必要があります。
- 任意で、タイムアウト期間を設定できます。

始める前に

OSPF 機能を有効化してあることを確認します（OSPFv2の有効化 （264ページ） セクションを参照してください）。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**redistribute** {**bgp** *id* | **direct** | **eigrp** *id* | **isis** *id* | **ospf** *id* | **rip** *id* | **static**} **route-map** *map-name*
	例：
	`switch(config-router)# redistribute bgp`
	`route-map FilterExternalBGP`
		設定したルート マップ経由で、選択したプロトコルを OSPF に再配布します。

ステップ 4	**redistribute maximum-prefix** *max* [*threshold*] [**warning-only | withdraw** [*num-retries timeout*]] 例： `switch(config-router)# redistribute maximum-prefix 1000 75 warning-only`	OSPFv2 が配布するプレフィックスの最大数を指定します。指定できる範囲は 0 ～ 65536 です。任意で次のオプションを指定します。 • *threshold*：警告メッセージをトリガーする最大プレフィクス数のパーセンテージ。 • **warning-only**：プレフィックスの最大数を超えた場合に警告メッセージを記録します。 • **withdraw**：再配布されたすべてのルートを取り消します。任意で再配布されたルートを取得しようと試みます。*num-retries* の範囲は 1 ～ 12 です。*timeout* の範囲は 60 ～ 600 秒です。デフォルトは 300 秒です。**clear ip ospf redistribution** コマンドは、すべてのルートが取り消された場合に使用します。
ステップ 5	（任意） **show running-config ospf** 例： `switch(config-router)# show running-config ospf`	OSPFv2 設定を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

例

次に、OSPF に再配布されるルートの数を制限する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# redistribute maximum-prefix 1000 75
```

ルート集約の設定

集約したアドレス範囲を設定することにより、エリア間ルートのルート集約を設定できます。また、ASBR 上のこれらのルートのサマリ アドレスを設定して、外部の再配布されたルートのルート集約を設定することもできます。詳細については、ルート集約 （260ページ）を参照してください。

始める前に

OSPF機能を有効化してあることを確認します（OSPFv2の有効化 （264ページ）セクションを参照してください）。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規OSPFv2インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**area** *area-id* **range** *ip-prefix/length* [**no-advertise**] [**cost** *cost*] 例： `switch(config-router)# area 0.0.0.10 range 10.3.0.0/16`	一定の範囲のアドレスのサマリ アドレスを ABR 上に作成します。このサマリ アドレスをネットワーク集約（タイプ 3）LSA にアドバタイズしないようにすることもできます。*cost* の範囲は 0 ～ 16777215 です。
ステップ 4	**summary-address** *ip-prefix/length* [**no-advertise** | **tag** *tag*] 例： `switch(config-router)# summary-address 10.5.0.0/16 tag 2`	一定の範囲のアドレスのサマリ アドレスを ABR 上に作成します。ルート マップによる再配布で使用できるよう、このサマリ アドレスにタグを割り当てることもできます。

	コマンドまたはアクション	目的
ステップ 5	（任意） **show ip ospf summary-address** 例： `switch(config-router)# show ip ospf summary-address`	OSPF サマリ アドレスに関する情報を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

例

次に、ABR 上のエリア間のサマリ アドレスを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)#  area 0.0.0.10 range 10.3.0.0/16
switch(config-router)# copy running-config startup-config
```

次に、ASBR 上のサマリ アドレスを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# summary-address 10.5.0.0/16
switch(config-router)# copy running-config startup-config
```

スタブ ルート アドバタイズメントの設定

短期間だけ、このルータ経由の OSPFv2 トラフィックを制限する場合は、スタブ ルート アドバタイズメントを使用します。詳細については、OSPFv2 スタブ ルータ アドバタイズメント（261 ページ）を参照してください。

スタブ ルート アドバタイズメントは、省略可能な次のパラメータで設定できます。

- On startup：指定した宣言期間だけ、スタブ ルート アドバタイズメントを送信します。
- Wait for BGP：BGP がコンバージェンスするまで、スタブ ルート アドバタイズメントを送信します。

（注） ルータの実行コンフィギュレーションがグレースフル シャットダウンを行うよう設定されている場合は、その実行コンフィギュレーションを保存しないでください。保存すると、ルータが、リロード後に最大メトリックをアドバタイズし続けることになります。

始める前に

OSPF 機能を有効化してあることを確認します（OSPFv2の有効化 （264ページ） セクションを参照してください）。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** {*seconds* | **wait-for bgp** *tag*}] [**summary-lsa** [*max-metric-value*}] 例： `switch(config-router)# max-metric router-lsa`	OSPFv2 スタブ ルート アドバタイズメントを設定します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、起動時にスタブ ルータ アドバタイズメントを、デフォルトの 600 秒間イネーブルにする例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# max-metric router-lsa on-startup
switch(config-router)# copy running-config startup-config
```

ルートのアドミニストレーティブ ディスタンスの設定

OSPFv2 によって RIB に追加されるルートのアドミニストレーティブ ディスタンスを設定できます。

アドミニストレーティブディスタンスは、ルーティング情報源の信頼性を示す評価基準です。値が高いほど信頼性の評価は低くなります。一般的にルートは、複数のルーティングプロトコルを通じて検出されます。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコルから学習したルートを区別するために使用されます。最もアドミニストレーティブ ディスタンスが低いルートが IP ルーティング テーブルに組み込まれます。

始める前に

OSPF 機能がイネーブルにされていることを確認してください（「OSPFv2の有効化 」の項を参照）。

「OSPFv2 の注意事項および制約事項」の項にあるこの機能の注意事項と制限事項を参照してください。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規OSPFv2インスタンスを作成して、設定済みのインスタンスタグを割り当てます。

ステップ 3	[**no**] **table-map** *map-name* 例： `switch(config-router)# table-map foo`	OSPFv2 ルートを RIB に送信する前に、OSPFv2 ルートをフィルタリングまたは変更するポリシーを設定します。マップ名には最大 63 文字の英数字を入力できます。

ステップ 4	**exit**
	例：
	`switch(config-router)# exit`
	`switch(config)#`
		ルータ 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	**route-map** *map-name* [**permit** | **deny**] [*seq*]
	例：
	`switch(config)# route-map foo permit 10`
	`switch(config-route-map)#`
		ルートマップを作成するか、または既存のルート マップに対応するルート マップ設定モードを開始します。ルート マップのエントリを順序付けるには、*seq* を使用します。

	コマンドまたはアクション	目的
		（注） **permit** オプションで、ディスタンスを設定することができます。**deny** オプションを使用すると、デフォルトのディスタンスが適用されます。
ステップ 6	**match route-type** *route-type* 例： `switch(config-route-map)# match route-type external`	次のルートタイプのいずれかと照合します。 • external：外部ルート（BGP、EIGRP、OSPF タイプ 1 または 2） • inter-area：OSPF エリア間ルート • internal：内部ルート（OSPF エリア内またはエリア間ルートを含む） • intra-area：OSPF エリア内ルート • nssa-external：NSSA 外部ルート（OSPF タイプ 1 または 2） • type-1：OSPF 外部タイプ 1 ルート • type-2：OSPF 外部タイプ 2 ルート
ステップ 7	**match ip route-source prefix-list** *name* 例： `switch(config-route-map)# match ip route-source prefix-list p1`	1 つまたは複数の IP プレフィックス リストに対して、ルートの IPv4 ルート送信元アドレスまたはルータ ID と照合します。プレフィックス リストは **ip prefix-list** コマンドを使用して作成します。
ステップ 8	**match ip address prefix-list** *name* 例： `switch(config-route-map)# match ip address prefix-list p1`	1 つまたは複数の IPv4 プレフィックス リストと照合。プレフィックス リストは **ip prefix-list** コマンドを使用して作成します。
ステップ 9	**set distance** *value* 例： `switch(config-route-map)# set distance 150`	OSPFv2 のルートのアドミニストレーティブディスタンスを設定します。範囲は 1 ～ 255 です。
ステップ 10	（任意） **copy running-config startup-config** 例：	この設定変更を保存します。

	コマンドまたはアクション	目的
	`switch(config-route-map)# copy running-config startup-config`	

例

次に、OSPFv2 アドミニストレーティブ ディスタンスについて、エリア間ルートを 150、外部ルートを 200、およびプレフィックス リスト p1 内のすべてのプレフィックスを 190 に設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# table-map foo
switch(config-router)# exit
switch(config)# route-map foo permit 10
switch(config-route-map)# match route-type inter-area
switch(config-route-map)# set distance 150
switch(config-route-map)# exit
switch(config)# route-map foo permit 20
switch(config-route-map)# match route-type external
switch(config-route-map)# set distance 200
switch(config-route-map)# exit
switch(config)# route-map foo permit 30
switch(config-route-map)# match ip route-source prefix-list p1
switch(config-route-map)# match ip address prefix-list p1
switch(config-route-map)# set distance 190
```

デフォルト タイマーの変更

OSPFv2 には、プロトコル メッセージの動作および最短パス優先（SPF）の計算を制御する多数のタイマーが含まれています。OSPFv2 には、省略可能な次のタイマー パラメータが含まれます。

- LSA arrival time：ネイバーから着信する LSA 間で許容される最小間隔を設定します。この時間より短時間で到着する LSA はドロップされます。
- Pacing LSAs：LSA が集められてグループ化され、リフレッシュされて、チェックサムが計算される間隔、つまり期限切れとなる間隔を設定します。このタイマーは、LSA 更新が実行される頻度を制御し、LSA 更新メッセージで送信される LSA 更新の数を制御します（「フラッディングと LSA グループ ペーシング」を参照）。
- Throttle LSAs：LSA 生成のレート制限を設定します。このタイマーは、トポロジが変更された後に LSA が生成される頻度を制御します。
- Throttle SPF calculation：SPF 計算の実行頻度を制御します。

インターフェイス レベルでは、次のタイマーも制御できます。

- Retransmit interval：連続する LSA 間の推定時間間隔を設定します。
- Transmit delay：LSA をネイバーに送信する推定時間を設定します。

hello 間隔とデッド タイマーに関する情報の詳細については、「OSPFv2でのネットワークの設定」の項を参照してください。

始める前に

OSPF 機能を有効にしてあることを確認します（「OSPFv2の有効化」の項を参照）。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規OSPFv2インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**timers lsa-arrival** *msec* 例： `switch(config-router)# timers lsa-arrival 2000`	LSA 到着時間をミリ秒で設定します。範囲は 10 ～ 600000 です。デフォルトは 1000 ミリ秒です。
ステップ 4	**timers lsa-group-pacing** *seconds* 例： `switch(config-router)# timers lsa-group-pacing 1800`	LSA がグループ化される間隔を秒で設定します。範囲は 1 ～ 1800 です。デフォルトは 240 秒です。
ステップ 5	**timers throttle lsa** *start-time hold-interval max-time* 例： `switch(config-router)# timers throttle lsa 3000 6000 6000`	次のタイマーを使用して、LSA 生成のレート制限をミリ秒で設定します。 • *start-time*：指定できる範囲は 50 ～ 5000 ミリ秒です。デフォルト値は 50 ミリ秒です。 • *hold-interrval*：指定できる範囲は 50 ～ 30,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。 • *max-time*：指定できる範囲は 50 ～ 30,000 ミリ秒です。デフォルト値は 5000 ミリ秒です
ステップ 6	**timers throttle spf** *delay-time hold-time max-wait* 例：	SPF 最適パス スケジュール初期遅延時間と、各 SPF 最適パス計算間の最小ホールドタイム（秒単位）を設定しま

	コマンドまたはアクション	目的
	`switch(config-router)# timers throttle spf 3000 2000 4000`	す。指定できる範囲は 1 ～ 600000 です。デフォルトは、遅延時間なし、およびホールドタイム 5000 ミリ秒です。

ステップ 7	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)`
		インターフェイス設定モードを開始します。

ステップ 8	**ip ospf hello-interval** *seconds* 例： `switch(config-if)# ip ospf hello-interval 30`	このインターフェイスの hello 間隔を設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 です。

ステップ 9	**ip ospf dead-interval** *seconds*
	例：
	`switch(config-if)# ip ospf dead-interval`
	`30`
		このインターフェイスのデッド間隔を設定します。有効な範囲は 1 ～ 65535 です。

ステップ 10	**ip ospf retransmit-interval** *seconds* 例： `switch(config-if)# ip ospf retransmit-interval 30`	このインターフェイスから送信される各 LSA 間の推定時間間隔を設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 5 分です。

ステップ 11	**ip ospf transmit-delay** *seconds*
	例：
	`switch(config-if)# ip ospf transmit-delay 450`
	`switch(config-if)#`
		LSA をネイバーに送信する推定時間間隔を秒で設定します。指定できる範囲は 1 ～ 450 です。デフォルトは 1 です。

ステップ 12	（任意） **show ip ospf** 例： `switch(config-if)# show ip ospf`	OSPF に関する情報を表示します。
ステップ 13	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、lsa-group-pacing オプションで LSA フラッディングを制御する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# timers lsa-group-pacing 300
switch(config-router)# copy running-config startup-config
```

グレースフル リスタートの設定

デフォルトでは、グレースフル リスタートは有効です。OSPFv2 インスタンスのグレースフル リスタートには、省略可能な次のパラメータを設定できます。

- Grace period：グレースフル リスタートの開始後に、ネイバーが隣接関係を解消するまでに待つ時間を設定します。
- Helper mode disabled：ローカル OSPFv2 インスタンスのヘルパー モードを無効にします。OSPFv2 は、ネイバーのグレースフル リスタートには関与しません。
- Planned graceful restart only：予定された再起動の場合にだけグレースフル リスタートがサポートされるように OSPFv2 を設定します。

始める前に

OSPF 機能が有効にされていることを確認してください（「OSPFv2の有効化」のセクションを参照）。

すべてのネイバーで、一致した省略可能なパラメータ一式とともにグレースフル リスタートが設定されていることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**router ospf** *instance-tag*
	例：
	`switch(config)# router ospf 201`
	`switch(config-router)#`
		新規 OSPFv2 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3	**graceful-restart** 例： `switch(config-router)# graceful-restart`	グレースフル リスタートを有効にします。グレースフルリスタートは、デフォルトで有効にされています。
ステップ 4	（任意） **graceful-restart grace-period** *seconds* 例：	猶予期間を秒で設定します。指定できる範囲は 5 ～ 1800 です。デフォルトは 60 秒です。

	コマンドまたはアクション	目的
	`switch(config-router)# graceful-restart grace-period 120`	
ステップ 5	（任意） **graceful-restart helper-disable** 例： `switch(config-router)# graceful-restart helper-disable`	ヘルパー モードを無効にします。この機能はデフォルトで有効になっています。
ステップ 6	（任意） **graceful-restart planned-only** 例： `switch(config-router)# graceful-restart planned-only`	予定された再起動時にのみグレースフル リスタートを設定します。
ステップ 7	（任意） **show ip ospf** *instance-tag* 例： `switch(config-router)# show ip ospf 201`	OSPF 情報を表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、ディセーブルにされているグレースフル リスタートをイネーブルにし、猶予期間を 120 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# graceful-restart
switch(config-router)# graceful-restart grace-period 120
switch(config-router)# copy running-config startup-config
```

OSPFv2 インスタンスの再起動

OSPv2インスタンスを再起動できます。この処理では、インスタンスのすべてのネイバーが消去されます。

OSPFv2 インスタンスを再起動して、関連付けられたすべてのネイバーを削除するには、次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**restart ospf** *instance-tag* 例： `switch(config)# restart ospf 201`	OSPFv2 インスタンスを再起動して、すべてのネイバーを削除します。

OSPFv2 設定の確認

OSPFv2 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 ip ospf [*instance-tag*]	1 つ以上の OSPF ルーティング インスタンスに関する情報を表示します。出力には、次のエリア レベルのカウントが含まれます。 • このエリアのインターフェイス：このエリアに追加されたすべてのインターフェイスの数（設定されたインターフェイス）。 • アクティブインターフェイス：ルータリンクステートおよび SPF（UP インターフェイス）にあると見なされるすべてのインターフェイスの数。 • パッシブ インターフェイス：OSPF パッシブと見なされるすべてのインターフェイスの数（隣接関係は形成されません）。 • ループバックインターフェイス：すべてのローカルループバックインターフェイスの数。
show ip ospf border-routers [**vrf** {**default** | **management** }]	OSPFv2 境界ルータ設定を表示します。
show ip ospf database [**vrf** { **default** | **management**}]	OSPFv2 リンクステート データベースの要約を表示します。
show ip ospf interface *number* [**vrf** {**default** | **management** }]	OSPFv2-related インターフェイスの情報を表示します。
show ip ospf lsa-content-changed-list *neighbor-id interface - type number* [**vrf** {**default** | **management** }]	変更された OSPFv2 LSA を表示します。

コマンド	目的
show ip ospf neighbors [*neighbor-id*] [**detail**] [*interface - type number*] [**vrf** { **default** | **management** }] [**summary**]	OSPFv2 ネイバーの一覧を表示します。
show ip ospf request-list *neighbor-id interface - type number* [**vrf** {**default** | **management** }]	OSPFv2 リンクステート要求の一覧を表示します。
show ip ospf retransmission-list *neighbor-id interface - type number* [**vrf** { **default** | **management** }]	OSPFv2 リンクステート再送の一覧を表示します。
show ip ospf route [*ospf-route*] [**summary**] [**vrf** { **default** | **management** }]	内部 OSPFv2 ルートを表示します。
show ip ospf summary-address [**vrf** {**default** | **management** }]	OSPFv2 サマリ アドレスに関する情報を表示します。
show ip ospf vrf {**default** | **management** }	VRF ベースの OSPFv2 設定に関する情報を表示します。
show running-configuration ospf	現在実行中の OSPFv2 設定を表示します。

OSPFv2 のモニタリング

OSPFv2 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show ip ospf policy statistics area *area-id* **filter list** {**in** | **out**} [**vrf** {**default** | **management**}]	エリアの OSPFv2 ルート ポリシー統計情報を表示します。
show ip policy statistics redestribute {**bgp** *id* | **direct** | **ospf** *id* | **static**} [**vrf** {**default** | **management**}]	OSPFv2 ルート ポリシー統計情報を表示します。
show ip ospf statistics [**vrf** { **default** | **management**}]	OSPFv2 イベント カウンタを表示します。
show ip ospf traffic [*interface-type number*] [**vrf** {**default** | **management**}]	OSPFv2 パケット カウンタを表示します。

OSPFv2 の設定例

次に、OSPFv2 を設定する例を示します。

```
feature ospf
router ospf 201
 router-id 290.0.2.1
interface ethernet 1/2
 ip router ospf 201 area 0.0.0.10
 ip ospf authentication
 ip ospf authentication-key 0 mypass
```

OSPF RFC 互換モードの例

次に、RFC 1583 互換ルータと互換性を持つように OSPF を設定する例を示します。

（注） RFC1583 互換の OSPF のみを実行するルータに接続するすべての VRF で、RFC 1583 の互換性を設定する必要があります。

```
switch# configure terminal
switch(config)# feature ospf
switch(config)# router ospf Test1
switch(config-router)# rfc1583compatibility
```

その他の参考資料

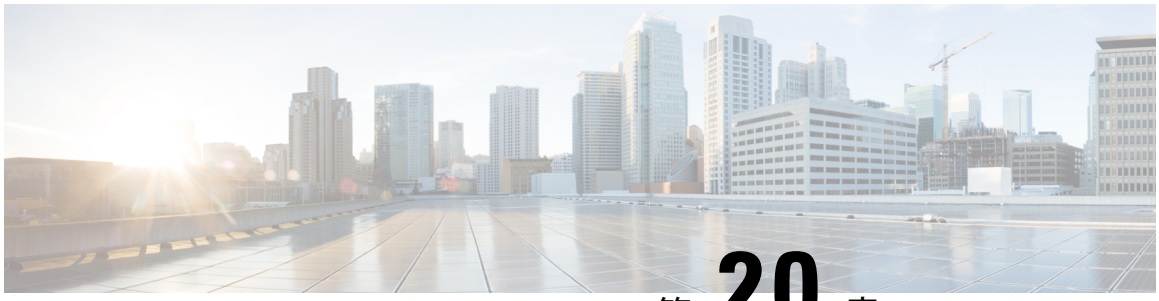
OSPF の実装に関する詳細情報については、次のページを参照してください。

OSPFv2 の関連資料

関連項目	マニュアル タイトル
キーチェーン	「*Cisco Nexus® 3550-T* セキュリティの設定」セクション
ルート マップ	詳細については、「ルート ポリシー マネージャの構成」のセクションを参照してください。

MIB

MIB	MIB のリンク
OSPFv2 に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 20 章

基本的 BGP の設定

この章では、Cisco NX-OS デバイス上でボーダー ゲートウェイ プロトコル（BGP）を設定する方法について説明します

この章は、次の項で構成されています。

基本的な BGP について

Cisco NX-OS は BGP バージョン 4 をサポートします。BGP v4 に組み込まれているマルチ プロトコル拡張機能を使用すると、IP マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリに関するルーティング情報を BGP に伝送させることができます。BGP では、他の BGP 対応デバイスとの間で TCP セッションを確立するための、信頼できるトランスポート プロトコルとして TCP を使用します。

BGP ではパスベクトル ルーティング アルゴリズムを使用して、BGP 対応ネットワーク デバイスまたは BGP スピーカ間でルーティング情報を交換します。各 BGP スピーカはこの情報を使用して、特定の宛先までのパスを判別し、なおかつルーティング ループを伴うパスを検出して回避します。ルーティング情報には、宛先の実際のルート プレフィックス、宛先に対する自律システムのパス、およびその他のパス属性が含まれます。

BGP はデフォルトで、宛先ホストまたはネットワークへのベストパスとして、1 つだけパスを選択します。各パスは、BGP ベストパス分析で使用される well-known mandatory、well-known

discretionary、optional transitive の各属性を伝送します。BGP ポリシーを設定し、これらの属性の一部を変更することによって、BGP パス選択を制御できます。詳細については、ルート ポリシーおよび BGP セッションのリセット （323 ページ）を参照してください。

BGP はロード バランシングもサポートしています。詳細については、BGP ベストパスの選択（328 ページ）を参照してください。

（注） Cisco Nexus 3550-T ハードウェアは、ECMP ルートのインストールをサポートしていません。

BGP 自律システム

自律システム（AS）とは、単一の管理エンティティにより制御されるネットワークです。自律システムは 1 つまたは複数の IGP および整合性のある一連のルーティング ポリシーを使用して、ルーティング ドメインを形成します。BGP は 16 ビットおよび 32 ビットの自律システム番号をサポートします。

個々の BGP 自律システムは外部 BGP（eBGP）ピアリング セッションを通じて、ルーティング情報をダイナミックに交換します。同じ自律システム内の BGP スピーカは、内部 BGP（iBGP）を通じて、ルーティング情報を交換できます。

4 バイトの AS 番号のサポート

BGP は、プレーン テキスト表記法または AS ドット付き表記法の 2 バイトの自律システム（AS）番号、もしくはプレーン テキスト表記法の 4 バイトの AS 番号をサポートします。

アドミニストレーティブ ディスタンス

アドミニストレーティブディスタンスは、ルーティング情報源の信頼性を示す評価基準です。デフォルトで、BGP は表に示されたアドミニストレーティブ ディスタンスを使用します。

表 *18 :* デフォルトの *BGP* アドミニストレーティブ ディスタンス

ディスタンス	デフォルト値	機能
外部	20	eBGP から学習したルートに適用されます。
内部	200	iBGP から学習したルートに適用されます。
ローカル	220	ルータを起点とするルートに適用されます。

（注） アドミニストレーティブ ディスタンスが BGP パス選択アルゴリズムに影響を与えることはありませんが、BGP で学習されたルートが IP ルーティング テーブルに組み込まれるかどうかを左右します。

BGP ピア

BGP スピーカーは他の BGP スピーカーを自動的に検出しません。ユーザ側で BGP スピーカ間の関係を設定する必要があります。BGP ピアは、別の BGP スピーカへのアクティブな TCP 接続を持つ BGP スピーカです。

BGP セッション

BGP は TCP ポート 179 を使用して、ピアとの TCP セッションを作成します。ピア間で TCP 接続が確立されると、各 BGP ピアは最初に相手と、それぞれのすべてのルートを交換し、BGP ルーティング テーブルを完成させます。初期交換以後、BGP ピアはネットワーク トポロジが変化したとき、またはルーティング ポリシーが変更されたときに、差分アップデートだけを送信します。更新と更新の間の非アクティブ期間には、ピアは「キープアライブ」と呼ばれる特別なメッセージを交換します。ホールド タイムは、は、次の BGP アップデートまたはキープアライブ メッセージを受信するまでに経過することが許容される、最大時間限度です。

Cisco NX-OS は、次のピア設定オプションをサポートします。

- 個別の IPv4 アドレス：BGP は、リモート アドレスと AS 番号が一致する BGP スピーカとのセッションを確立します。
- 単一 AS 番号の IPv4 プレフィックス ピア：BGP は、プレフィックスおよび AS 番号が一致する BGP スピーカとのセッションを確立します。
- ダイナミック AS 番号プレフィックス ピア：BGP は、プレフィックスと、設定済み AS 番号のリストに載っている AS 番号と一致する BGP スピーカとのセッションを確立します。

プレフィックス ピアおよびインターフェイス ピアのダイナミック AS 番号

Cisco NX-OS では、BGP セッションを確立する AS 番号の範囲またはリストを受け入れます。たとえば IPv4 プレフィックス 192.0.2.0/8 および AS 番号 33、66、99 を使用するように BGP を設定する場合、BGP は 192.0.2.1 および AS 番号 66 を使用してセッションを確立しますが、192.0.2.2 および AS 番号 50 からのセッションは拒否します。

Cisco NX-OS では、セッションが確立されるまで内部 BGP（iBGP）または外部 BGP（eBGP）セッションとして、プレフィックス ピアをダイナミック AS 番号と関連付けません。iBGP および eBGP の詳細については、「高度な BGP の設定」の章を参照してください。

（注） ダイナミック AS 番号プレフィックス ピア設定は、BGP テンプレートから継承した個々の AS 番号の設定よりも優先します。詳細については、「高度な BGP の設定」の章を参照してください。

BGP ルータ ID

ピア間で BGP セッションを確立するには、BGP セッションの確立時に、OPEN メッセージで BGP ピアに送信されるルータ ID を BGP に設定する必要があります。BGP ルータ ID は 32 ビット値であり、IPv4 アドレスで表すことがよくあります。ルータ ID はユーザ側で設定できます。ルータ ID はデフォルトで、Cisco NX-OS によってルータのループバック インターフェイスの IPv4 アドレスに設定されます。ルータ上でループバック インターフェイスが設定されていない場合は、ルータ上の物理インターフェイスに設定されている最大の IPv4 アドレスが BGP ルータ ID を表すものとして、ソフトウェアによって選択されます。BGP ルータ ID は、ネットワーク内の BGP ピアごとに一意である必要があります。

BGP にルータ ID が設定されていない場合、BGP ピアとのピアリング セッションを確立できません。

BGP およびユニキャスト RIB

BGP はユニキャスト RIB（ルーティング情報ベース）と通信して、ユニキャスト ルーティング テーブルに IPv4 ルートを格納します。ベスト パスの選択後、ベスト パスの変更をルーティング テーブルに反映させる必要があると BGP が判別した場合、BGP はユニキャスト RIB にルート アップデートを送信します。

BGP はユニキャスト RIB における BGP ルートの変更に関して、ルート通知を受け取ります。さらに、再配布をサポートする他のプロトコル ルートに関するルート通知を受け取ります。

BGP はネクストホップの変更に関する通知も、ユニキャスト RIB から受け取ります。BGP はこれらの通知を使用して、ネクストホップ アドレスへの到達可能性および IGP メトリックを追跡します。

ユニキャスト RIB でネクストホップ到達可能性または IGP メトリックが変更されるたびに、BGP は影響を受けるルートについて、ベスト パス再計算を開始させます。

BGP の前提条件

BGP を使用するには、次の前提条件を満たしている必要があります。

- BGP を有効にする必要があります（「BGPの有効化」の項を参照）。
- システムに有効なルータ ID を設定しておく必要があります。

- Regional Internet Registry（RIR）によって割り当てられたか、またはローカル管理の AS 番号を取得しておく必要があります。
- 再帰ネクストホップ解決に対応できる IGP を 1 つ以上設定する必要があります。
- BGP セッションを確立するネイバー環境で、アドレス ファミリを設定する必要があります。

基本 BGP に関する注意事項と制約事項

BGP 設定時の注意事項および制約事項は、次のとおりです。

- 十分な規模（ピアあたり数百のピアや数千のルートなど）では、デフォルトの5分間の古いパス タイマーでは、BGP コンバージェンスが完了しないためにタイマーが期限切れになる可能性があるため、グレースフル リスタート メカニズムが失敗する可能性があります。次のコマンドを使用して、コンバージェンス プロセスにかかる実際の時間を確認します。

```
switch# show bgp vrf all all neighbors | in First|RIB
  Last End-of-RIB received 0.022810 after session start
  Last End-of-RIB sent 00:08:36 after session start
  First convergence 00:08:36 after session start with 398002 routes sent
```

（注） Cisco Nexus 3550-T では、BGP はデフォルトの VRF でのみサポートされています。

- ダイナミック AS 番号プレフィックス ピア設定は、BGP テンプレートから継承した個々の AS 番号の設定よりも優先します。
- AS 連合でプレフィックス ピアにダイナミック AS 番号を設定した場合、BGP はローカル連合の AS 番号のみでセッションを確立します。
- ダイナミック AS 番号プレフィックス ピアで作成された BGP セッションは、設定済みの eBGP マルチホップ存続可能時間（TTL）値や直接接続ピアに対するディセーブル済みのチェックを無視します。
- ルータ ID の自動変更およびセッション フラップを避けるために、BGP 用のルータ ID を設定します。
- ピアごとに最大プレフィックス設定オプションを使用し、受信するルート数および使用するシステム リソース数を制限してください。
- update-source を設定し、BGP/eBGP マルチホップ セッションでセッションを確立します。
- 再配布を設定する場合は、BGP ポリシーを指定します。
- キープアライブおよびホールド タイマーの値を小さくすると、BGP セッション フラップが発生する可能性があります。

- **show ip bgp** コマンドは BGP 設定の確認に使用できますが、代わりに **show bgp** コマンドを使用することを推奨します。
- BGP プレフィックス独立コンバージェンス（PIC）エッジ機能は、Cisco Nexus 3550-T ではサポートされていません。

デフォルト設定

表 *19:* デフォルトの *BGP* パラメータ

パラメータ	デフォルト
BGP 機能	ディセーブル
キープアライブインターバル	60 秒
ホールド タイマー	180 秒
Auto-summary	常に無効
同期	常に無効

CLI コンフィギュレーション モード

以下の項では、BGP に対応する各 CLI コンフィギュレーション モードの開始方法について説明します。現行のモードで **?** コマンドを入力すると、そのモードで使用可能なコマンドを表示できます。

グローバル コンフィギュレーション モード

グローバル コンフィギュレーション モードは、BGP プロセスを作成したり、AS 連合、ルート ダンプニングなどの拡張機能を設定したりする場合に使用します。

次に、ルータ コンフィギュレーション モードを開始する例を示します。

```
switch# configuration
switch(config)# router bgp 64496
switch(config-router)#
```

ネイバー コンフィギュレーション モード

Cisco NX-OS には、BGP ピアを設定するためのネイバー コンフィギュレーション モードがあります。ネイバー コンフィギュレーション モードを使用して、ピアのあらゆるパラメータを設定できます。

次に、ネイバー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.1
switch(config-router-neighbor)#
```

基本的 BGP の設定

ベーシック BGP を設定するには、BGP を有効にして、BGP ピアを設定する必要があります。ベーシック BGP ネットワークの設定は、いくつかの必須作業と多数の任意の作業からなります。BGP ルーティング プロセスおよび BGP ピアの設定は必須です。

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

BGPの有効化

BGP を設定するには、その前に BGP を有効にする必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		設定モードに入ります。

ステップ 2	**[no] feature bgp** 例： `switch(config)# feature bgp`	BGP を有効にします。 この機能を無効化するには、このコマンドの **no** 形式を使用します。
ステップ 3	（任意） **show feature** 例： `switch(config)# show feature`	有効および無効にされた機能を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	この設定変更を保存します。

BGP インスタンスの作成

BGP インスタンスを作成し、BGP インスタンスにルータ ID を割り当てることができます。詳細については、「BGP ルータ ID」の項を参照してください。

始める前に

- BGP をイネーブルにする必要があります（「BGPの有効化」の項を参照）。
- BGP はルータ ID（設定済みループバック アドレスなど）を取得できなければなりません。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	[**no**] **router bgp** *autonomous-system-number*
	例：
	`switch(config)# router bgp 64496`
	`switch(config-router)#`
		BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
		BGP プロセスおよび関連する設定を削除するには、このコマンドで **no** オプションを使用します。

ステップ 3	（任意） **router-id** *ip-address* 例： `switch(config-router)# router-id 192.0.2.255`	BGP ルータ ID を設定します。この IP アドレスによって、この BGP スピーカを特定します。

ステップ 4	（任意） **address-family** {**ipv4**} {**unicast**}
	例：
	`switch(config-router)# address-family ipv4 unicast`
	`switch(config-router-af)#`
		IPv4 アドレス ファミリに対応するグローバル アドレス ファミリ コンフィギュレーション モードを開始します。
		（注） Cisco Nexus 3550-T では、BGP は IPv4 ユニキャスト アドレス ファミリのみをサポートします。

	コマンドまたはアクション	目的

ステップ 5	（任意） **network** {*ip-address/length* | *ip-address* **mask** *mask*} [**route-map** *map-name*]
	例：
	`switch(config-router-af)# network 10.10.10.0/24`
	例：
	`switch(config-router-af)# network 10.10.10.0 mask 255.255.255.0`
		ネットワークを、この自律システムに対してローカルに設定し、BGP ルーティング テーブルに追加します。
		エクステリア プロトコルの場合、network コマンドでアドバタイズするネットワークを制御します。内部プロトコルは **network** コマンドを使用して、アップデートの送信先を決定します。

ステップ 6	（任意） **show bgp all** 例： `switch(config-router-af)# show bgp all`	すべての BGP アドレス ファミリに関する情報を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config-router-af)# copy running-config startup-config`	この設定変更を保存します。

例

次に、IPv4 ユニキャスト アドレス ファミリを指定して BGP をイネーブルに設定し、アドバタイズするネットワークを 1 つ追加する例を示します。

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# network 192.0.2.0
switch(config-router-af)# copy running-config startup-config
```

BGP インスタンスの再起動

BGP インスタンスを再起動し、そのインスタンスのすべてのピア セッションをクリアできます。

BGPインスタンスを再起動し、関連付けられたすべてのピアを削除するには、次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**restart bgp***instance-tag* 例： `switch(config)# restart bgp 201`	BGP インスタンスを再起動し、すべてのピアリング セッションをリセットまたは再確立します。

BGP のシャットダウン

設定を維持しながら、BGP プロトコルをシャット ダウンして BGP を正常に無効にできます。

BGP をシャットダウンするには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**shutdown** 例： `switch(config-router)# shutdown`	BGP インスタンスを再起動し、すべてのピアリング セッションをリセットまたは再確立します。

BGP ピア設定

BGP プロセス内で BGP ピアを設定できます。BGP ピアごとに、関連付けられたキープアライブ タイマーとホールド タイマーがあります。これらのタイマーは、グローバルに設定することも、BGP ピアごとに設定することもできます。ピア設定はグローバル設定を上書きします。

（注） ピアごとに、ネイバー コンフィギュレーション モードでアドレス ファミリを設定する必要があります。

始める前に

- BGP を有効にする必要があります（「BGPの有効化」の項を参照）。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的

ステップ 2	**router bgp** *autonomous-system-number*
	例：
	`switch(config)# router bgp 64496`
	`switch(config-router)#`
		BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。

ステップ 3	**neighbor** {*ip-address*} **remote-as** *as-number*
	例：
	`switch(config-router)# neighbor 209.165.201.1 remote-as 64497`
	`switch(config-router-neighbor)#`
		リモート BGP ピアの IPv4 アドレスおよび AS 番号を設定します。*The ip-address* 形式は x.x.x.x です。形式は A:B::C:D です。

ステップ 4	**neighbor-as** *as-number* 例： `switch(config-router-neighbor)# remote-as 64497`	リモート BGP ピアの AS 番号を設定します。

ステップ 5	（任意） **description***text*
	例：
	`switch(config-router-neighbor)# description Peer Router B`
	`switch(config-router-neighbor)#`
		ネイバーの説明を追加します。最大 80 文字の英数字ストリングを使用できます。

ステップ 6	（任意） **timers***keepalive-time hold-time* 例： `switch(config-router-neighbor)# timers 30 90`	ネイバーのキープアライブおよびホールド タイムを表す BGP タイマー値を追加します。指定できる範囲は 0 ～ 3600 秒です。デフォルトは、キープアライブ タイムで 60 秒、ホールド タイムで 180 秒です。
ステップ 7	（任意） **shutdown** 例： `switch(config-router-neighbor)# shutdown`	この BGP ネイバーを管理目的でシャットダウンします。このコマンドによって、BGP ネイバーセッションの自動通知およびセッション リセットが開始されます。

ステップ 8	**address-family**{**ipv4**} {**unicast**}
	例：
	`switch(config-router-neighbor)# address-family ipv4 unicast`
	`switch(config-router-neighbor-af)#`
		ユニキャスト IPv4 アドレス ファミリに対応するネイバー アドレス ファミリ 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 9	（任意） **weight** *value* 例： `switch(config-router-neighbor-af)# weight 100`	このネイバーからのルートのデフォルトの重みを設定します。範囲は 0 ～ 65535 です。 このネイバーから学習したすべてのルートに、まず重みが割り当てられます。特定のネットワークへのルートが複数ある場合、最大の重みを持つルートが優先ルートとして選ばれます。**set weight route-map** コマンドで割り当てられた重みは、このコマンドで割り当てられた重みを上書きします。 BGP ピア ポリシー テンプレートを指定した場合、テンプレートのメンバーすべてが、このコマンドで設定された特性を継承します。
ステップ 10	（任意） **show bgp** {**ipv4**} {**unicast**} **neighbors** 例： `switch(config-router-neighbor-af)# show bgp ipv4 unicast neighbors`	BGP ピアに関する情報を表示します。
ステップ 11	（任意） **copy running-config startup-config** 例： `switch(config-router-neighbor-af)# copy running-config startup-config`	この設定変更を保存します。

例

次に、BGP ピアの設定例を示します。

```
switch# configure terminal
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.1 remote-as 64497
switch(config-router-neighbor)# description Peer Router B
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor)# weight 100
switch(config-router-neighbor-af)# copy running-config startup-config
```

プレフィックス ピアのダイナミック AS 番号の設定

BGP プロセス内で複数の BGP ピアを設定できます。BGP セッションの確立をルート マップの単一の AS 番号または複数の AS 番号に制限できます。

プレフィックス ピアのダイナミック AS 番号を介して設定された BGP セッションは、**ebgp-multihop** を無視します コマンドと **disable-connected-check** コマンドを使用する必要があります。

ルートマップの AS 番号のリストは変更できますが、ルートマップ名を変更するには no neighbor コマンドを使用する必要があります。設定されたルート マップの AS 番号に変更を加えた場合、新しいセッションのみに影響します。

始める前に

- BGP を有効にする必要があります（「BGP の有効化」の項を参照）。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**router bgp** *autonomous-system-number*
	例：
	`switch(config)# router bgp 64496`
	`switch(config-router)#`
		BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。

ステップ 3	**neighbor** *prefix* **remote-as route-map** *map-name*
	例：
	`switch(config-router)# neighbor 192.0.2.0/8 remote-as routemap BGPPeers`
	`switch(config-router-neighbor)#`
		IPv4 プレフィックス、およびリモート BGP ピアの受け付けられた AS 番号のリストのルートマップを構成します。IPv4 の *prefix* 形式は、x.x.x.x/長さ長さの範囲は 1 ～ 32 です。
		マップ-名には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。

ステップ 4	**neighbor-as** *as-number* 例： `switch(config-router-neighbor)# remote-as 64497`	リモート BGP ピアの AS 番号を設定します。

	コマンドまたはアクション	目的
ステップ 5	（任意） **show bgp** {**ipv4** {**unicast** } **neighbors** 例： `switch(config-router-neighbor-af)# show bgp ipv4 unicast neighbors`	BGP ピアに関する情報を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config-router-neighbor-af)# copy running-config startup-config`	この設定変更を保存します。

例

次に、プレフィックス ピアのダイナミック AS 番号を設定する例を示します。

```
switch# configure terminal
switch(config)# route-map BGPPeers
switch(config-route-map)# match as-number 64496, 64501-64510
switch(config-route-map)# match as-number as-path-list List1, List2
switch(config-route-map)# exit
switch(config)# router bgp 64496
switch(config-router)# neighbor 192.0.2.0/8 remote-as route-map BGPPeers
switch(config-router-neighbor)# description Peer Router B
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

BGP 情報の消去

BGP 情報を消去するには、次のコマンドを使用します。

コマンド	目的
clear bgp all {*neighbor* | * | *as-number* | **peer-template** *name* | *prefix*}	すべてのアドレス ファミリから 1 つ以上のネイバーをクリアします。*を指定すると、すべてのアドレス ファミリのすべてのネイバーが消去されます。引数は次のとおりです。 • neighbor：ネイバーの IPv4 アドレス。 • *as-number*：自律システム番号。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 • *name*：ピア テンプレート名。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • prefix：IPv4 プレフィックス。そのプレフィックス内のすべてのネイバーがクリアされます。
clear bgp all dampening	すべてのアドレスファミリのルートフラップ ダンプニング ネットワークをクリアします。
clear bgp all flap-statistics	すべてのアドレスファミリのルートフラップ統計情報をクリアします。
clear bgp {**ipv4** } {**unicast**} **dampening**	選択したアドレスファミリのルートフラップ ダンプニング ネットワークをクリアします。
clear bgp {**ipv4** } {**unicast**} **flap-statistics**	選択したアドレスファミリのルートフラップ統計情報をクリアします。

コマンド	目的
clear bgp {**ipv4** } {*neighbor* |* | *as-number* | **peer-template** *name* | *prefix*}	選択したアドレス ファミリから 1 つ以上のネイバーをクリアします。* を指定すると、そのアドレス ファミリのすべてのネイバーが消去されます。引数は次のとおりです。 • neighbor：ネイバーの IPv4 アドレス。 • *as-number*：自律システム番号。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 • *name*：ピア テンプレート名。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • prefix：IPv4 プレフィックス。そのプレフィックス内のすべてのネイバーがクリアされます。
clear bgp {**ip** {**unicast**}} {*neighbor* |* |*as-number* | **peer-template** *name* | *prefix*}	1 つ以上のネイバーをクリアします。* を指定すると、そのアドレス ファミリのすべてのネイバーが消去されます。引数は次のとおりです。 • neighbor：ネイバーの IPv4 アドレス。 • *as-number*：自律システム番号。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。 • *name*：ピア テンプレート名。名称は 64 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • prefix：IPv4 プレフィックス。そのプレフィックス内のすべてのネイバーがクリアされます。

コマンド	目的
clear bgp dampening [*ip-neighbor* | *ip-prefix*]	1 つ以上のネットワークのルート フラップ ダンプニングをクリアします。引数は次のとおりです。 • *ip-neighbor*：ネイバーの IPv4 アドレス。 • *ip-prefix*： IPv4 そのプレフィックス内のすべてのネイバーがクリアされます。
clear bgp flap-statistics [*ip-neighbor* | *ip-prefix*]	1 つ以上のネットワークのルート フラップ統計情報をクリアします。引数は次のとおりです。 • *ip-neighbor*：ネイバーの IPv4 アドレス。 • *ip-prefix*： IPv4 そのプレフィックス内のすべてのネイバーがクリアされます。

ベーシック BGP の設定の確認

BGP の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 bgp all [summary]	すべてのアドレス ファミリについて、BGP 情報を表示します。
show bgp convergence	すべてのアドレス ファミリについて、BGP 情報を表示します。
show bgp {**ipv4** } {**unicast**} [*ip-address* **community** [**regexp** *expression* | [**community**] [**no-advertise**] [**no-export**] [**no-export-subconfed**]}	BGP コミュニティと一致する BGP ルートを表示します。
show bgp {**ipv4** } {**unicast**} [*ip-address*] **community-list** *list-name*	BGP コミュニティ リストと一致する BGP ルートを表示します。
show bgp {**ipv4** } {**unicast**} [*ip-address* | **extcommunity** [**regexp** *expression* | [**generic** [**non-transitive** | **transitive**] *aa4:nn* [**exact-match**]}	BGP 拡張コミュニティと一致する BGP ルートを表示します。
show bgp {**ipv4** } {**unicast**} [*ip-address* | **extcommunity-list** *list-name* [**exact-match**]}	BGP 拡張コミュニティ リストと一致する BGP ルートを表示します。

コマンド	目的
show bgp {**ipv4** } {**unicast**} [*ip-address* | {**dampening dampened-paths** [**regexp** *expression*]}	BGP ルート ダンプニングの情報を表示します。ルート フラップ ダンプニング情報を消去するには、**clear bgp dampening** コマンドを使用します。
show bgp {**ipv4** } {**unicast**} [*ip-address* | **history-paths** [**regexp** *expression*]	BGP ルート ヒストリ パスを表示します。
show bgp {**ipv4** } {**unicast**} [*ip-address* | **filter-list** *list-name*	BGP フィルタ リストの情報を表示します。
show bgp {**ipv4** } {**unicast**} [*ip-address*] **neighbors** [*ip-address*]	BGP ピアの情報を表示します。これらのネイバーを消去するには、**clear bgp neighbors** コマンドを使用します。
show bgp {**ipv4** } {**unicast**} [*ip-address*] **neighbors** [*ip-address*] {**nexthop** | **nexthop-database**}	BGPルート ネクスト ホップの情報を表示します。
show bgp paths	BGP パス情報を表示します。
show bgp {**ipv4** } {**unicast**} [*ip-address*] **policy** *name*	BGP ポリシー情報を表示します。ポリシー情報を消去するには、**clear bgp polic** コマンドを使用します。
show bgp {**ipv4** } {**unicast**} [*ip-address*] **prefix-list** *list-name*	プレフィックス リストと一致するBGPルートを表示します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **received-paths**	ソフト再構成用に保管されているBGPパスを表示します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **regexp** *expression*	AS_path 正規表現と一致する BGP ルートを表示します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **route-map** *map-name*	ルートマップと一致するBGPルートを表示します。
show bgp peer-policy *name*	BGP ピア ポリシー情報を表示します。
show bgp peer-session *name* show bgp peer-session	BGP ピア セッション情報を表示します。
show bgp peer-template *name*	BGP ピア テンプレート情報を表示します。ピア テンプレートのすべてのネイバーを消去するには、**clear bgp peer-template** コマンドを使用します。
show bgp process	BGP プロセス情報を表示します。

コマンド	目的
show {**ipv4**} **bgp** [*options*]	BGP のステータスと構成情報を表示します。
show {**ipv4**} **mbgp** [*options*]	BGP のステータスと構成情報を表示します。
show running-configuration bgp	現在実行中の BGP コンフィギュレーションを表示します。

BGP 統計情報のモニタリング

BGP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show bgp {**ipv4** } {**unicast**} [*ip-address*] **flap-statistics**	BGP ルート フラップの統計情報を表示します。これらの統計情報をクリアするには、**clear bgp flap-statistics command** を使用します。
show bgp sessions	すべてのピアの BGP セッションを表示します。これらの統計情報をクリアするには、**clear bgp sessions** コマンドを使用します。
show bgp statistics	BGP 統計情報を表示します。

ベーシック BGP の設定例

次に、ベーシック BGP 設定の例を示します。

```
switch(config)# feature bgp
switch(config)# router bgp 64496
switch(config-router)# neighbor 10.10.10.10 remote-as 64496
switch(config-router-af)# next-hop-self
```

関連項目

BGP の関連項目は、次のとおりです。

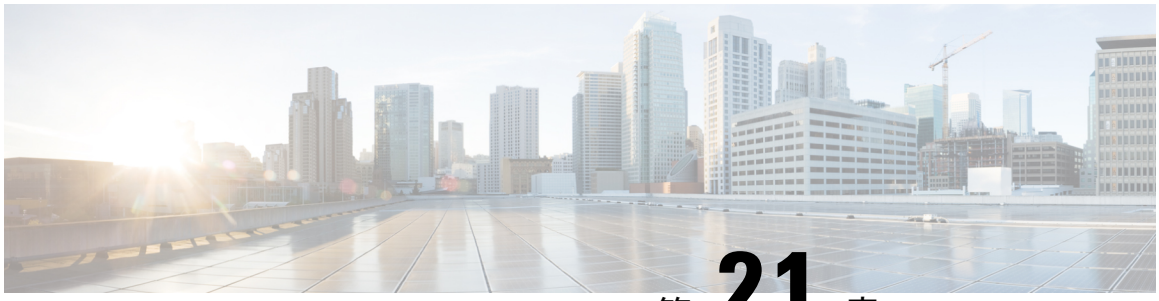
- 高度な BGP の設定 （321 ページ）

次の作業

次の機能の詳細については、高度な BGP の設定 （321 ページ）を参照してください。

次の作業

- ピア テンプレート
- ルートの再配布
- ルート マップ



第 21 章

高度な BGP の設定

この章は、次の項で構成されています。

拡張 BGP について

BGP は、組織または自律システム間のループフリー ルーティングを実現する、インタードメイン ルーティング プロトコルです。Cisco NX-OS は BGP バージョン 4 をサポートしています。BGP v4 に組み込まれているマルチプロトコル拡張機能を使用すると、IP マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリに関するルーティング情報を BGP に伝送させることができます。BGP では、他の BGP 対応デバイス（BGP ピア）との間で TCP セッションを確立するために、信頼できるトランスポート プロトコルとして TCP を使用します。外部組織に接続するときには、ルータが外部 BGP（eBGP）ピアリング セッションを作成

します。同じ組織内の BGP ピアは、内部 BGP（iBGP）ピアリング セッションを通じて、ルーティング情報を交換します。

ピア テンプレート

BGP ピア テンプレートを使用すると、類似した BGP ピア間で再利用できる共通のコンフィギュレーションブロックを作成できます。各ブロックでは、ピアに継承させる一連の属性を定義できます。継承した属性の一部を上書きすることもできるので、非常に柔軟性のある方法で、繰り返しの多い BGP の設定を簡素化できます。

Cisco NX-OS は、3 種類のピア テンプレートを実装します。

- peer-session テンプレートでは、トランスポートの詳細、ピアのリモート自律システム番号、セッション タイマーなど、BGP セッション属性を定義します。peer-session テンプレートは、別の peer-session テンプレートから属性を継承することもできます（ローカル定義の属性によって、継承した peer-session 属性は上書きされます）。
- peer-policy テンプレートでは、着信ポリシー、発信ポリシー、フィルタ リスト、プレフィックス リストを含め、アドレス ファミリに依存する、ピアのポリシー要素を定義します。peer-policy テンプレートは、一連の peer-policy テンプレートからの継承が可能です。Cisco NX-OS は、継承設定のプリファレンス値で指定された順序で、これらの peer-policy テンプレートを評価します。最小値が大きい値よりも優先されます。
- peer テンプレートは、peer-session および peer-policy テンプレートからの継承が可能であり、ピアの定義を簡素化できます。peer テンプレートの使用は必須ではありませんが、peer テンプレートによって再利用可能なコンフィギュレーション ブロックが得られるので、BGP の設定を簡素化できます。

認証

BGP ネイバー セッションに認証を設定できます。この認証方式によって、ネイバーに送られる各 TCP セグメントに MD5 認証ダイジェストが追加され、不正なメッセージや TCP セキュリティ アタックから BGP が保護されます。

（注） MD5 パスワードは、BGP ピア間で一致させる必要があります。

ルート ポリシーおよび BGP セッションのリセット

BGP ピアにルート ポリシーを関連付けることができます。ルート ポリシーではルート マップを使用して、BGP が認識するルートを制御または変更します。着信または発信ルート アップデートに関するルート ポリシーを設定できます。ルート ポリシーはプレフィックス、AS_path 属性など、さまざまな条件で一致が必要であり、ルートを選択して受け付けるかまたは拒否します。ルート ポリシーでパス属性を変更することもできます。

BGP ピアに適用するルート ポリシーを変更する場合は、そのピアの BGP セッションをリセットする必要があります。Cisco NX-OS は、BGP セッションをリセットするため、次の 3 つのメカニズムをサポートしています。

- ハード リセット：ハード リセットでは、指定されたピアリング セッションが TCP 接続を含めて切断され、指定のピアからのルートが削除されます。このオプションを使用すると、BGP ネットワーク上のパケット フローが中断します。ハード リセットは、デフォルトでディセーブルです。
- ソフト再構成着信：ソフト再構成着信によって、セッションをリセットすることなく、指定されたピアのルーティング アップデートが開始されます。このオプションを使用できるのは、着信ルート ポリシーを変更する場合です。ソフト再構成着信の場合、ピアから受け取ったすべてのルートのコピーを保存したあとで、着信ルート ポリシーを介してルートが処理されます。着信ルート ポリシーを変更する場合、Cisco NX-OS は変更された着信ルート ポリシーを介して保存ルートを渡し、既存のピアリング セッションを切断することなく、ルート テーブルをアップデートします。ソフト再構成着信の場合、まだフィルタリングされていない BGP ルートの保存に、大量のメモリ リソースを使用する可能性があります。ソフト再構成着信は、デフォルトでディセーブルです。
- ルート リフレッシュ：ルート リフレッシュでは、着信ルート ポリシーの変更時に、サポートするピアにルート リフレッシュ要求を送信することによって、着信ルーティング テーブルがダイナミックにアップデートされます。リモート BGP ピアは新しいルート コピーで応答し、ローカル BGP スピーカが変更されたルート ポリシーでそれを処理します。Cisco NX-OS は自動的に、プレフィックスのアウトバウンド ルートの更新をピアに送信します。
- BGP ピアは、BGP ピア セッションの確立時に、BGP 機能ネゴシエーションの一部として、ルート リフレッシュ機能をアドバタイズします。ルート リフレッシュは優先オプションであり、デフォルトでイネーブルです。

（注） BGP はさらに、ルート再配布、ルート集約、ルート ダンプニングなどの機能にルート マップを使用します。

eBGP

eBGP を使用すると、異なる AS からの BGP ピアを接続し、ルーティング アップデートを交換できます。外部ネットワークへの接続によって、自分のネットワークから他のネットワークへ、またインターネットを介して、トラフィックを転送できます。

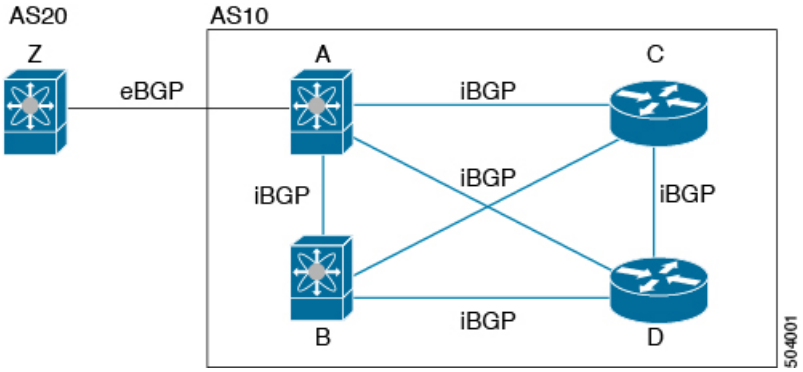
通常、eBGP ピアリングは、インターフェイスがダウンしたときにコンバージェンスが高速になるように、直接接続されたインターフェイス上で行う必要があります。

iBGP

iBGP を使用すると、同じ自律システム内の BGP ピアを接続できます。iBGP はマルチホーム BGP ネットワーク（同じ外部自律システムに対して複数の接続があるネットワーク）に使用できます。

図に、大きい BGP ネットワークの中の iBGP ネットワークを示します。

図 *16 : iBGP* ネットワーク



iBGP ネットワークはフルメッシュです。各 iBGP ピアは、ネットワーク ループを防止するために、他のすべての iBGP ピアに対して直接接続されています。

ネイバー コンフィギュレーション モードで update-source が設定された単一ホップ iBGP ピアでは、ピアは高速外部フェールオーバーをサポートします。

iBGP ピアリング セッションの確立には、ループバック インターフェイスを使用します。ループバック インターフェイスは、インターフェイス フラップが発生する可能性が小さいからです。インターフェイス フラップが発生するのは、障害またはメンテナンスが原因で、インターフェイスが管理上アップまたはダウンになったときです。マルチホップ、高速外部フォールオーバー、ASパス属性のサイズ制限については、eBGP の設定（353 ページ） セクションを参照してください。

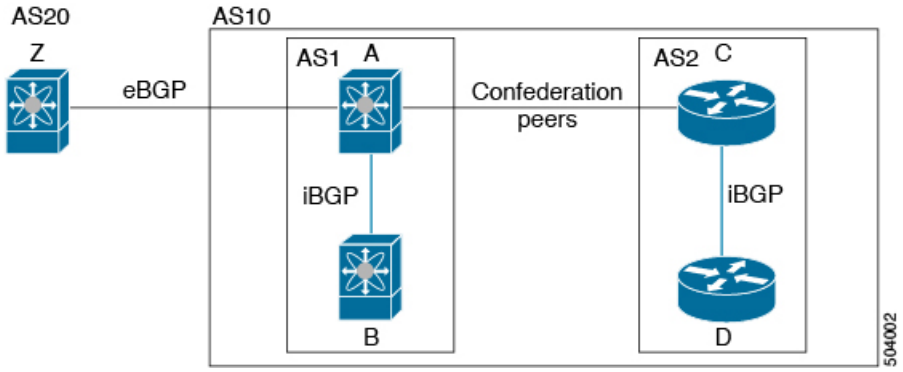
（注） iBGP ネットワークでは別個のインテリア ゲートウェイ プロトコルを設定する必要があります。

AS 連合

フルメッシュの iBGP ネットワークは、iBGP ピア数が増えるにしたがって複雑になります。自律システムを複数のサブ自律システムに分割し、それを 1 つの連合としてまとめることによって、iBGP メッシュを緩和できます。連合は、同じ自律システム番号を使用して外部ネットワークと通信する、iBGP ピアからなるグループです。各サブ AS はその中ではフルメッシュであり、同じ連合内の他のサブ AS に対する少数の接続があります。

図に BGP ネットワークが 2 つのサブ AS と 1 つの連合に分けられて表示されます。

図 *17* : *AS* 連合



この例では、AS10 が 2 つの AS（AS1 および AS2）に分割されています。各サブ AS はフルメッシュですが、サブ AS 間のリンクは 1 つだけです。AS 連合を使用することによって、 のフルメッシュ AS に比べて、リンク数を少なくできます。

ルート リフレクタ

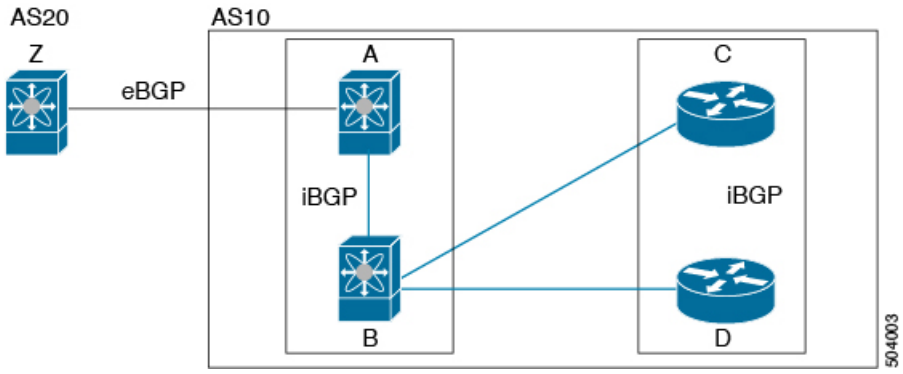
すべての iBGP ピアが完全に一致する必要がないように、ルート リフレクタが学習したルートをネイバーに渡すルート リフレクタ構成を使用することによって、iBGP メッシュを削減できます。

ある iBGP ピアをルート リフレクタとして設定すると、そのピアが iBGP で学習したルートを一連の iBGP ネイバーに渡す役割を担います。

図に、メッシュの iBGP スピーカを 4 つ（ルータ A、B、C、D）使用する、単純な iBGP 構成を示します。ルート リフレクタを使用しなかった場合、外部ネイバーからルートを受け取ったルータ A は、3 つの iBGP ネイバーのすべてにルートをアドバタイズします。

図では、ルータ B がルート リフレクタです。ルート リフレクタは、ルータ A からアドバタイズされたルートを受信すると、ルータ C と D へのルートをアドバタイズ（リフレクト）します。ルータ A は、ルータ C と D の両方にアドバタイズする必要がなくなります。

図 *18* : ルート リフレクタ



ルート リフレクタおよびそのクライアント ピアは、クラスタを形成します。ルート リフレクタのクライアント ピアとして動作するように、すべての iBGP ピアを設定する必要はありませ

ん。ただし、完全な BGP アップデートがすべてのピアに届くように、非クライアント ピアはフルメッシュとして設定する必要があります。

機能ネゴシエーション

BGP スピーカは機能ネゴシエーション機能を使用することによって、ピアでサポートされている BGP 拡張機能を学習できます。機能ネゴシエーションによって、リンクの両側の BGP ピアがサポートする機能セットだけを BGP に使用させることができます。

BGP ピアが機能ネゴシエーションをサポートしない場合で、なおかつアドレス ファミリが IPv4 として設定されている場合、Cisco NX-OS は機能ネゴシエーションを行わずに、ピアとの新規セッションを試みます。

ルート ダンプニング

ルート ダンプニングは、インターネットワーク上でのフラッピング ルートの伝搬を最小限に抑える BGP 機能です。ルート フラップが発生するのは、使用可能ステートと使用不能ステートが短時間で次々切り替わる場合です。

AS1、AS2、および AS3 という 3 つの BGP 自律システムからなるネットワークの場合について考えてみます。AS1 のルートがフラップした（使用不能になった）とします。ルート ダンプニングを使用しない場合、AS1 は AS2 に回収メッセージを送信します。AS2 は AS3 にその回収メッセージを伝達します。フラッピング ルートが再び発生すると、AS1 から AS2 にアドバタイズメント メッセージを送信し、AS2 は AS3 にそのアドバタイズメントを送信します。ルートの使用不能と使用可能が繰り返されると、AS1 は多数の回収メッセージおよびアドバタイズメント メッセージを送信することになり、それが他の自律システムに伝播します。

ルート ダンプニングによって、フラッピングを最小限に抑えることができます。ルート フラップが発生したとします。（ルート ダンプニングがイネーブルの）AS2 がルートにペナルティとして 1000 を割り当てます。AS2 は引き続き、ネイバーにルートの状態をアドバタイズします。ルート フラップが発生するたびに、AS2 がペナルティ値を追加します。ルート フラップが頻繁に発生して、ペナルティが設定可能な抑制限度を超えると、AS2 はフラップ回数に関係なく、ルートのアドバタイズを中止します。その結果、ルートが減衰（ダンプニング）します。

ルートに与えられたペナルティは、再使用限度に達するまで減衰します。その時点で、AS2 は再びルートをアドバタイズします。再使用限度が 50% になると、AS2 はそのルートのダンプニング情報を削除します。

（注） ルート ダンプニングがイネーブルの場合は、ピアのリセットによってルートが回収されても、リセット中の BGP にはペナルティは適用されません。

BGP ベストパスの選択

BGP ベストパス アルゴリズムでは、次の属性が同じ場合に、等コスト パスと見なされます。

- 重量
- ローカル プリファレンス
- AS_path
- オリジン コード
- Multi-Exit Discriminator（MED）
- BGP ネクスト ホップまでの IGP コスト

BGP はこれら複数のパスの中から、ベスト パスとして 1 つだけ選択し、そのパスを BGP ピアにアドバタイズします。詳細については、BGP の追加パス （328 ページ）を参照してください。

（注） 異なる AS 連合から受け取ったパスは、外部 AS_path 値およびその他の属性が同じ場合に、等コスト パスと見なされます。

（注） iBGP マルチパスに関してルート リフレクタを設定すると、ルート リフレクタが、選択されたベスト パスをピアにアドバタイズします。そのパスのネクスト ホップは変更されません。

BGP の追加パス

1 つの BGP 最良パスだけがアドバタイズされ、BGP スピーカは特定ピアからの特定プレフィックスの 1 パスだけを受け入れます。BGP スピーカが同じセッション内で同じプレフィックスの複数のパスを受信した場合、最新のアドバタイズメントを使用します。

BGP は、以前のパスに代わる新しいパスなしで、BGP スピーカが同じプレフィックスに対して複数のパスを伝播し、受け入れることを可能にする追加のパス機能をサポートします。この機能は、BGP スピーカのピアが、プレフィックスごとの複数パスのアドバタイズおよび受信をサポートし、また、そのパスのアドバタイズをサポートするかどうかネゴシエートすることを可能にします。特別な 4 バイトのパス ID は、ピア セッションを介して送信される同じプレフィックスに対して複数のパスを区別するため、ネットワーク層到達可能性情報（NLRI）に追加されます。次の図に、追加の BGP パス機能を示します。

図 *19 :* 追加パスの機能を持つ *BGP* ルート アドバタイズメント

BGP 追加パス設定の詳細については、BGP 追加パスの設定 （349 ページ） のセクションを参照してください。

（注） Cisco Nexus 3550-T ハードウェアは、ECMP ルートをインストールしません。

ルート集約

集約アドレスを設定できます。ルート集約を使用すると、固有性の強い一連のアドレスをすべての固有アドレスを代表する 1 つのアドレスに置き換えることによって、ルート テーブルを簡素化できます。たとえば、10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 という固有性の強い 3 つのアドレスを 1 つの集約アドレス 10.1.0.0/16 に置き換えることができます。

アドバタイズされるルートが少なくなるように、BGP ルート テーブル内には集約プレフィックスが存在します。

（注） Cisco NX-OS は、自動ルート集約をサポートしません。

ルート集約はフォワーディング ループにつながる可能性があります。この問題を回避するために、集約アドレスのアドバタイズメントを生成するときに、BGP はローカル ルーティング テーブルに、その集約アドレスに対応するサマリー廃棄ルートを自動的に組み込みます。BGP はサマリー廃棄のアドミニストレーティブ ディスタンスを 220 に設定し、ルート タイプを廃棄に設定します。BGP はネクストホップ解決に廃棄ルートを使用しません。

ユーザが **aggregate-address** コマンドを発行すると、BGP テーブルにサマリー エントリが作成されますが、サマリーエントリは、集約のサブセットがテーブルで見つかるまでアドバタイズできません。

BGP 条件付きアドバタイズメント

BGP 条件付きアドバタイズメントを使用すると、プレフィックスが BGP テーブルに存在するかどうかに基づいてルートをアドバタイズまたは撤回するように BGP を設定できます。この機能は、たとえば、BGP でいずれかのプロバイダーにプレフィックスをアドバタイズするようなマルチホーム ネットワーク（他のプロバイダーからの情報が存在しない場合のみ）で便利です。

AS1、AS2、および AS3 という 3 つの BGP 自律システムからなるネットワークの例について考えてみます。この例で、AS1 と AS3 はインターネットと AS2 に接続しています。条件付きアドバタイズメントを使用しない場合、AS2 はすべてのルートを AS1 と AS3 の両方にプロパゲートします。条件付きアドバタイズメントを使用すれば、AS1 からのルートが存在しない場合のみ（たとえば AS1 へのリンクがダウンした場合）、特定のルートを AS3 にアドバタイズするように AS2 を設定できます。

BGP 条件付きアドバタイズメントでは、設定されたルート マップに一致する各ルートに、存在テストまたは非存在テストが追加されます。詳細については、BGP 条件付きアドバタイズメントの設定 （364 ページ）を参照してください。

BGP ネクスト ホップ アドレス トラッキング

BGP は、インストールされているルートのネクスト ホップ アドレスをモニタして、ネクスト ホップの到達可能性の確認、およびBGPベストパスの選択、インストール、検証を行います。BGP ネクストホップ アドレスのトラッキングを行うと、ネクストホップの到達可能性に影響を及ぼす可能性のあるルート変更がルーティング情報ベース（RIB）で行われたときに確認プロセスをトリガーすることで、このようなネクストホップ到達可能性テストの速度が向上します。

ネクスト ホップ情報が変更されると、BGP は RIB から通知を受信します（イベント駆動型の通知）。BGP は、次のいずれかのイベントが発生したときに通知を受けます。

- ネクスト ホップが到達不能になった。
- ネクスト ホップが到達可能になった。
- ネクスト ホップへの完全再帰のインテリア ゲートウェイ プロトコル（IGP）メトリックが変更された。
- ファースト ホップの IP アドレスまたはファースト ホップのインターフェイスが変更された。
- ネクスト ホップが接続された。
- ネクスト ホップが接続解除された。
- ネクスト ホップがローカル アドレスになった。
- ネクスト ホップが非ローカル アドレスになった。

（注） 到達可能性および再帰メトリック イベントは、最適パスの再計算をトリガーします。

RIB からのイベント通知は、クリティカルおよび非クリティカルとして分類されます。クリティカルおよび非クリティカルイベントの通知は、別々のバッチで送信されます。ただし、非クリティカルイベントが保留中であり、クリティカルイベントを読み込む要求がある場合は、非クリティカル イベントがクリティカル イベントとともに送信されます。

- クリティカルなイベントとは、異なるパスに対してスイッチオーバーの原因となるネクスト ホップの消失など、ネクスト ホップの到達可能性に関連しています。異なるパスに対してスイッチオーバーの原因となるネクストホップの IGP メトリックの変更は、クリティカルなイベントと見なすことができます。
- 非クリティカルなイベントとは、最適パスに影響を与えたり、単一のネクスト ホップに IGP メトリックを変更したりせずに追加されるネクスト ホップに関連しています。

詳細については、BGP ネクスト ホップ アドレス トラッキングの設定 （345 ページ）を参照してください。

ルートの再配布

スタティック ルートまたは他のプロトコルからのルートを再配布するように、BGP を設定できます。再配布を指定したルート マップを設定して、どのルートが BGP に渡されるかを制御する必要があります。ルートマップを使用すると、宛先、送信元プロトコル、ルートタイプ、ルートタグなどの属性に基づいて、ルートをフィルタリングできます。詳細については、「ルート ポリシー マネージャの構成」のセクションを参照してください。

ルート マップを使用して両シナリオのデフォルト動作を無効にできますが、ルート マップの正しくない使用によってネットワーク ループが発生することがあるため、そうする場合は注意が必要です。次に、デフォルトの動作の変更にルート マップを使用する例を示します。

ルート マップの変更によって、シナリオ 1 のデフォルトの動作を次のように変更できます。

```
route-map foo permit 10
   match route-type internal
router ospf 1
   redistribute bgp 100 route-map foo
```

同様に、ルートマップの変更によって、シナリオ2のデフォルトの動作を次のように変更できます。

```
route-map foo deny 10
  match route-type internal
router ospf 1
   vrf bar
     redistribute bgp 100 route-map foo
```

BGP の調整

BGP タイマーによって、さらにベストパス アルゴリズムの調整によって、BGP のデフォルト動作を変更できます。

BGP タイマー

BGP では、ネイバー セッションおよびグローバル プロトコル イベントにさまざまなタイプのタイマーを使用します。確立されたセッションごとに、最低限2つのタイマーがあります。定期的にキープアライブ メッセージを送信するためのタイマー、さらに想定時間内にピアのキープアライブが届かなかった場合に、セッションをタイムアウトさせるためのタイマーです。また、個々の機能を処理するための、その他のタイマーがあります。これらのタイマーは通常、秒単位で設定します。タイマーには、異なる BGP ピアで同じタイマーが異なるタイミングでスタートするように、ランダム アジャストメントが組み込まれています。

ベストパス アルゴリズムの調整

オプションの設定パラメータによって、ベストパスアルゴリズムのデフォルト動作を変更できます。たとえば、アルゴリズムでの Multi-Exit Discriminator（MED）属性およびルータ ID の扱い方を変更できます。

グレースフル リスタートおよびハイ アベイラビリティ

Cisco NX-OS は、BGP に対してノンストップ フォワーディングとグレースフル リスタートをサポートしています。

Cisco NX-OS ルータでコールドリブートが発生した場合、ネットワークはルータへのトラフィック転送を中止し、ネットワーク トポロジからルータを削除します。この状況では、BGP は非グレースフル リスタートになり、すべてのルートが削除されます。Cisco NX-OS がスタートアップ コンフィギュレーションを適用すると、BGP はピアリング セッションを再び確立して、ルートを再学習します。

グレースフル リスタート動作中であることがルータで検出されると、両方のルータがそれぞれのトポロジ テーブルを交換します。すべての BGP ピアからルート アップデートを受信したルータは、古いルートをすべて削除し、アップデートされたルートでベストパス アルゴリズムを実行します。

ネイバー コンフィギュレーション モードで update-source が設定された単一ホップ iBGP ピアでは、ピアは高速外部フェールオーバーをサポートします。

追加 BGP パス機能により、特定のプレフィックスにアドバタイズされるパス数が再起動の前後で同じ場合、パス ID の選択は古いパスの最終状態および削除を保証します。いくつかのパスが指定されたプレフィックスにアドバタイズされる場合、古いパスがグレースフル リスタート ヘルパー ピアに発生する可能性があります。

メモリ不足の処理

BGP は、次の条件でメモリ不足に対処します。

- マイナー アラート：BGP は新しい eBGP ピアを確立しません。BGP は新しい iBGP ピアおよび連合ピアの確立は続行します。ピアは存続しますが、リセット ピアは再確立されません。
- 重大アラート：BGP は、メモリ アラートがマイナーになるまで、選択した確立済み eBGP ピアを 2 分おきにシャット ダウンします。eBGP ピアごとに、受信したパスの合計数と最適パスとして選択されたパスの数の比率が計算されます。比率が最高のピアが、メモリ使用状況を削減するためのシャットダウン対象として選択されます。オシレーションを回避するために、シャットダウンされた eBGP ピアを復帰する前にその eBGP ピアをクリアする必要があります。

（注） 重要な eBGP ピアをこの選択プロセスから除外できます。

- クリティカルアラート：BGP は確立されたすべてのピアを正常にシャットダウンします。シャットダウンされた eBGP ピアを復帰する前にその eBGP ピアをクリアする必要があります。

メモリ不足状態によるシャットダウンから BGP ピアを除外する方法の詳細については、BGP の調整 （331 ページ） のセクションを参照してください。

拡張 BGP の前提条件

拡張 BGP の前提条件は次のとおりです。

- BGP を有効にする必要があります（「BGP の有効化」の項を参照）。
- システムに有効なルータ ID を設定しておく必要があります。
- Regional Internet Registry（RIR）によって割り当てられたか、またはローカル管理の AS 番号を取得しておく必要があります。
- ネイバー関係を作成しようとするピアに到達可能でなければなりません（Interior Gateway Protocol（IGP）、スタティック ルート、直接接続など）。
- BGP セッションを確立するネイバー環境で、アドレス ファミリを明示的に設定する必要があります。

拡張 BGP に関する注意事項と制限事項

（注） ***Cisco Nexus 3550-T - 10.1(2t)* リリース**、BGP はデフォルトの VRF のみをサポートします。

拡張 BGP 設定時の注意事項および制約事項は、次のとおりです。

- プレフィックス ピアリングは、パッシブ TCP モードでのみ動作します。ピア アドレスがプレフィックス内にある場合、リモート ピアからの着信接続を受け入れます。
- **advertise-maps** コマンドを複数回設定することはサポートされていません。
- ダイナミック AS 番号プレフィックス ピア設定は、BGP テンプレートから継承した個々の AS 番号の設定よりも優先します。
- AS 連合でプレフィックス ピアにダイナミック AS 番号を設定した場合、BGP はローカル連合の AS 番号のみでセッションを確立します。
- ダイナミック AS 番号プレフィックス ピアで作成された BGP セッションは、設定済みの eBGP マルチホップ存続可能時間（TTL）値や直接接続ピアに対するディセーブル済みのチェックを無視します。
- ルータ ID の自動変更およびセッション フラップを避けるために、BGP 用のルータ ID を設定します。
- ピアごとに最大プレフィックス設定オプションを使用し、受信するルート数および使用するシステム リソース数を制限してください。

- update-source を設定し、eBGP マルチホップ セッションでセッションを確立します。
- 再配布を設定する場合は、BGP ルート マップを指定します。
- VRF 内で BGP ルータ ID を設定します。

（注） Cisco Nexus 3550-T では、48 の BGP セッションのみが検証されます。

- キープアライブおよびホールドタイマーの値を小さくすると、ネットワークでセッションフラップが発生する可能性があります。
- BGP をIGP に再配布するとき、iBGP も再配布されます。この動作を無効にするには、ルート マップに追加 deny 文を挿入します。
- VLAN には、次の注意事項および制約事項が **remove-private-as** コマンドに適用されます。
  - これは、eBGP ピアにだけ適用されます。
  - ネイバー コンフィギュレーション モードだけで設定可能となり、ネイバー アドレス ファミリ モードでは設定できません。
  - AS パスにプライベートとパブリック AS 番号を含める場合、プライベート AS 番号は削除されません。
  - AS パスに eBGP ネイバーの AS 番号が含まれている場合、プライベート AS 番号は削除されません。
  - その AS パス内のすべての AS 番号がプライベート AS 番号範囲に属する場合のみ、プライベート AS 番号は削除されます。ピアの AS 番号または非プライベート AS 番号が AS パス セグメントに存在する場合、プライベート AS 番号は削除されません。
- ネイバー、テンプレート ピア、テンプレート ピアセッション、またはテンプレート ピア ポリシー コンフィギュレーション モードでコマンドを無効にした場合（**inherit peer** または **inherit peer-session** コマンドが存在する場合）、**default** キーワードを使用してコマンドをデフォルトの状態に戻す必要があります。たとえば、実行コンフィギュレーションから **default update-source loopback 0** コマンドを無効にするには、**update-source loopback 0** コマンドを入力する必要があります。
- route-reflector クライアントに next-hop-self が設定されている場合、ルート リフレクタは自身をネクスト ホップとしてクライアントにルートをアドバタイズします。

デフォルト設定

高度な BGP パラメータのデフォルト設定値を表に示します。

パラメータ	デフォルト
BGP 機能	ディセーブル
BGP の追加パス	ディセーブル
キープアライブインターバル	60 秒
ホールド タイマー	180 秒
ダイナミック機能	有効（Enabled）

BGP セッション テンプレートの設定

BGP セッション テンプレートを使用すると、類似した設定が必要な複数の BGP ピアで、BGP の設定を簡素化できます。BGPテンプレートによって、共通のコンフィギュレーションブロックを再利用できます。先に BGP テンプレートを設定し、BGP ピアにテンプレートを適用します。

BGP セッション テンプレートでは、継承、パスワード、タイマー、セキュリティなどのセッション属性を設定できます。

peer-session テンプレートは、別の peer-session テンプレートからの継承が可能です。第 3 のテンプレートから継承するように第2テンプレートを設定できます。さらに最初のテンプレートもこの第3のテンプレートから継承させることができます。この間接継承を続けることができる peer-session テンプレートの数は、最大 7 つです。

ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。

始める前に

BGP を有効にする必要があります（「BGP の有効化」の項を参照）。

（注） テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、default 形式のコマンドを使用する必要があります。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的

ステップ 2	**router bgp** *autonomous-system-number*
	例：
	`switch(config)# router bgp 65535`
	`switch(config-router)#`
		BGP を有効にして、ローカル BGP スピーカに自律システム番号を割り当てます。

ステップ 3	**template peer-session** *template-name*
	例：
	`switch(config-router)# template peer-session BaseSession`
	`switch(config-router-stmp)#`
		peer-session テンプレート コンフィギュレーション モードを開始します。

ステップ 4	（任意） **password** *number password* 例： `switch(config-router-stmp)# password 0 test`	ネイバーにクリアテキストのパスワード「test」を追加します。パスワードは 3DES（タイプ 3 暗号形式）で保存および表示されます。
ステップ 5	（任意） **timers** *keepalive hold* 例： `switch(config-router-stmp)# timers 30 90`	peer-session テンプレートに BGP キープアライブおよびホールドタイマー値を追加します。 デフォルトのキープアライブインターバルは 60 です。デフォルトのホールドタイムは 180 です。

ステップ 6	**exit**
	例：
	`switch(config-router-stmp)# exit`
	`switch(config-router)#`
		peer-session テンプレート コンフィギュレーション モードを終了します。

ステップ 7	**neighbor** *ip-address* **remote-as** *as-number*
	例：
	`switch(config-router)# neighbor 192.168.1.2 remote-as 65535`
	`switch(config-router-neighbor)#`
		BGP ルーティング用のネイバー コンフィギュレーションモードを開始し、ネイバー IP アドレスを設定します。

ステップ 8	**inherit peer-session** *template-name*
	例：
	`switch(config-router-neighbor)# inherit peer-session BaseSession`
	`switch(config-router-neighbor)#`
		ピアに peer-session テンプレートを適用します。

ステップ 9	（任意） **description** *text*
	例：
	`switch(config-router-neighbor)# description Peer Router A`
	`switch(config-router-neighbor)#`
		ネイバーの説明を追加します。

	コマンドまたはアクション	目的
ステップ 10	（任意） **show bgp peer-session** *template-name* 例： `switch(config-router-neighbor)# show bgp peer-session BaseSession`	peer-policyテンプレートを表示します。
ステップ 11	（任意） **copy running-config startup-config** 例： `switch(config-router-neighbor)# copy running-config startup-config`	この設定変更を保存します。 **show bgp neighbor** コマンドを使用し、コマンドを実行して、適用されたテンプレートを確認します。

例

BGP peer-session テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer-session BaseSession
switch(config-router-stmp)# timers 30 90
switch(config-router-stmp)# exit
switch(config-router)# neighbor 192.168.1.2 remote-as 65536
switch(config-router-neighbor)# inherit peer-session BaseSession
switch(config-router-neighbor)# description Peer Router A
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# copy running-config startup-config
```

BGP peer-policy テンプレートの設定

peer-policyテンプレートを設定すると、特定のアドレス ファミリに対応する属性を定義できます。各 peer-policyテンプレートにプリファレンスを割り当て、指定した順序でテンプレートが継承されるようにします。ネイバー アドレス ファミリでは最大 5 つの peer-policy テンプレートを使用できます。

Cisco NX-OS は、プリファレンス値を使用して、アドレス ファミリの複数のピア ポリシーを評価します。プリファレンス値が最小のものが最初に評価されます。ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。

peer-policyテンプレートでは、AS-path フィルタ リスト、プレフィックス リスト、ルート リフレクション、ソフト再構成など、アドレス ファミリ固有の属性を設定できます。

（注） **show bgp neighbor** コマンドを使用し、 コマンドを実行して、適用されたテンプレートを確認します。

始める前に

BGP を有効にする必要があります（「BGP の有効化」の項を参照）。

（注） テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、default 形式のコマンドを使用する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	コンフィギュレーション モードに入ります。

ステップ 2	**router bgp** *autonomous-system-number*
	例：
	`switch(config)# router bgp 65535`
	`switch(config-router)#`
		BGP を有効にして、ローカル BGP スピーカに自律システム番号を割り当てます。

ステップ 3	**template peer-session** *template-name*
	例：
	`switch(config-router)# template peer-policy BasePolicy`
	`switch(config-router-ptmp)#`
		peer-policy テンプレートを作成します。

ステップ 4	（任意） **advertise-active-only** 例： `switch(config-router-ptmp)# advertise-active-only`	アクティブ ルートのみをピアにアドバタイズします。
ステップ 5	（任意） **maximum-prefix** *number* 例： `switch(config-router-ptmp)# maximum-prefix 20`	このピアに認めるプレフィックスの最大数を設定します。

ステップ 6	**exit**
	例：
	`switch(config-router-ptmp)# exit`
	`switch(config-router)#`
		peer-policy テンプレート コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的

ステップ 7	**neighbor** *ip-address* **remote-as** *as-number*
	例：
	`switch(config-router)# neighbor 192.168.1.2 remote-as 65535`
	`switch(config-router-neighbor)#`
		BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。

ステップ 8	**address-family** {**ipv4**} {**unicast**}
	例：
	`switch(config-router-neighbor)# address-family ipv4 unicast`
	`switch(config-router-neighbor-af)#`
		指定のアドレス ファミリに対しグローバル アドレス ファミリ設定モードを開始します。

ステップ 9	**inherit peer-policy** *template-name preference* 例： `switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1`	ピア アドレス ファミリ設定に peer-policy テンプレートを適用し、このピア ポリシーのプリファレンス値を割り当てます。
ステップ 10	（任意） **show bgp peer-policy** *template-name* 例： `switch(config-router-neighbor-af)# show bgp peer-policy BasePolicy`	peer-policy テンプレートを表示します。
ステップ 11	（任意） **copy running-config startup-config** 例： `switch(config-router-neighbor-af)# copy running-config startup-config`	この設定変更を保存します。 **show bgp neighbor** コマンドを使用し、コマンドを実行して、適用されたテンプレートを確認します。

例

BGP peer-policy テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer-session BasePolicy
switch(config-router-ptmp)# maximum-prefix 20
switch(config-router-ptmp)# exit
switch(config-router)# neighbor 192.168.1.1 remote-as 65536
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# inherit peer-policy BasePolicy
switch(config-router-neighbor-af)# copy running-config startup-config
```

BGP peer テンプレートの設定

BGP peer テンプレートを設定すると、1 つの再利用可能なコンフィギュレーション ブロックで、セッション属性とポリシー属性を結合することができます。peer テンプレートも、peer-session または peer-policy テンプレートを継承できます。ネイバーに設定した属性は、ネイバーが BGP テンプレートから継承した属性よりも優先されます。ネイバーに設定できる peer テンプレートは 1 つだけですが、peer テンプレートは peer-session および peer-policy テンプレートを継承できます。

peer テンプレートは、eBGP マルチホップ TTL、最大プレフィックス数、ネクストホップ セルフ、タイマーなど、セッション属性およびアドレス ファミリ属性をサポートします。

始める前に

BGP を有効にする必要があります（「BGP の有効化」の項を参照）。

（注） テンプレートを編集するときには、ピアまたはテンプレートのレベルで **no** 形式のコマンドを使用すると、テンプレートの設定を明示的に上書きできます。属性をデフォルトの状態にリセットするには、default 形式のコマンドを使用する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* 例： `switch(config)# router bgp 65535`	BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。
ステップ 3	**template peer** *template-name* 例： `switch(config-router)# template peer BasePeer`	peer テンプレート コンフィギュレーション モードを開始します。
ステップ 4	（任意） **inherit peer-session** *template-name* 例： `switch(config-router-neighbor)# inherit peer-session BaseSession`	ピア テンプレートに peer-session テンプレートを適用します。

	コマンドまたはアクション	目的

ステップ 5	（任意） **address-family** {**ipv4**} {**unicast**}
	例：
	`switch(config-router-neighbor)# address-family ipv4 unicast`
	`switch(config-router-neighbor-af)`
		指定のアドレスファミリに対しグローバル アドレス ファミリ コンフィギュレーション モードを設定します。

ステップ 6	（任意） **inherit peer-policy** *template-name* 例： `switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1`	ネイバー アドレス ファミリ設定に peer-policy テンプレートを適用します。
ステップ 7	**exit** 例： `switch(config-router-neighbor-af)# exit`	BGP ネイバー アドレス ファミリ 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	（任意） **timers** *keepalive hold* 例： `switch(config-router-neighbor)# timers 45 100`	ピアに BGP タイマー値を追加します。 これらの値によって、peer-session テンプレート、BaseSession のタイマー値が上書きされます。
ステップ 9	**exit** 例： `switch(config-router-neighbor)# exit`	BGP ネイバー コンフィギュレーション モードを終了します。

ステップ 10	**neighbor** *ip-address* **remote-as** *as-number*
	例：
	`switch(config-router)# neighbor 192.168.1.2 remote-as 65535`
	`switch(config-router-neighbor)#`
		BGP ルーティング用のネイバー設定モードを開始し、ネイバー IP アドレスを設定します。

ステップ 11	**inherit peer** *template-name*
	例：
	`switch(config-router-neighbor)# inherit`
	`peer BasePeer`
		peer テンプレートを継承します。

ステップ 12	（任意） **timers** *keepalive hold* 例： `switch(config-router-neighbor)# timers 60 120`	このネイバーに BGP タイマー値を追加します。 これらの値によって、peer テンプレートおよび peer-session テンプレートのタイマー値が上書きされます。

	コマンドまたはアクション	目的
ステップ 13	（任意） **show bgp peer-template** *template-name* 例： `switch(config-router-neighbor)# show bgp peer-template BasePeer`	peer テンプレートを表示します。
ステップ 14	（任意） **copy running-config startup-config** 例： `switch(config-router-neighbor)# copy running-config startup-config`	この設定変更を保存します。 **show bgp neighbor** コマンドを使用し、コマンドを実行して、適用されたテンプレートを確認します。

例

BGP peer テンプレートを設定して、BGP ピアに適用する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# template peer BasePeer
switch(config-router-neighbor)# inherit peer-session BaseSession
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# inherit peer-policy BasePolicy 1
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# neighbor 192.168.1.2 remote-as 65536
switch(config-router-neighbor)# inherit peer BasePeer
switch(config-router-neighbor)# copy running-config startup-config
```

プレフィックス ピアリングの設定

BGP では IPv4 の両方のプレフィックスを使用して、ピア セットを定義できます。この機能を使用すると、各ネイバーを設定に追加する必要がありません。

プレフィックス ピアリングを定義する場合は、プレフィックスとともにリモート AS 番号を指定する必要があります。プレフィックス ピアリングが設定されている許容最大ピア数を超えない場合、BGP はプレフィックスおよび自律システムから接続するピアを受け付けます。

プレフィックス ピアリングに含まれている BGP ピアが切断されると、Cisco NX-OS は定義されているプレフィックス ピア タイムアウト値まで、ピア構造を維持します。この場合、そのプレフィックス ピアリングのすべてのスロットを他のピアが使い果たした結果、ブロックされるという危険性を伴わずに、確立されたピアのリセットまたは再接続が可能になります。

手順

	コマンドまたはアクション	目的
ステップ 1	**timers prefix-peer-timeout** *value* 例： `switch(config-router-neighbor)# timers prefix-peer-timeout 120`	ルータ コンフィギュレーション モードで BGP プレフィックス ピアリングのタイムアウト値を設定します。有効な範囲は 0 ～ 1200 秒です。デフォルト値は 30 です。 （注） プレフィックス ピアの場合は、プレフィックス ピア タイムアウトを、設定されたグレースフル リスタート タイマーよりも大きく設定します。プレフィックス ピア タイムアウトがグレースフル リスタート タイマーよりも大きければ、ピアのルートは再起動中に保持されます。プレフィックス ピア タイムアウトがグレースフル リスタート タイマーよりも小さいと、ピアのルートはプレフィックス ピア タイムアウトによって消去されます。これは、再起動が完了する前に発生する可能性があります。
ステップ 2	**maximum-peers** *value* 例： `switch(config-router-neighbor)# maximum-peers 120`	ネイバー設定モードのこのプレフィックス ピアリングの最大ピア数を設定します。範囲は 1 ～ 1000 です。

例

最大 10 のピアを受け付けるプレフィックス ピアリングの設定例を示します。

```
switch(config)# router bgp 65536
switch(config-router)# timers prefix-peer-timeout 120
switch(config-router)# neighbor 10.100.200.0/24 remote-as 65536
switch(config-router-neighbor)# maximum-peers 10
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)#
```

show bgp ipv4 unicast neighbors コマンドを使用し、すると、所定のプレフィックス ピアリングの設定の詳細とともに、現在受け付けられているインスタンスのリスト、アクティブ ピア数、最大同時ピア数、および受け付けたピアの合計数を表示できます。

BGP 認証の設定

MD5 ダイジェストを使用してピアからのルート更新を認証するように、BGP を設定できます。

MD5 ダイジェストを使用するように BGP を設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**password** {**0** | **3** | **7**} *string* 例： `switch(config-router-neighbor)# password BGPpassword`	MGP ネイバー セッションの MD5 パスワードを設定します。

BGP セッションのリセット

BGP のルート ポリシーを変更した場合は、関連付けられた BGP ピア セッションをリセットする必要があります。BGP ピアがルート リフレッシュをサポートしない場合は、着信ポリシー変更に関するソフト再構成を設定できます。Cisco NX-OS は自動的に、セッションのソフト リセットを試みます。

ソフト再構成着信を設定するには、ネイバー アドレス ファミリ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**soft-reconfiguration inbound** 例： `switch(config-router-neighbor-af)# soft-reconfiguration inbound`	着信 BGP ルート アップデートを格納するために、ソフト再構成をイネーブルにします。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。
ステップ 2	（任意） **clear bgp** {**ipv4** } {**unicast** *ip-address* **soft** {**in** | **out**} 例： `switch# clear bgp ip unicast 192.0.2.1 soft in`	TCP セッションを切断しないで、BGP セッションをリセットします。

ネクストホップ アドレスの変更

次の方法で、ルートアドバタイズメントで使用するネクストホップアドレスを変更できます。

- ネクストホップ計算をディセーブルにして、ローカル BGP スピーカ アドレスをネクストホップ アドレスとして使用します。
- ネクストホップ アドレスをサードパーティ アドレスとして設定します。この機能は、元のネクスト ホップ アドレスがルートの送り先のピアと同じサブネット上にある場合に使用します。この機能を使用すると、フォワーディング時に余分なホップを節約できます。

ネクストホップ アドレス トラッキングを変更するには、アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**next-hop-self** **例：** `switch(config-router-neighbor-af)# next-hop-self`	ルート アップデートのネクストホップ アドレスとして、ローカル BGP スピーカ アドレスを使用します。このコマンドによって、BGP ネイバー セッションの自動ソフトクリアまたはリフレッシュが開始されます。
ステップ 2	**next-hop-third-party** **例：** `switch(config-router-neighbor-af)# next-hop-third-party`	ネクストホップ アドレスをサードパーティ アドレスとして設定します。このコマンドは、**next-hop-self** が設定されていないシングル ホップの EBGP ピアに使用します。 configured.

BGP ネクスト ホップ アドレス トラッキングの設定

BGP ネクスト ホップ アドレス トラッキングはデフォルトで有効であり、無効にすることができません。

BGP ネクスト ホップ トラッキングのパフォーマンスを向上するために、RIB チェック間の遅延インターバルを変更できます。

BGP ネクスト ホップ アドレス トラッキングを変更するには、アドレス ファミリ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**nexthop trigger-delay** {**critical** | **non-critical**} *milliseconds* 例： `switch(config-router-af)# nexthop trigger-delay critical 5000`	クリティカルなネクスト ホップの到達可能性ルートおよび非クリティカルなルートについて、ネクスト ホップ アドレス トラッキングの遅延タイマーを指定します。指定できる範囲は 1 ～ 4294967295 ミリ秒です。クリティカル タイマーのデフォルトは 3000 です。非クリティカル タイマーのデフォルトは 10000 です。

ネクスト ホップ フィルタリングの設定

BGP ネクストホップ フィルタリングを使用すると、RIB でネクストホップ アドレスがチェックされるときにそのネクストホップ アドレスの基盤となるルートがルート マップを経由します。ルート マップでそのルートが拒否されると、ネクストホップ アドレスは到達不能として扱われます。

BGP は、ルート ポリシーによって拒否されたすべてのネクストホップを無効であるとマークし、無効なネクストホップ アドレスを使用するルートについてベスト パスを計算しません。

BGP ネクストホップ フィルタリングを設定するには、アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**nexthop route-map** *name* 例： `switch(config-router-af)# nexthop route-map nextHopLimits`	BGP ネクストホップ ルートが一致するルート マップを指定します。63 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

デフォルト ルートによるネクストホップ解決の設定

BGP ネクストホップ解決では、IP デフォルト ルートを BGP ネクストホップ解決に使用するかどうかを指定できます。

BGP ネクストホップ解決を設定するには、ルータ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	[**no**] **nexthop suppress-default-resolution** 例： `switch(config-router)# nexthop suppress-default-resolution`	IP デフォルト ルートを介した BGP ネクストホップの解決を防止します。 このコマンドを有効にすると、以下のようになります。 • **show bgp process detail** コマンドの出力には、次の行が含まれます。 Use default route for nexthop Resolution：No • **show routing clients bgp** コマンドの出力には、次の行が含まれます。 Owned rnh will never resolve to 0.0.0.0/0

ネクストホップセルフによるリフレクト ルートの制御

NX-OS では、**next-hop-self** [all] 引数を使用して特定のピアに送信する際の iBGP ルートを制御できます。これらの引数を使用すると、ルートのリフレクトが実施されている場合でも、ルートのネクストホップを選択的に変更できます。

コマンド	目的
next-hop-self [all] 例： `switch(config-router-af)# next-hop-self all`	ルートアップデートのネクストホップアドレスとして、ローカルBGPスピーカアドレスを使用します。 all キーワードはオプションです。all を指定すると、すべてのルートが next-hop-self を使用するピアに送信されます。all を指定しなかった場合、リフレクトしたルートのネクストホップは変更されません。

セッションがダウンした場合のネクストホップ グループの縮小

この機能は、次の BGP パス障害イベントに適用されます。

- 1 つまたは複数のレイヤ 3 リンクの障害

- ライン カード障害
- BGP ネイバーの管理上のシャットダウン（shutdown コマンドを使用）

最初の2つのイベント（レイヤ3リンク障害とラインカード障害）の迅速な処理はデフォルトでイネーブルになっており、イネーブルにするための設定コマンドは必要ありません。

最後の2つのイベントの迅速な処理を設定するには、ルータ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ1	**neighbor-down fib-accelerate** **例：** `switch(config-router)# neighbor-down fib-accelerate`	BGP セッションがダウンするたびに、すべてのネクストホップ グループ（単一のネクストホップ ルート）から対応する次のネクスト ホップを取り消します。 （注） このコマンドは、IPv4 ルートの両方に適用されます。

機能ネゴシエーションのディセーブル化

機能ネゴシエーションをディセーブルにすると、機能ネゴシエーションをサポートしない古いBGP ピアとの相互運用が可能です。

機能ネゴシエーションをディセーブルにするには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ1	**dont-capability-negotiate** **例：** `switch(config-router-neighbor)# dont-capability-negotiate`	機能ネゴシエーションをディセーブルにします。このコマンドの設定後、BGP セッションを手動でリセットする必要があります。

ポリシーのバッチ処理の無効化

プレフィックスに一意の属性がある BGP 展開では、BGP は、同じ BGP アップデートメッセージでバンドルする類似の属性を持つルートを識別しようとします。この追加の BGP 処理のオーバーヘッドを回避するには、バッチ処理をディセーブルにします。

固有のネクスト ホップを持つ多数のルートがある BGP 展開では、ポリシーバッチ処理を無効にすることを推奨します。

ポリシー バッチ処理を無効にするには、ルータ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**disable-policy-batching** 例： `switch(config-router)# disable-policy-batching`	すべてのピアへのプレフィックスアドバタイズメントのバッチ評価をディセーブルにします。

BGP 追加パスの設定

BGPは、プレフィックスごとの複数パスの送受信と、このパスのアドバタイジングをサポートします。

追加パスの送受信機能のアドバタイズ

BGP ピア間の追加パスの送受信機能をアドバタイズするように BGP を設定できます。これを行うには、ネイバー アドレス ファミリ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	[**no**] **capability additional-paths send** [**disable**] 例： `switch(config-router-neighbor-af)# capability addtional-paths send`	BGP ピアに追加パスを送信する機能をアドバタイズします。**disable** オプションは、追加パス送信機能のアドバタイズをディセーブルにします。 このコマンドの **no** 形式を使用すると、追加パスの送信機能がディセーブルになります。
ステップ 2	[**no**] **capability additional-paths receive** [**disable**] 例： `switch(config-router-neighbor-af)# capability addtional-paths receive`	BGP ピアから追加パスを受信する機能をアドバタイズします。**disable** オプションは、追加パス受信機能のアドバタイズをディセーブルにします。 このコマンドの **no** 形式は、追加パスの受信機能をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**show bgp neighbor** 例： `switch(config-router-neighbor-af)# show bgp neighbor`	ローカル ピアがリモート ピアへの追加パス送受信機能をアドバタイズしたかを表示します。

例

BGP ピアに追加のパスを送受信する機能をアドバタイズする BGP の設定例を示します。

```
switch# configure terminal
switch(config)# router bgp 100
switch(config-router)# neighbor 10.131.31.2 remote-as 100
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# capability additional-paths send
switch(config-router-neighbor-af)# capability additional-paths receive
```

追加パスの送受信の設定

BGP ピア間の追加パスの送受信機能を設定できます。これを行うには、アドレス ファミリ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	[**no**] **additional-paths send** 例： `switch(config-router-af)# additional-paths send`	機能が無効になっていないこのアドレス ファミリで、すべてのネイバーの追加パスの送信機能を有効にします。 このコマンドの **no** 形式を使用すると、送信機能が無効になります。
ステップ 2	[**no**] **additional-paths receive** 例： `switch(config-router-af)# additional-paths receive`	機能が無効になっていないこのアドレス ファミリで、すべてのネイバーの追加パスの受信機能を有効にします。 このコマンドの **no** 形式を使用すると、受信機能が無効になります。
ステップ 3	**show bgp neighbor** 例： `switch(config-router-af)# show bgp neighbor`	ローカル ピアがリモート ピアへの追加パス送受信機能をアドバタイズしたものとして表示します。

例

機能が無効になっていない指定されたアドレス ファミリで、すべてのネイバーの追加パスの受信機能を有効にする例を示します。

```
switch# configure terminal
switch(config)# router bgp 100
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# additional-paths send
switch(config-router-af)# additional-paths receive
```

アドバタイズされるパスの設定

BGPにアドバタイズされたパスを指定できます。これを行うには、ルートマップ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**[no] set ip next-hop unchanged** 例： `switch(config-route-map)# set ip next-hop unchanged`	不変のネクストホップ IP アドレスを指定します。
ステップ 2	**[no] set path-selection { all | backup | best2}** | advertise 例： `switch(config-route-map)# set path-selection all advertise`	すべてのパスが指定されたプレフィックスにアドバタイズされるように指定します。次のいずれかのオプションを選択できます。 • all：使用可能なすべての有効なパスをアドバタイズします。 • backup：バックアップ パスとしてマークされたパスをアドバタイズします。このオプションでは、additional-path install backup コマンドを使用してバックアップ パスを有効にする必要があります。 • best2：2番目に最適なパスをアドバタイズします。これは、すでに計算されているベスト パスを除き、残りの使用可能なパスのベスト パスです。

	コマンドまたはアクション	目的
		このコマンドの **no** 形式は、最適パスだけがアドバタイズされるように指定します。
ステップ 3	**show bgp** {**ipv4** } **unicast** [*ip-address*] 例： `switch(config-route-map)# show bgp ipv4 unicast`	プレフィックスの追加パスのパス ID とこれらのパスのアドバタイズメント情報を表示します。

例

すべてのパスがプレフィックス リスト p1 にアドバタイズされるよう指定する例を示します。

```
switch# configure terminal
switch(config)# route-map PATH_SELECTION_RMAP
switch(config-route-map)# match ip address prefix-list p1
switch(config-route-map)# set path-selection all advertise
```

追加パス選択の設定

プレフィックスに追加のパスを選択する機能を設定できます。これを行うには、アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的

ステップ 1	[**no**] **additional-paths selection route-map** *map-name*
	例：
	`switch(config-router-af)# additional paths`
	`selection route-map map1`
		プレフィックスに追加のパスを選択する機能を設定します。
		このコマンドの **no** 形式は、追加パス選択機能をディセーブルにします。

ステップ 2	**show bgp** {**ipv4** } **unicast** [*ip-address*] 例： `switch(config-route-af)# show bgp ipv4 unicast`	プレフィックスの追加パスのパス ID とこれらのパスのアドバタイズメント情報を表示します。

例

指定されたアドレス ファミリで追加パス選択を設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 100
```

```
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# additional-paths selection route-map PATH_SELECTION_RMAP
```

eBGP の設定

eBGP シングルホップ チェックの無効化

シングルホップ eBGP ピアがローカル ルータに直接接続されているかどうかのチェック機能を無効にするように、eBGP を設定できます。このオプションは、直接接続されたスイッチ間のシングルホップ ループバック eBGP セッションの設定に使用します。

シングルホップ eBGP ピアが直接接続されているかどうかのチェックを無効にするには、ネイバー設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**disable-connected-check** 例： `switch(config-router-neighbor)# disable-connected-check`	シングルホップ eBGP ピアが直接接続されているかどうかのチェックを無効にします。このコマンドの使用後、BGP セッションを手動でリセットする必要があります。

eBGP マルチホップの設定

eBGP マルチホップをサポートする eBGP 存続可能時間（TTL）値を設定できます。eBGP ピアは状況によって、別の eBGP ピアに直接接続されず、リモート eBGP ピアに到達するために複数のホップを必要とします。ネイバー セッションに eBGP TTL 値を設定すると、このようなマルチホップ セッションが可能になります。

（注） この設定は、BGP インターフェイス ピアリングではサポートされません。

eBGP マルチホップを設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**ebgp-multihop** *ttl-value* 例：	eBGP マルチホップの eBGP TTL を設定します。有効な範囲は 2 ～ 255 です。こ

	コマンドまたはアクション	目的
	`switch(config-router-neighbor)# ebgp-multihop 5`	のコマンドの使用後、BGP セッションを手動でリセットする必要があります。

高速外部フォールオーバーの無効化

Cisco NX-OS デバイスは、すべての VRF のネイバーおよびアドレス ファミリ（IPv4）の高速外部フォールオーバーをデフォルトでサポートします。通常、BGP ルータと直接接続 eBGP ピア間の接続が失われると、ピアとの eBGP セッションをリセットすることによって、BGP が高速外部フォールオーバーを開始します。この高速外部フォールオーバーをディセーブルにすると、リンク フラップが原因の不安定さを制限できます。

高速外部フォールオーバーをディセーブルにするには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**no fast-external-fallover** **例：** `switch(config-router)# no fast-external-fallover`	eBGP ピアの高速外部フォールオーバーをディセーブルにします。このコマンドは、デフォルトでイネーブルになっています。

AS パス属性の制限

AS パス属性で自律システム番号が高いルートを廃棄するように eBGP を設定できます。

AS パス属性で AS 番号の多いルートを廃棄するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**maxas-limit** *number* **例：** `switch(config-router)# maxas-limit 50`	AS パス セグメントの番号が指定された上限を超えている eBGP ルートを廃棄します。指定できる範囲は 1 ～ 2000 です。

ローカル AS サポートの設定

ローカル AS 機能では、ルータが実際の AS に加えて、2 番めの自律システム（AS）のメンバであるように見せることができます。ローカル AS を使用すると、ピアリングの調整を変更せ

ずに 2 つの ISP をマージできます。マージされた ISP 内のルータは、新しい自律システムのメンバになりますが、使用者に対しては古い自律システム番号を使用し続けます。

この機能は、正しい eBGP ピアにしか使用できません。別のコンフェデレーションのサブ自律システムのメンバである 2 ピアに対しては、この機能は使用できません。

eBGP ローカル AS のサポートを設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**local-as** *number* [**no-prepend** [**replace-as** [**dual-as**]]] **例：** `switch(config-router-neighbor)# local-as 1.1`	AS_PATH 属性にローカル AS の *number* を付加するよう eBGP を設定します。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。

例

次に、VRF のローカル AS サポートを設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 1
switch(config-router)# neighbor 10.1.1.1
switch(config-router-neighbor)# local-as 1
switch(config-router-neighbor)# show running-config bgp
```

AS 連合の設定

AS連合を設定するには、連合識別情報を指定する必要があります。AS連合内の自律システムグループは、自律システム番号として連合 ID を持つ、1 つの自律システムとして外部で認識されます。

BGP 連合 ID を設定するには、ルータ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**confederation identifier** *as-number* **例：** `switch(config-router)# confederation identifier 4000`	ルータ設定モードで、このコマンドは BGP 連合 ID を設定します。 このコマンドによって、BGP ネイバーセッションの自動通知およびセッションリセットが開始されます。

	コマンドまたはアクション	目的
ステップ 2	**bgp confederation peers** *as-number* [*as-number2...*] 例： `switch(config-router)# bgp confederation peers 5 33 44`	ルータ設定モードで、このコマンドはAS 連合に属する自律システムを設定します。 このコマンドは、連合に属する自律システムのリストを指定し、BGP ネイバーセッションの自動通知とセッションリセットをトリガーします。

ルート リフレクタの設定

ルート リフレクタとして動作するローカル BGP スピーカに対するルート リフレクタ クライアントとして、iBGP ピアを設定できます。ルート リフレクタとそのクライアントがともにクラスタを形成します。クライアントからなるクラスタには通常、ルート リフレクタが 1 つ存在します。このような状況では、ルート リフレクタのルータ ID でクラスタを識別します。ネットワークの冗長性を高め、シングル ポイント障害を回避するために、複数のルート リフレクタからなるクラスタを設定できます。クラスタ内のすべてのルート リフレクタは、同じ 4 バイト クラスタ ID で設定する必要があります。これは、ルート リフレクタが同じクラスタ内のルート リフレクタからのアップデートを認識できるようにするためです。

始める前に

BGPをイネーブルにする必要があります。

手順

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

ステップ 2	**router bgp** *as-number*
	例：
	`switch(config)# router bgp 65535`
	`switch(config-router)#`
		BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。

ステップ 3	**cluster-id** *cluster-id* 例： `switch(config-router)# cluster-id 192.0.2.1`	クラスタに対応するルート リフレクタの 1 つとして、ローカル ルータを設定します。クラスタを識別するクラスタ ID を指定します。このコマンドによって、BGP ネイバーセッションの自動ソフト クリアまたはリフレッシュが開始されます。

	コマンドまたはアクション	目的

ステップ 4	**address-family** {**ipv4**} {**unicast**}
	例：
	`switch(config-router)# address-family ipv4 unicast`
	`switch(config-router-af)#`
		指定のアドレス ファミリに対応するグローバル アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 5	（任意） **client-to-client reflection** 例： `switch(config-router-af)# client-to-client reflection`	クライアント間のルート リフレクションを設定します。この機能は、デフォルトでイネーブルになっています。このコマンドによって、BGP ネイバー セッションの自動ソフト クリアまたはリフレッシュが開始されます。

ステップ 6	**exit**
	例：
	`switch(config-router-af)# exit`
	`switch(config-router)#`
		ルータ アドレス コンフィギュレーション モードを終了します。

ステップ 7	**neighbor** *ip-address* **remote-as** *as-number*
	例：
	`switch(config-router)# neighbor 192.0.2.10 remote-as 65535`
	`switch(config-router-neighbor)#`
		リモート BGP ピアの IP アドレスおよび AS 番号を設定します。

ステップ 8	**address-family** {**ipv4**} {**unicast**}
	例：
	`switch(config-router-neighbor)# address-family ipv4 unicast`
	`switch(config-router-neighbor-af)#`
		ユニキャスト IPv4 アドレス ファミリに対応するネイバー アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 9	**route-reflector-client** 例： `switch(config-router-neighbor-af)# route-reflector-client`	BGP ルート リフレクタとしてデバイスを設定し、そのクライアントとしてネイバーを設定します。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。
ステップ 10	（任意） **show bgp** {**ipv4**} {**unicast**} **neighbors** 例： `switch(config-router-neighbor-af)# show bgp ipv4 unicast neighbors`	BGP ピアを表示します。
ステップ 11	（任意） **copy running-config startup-config** 例：	この設定変更を保存します。

	コマンドまたはアクション	目的
	`switch(config-router-neighbor-af)# copy running-config startup-config`	

例

次に、ルート リフレクタとしてルータを設定し、クライアントとしてネイバーを 1 つ追加する例を示します。

```
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.10 remote-as 65536
switch(config-router-neighbor)# address-family ip unicast
switch(config-router-neighbor-af)# route-reflector-client
switch(config-router-neighbor-af)# copy running-config startup-config
```

アウトバウンド ルート マップを使用した、反映されたルートのネクスト ホップの設定

アウトバウンド ルート マップを使用して、BGP ルート リフレクタの反映されたルートのネクスト ホップを変更できます。ネクスト ホップ アドレスとしてピアのローカル アドレスを指定するため、アウトバウンド ルート マップを設定できます。

（注） この項で説明している **next-hop-self** コマンドは、ルート リフレクタによってクライアントに反映されるルートに対してこの機能を有効にしません。この機能は、アウトバウンド ルート マップを使用した場合にだけ有効にできます。

始める前に

BGP を有効にする必要があります（「BGP の有効化」の項を参照）。

set next-hop を入力する必要がありますコマンドを入力して、アドレス ファミリ固有のネクスト ホップ アドレスを設定する必要があります。

- ルートマップを使用して IPv4 ネクストホップを設定する場合： **set ip next-hop peer-address** がルートマップと一致する場合、ネクストホップはピアのローカルアドレスに設定されます。ネクスト ホップがルート マップで設定されていない場合、ネクスト ホップはパスに保存されているネクスト ホップに設定されます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**router bgp** *as-number*
	例：
	`switch(config)# router bgp 200`
	`switch(config-router)#`
		BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。

ステップ 3	**neighbor** *ip-address* **remote-as** *as-number*
	例：
	`switch(config-router)# neighbor 192.0.2.12 remote-as 200`
	`switch(config-router-neighbor)#`
		リモート BGP ピアの IP アドレスおよび AS 番号を設定します。

ステップ 4	（任意） **update-source** *interface number* 例： `switch(config-router-neighbor)# update-source loopback 300`	BGP セッションの送信元を指定し、更新します。

ステップ 5	**address-family** {**ipv4** } {**unicast**}
	例：
	`switch(config-router-neighbor)# address-family ipv4 unicast`
	`switch(config-router-neighbor-af)#`
		指定のアドレス ファミリに対応するグローバル アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 6	**route-reflector-client** 例： `switch(config-router-neighbor-af)# route-reflector-client`	BGP ルート リフレクタとしてデバイスを設定し、そのクライアントとしてネイバーを設定します。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。
ステップ 7	**route-map** *map-name* **out** 例： `switch(config-router-neighbor-af)# route-map setrrnh out`	発信ルートに設定された BGP ポリシーを適用します。
ステップ 8	（任意） **show bgp** {**ipv4** } {**unicast**} [**ip-address**] **route-map** *map-name*] 例： `switch(config-router-neighbor-af)# show bgp ipv4 unicast route-map setrrnh`	ルート マップと一致する BGP ルートを表示します。

	コマンドまたはアクション	目的
ステップ 9	（任意） **copy running-config startup-config** 例： `switch(config-router-neighbor-af)# copy running-config startup-config`	この設定変更を保存します。

例

アウトバウンド ルート マップを使用して、BGP ルート リフレクタの反映されたルートのネクスト ホップを設定する例を示します。

```
switch(config)# interface loopback 300
switch(config-if)# ip address 192.0.2.11/32
switch(config-if)# ip router ospf 1 area 0.0.0.0
switch(config-if)# exit
switch(config)# route-map setrrnh permit 10
switch(config-route-map)# set ip next-hop peer-address
switch(config-route-map)# exit
switch(config)# router bgp 200
switch(config-router)# neighbor 192.0.2.12 remote-as 200
switch(config-router-neighbor)# update-source loopback 300
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# route-reflector-client
switch(config-router-neighbor-af)# route-map setrrnh out
switch(config-router-neighbor-af)# exit
```

ルート ダンプニングの設定

iBGP ネットワーク上でのルート フラップの伝播を最小限に抑えるために、ルート ダンプニングを設定できます。

ルート ダンプニングを構成するには、アドレス ファミリ構成モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**dampening** [{*half-life reuse-limit suppress-limit max-suppress-time* | **route-map** *map-name*}] 例： `switch(config-router-af)# dampening route-map bgpDamp`	機能ネゴシエーションをディセーブルにします。パラメータ値は次のとおりです。 • *half-life*：指定できる範囲は 1 ～ 45 です。 • *resuse-limit*指定できる範囲は 1 ～ 20000 です。

	コマンドまたはアクション	目的
		• *suppress-limit*：指定できる範囲は 1 ～ 20000 です。 • *max-suppress-time*：指定できる範囲は 1 ～ 20000 です。

最大プレフィックス数の設定

BGP が BGP ピアから受け取ることのできるプレフィックスの最大数を設定できます。任意で、プレフィックス数がこの値を超えた場合に、BGP に警告メッセージを生成させる、またはピアとの BGP セッションを切断させることを設定できます。

BPG ピアに認めるプレフィックスの最大数を設定するには、ネイバー アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**maximum-prefix** *maximum* [*threshold*] [**restart** *time* | **warning-only**] **例**： `switch(config-router-neighbor-af)# maximum-prefix 12`	ピアからのプレフィックスの最大数を設定します。パラメータの範囲は次のとおりです。 • *maximum*：指定できる範囲は 1 ～ 300000 です。 • *threshold*：指定できる範囲は 1 ～ 100 % です。デフォルトは 75% です。 • *time*：指定できる範囲は 1 ～ 65535 分です。 このコマンドによって、プレフィックス限度を超えた場合に、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

DSCP の設定

ネイバーの differentiated services code point（DSCP）を設定します。IPv4 のローカル発信パケットの DSCP 値を指定できます。

DSCP 値を設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的

ステップ 1	**dscp** *dscp_value*
	例：
	`switch(config-router-neighbor)# dscp 63`
	次に、対応する **show** コマンドの例を示します。
	`show ipv4 bgp neighbors`
	`BGP neighbor is 10.1.1.1, remote AS 0, unknown link, Peer index 4`
	`BGP version 4, remote router ID 0.0.0.0`
	`BGP state = Idle, down for 00:13:34, retry in 0.000000`
	`DSCP (DiffServ CodePoint): 0`
	`Last read never, hold time = 180, keepalive interval is 60 seconds`
		ネイバーの Differentiated Services Code Point（DSCP）の値を設定します。DSCP 値には、0 ～ 63 の数字、または、**ef**、**af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、または **cs7** のいずれかのキーワードを指定できます。
		デフォルト値は cs6 です。
		（注） Cisco Nexus 3550-T ハードウェアは、パケット内の DSCP 値を確認しません。

ダイナミック機能の設定

BGP ピアのダイナミック機能を設定できます。

ダイナミック機能を設定するには、ネイバー コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**dynamic-capability** 例： `switch(config-router-neighbor)# dynamic-capability`	ダイナミック機能をイネーブルにします。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

集約アドレスの設定

BGP ルート テーブルの集約アドレス エントリを設定できます。

集約アドレスを設定するには、ルータ アドレス ファミリ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**aggregate-address** *ip-prefix/length* [**as-set**] [**summary-only**] [**advertise-map** *map-name*] [**attribute-map** *map-name*] [**suppress-map** *map-name*] 例： `switch(config-router-af)# aggregate-address 192.0.2.0/8 as-set`	集約アドレスを作成します。このルートに関してアドバタイズされるパスは、集約されているすべてのパスに含まれるすべての要素からなる、自律システムセットです。 • **as-set** キーワードは、関係するパスから自律システム セット パス情報およびコミュニティ情報を生成します。 • **summary-only** キーワードは、アップデートから具体的なルートをすべてフィルタリングします。 • **advertise-map** キーワードおよび引数では、選択されたルートから属性情報を選択するためのルート マップを指定します。 • **attribute-map** キーワードおよび引数では、集約から属性情報を選択するためのルート マップを指定します。 • **suppress-map** キーワードおよび引数によって、固有性の強いルートを条件付きでフィルタリングします。BGPルート集約の実行中に **suppress-map** オプションを指定すると、特定のより具体的なルートがピアにアドバタイズされないように抑制したり、suppress-map route-map 設定に応じて、いくつかのコミュニティ属性が設定されたより具体的なルートをアドバタイズしたりすることができます。match 句だけで設定されたルートマップは、一致基準を満たすより具体的なルートを抑制します。ただし、ルートマップが match および set 句で設定されている場合、一致基準を満たすルートは、ルートマップによって変更された適切な属性でアドバタイズされま

	コマンドまたはアクション	目的
		す。2番目のオプションでは、より具体的なルートにコミュニティ属性を設定できます。

BGP ルートの抑制

新しく学習されたBGPルートが転送情報ベース（FIB）により確認され、ハードウェアでプログラミングされた後にのみ、これらのルートをアドバタイズするようにCisco NX-OSを設定できます。ルートがプログラミングされた後は、これらのルートに対する以降の変更にはこのハードウェア プログラミングのチェックは必要ありません。

BGP ルートを抑制するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**suppress-fib-pending** 例： `switch(config-router)# suppress-fib-pending`	新しく学習された BGP ルート（IPv4 ）がハードウェアでプログラミングされるまで、ダウンストリームの BGP ネイバーにアドバタイズされることを抑制します。

BGP 条件付きアドバタイズメントの設定

BGP がプロパゲートするルートを制限するように BGP 条件付きアドバタイズメントを設定できます。次の 2 つのルート マップを定義します。

- アドバタイズ マップ：BGP が条件付きアドバタイズメントを考慮する前にルートが一致する必要のある条件を指定します。このルートマップには、適切なmatch文を含めることができます。
- 存在マップまたは非存在マップ：BGP がアドバタイズ マップに一致するルートをプロパゲートする前に BGP テーブルに存在する必要のあるプレフィックスを定義します。非存在マップは、BGP がアドバタイズ マップに一致するルートをプロパゲートする前に BGP テーブルに存在してはならないプレフィックスを定義します。BGP は、これらのルートマップでプレフィックス リストの match 文内にある permit 文のみを処理します。

ルートが条件を渡さない場合、そのルートがBGPテーブルにあればBGPによってルートが取り消されます。

始める前に

BGP を有効にする必要があります（「BGP の有効化」の項を参照）。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**router bgp** *as-number*
	例：
	`switch(config)# router bgp 65535`
	`switch(config-router)#`
		BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。

ステップ 3	**neighbor** *ip-address* **remote-as** *as-number*
	例：
	`switch(config-router)# neighbor 192.168.1.2 remote-as 65534`
	`switch(config-router-neighbor)#`
		BGPルーティング用のネイバー設定モードを開始し、ネイバー IP アドレスを設定します。

ステップ 4	**address-family** {**ipv4**} {**unicast**}
	例：
	`switch(config-router-neighbor)# address-family ipv4 unicast`
	`switch(config-router-neighbor-af)#`
		アドレス ファミリ設定モードを開始します。

ステップ 5	**advertise-map** *adv-map* {**exist-map** *exist-rmap*|**non-exist-map** *nonexist-rmap*} 例： `switch(config-router-neighbor-af)# advertise-map advertise exist-map exist`	2 つの設定済みルート マップに従い、ルートを条件付きでアドバタイズするように BGP を設定します。 • *adv-map*：BGPがルートを次のルート マップに渡す前に、そのルートが渡す必要のある **match** 文を含むルート マップを指定します。*adv-map* には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。 • *exist-rmap*：プレフィックス リストの match ステートメントを使用してルート マップを指定します。BGP テーブル内のプレフィックスは、BGP がルートをアドバタイズする前に、プレフィックス リスト内のプレフィックスと一致する必要があ

	コマンドまたはアクション	目的
		ります。*exist-rmap* には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。 • *nonexist-rmap*：プレフィックス リストの match ステートメントを使用してルートマップを指定します。BGP テーブル内のプレフィックスは、BGP がルートをアドバタイズする前に、プレフィックス リスト内のプレフィックスと一致してはいけません。*nonexist-rmap* には最大 63 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 6	（任意） **show bgp** {**ipv4**} {**unicast**} **neighbors** 例： `switch(config-router-neighbor-af)# show ip bgp neighbor`	BGP に関する情報、および設定した条件付きアドバタイズメントのルートマップに関する情報を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config-router-neighbor-af)# copy running-config startup-config`	この設定変更を保存します。

例

次に、BGP 条件付きアドバタイズメントを設定する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# neighbor 192.0.2.2 remote-as 65537
switch(config-router-neighbor)# address-family ipv4 unicast
switch(config-router-neighbor-af)# advertise-map advertise exist-map exist
switch(config-router-neighbor-af)# exit
switch(config-router-neighbor)# exit
switch(config-router)# exit
switch(config)# route-map advertise
switch(config-route-map)# match as-path pathList
switch(config-route-map)# exit
switch(config)# route-map exit
switch(config-route-map)# match ip address prefix-list plist
switch(config-route-map)# exit
switch(config)# ip prefix-list plist permit 209.165.201.0/27
```

ルートの再配布の設定

別のルーティング プロトコルからのルーティング情報を受け入れて、BGP ネットワークを通じてその情報を再配布するように、BGP を設定できます。任意で、再配布ルートのためのデフォルト ルートを割り当てることができます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**router bgp** *as-number*
	例：
	`switch(config)# router bgp 65535`
	`switch(config-router)#`
		BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。

ステップ 3	**address-family ipv4** {**unicast**}
	例：
	`switch(config-router)# address-family ipv4 unicast`
	`switch(config-router-af)#`
		アドレス ファミリ設定モードを開始します。

ステップ 4	**redistribute** {**direct**| {**ospf** } *instance-tag* | **static**} **route-map** *map-name* 例： `switch(config-router-af)# redistribute ospf 201 route-map Ospfmap`	他のプロトコルからのルートを BGP に再配布します。

ステップ 5	（任意） **default-metric** *value*
	例：
	`switch(config-router-af)# default-metric`
	`33`
		BGP へのデフォルト ルートを生成します。

ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config-router-af)# copy running-config startup-config`	この設定変更を保存します。

例

次に、EIGRP を BGP に再配布する例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# redistribute ospf 201 route-map Ospfmap
switch(config-router-af)# copy running-config startup-config
```

デフォルト ルートのアドバタイズ

デフォルトのルート（ネットワーク 0.0.0.0）をアドバタイズするように BGP を設定できます。

始める前に

BGP をイネーブルにする必要があります（「BGP のイネーブル化」の項を参照）。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**route-map allow permit**
	例：
	`switch(config)# route-map allow permit`
	`switch(config-route-map)#`
		ルータのマップ コンフィギュレーション モードを開始し、ルートを再配布する条件を定義します。。

ステップ 3	**exit**
	例：
	`switch(config-route-map)# exit`
	`switch(config)#`
		ルータのマップ設定モードを終了します。

ステップ 4	**ip route** *ip-address network-mask* **null** *null-interface-number* 例： `switch(config)# ip route 192.0.2.1 255.255.255.0 null 0`	IP アドレスを設定します。

ステップ 5	**router bgp** *as-number*
	例：
	`switch(config)# router bgp 65535`
	`switch(config-router)#`
		BGP モードを開始し、AS 番号をローカルの BGP スピーカに割り当てます。

	コマンドまたはアクション	目的

ステップ 6	**address-family** {**ipv4**} **unicast**
	例：
	`switch(config-router)# address-family ipv4 unicast`
	`switch(config-router-af)#`
		アドレスファミリ設定モードに入ります。

ステップ 7	**default-information originate** 例： `switch(config-router-af)# default-information originate`	デフォルトのルートをアドバタイズします。
ステップ 8	**redistribute static route-map allow** 例： `switch(config-router-af)# redistribute static route-map allow`	デフォルトのルートを再配布します。
ステップ 9	（任意） **copy running-config startup-config** 例： `switch(config-router-af)# copy running-config startup-config`	この設定変更を保存します。

BGP 属性フィルタリングの設定とエラー処理

BGP属性フィルタリングとエラー処理を構成して、セキュリティ レベルを向上させることができます。次の機能を利用でき、次の順序で実装されます。

- **パス属性 treat-as-withdraw:** アップデートに指定した属性タイプが含まれている場合に、指定したネイバーから受け取った BGP アップデートを treat-as-withdraw とすることを許可します。アップデートに含まれるプレフィックスは、ルーティング テーブルから削除されます。
- **パス属性 discard:**BGP アップデートの特定のパス属性を特定のネイバーから削除できます。
- **拡張属性エラー処理:** 形式が誤っているアップデートに起因するピア セッションのフラッピングを防止します。

属性タイプ 1、2、3、4、8、14、15、16 は、パス属性 treat-as-withdraw とパス属性 discard に対して設定できません。属性タイプ 9（Originator）、タイプ 10（Cluster-id）は、eBGP ネイバーでのみ設定できます。

BGP 更新メッセージからのパス属性の取り消しとしての処理

特定のパス属性を含むBGP更新を「扱うように」処理するには、ルータネイバーコンフィギュレーションモードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的

ステップ 1	[**no**] **path-attribute treat-as-withdraw** [*value* | **range** *start end*] **in**
	例：
	`switch#(config-router)# neighbor 10.20.30.40`
	`switch(config-router-neighbor)# path-attribute treat-as-withdraw 100 in`
	例：
	`switch#(config-router)# neighbor 10.20.30.40`
	`switch(config-router-neighbor)# path-attribute treat-as-withdraw range 21 255 in`
		指定されたパス属性またはパス属性の範囲を含む着信BGP更新メッセージをすべて取り消すものとして扱い、ルーティングテーブルが最新であることを確認するために着信ルートリフレッシュをトリガーします。treat-as-withdraw であるBGP更新のプレフィックスは、BGPルーティング テーブルから削除されます。
		このコマンドは、BGP テンプレート ピアおよびBGP テンプレート ピア セッションでもサポートされます。

BGP 更新メッセージからのパス属性の破棄

特定のパス属性を含むBGP アップデートを廃棄するには、ルータ ネイバー コンフィギュレーション モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的

ステップ 1	[**no**] **path-attribute discard** [*value* | **range** *start end*] **in**
	例：
	`switch#(config-router)# neighbor 10.20.30.40`
	`switch(config-router-neighbor)# path-attribute discard 100 in`
	例：
	`switch#(config-router)# neighbor 10.20.30.40`
	`switch(config-router-neighbor)# path-attribute discard range 100 255 in`
		指定されたネイバーの BGP アップデート メッセージ内の指定されたパス属性をドロップし、ルーティング テーブルが最新であることを確認するために着信ルートリフレッシュをトリガーします。特定の属性または不要な属性の範囲全体を設定できます。
		このコマンドは、BGP テンプレート ピアおよびBGP テンプレート ピア セッションでもサポートされます。
		（注） discard と treat-as-withdaw の両方に同じパス属性が設定されている場合、treat-as-withdaw の優先順位が高くなります。

拡張属性エラー処理のイネーブル化またはディセーブル化

BGP拡張属性エラー処理はデフォルトで有効になっていますが、無効にすることもできます。この機能は、RFC 7606 に準拠しており、不正な更新によるピア セッションのフラッピングを防止します。デフォルトの動作は、eBGP ピアと iBGP ピアの両方に適用されます。

拡張エラー処理を無効または再度有効にするには、ルータ設定モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的

ステップ 1	[**no**] **enhanced-error**
	例：
	`switch(config)# router bgp 1000`
	`switch(config-router)# enhanced-error`
		BGP 拡張属性エラー処理をいネーブルまたはディセーブルにします。

取り消されたパス属性または破棄されたパス属性の表示

廃棄または不明なパス属性に関する情報を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show bgp {**ipv4** } **unicast path-attribute discard**]	属性が破棄されたすべてのプレフィックスを表示します。
show bgp {**ipv4** } **unicast path-attribute unknown**]	不明な属性を持つすべてのプレフィックスを表示します。
show bgp {**ipv4** } **unicast** *ip-address*	プレフィックスに関連付けられている不明な属性および破棄された属性を表示します。

次の例は、属性が廃棄されたプレフィックスを示しています。

```
switch# show bgp ipv4 unicast path-attribute discard
Network            Next Hop
1.1.1.1/32         20.1.1.1
1.1.1.2/32         20.1.1.1
1.1.1.3/32         20.1.1.1
```

次の例は、不明な属性を持つプレフィックスを示しています。

```
switch# show bgp ipv4 unicast path-attribute unknown
Network            Next Hop
2.2.2.2/32         20.1.1.1
2.2.2.3/32         20.1.1.1
```

次の例は、プレフィックスに関連付けられている不明な属性および破棄された属性を表示します。

```
switch# show bgp ipv4 unicast 2.2.2.2
BGP routing table entry for 2.2.2.2/32, version 6241
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  1000
    20.1.1.1 from 20.1.1.1 (20.1.1.1)
      Origin IGP, localpref 100, valid, external, best
      unknown transitive attribute: flag 0xE0 type 0x62 length 0x64
        value 0000 0000 0100 0000 0200 0000 0300 0000
              0400 0000 0500 0000 0600 0000 0700 0000
              0800 0000 0900 0000 0A00 0000 0B00 0000
              0C00 0000 0D00 0000 0E00 0000 0F00 0000
              1000 0000 1100 0000 1200 0000 1300 0000
              1400 0000 1500 0000 1600 0000 1700 0000
              1800 0000
      rx pathid: 0, tx pathid: 0x0
      Updated on Jul 20 2019 07:50:43 PST
```

BGP の調整

一連のオプション パラメータを使用することによって、BGP 特性を調整できます。

BGP を調整するには、ルータ コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
bestpath [**always-compare-med** | **as-pathmultipath-relax** | **compare-routerid** |**cost-community ignore** | **igp-metric ignore** |**med** {**confed** |**missing-as-worst**| **non-deterministic**}] 例： `switch(config-router)# bestpath always-compare-med` （注） BGP が ECMP ルートを計算する場合、次の場所にインストールされます。 ユニパスとしての Cisco Nexus 3550-T ハードウェアと、「ECMP のインストールに失敗しました」という警告システム ログが生成されます。	ベストパス アルゴリズムを変更します。オプション パラメータは次のとおりです。 • **always-compare-med** ：異なる自律システム（AS）からのパスの MED を比較します。 • **as-path multipath-relax** ：異なる（ただし長さが等しい）AS パスを持つプロバイダー間でのロード シェアリングを許可します。このオプションを指定しないと、AS パスはロードシェアリングの場合に同一である必要があります。 • **compare-routerid** ：同一の eBGP パスのルータ ID を比較します。 • **cost-community ignore** ：BGP ベストパス計算のコストコミュニティを無視します。 • **igp-metric ignore** ：ベスト パス選択時に内部ゲートウェイ プロトコル（IGP）メトリックを無視します。 • **med confed** ：コンフェデレーション内からのパス間のみで MED を比較するように最適なパスを強制します。 • **med missing-as-worst** ：消失 MED を最高の MED と見なします。 • **med non-deterministic** ：同じ自律システムからのパスの中から最適な MED パスを決して選択しません。
enforce-first-as 例： `switch(config-router)# enforce-first-as`	ネイバー自律システムを eBGP の AS_path 属性で指定する最初の AS 番号にします。

コマンド	目的
log-neighbor-changes 例： `switch(config-router)# log-neighbor-changes`	ネイバーでステートが変化したときに、システム メッセージを生成します。 （注） 特定のネイバーのネイバー ステータス変化に関するメッセージを抑制するには、ルータ アドレスファミリ コンフィギュレーション モードで **log-neighbor-changes disable** コマンドを使用できます。
router-id *id* 例： `switch(config-router)# router-id 10.165.20.1`	この BGP スピーカのルータ ID を手動で設定します。
timers [**bestpath-delay** *delay* | *bgpkeepalive holdtime* | **prefix-peer-timeout** *timeout*] 例： `switch(config-router)# timers bgp 90 270`	BGP タイマー値を設定します。オプション パラメータは次のとおりです。 • *delay*：再起動後の初期最適パス タイムアウト値。有効な範囲は 0 ～ 3600 秒です。デフォルト値は 300 です。 • *keepalive* ：BGP セッション キープアライブ タイム。有効な範囲は 0 ～ 3600 秒です。デフォルト値は 60 です。 • *holdtime* ：BGP セッションの保持時間。指定できる範囲は 0 ～ 3600 秒です。デフォルト値は 180 です。 • *timeout*：プレフィックス ピア タイムアウト値。有効な範囲は 0 ～ 1200 秒です。デフォルト値は 30 です。 このコマンドの設定後、BGP セッションを手動でリセットする必要があります。

BGP を調整するには、ルータ アドレス ファミリ設定モードで次のオプション コマンドを使用します。

コマンド	目的
distance *ebgp-distance ibgp-distance local-distance* **例：** `switch(config-router-af)# distance 20 100 200`	BGP のアドミニストレーティブディスタンスを設定します。範囲は 1 ～ 255 です。デフォルトの設定は次のとおりです。 • *ebgp-distance* —20 • *ibgp-distance* —200 • *local-distance* —220 ローカル ディスタンスは、集約廃棄ルートが RIB に組み込まれている場合に、集約廃棄ルートに使用するアドミニストレーティブディスタンスです。 外部アドミニストレーティブディスタンスの値を入力したら、要件に応じて内部ルートのアドミニストレーティブディスタンスの値またはローカル ルートのアドミニストレーティブディスタンスの値を入力する必要があります。内部/ローカル ルートもルート管理で考慮されます。
log-neighbor-changes [**disable**] **例：** `switch(config-router-af)# log-neighbor-changes disable`	この特定のネイバーの状態が変化すると、システム メッセージを生成します。 **disable** オプションを使用すると、この特定のネイバーのネイバー ステータス変化に関するメッセージが抑制されます。

BGP を調整するには、ネイバー コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
description *string* **例：** `switch(config-router-neighbor)# description main site`	この BGP ピアを説明するストリングを設定します。ストリングには最大 80 の英数字を使用できます。
low-memory exempt **例：** `switch(config-router-neighbor)# low-memory exempt`	メモリ不足状態によるシャットダウンからこの BGP ネイバーを除外します。

コマンド	目的
transport connection-mode passive 例： `switch(config-router-neighbor)# transport connection-mode passive`	受動接続の確立だけが可能です。このBGPスピーカはBGP ピアへの TCP 接続を開始しません。このコマンドの設定後、BGPセッションを手動でリセットする必要があります。
[**no** | **default**] **remove-private-as** [**all** | **replace-as**] 例： `switch(config-router-neighbor)# remove-private-as`	eBGP ピアへの発信ルート アップデートからプライベート AS 番号を削除します。このコマンドによって、BGPネイバーセッションの自動ソフトクリアまたはリフレッシュが開始されます。 オプション パラメータは次のとおりです。 • **no** ：コマンドをディセーブルにします。 • **default** ：デフォルト モードにコマンドを移動します。 • **all** ：AS パスからすべてのプライベート AS 番号を削除します。 • **replace-as** ：すべてのプライベートAS番号を replace-as AS-path 値に置き換えます。 このコマンドの詳細については、拡張BGPに関する注意事項と制限事項 （333 ページ）を参照してください。
update-source *interface-type number* 例： `switch(config-router-neighbor)# update-source ethernet 1/1`	ピアとのBGPセッション用に設定されたインターフェイスの送信元IPアドレスを使用するように、BGPスピーカを設定します。このコマンドによって、BGPネイバーセッションの自動通知およびセッション リセットが開始されます。単一ホップ iBGP ピアでは、**update-source** が設定されている場合に、高速外部フォールオーバーをサポートします。

BGPを調整するには、ネイバー アドレス ファミリ コンフィギュレーション モードで次のオプション コマンドを使用します。

コマンド	目的
allowas in 例： `switch(config-router-neighbor-af)# allowas in`	BRIP にインストールする AS パスにルート自体の AS を持つことを可能にします。

コマンド	目的
default-originate [**route-map** *map-name*] 例： `switch(config-router-neighbor-af)# default-originate`	BGP ピアへのデフォルト ルートを作成します。
disable-peer-as-check 例： `switch(config-router-neighbor-af)# disable-peer-as-check`	デバイスが同じASパスで一方のノードからもう一方のノードに学習されたルートをアドバタイズすると同時に、ピアAS番号のチェックをディセーブルにします。
filter-list *list-name* {**in** | **out**} 例： `switch(config-router-neighbor-af)# filter-list BGPFilter in`	着信または発信ルートアップデートに関して、このBGPピアにAS_pathフィルタ リストを適用します。このコマンドによって、BGP ネイバーセッションの自動ソフトクリアまたはリフレッシュが開始されます。
prefix-list *list-name* {**in** | **out**} 例： `switch(config-router-neighbor-af)# prefix-list PrefixFilter in`	着信または発信ルートアップデートに関して、このBGPピアにプレフィックスリストを適用します。このコマンドによって、BGPネイバーセッションの自動ソフトクリアまたはリフレッシュが開始されます。
send-community 例： `switch(config-router-neighbor-af)# send-community`	このBGPピアにコミュニティ属性を送信します。このコマンドによって、BGP ネイバーセッションの自動ソフトクリアまたはリフレッシュが開始されます。
send-community extended 例： `switch(config-router-neighbor-af)# send-community extended`	このBGPピアに拡張コミュニティ属性を送信します。このコマンドによって、BGPネイバーセッションの自動ソフトクリアまたはリフレッシュが開始されます。
suppress-inactive 例： `switch(config-router-neighbor-af)# suppress-inactive`	ベスト（アクティブ）ルートだけをBGPピアにアドバタイズします。このコマンドによって、BGPネイバーセッションの自動ソフトクリアまたはリフレッシュが開始されます。
[no | default] as-override 例： `switch(config-router-neighbor-af)# as-override`	**no**-（オプション）コマンドを無効にします。 **default**：（オプション）デフォルトモードにコマンドを移動します。 **as-override**：eBGP ピアに更新を送信する際に、パス属性内のピアのAS番号をすべてローカル AS 番号に置き換えます。

ポリシーベースのアドミニストレーティブディスタンスの設定

設定されたルートマップで説明されているポリシーに一致する外部BGP（eBGP）と内部BGP（iBGP）の距離を設定できます。ルート マップで設定された距離は、一致するルートとともにユニキャストRIBにダウンロードされます。BGPは最適パスを使用して、ユニキャストRIBテーブルのネクスト ホップをダウンロードするときのアドミニストレーティブ ディスタンスを決定します。ポリシーに match 句または deny 句がない場合、BGP は distance コマンドで設定された距離またはルートのデフォルトの距離を使用します。

ポリシーベースのアドミニストレーティブディスタンス機能は、2つの異なるルーティングプロトコルから同じ宛先に 2 つ以上のルートが存在する場合に役立ちます。

始める前に

BGP を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip prefix-list** *name* **seq** *number* **permit** *prefix-length*	permit キーワードを使用して、IP パケットまたはルートを照合するためのプレフィクス リストを作成します。
ステップ 3	switch(config)# **route-map** *map-tag* **permit** *sequence-number*	permit キーワードを使用してルート マップを作成し、ルート マップ コンフィギュレーション モードを開始します。ルートの一致基準がポリシー内で満たされると、パケットはポリシーでルーティングされます。
ステップ 4	switch(config-route-map)# **match ip address prefix-list** *prefix-list-name*	プレフィクス リストに基づいて IPv4 ネットワーク ルートを照合します。プレフィクス リスト名には最大 63 文字の英数字を使用できます。
ステップ 5	switch(config-route-map)# **set distance** *value1 value2 value3*	ローカル自律システムから発信される内部 BGP（iBGP）または外部 BGP（eBGP）ルートおよび BGP ルートのアドミニストレーティブディスタンスを指定します。範囲は 1 ～ 255 です。

	コマンドまたはアクション	目的
		外部アドミニストレーティブディスタンスの値を入力したら、要件に応じて内部ルートのアドミニストレーティブディスタンスの値またはローカルルートのアドミニストレーティブディスタンスの値を入力する必要があります。内部/ローカルルートもルート管理で考慮されます。
ステップ 6	switch(config-route-map)# **exit**	ルート マップ設定モードを終了します。
ステップ 7	switch(config)# **router bgp** *as-number*	BGP モードを開始し、AS 番号をローカルの BGP スピーカに割り当てます。
ステップ 8	switch(config-router)# **address-family** {**ipv4** | **vpnv4**} **unicast**	アドレス ファミリ設定モードを開始します。
ステップ 9	switch(config-router-af)# **table-map** *map-name*	BGP ルートを RIB テーブルに転送する前にそのルートのルートマップの選択的アドミニストレーティブディスタンスを設定します。テーブルマップ名には最大 63 文字の英数字を使用できます。 （注） VRF アドレスファミリ設定モードで **table-map** コマンドを設定することもできます。
ステップ 10	（任意） switch(config-router-af)# **show forwarding distribution**	フォワーディング情報の配布を表示します。
ステップ 11	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

マルチプロトコル BGP の設定

複数のアドレス ファミリ（IPv4 のユニキャストおよびマルチキャスト ルートを含む）をサポートするように MP-BGP を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**router bgp** *as-number*
	例：
	`switch(config)# router bgp 65535`
	`switch(config-router)#`
		BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。

ステップ 3	**neighbor** *ip-address* **remote-as** *as-number*
	例：
	`switch(config-router)# neighbor 192.168.1.2 remote-as 65534`
	`switch(config-router-neighbor)#`
		BGP ルーティング用のネイバー設定モードを開始し、ネイバー IP アドレスを設定します。

ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config-router-neighbor-af)# copy running-config startup-config`	この設定変更を保存します。

例

BMP の設定

Cisco Nexus® 3550-T デバイスで BMP を構成できます。

始める前に

BGP をイネーブルにする必要があります（「BGP のイネーブル化」の項を参照）。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的

ステップ 2	**router bgp as-number**
	例：
	`switch(config)# router bgp 200`
	`switch(config-router)#`
		BGP モードを開始し、ローカル BGP スピーカに自律システム番号を割り当てます。

ステップ 3	**bmp server** *server-number* 例： `switch(config-router)# bmp server 1`	BGP が情報を送信する BMP サーバを設定します。サーバ番号がキーとして使用されます。 （注） 最大 2 つの BMP サーバを設定できます。
ステップ 4	**address ip-address port-number port-number** 例： `switch(config-router)# address 10.1.1.1 port-number 2000`	ホストの IPv4 アドレスと、BMP スピーカーが BMP サーバーに接続するポート番号を構成します。
ステップ 5	**description** *string* 例： `switch(config-router)# description BMPserver1`	BMP サーバの説明を設定します。最大 256 文字の英数字を入力できます。
ステップ 6	**initial-refresh** { *skip* | *delay time*} 例： `switch(config-router)# initial-refresh delay 100`	BGP がコンバージされ、後で BMP サーバ接続が確立されたときにルートリフレッシュを送信するオプションを設定します。 skip オプションは、BMP サーバ接続が後でアップした場合にルートリフレッシュを送信しないことを指定します。 delay オプションは、ルート更新を送信するまでの時間を秒単位で指定します。有効範囲は 30 ～ 720 秒で、デフォルトは 30 秒です。
ステップ 7	**initial-delay** *time* 例： `switch(config-router)# initial-delay 120`	BMP サーバへの接続が試行されるまでの遅延を設定します。有効範囲は 30 ～ 720 秒で、デフォルトは 45 秒です。
ステップ 8	**stats-reporting-period** *time* 例： `switch(config-router)# stats-reporting-period 50`	BMP サーバが BGP ネイバーから統計レポートを受信する時間間隔を設定します。有効範囲は 30 ～ 720 秒で、デフォルトはディスエーブルです。

	コマンドまたはアクション	目的
ステップ 9	shutdown 例： `switch(config-router)# shutdown`	BMP サーバへの接続を無効にします。

ステップ 10	**neighbor ip-address**
	例：
	`switch(config-router)# neighbor 192.168.1.2`
	`switch(config-router-neighbor)#`
		BGP ルーティング用のネイバー コンフィギュレーション モードを開始し、ネイバー IP アドレスを設定します。

ステップ 11	**remote-as** *as-number* 例： `switch(config-router-neighbor)# remote-as 65535`	リモート BGP ピアの AS 番号を設定します。
ステップ 12	**bmp-activate-server** *server-number* 例： `switch(config-router-neighbor)# bmp-activate-server 1`	ネイバーの情報の送信先となる BMP サーバを設定します。
ステップ 13	（任意） **show bgp bmp** *server [server-number] [detail]* 例： `switch(config-router-neighbor)# show bgp bmp server`	BMP サーバ情報を表示します。
ステップ 14	（任意） **copy running-config startup-config** 例： `switch(config-router-neighbor)# copy running-config startup-config`	この設定変更を保存します。

BGP グレース フル シャットダウンに関する情報

BGP はグレースフル シャットダウン機能をサポートしています。この BGP 機能は、BGP **shutdown** コマンドと連携して次のことを行います。

- ルータまたはリンクがオフラインになったときのネットワーク コンバージェンス時間を大幅に短縮します。
- ルータまたはリンクがオフラインになったときに、転送中のドロップされたパケットを削減または排除します。

名前にかかわらず、BGP グレースフル シャットダウンは実際にはシャットダウンを引き起こしません。代わりに、ルータまたはリンクが間もなくダウンすることを、接続されているルータに通知します。

グレースフル シャットダウン機能は、GRACEFUL_SHUTDOWN ウェルノウン コミュニティ（0xFFFF0000 または 65535:0）を使用します。これは、IANA および IETF によって RFC 8326 によって識別されます。この既知のコミュニティは任意のルートにアタッチでき、ルートの他の属性と同様に処理されます。

この機能は、ルータまたはリンクがダウンすることを通知するため、メンテナンス時間帯または計画停止の準備に役立ちます。トラフィックへの影響を制限するには、BGP をシャットダウンする前にこの機能を使用します。

グレースフル シャットダウンの認識とアクティブ化

BGPルータは、すべてのルートの優先事項を、GRACEFUL SHUTDOWN 対応というコンセプトを通し、GRACEFUL_SHUTDOWN コミュニティによって制御できます。グレースフル シャットダウン対応は、デフォルトでイネーブルになっています。これにより、受信側ピアは、GRACEFUL_SHUTDOWN コミュニティを伝える着信ルートを優先しなくなります。一般的な使用例ではありませんが、**graceful-shutdown aware** コマンドを使用して、グレースフル シャットダウン対応を無効にしてから再度有効にすることもできます。

グレースフル シャットダウン対応は、BGP グローバル コンテキストでのみ適用されます。コンテキストの詳細については、グレースフル シャットダウンのコンテキスト（384 ページ）を参照してください。対応のためのオプションは、**activate** という別のオプションと一緒に動作します。このオプションをルートマップに割り当てると、グレースフル シャットダウンのルートをより詳細に制御できます。

グレースフル シャットダウン対応オプションとアクティブ化オプションの協同作用

グレースフル シャットダウンがアクティブな場合、**activate** キーワードを指定した場合にのみ、GRACEFUL_SHUTDOWN コミュニティがルート更新に追加されます。この時点で、コミュニティを含む新しいルート更新が生成され、送信されます。**graceful-shutdown aware** コマンドが設定されると、コミュニティを受信するすべてのルータは、アップデート内のルートの優先を解除します（そのルート優先度を下げます）。**graceful-shutdown aware** コマンドを使用しなかった場合、BGPはGRACEFUL_SHUTDOWN コミュニティの設定されたルートの優先度を下げません。

この機能がアクティブになり、ルータがグレースフル シャットダウンの対応状態になった場合でも、BGP は引き続き、GRACEFUL_SHUTDOWN コミュニティが有効だとしてルートを考慮します。ただし、これらのルートには、最適パスの計算で最低の優先度が与えられます。代替パスが使用可能な場合は、新しい最適パスが選択され、まもなくダウンするルータまたはリンクに対応するためのコンバージェンスが行われます。

グレースフル シャットダウンのコンテキスト

BGPのグレースフルシャットダウン機能には、機能の影響と使用可能な機能を決定する2つのコンテキストがあります。

コンテキスト	影響	コマンド
グローバル	スイッチ全体と、スイッチによって処理されるすべてのルート。たとえば、GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートを再アドバタイズします。	**graceful-shutdown activate [route-map** ルート マップ**]** **graceful-shutdown aware**
Peer	BGP ピアまたはネイバー間のリンク。たとえば、ピア間のリンクを 1 つだけ GRACEFUL_SHUTDOWNコミュニティでアドバタイズします。	**graceful-shutdown activate [route-map** ルート マップ**]**

ルート マップによるグレースフル シャットダウン

グレースフル シャットダウンは、ルート ポリシー マネージャ（RPM）機能と連携して、スイッチの BGP ルータが GRACEFUL_SHUTDOWN コミュニティを使用してルートを送受信する方法を制御します。ルート マップは、インバウンドおよびアウトバウンド方向でコミュニティとのルート更新を処理できます。通常、ルートマップは必要ありません。ただし、必要に応じて、グレースフルシャットダウンルートの制御をカスタマイズするために使用できます。

通常のインバウンド ルート マップ

通常のインバウンド ルート マップは、BGP ルータに着信するルートに影響します。ルータはデフォルトでグレースフル シャットダウンを認識するため、通常のインバウンド ルート マップはグレースフル シャットダウン機能では一般的に使用されません。

Cisco Nexus® スイッチでは、グレースフル シャットダウン機能のインバウンド ルート マップは必要ありません。Cisco NX-OS スイッチには、BGPルータがグレースフルシャットダウン対応である場合にGRACEFUL_SHUTDOWNコミュニティを持つすべてのルートを自動的に非優先にする、暗黙のインバウンドルート マップがあります。

通常のインバウンド ルート マップは、既知の GRACEFUL_SHUTDOWN コミュニティと一致するように設定できます。これらの着信ルートマップは一般的ではありませんが、使用される場合があります。

- スイッチが暗黙のインバウンド ルート マップを持たない Cisco NX-OS リリースを実行している場合、グレースフル シャットダウン インバウンド ルート マップは、これらのスイッチでグレースフル シャットダウン機能を使用します。ルート マップは、既知の GRACEFUL_SHUTDOWN コミュニティを持つインバウンドルートと一致し、それらを許可し、それらを非優先にする必要があります。インバウンド ルート マップが必要な場合は、互換性があるバージョンの NX-OS を実行中で、グレースフル シャットダウン ルートを受信している BGP ピアで作成します。
- グレースフル シャットダウン認識をディセーブルにし、一部の BGP ネイバーからの GRACEFUL_SHUTDOWN コミュニティを持つ着信ルートでルータを動作させる場合は、それぞれのピアでインバウンド ルート マップを設定できます。

通常のアウトバウンド ルート マップ

通常のアウトバウンド ルート マップは、BGP ルータが送信するルートの転送を制御します。通常のアウトバウンド ルート マップは、グレースフル シャットダウン機能に影響を与える可能性があります。たとえば、GRACEFUL_SHUTDOWN コミュニティで一致するようにアウトバウンド ルート マップを設定し、属性を設定できます。これは、グレースフル シャットダウン アウトバウンド ルート マップよりも優先されます。

グレースフル シャットダウン アウトバウンド ルート マップ

アウトバウンド グレースフル シャットダウン ルートマップは、グレースフル シャットダウン機能のアウトバウンド ルート マップの特定のタイプです。これらはオプションですが、ルート マップに関連付けられているコミュニティ リストがすでにある場合に役立ちます。通常のグレースフル シャットダウン アウトバウンド ルート マップには、特定の属性を設定または変更するための `set` 句のみが含まれています。

アウトバウンド ルート マップは、次の方法で使用できます。

- 既存のアウトバウンド ルート マップをすでに持っている顧客の場合は、より大きいシーケンス番号を持つ新しいエントリを追加し、GRACEFUL_SHUTDOWN ウェルノウンコミュニティで照合し、必要な属性を追加できます。
- **graceful-shutdown activate route-map** *name* オプションを使用してグレースフル シャットダウン アウトバウンドルート マップを使用することもできます。これが一般的な使用例です。

  このルート マップには match 句が必要ないため、ルート マップはネイバーに送信されるすべてのルートで一致します。

ルート マップの優先順位

同じルータ上に複数のルートマップが存在する場合は、次の優先順位が適用されて、コミュニティとのルートの処理方法が決定されます。次の例を考慮してください。60 のローカル設定を設定する標準の発信ルートマップ名 Red があるとします。また、Blue という名前のピア グレースフル シャットダウン ルートマップがあり、local-pref が 30 に設定されているとします。ルー

ト更新が処理されると、Red は Blue を上書きするため、ローカル プリファレンスは 60 に設定されます。

- 通常の発信ルート マップは、ピア グレースフル シャットダウン マップよりも優先されます。
- ピア グレースフル シャットダウン マップは、グローバル グレースフル シャットダウン マップよりも優先されます。

ガイドラインと制約事項

BGP グローバル シャットダウンの制限事項と注意事項は、次のとおりです。

- グレースフル シャットダウン機能は、影響を受けるルータの代替ルートがネットワークに存在する場合にのみ、トラフィック損失を回避するのに役立ちます。ルータに代替ルートがない場合は、GRACEFUL_SHUTDOWN コミュニティを伝送するルートが使用可能な唯一のルートであるため、最適パスの計算に使用されます。この状況では、機能の目的が失われます。
- GRACEFUL_SHUTDOWN コミュニティを送信するには、BGP 送信コミュニティの設定が必要です。
- ルート マップの場合:
  - グローバル ルート マップとネイバー ルート マップが設定されている場合、ネイバー単位のルート マップが優先されます。
  - 発信ルート マップは、グレースフル シャットダウン用に設定されたグローバル ルート マップよりも優先されます。
  - 発信ルート マップは、グレースフル シャットダウン用に設定されたピア ルート マップよりも優先されます。
  - レガシー（既存の）インバウンド ルート マップにグレースフル シャットダウン機能を追加するには、次の手順を実行します。
    1. graceful shutdown match 句をルート マップの先頭に追加します。これには、句に低いシーケンス番号（たとえば、シーケンス番号 0）を設定します。
    2. graceful shutdown 句の後に continue ステートメントを追加します。continue ステートメントを省略すると、graceful shutdown 句と一致するルートマップ処理が停止します。シーケンス番号が大きい他の句（たとえば、1以上）は処理されません。

グレースフル シャットダウン タスクの概要

グレースフル シャットダウン機能を使用するには、通常、すべての Cisco Nexus スイッチでグレースフル シャットダウン対応をイネーブルにし、機能をイネーブルのままにします。BGP ルータをオフラインにする必要がある場合は、graceful-shutdown activate を設定します。

次の詳細に、グレースフル シャットダウン機能を使用するためのベスト プラクティスを示します。

ルータまたはリンクをダウンさせるには、次の手順を実行します。

1. グレースフル シャットダウン機能を設定します。
2. ネイバーでベスト パスを確認します。
3. 最適パスが再計算されたら、BGP を無効にする **shutdown** コマンドを発行します。
4. ルータまたはリンクをシャットダウンする必要がある作業を実行します。

ルータまたはリンクをオンラインに戻すには、次の手順を実行します。

1. シャットダウンが必要な作業が完了したら、BGP を再度イネーブルにします（**no shutdown**）。
2. グレースフル シャットダウン機能を無効にします（config モードの **no graceful-shutdown activate**）。

リンクのグレースフル シャットダウンの設定

この作業では、2 つの BGP ルータ間の特定のリンクでグレースフル シャットダウンを設定できます。

始める前に

BGP をまだ有効にしていない場合は、ここで有効にします（**feature bgp**）。

手順

	コマンドまたはアクション	目的

ステップ 1	**config terminal**
	例：
	`switch-1# configure terminal`
	`switch-1(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	**router bgp** *autonomous-system-number*
	例：
	`switch-1(config)# router bgp 110`
	`switch-1(config-router)#`
		ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。

ステップ 3	**neighbor {** *ipv4-address*} **remote-as** *as-number*
	例：
	`switch-1(config-router)# neighbor 10.0.0.3 remote-as 200`
	`switch-1(config-router-neighbor)#`
		ネイバーが属する自律システム（AS）を設定します。

ステップ 4	**graceful-shutdown activate [route-map** *map-name***]**
	例：
	`switch-1(config-router-neighbor)# graceful-shutdown activate route-map gshutPeer out`
	`switch-1(config-router-neighbor)#`
		ネイバーへのリンクでグレースフル シャットダウンを設定します。また、既知の GRACEFUL_SHUTDOWN コミュニティを使用してルートをアドバタイズし、アウトバウンド ルート更新にルートマップを適用します。
		ルートは、デフォルトでグレースフル シャットダウン コミュニティでアドバタイズされます。この例では、ルートは gshutPeer という名前のルート マップを使用して、グレースフル シャットダウン コミュニティを持つネイバーにアドバタイズされます。
		gshut コミュニティを受信したデバイスは、ルートのコミュニティを確認し、オプションでコミュニティを使用してルーティング ポリシーを適用します。

GRACEFUL_SHUTDOWN コミュニティに基づく BGP ルートのフィルタリングとローカルプリファレンスの設定

スイッチには、GRACEFUL_SHUTDOWN コミュニティ名と一致するインバウンドルートマップがありません。したがって、正しいルートを識別して先送りする方法はありません。

NX-OS のリリースを実行しているスイッチでは、グレースフル シャットダウン（65535:0）のコミュニティ値と一致するインバウンド ルート マップを構成し、ルートを非優先にする必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch-1# configure terminal`
	`switch-1<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 community list standard** *community-list-name* **seq** *sequence-number* **{ permit | deny }** *value*
	例：
	`switch-1(config)# ip community-list standard GSHUT seq 10 permit 65535:0`
	`switch-1(config)#`
		コミュニティ リストを設定し、よく知られたグレースフル シャットダウン コミュニティ値を持つルートを許可または拒否します。

ステップ 3	**route map** *map-tag* **{deny | permit}** *sequence-number*
	例：
	`switch-1(config)# route-map RM_GSHUT permit 10`
	`switch-1(config-route-map)#`
		ルート マップをシーケンス 10 として設定し、GRACEFUL_SHUTDOWN コミュニティを持つルートを許可します。

ステップ 4	**match community** *community-list-name*
	例：
	`switch-1(config-route-map)# match community GSHUT`
	`switch-1(config-route-map)#`
		IP コミュニティ リスト GSHUT に一致するルートがルート ポリシー マネージャ（RPM）により処理されるように設定します。

ステップ 5	**set local-preference** *local-pref-value*
	例：
	`switch-1(config-route-map)# set local-preference 10`
	`switch-1(config-route-map)#`
		IP コミュニティ リスト GSHUT に一致するルートに、指定されたローカルプリファレンスが与えられるように設定します。

ステップ 6	**exit**
	例：
	`switch-1(config-route-map)# exit`
	`switch-1(config)#`
		ルートマップ設定モードを終了し、グローバル設定モードに戻ります。

ステップ 7	**router bgp** *community-list-name*
	例：
	`switch-1(config)# router bgp 100`
	`switch-1(config-router)#`
		ルータ設定モードを開始し、BGP インスタンスを作成します。

ステップ 8	**neighbor {** *ipv4-address* **}** 例：	指定したネイバーのルート BGP ネイバー モードを開始します。

	コマンドまたはアクション	目的
	`switch-1(config-router)# neighbor 10.0.0.3` `switch-1(config-router-neighbor)#`	

ステップ 9	**address-family {** *address-family sub family* **}**
	例：
	`nxosv2(config-router-neighbor)# address-family ipv4 unicast`
	`nxosv2(config-router-neighbor-af)#`
		ネイバーをアドレスファミリ（AF）設定モードにします。

ステップ 10	**send community**
	例：
	`nxosv2(config-router-neighbor-af)# send-community`
	`nxosv2(config-router-neighbor-af)#`
		ネイバーとの BGP コミュニティ交換を可能にします。

ステップ 11	**route map** *map-tag* **in**
	例：
	`nxosv2(config-router-neighbor-af)# route-map RM_GSHUT in`
	`nxosv2(config-router-neighbor-af)#`
		ネイバーからの着信ルートにルートマップを適用します。この例では、RM_GSHUT という名前のルート マップは、ネイバーからの GRACEFUL_SHUTDOWN コミュニティを持つルートを許可します。

すべての BGP ネイバーのグレースフル シャットダウンの設定

グレースフル シャットダウン イニシエータのすべてのネイバーに GRACEFUL_SHUTDOWN ウェルノウン コミュニティを手動で適用できます。

すべての BGP ネイバーに対して、グローバル レベルでグレースフル シャットダウンを設定できます。

始める前に

BGP をまだ有効にしていない場合は、ここで有効にします（**feature bgp**）。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch-1# configure terminal`
	`switch-1(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	**router bgp** *autonomous-system-number*
	例：
	`switch-1(config)# router bgp 110`
	`switch-1(config-router)#`
		ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。

ステップ 3	**graceful-shutdown activate [route-map** *map-name***]**
	例：
	`switch-1(config-router-neighbor)# graceful-shutdown activate route-map gshutPeer`
	`switch-1(config-router-neighbor)#`
		すべてのネイバーへのリンクのグレースフル シャットダウン ルート マップを設定します。また、既知の GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートをアドバタイズし、ルートマップをアウトバウンドルート アップデートに適用します。
		ルートはデフォルトで GRACEFUL_SHUTDOWN コミュニティでアドバタイズされます。この例では、ルートが gshutPeer という名前のルートマップを持つコミュニティを持つすべてのネイバーにアドバタイズされます。ルートマップには set 句のみを含める必要があります。
		GRACEFUL_SHUTDOWN コミュニティを受信したデバイスは、ルートのコミュニティを確認し、オプションでコミュニティを使用してルーティング ポリシーを適用します。

GRACEFUL_SHUTDOWN コミュニティを使用したすべてのルートのプリファレンスの制御

Cisco NX-OS では、GRACEFUL_SHUTDOWN コミュニティを持つ着信ルートの優先順位を下げることができます。**graceful shutdown aware** が有効になっている場合、最適パス計算時に、BGP はコミュニティを伝送するルートを最も低い優先順位と見なします。デフォルトでは、プレファレンスの引き下げが有効になっていますが、このオプションを選択的に無効にすることもできます。

このオプションをイネーブルまたはディセーブルにするたびに、BGP のベストパス計算がトリガーされます。このオプションを使用すると、グレースフル シャットダウンのウェルノウンコミュニティにおける BGP のベストパス計算の動作を柔軟に制御できます。

始める前に

BGPを有効にしていない場合は、ここで有効にします（**feature bgp**）。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch-1(config)# config terminal`
	`switch-1(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	**router bgp** *autonoums-system*
	例：
	`switch-1(config)# router bgp 100`
	`switch-1(config-router)#`
		ルータ コンフィギュレーション モードを開始し、BGP ルーティング プロセスを設定します。

ステップ 3	（任意） **no graceful-shutdown aware**
	例：
	`switch-1(config-router)# no graceful-shutdown aware`
	`switch-1(config-router)#`
		このBGPルータでは、GRACEFUL_SHUTDOWN コミュニティを持つすべてのルートに低い優先順位を指定しないという意味です。グレースフル シャットダウン認識機能がディセーブルになっている場合、デフォルト アクションはルートを非優先にします。そのため、コマンドには **no** 形式というオプションが存在しており、これを使用すると、グレースフル シャットダウン ルートは非優先になりません。

GRACEFUL_SHUTDOWN コミュニティのピアへの送信の防止

発信ルート更新にルート属性として追加されたGRACEFUL_SHUTDOWNコミュニティが不要になった場合は、コミュニティを削除して、指定されたネイバーに送信しなくなります。1 つの使用例は、ルータが自律システム境界にあり、グレースフルシャットダウン機能が自律システム境界の外部に伝播しないようにする場合です。

GRACEFUL_SHUTDOWN がピアに送信されないようにするには、send community オプションを無効にするか、コミュニティを発信ルート マップから削除します。

次の方法の中から 1 つを選択してください。

- 実行コンフィギュレーションで send-community を無効にします。

  例：

```
nxosv2(config-router-neighbor-af)# no send-community standard
nxosv2(config-router-neighbor-af)#
```

このオプションを使用すると、スイッチはGRACEFUL_SHUTDOWNコミュニティを受信しますが、発信ルート マップを介してダウンストリーム ネイバーに送信されません。すべての標準コミュニティも送信されません。

- 次の手順に従って、発信ルートマップを介してGRACEFUL_SHUTDOWNコミュニティを削除します。

  1. GRACEFUL_SHUTDOWNコミュニティと一致するIPコミュニティ リストを作成します。
  2. GRACEFUL_SHUTDOWN コミュニティと照合する発信ルート マップを作成します。
  3. **set community-list delete** 句を使用して GRACEFUL_SHUTDOWN コミュニティを削除します。

  このオプションを使用すると、コミュニティ リストはGRACEFUL_SHUTDOWNコミュニティと一致し、許可されます。その後、発信ルートマップはコミュニティと照合され、発信ルート マップから削除されます。他のすべてのコミュニティは、問題なく発信ルートマップを通過します。

グレースフル シャットダウン情報の表示

グレースフル シャットダウン機能に関する情報は、次の **show** コマンドで確認できます。

コマンド	アクション
show ip bgp community-list graceful-shutdown	GRACEFUL_SHUTDOWNコミュニティを持つBGPルーティング テーブル内のすべてのエントリを表示します。
show running-config bgp	実行中のBGPのデフォルト設定を示します。
show running-config bgp all	グレースフル シャットダウン機能に関する情報など、実行中のBGP設定のすべての情報を表示します。
show bgp *address-family* **neighbors** *neighbor-address* （注） 入力 Cisco Nexus 3550-T BGP は、IPv4 ユニキャスト アドレス ファミリのみをサポートします。	機能がピアに設定されている場合、次のように表示されます。 • 指定されたネイバーの graceful-shutdown-activate 機能の状態 • 指定されたネイバーに設定されたグレースフル シャットダウン ルートマップの名前

コマンド	アクション
show bgp process	コンテキストに応じて異なる情報を表示します。 graceful-shutdown-activate オプションがピア コンテキストで設定されている場合、`graceful-shutdown-active` を介して機能の有効または無効状態を示します。 graceful-shutdown-activate オプションがグローバル コンテキストで設定され、graceful-shutdown ルートマップがある場合は、次のように機能の有効状態が表示されます。 • `graceful-shutdown-active` • `graceful-shutdown-aware` • `graceful-shutdown route-map`
show ip bgp *address*	指定されたアドレスについて、次を含む BGP ルーティング テーブル情報を表示します。 • 最適パスとして指定されたアドレスの状態 • 指定されたアドレスが GRACEFUL_SHUTDOWN コミュニティの一部であるかどうか

グレースフル シャットダウンの設定例

次に、グレースフル シャットダウン機能を使用するための設定例を示します。

BGP リンクのグレースフル シャットダウンの設定

次に、ローカル プリファレンスとコミュニティを設定しながらグレースフル シャットダウンを設定する例を示します。

- 指定されたネイバーへのリンクのグレースフル シャットダウン アクティブ化の設定
- ルートへの GRACEFUL_SHUTDOWN コミュニティの追加
- コミュニティとのアウトバウンド ルートに対して set 句のみを使用して gshutPeer という名前のルートマップを設定します。

```
router bgp 100
    neighbor 20.0.0.3 remote-as 200
         graceful-shutdown activate route-map gshutPeer
         address-family ipv4 unicast
```

```
                send-community

    route-map gshutPeer permit 10
        set local-preference 0
        set community 200:30
```

All-Neighbor BGP リンクのグレースフル シャットダウンの設定

次に例を示します。

- ローカル ルータとそのすべてのネイバーを接続するすべてのリンクに対してグレース フルシャットダウン アクティブ化を設定します。
- GRACEFUL_SHUTDOWN コミュニティをルートに追加しています。
- すべての発信ルートに対して set 句のみを使用して gshutAall という名前のルートマップを設定します。

```
router bgp 200
   graceful-shutdown activate route-map gshutAll

route-map gshutAll permit 10
   set as-path prepend 10 100 110
   set community 100:80

route-map Red permit 10
   set local-pref 20

router bgp 100
   graceful-shutdown activate route-map gshutAll
      router-id 2.2.2.2
         address-family ipv4 unicast
         network 2.2.2.2/32
         neighbor 1.1.1.1 remote-as 100
         update-source loopback0
         address-family ipv4 unicast
            send-community
         neighbor 20.0.0.3 remote-as 200
         address-family ipv4 unicast
            send-community
               route-map Red out
```

この例では、ネイバー 1.1.1.1 に対して `gshutAll` ルート マップが有効になりますが、ネイバー 20.0.0.3 で設定された発信ルートマップ `Red` が優先されるため、ネイバー 20.0.0.3 に対しては有効になりません。

ピアテンプレートでのグレースフル シャットダウンの設定

この例では、ピアセッションテンプレートでグレースフルシャットダウン機能を設定します。これはネイバーによって継承されます。

```
router bgp 200
   template peer-session p1
      graceful-shutdown activate route-map gshut_out
   neighbor 1.1.1.1 remote-as 100
      inherit peer-session p1
      address-family ipv4 unicast
         send-community
```

GRACEFUL_SHUTDOWN コミュニティの使用およびインバウンドルートマップに基づく BGP ルートのフィルタリングとローカル プリファレンスの設定

次に、コミュニティ リストを使用して、GRACEFUL_SHUTDOWN コミュニティを持つ着信ルートをフィルタリングする例を示します。この設定は、Cisco NX-OS 9.3(1) を最小バージョンとして実行していないレガシー スイッチに役立ちます。

次に例を示します。

- GRACEFUL_SHUTDOWN コミュニティを持つルートを許可する IP コミュニティ リスト。
- RM_GSHUT という名前のルート マップは、GSHUT という名前の標準コミュニティ リストに基づいてルートを許可します。
- また、ルートマップは、処理するルートの優先順位を 0 に設定します。これにより、ルータがオフラインになったときに、それらのルートに最適パス計算の優先順位が低くなります。ネイバー (20.0.0.2) からの着信 IPv4 ルートにルート マップが適用されます。

```
ip community-list standard GSHUT permit 65535:0

route-map RM_GSHUT permit 10
   match community GSHUT
   set local-preference 0

router bgp 200
   neighbor 20.0.0.2 remote-as 100
      address-family ipv4 unicast
         send-community
         route-map RM_GSHUT in
```

グレースフル リスタートの設定

グレースフル リスタートを設定し、BGP に対してグレースフル リスタート ヘルパー機能をイネーブルにできます。

始める前に

BGP を有効にする必要があります（「BGP の有効化」の項を参照）。

VRF を作成します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**router bgp** *as-number* 例：	自律システム番号を設定して、新しい BGP プロセスを作成します。

	コマンドまたはアクション	目的
	`switch(config)# router bgp 65535` `switch(config-router)#`	
ステップ 3	（任意） **timers prefix-peer-timeout** *timeout* 例： `switch(config-router)# timers prefix-peer-timeout 20`	BGP プレフィックス ピアのタイムアウト値を設定します（秒単位）。デフォルト値は 90 秒です。
ステップ 4	**graceful-restart** 例： `switch(config-router)# graceful-restart`	グレースフル リスタートおよびグレースフル リスタート ヘルパー機能をイネーブルにします。このコマンドは、デフォルトでイネーブルになっています。 このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。
ステップ 5	**graceful-restart** {**restart-time** *time*|**stalepath-time** *time*} 例： `switch(config-router)# graceful-restart restart-time 300`	グレースフル リスタート タイマーを設定します。 オプション パラメータは次のとおりです。 • **restart-time**：BGP ピアに送信されたリスタートの最大時間。有効な範囲は 1 ～ 3600 秒です。デフォルトは 120 です。 • **stalepath-time**：BGP が再起動中の BGP ピアからの古いルートを維持する最大時間有効な範囲は 1 ～ 3600 秒です。デフォルトは 300 です。 このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。
ステップ 6	**graceful-restart-helper** 例： `switch(config-router)# graceful-restart restart-time 300`	グレースフル リスタート ヘルパー機能をイネーブルにします。このコマンドは、グレースフル リスタートをディセーブルにしていながら、グレースフル リスタート ヘルパー機能はイネーブルにする必要がある場合に使用します。このコマンドによって、BGP ネイバー セッションの自動通知およびセッション リセットが開始されます。

	コマンドまたはアクション	目的
ステップ 7	（任意） **show running-config bgp** 例： `switch(config-router)# show running-config bgp`	BGP の設定を表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config-router)# copy running-config startup-config`	この設定変更を保存します。

例

次に、グレースフル リスタートを有効にする例を示します。

```
switch# configure terminal
switch(config)# router bgp 65536
switch(config-router)# graceful-restart
switch(config-router)# graceful-restart restart-time 300
switch(config-router)# copy running-config startup-config
```

拡張 BGP の設定の確認

BGP の設定を表示するには、次のいずれかの作業を行います。

（注） ***Cisco Nexus 3550-T - 10.1(2t)*** リリースでは、デフォルトの VRF と管理 VRF のみがサポートされます。

コマンド	目的
show bgp all [**summary**]	すべてのアドレス ファミリについて、BGP 情報を表示します。
show bgp convergence	すべてのアドレス ファミリについて、BGP 情報を表示します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **community** {**regexp** *expression* | [**community**] [**no-advertise**] [**no-export**] [**no-export-subconfed**]}	BGP コミュニティと一致する BGP ルートを表示します。

コマンド	目的
show bgp{**ipv4**} {**unicast**} [*ip-address*] **community-list** *list-name*	BGP コミュニティ リストと一致する BGP ルートを表示します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **extcommunity** {**regexp** *expression* | **generic** [**non-transitive** | **transitive**] *aa4:nn* [**exact-match**]}	BGP 拡張コミュニティと一致する BGP ルートを表示します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **extcommunity-list** *list-name* [**exact-match**]}	BGP 拡張コミュニティ リストと一致する BGP ルートを表示します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **extcommunity-list** *list-name* [**exact-match**]}	BGP ルート ダンプニングの情報を表示します。ルート フラップ ダンプニング情報を消去するには、**clear bgp dampening** コマンドを使用します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] {**dampening** **dampened-paths** [**regexp** *expression*]}	BGPルートヒストリパスを表示します。
show bgp {**ipv4** | **vpnv4**} {**unicast**} [*ip-address*] **filter-list** *list-name*	BGP フィルタ リストの情報を表示します。
show bgp {**ipv4** | **vpnv4**} {**unicast**} [*ip-address*] **neighbors** [*ip-address*]	BGP ピアの情報を表示します。これらのネイバーを消去するには、**clear bgp neighbors** コマンドを使用します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] {**nexthop** | **nexthop-database**}	BGPルートネクストホップの情報を表示します。
show bgp paths	BGP パス情報を表示します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **policy** *name*	BGP ポリシー情報を表示します。ポリシー情報を消去するには、**clear bgp policy** コマンドを使用します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **prefix-list** *list-name*	プレフィックス リストと一致する BGP ルートを表示します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **received-paths**	ソフト再構成用に保管されている BGP パスを表示します。

コマンド	目的
show bgp {**ipv4** } {**unicast**} [*ip-address*] **regexp** *expression*	AS_path 正規表現と一致する BGP ルートを表示します。
show bgp {**ipv4**} {**unicast**} [*ip-address*] **route-map** *map-name*	ルート マップと一致する BGP ルートを表示します。
show bgp peer-policy *name*	BGP ピア ポリシー情報を表示します。
show bgp peer-session *name*	BGP ピア セッション情報を表示します。
show bgp peer-template *name*	BGP ピア テンプレート情報を表示します。ピア テンプレートのすべてのネイバーを消去するには、**clear bgp peer-template** コマンドを使用します。
show bgp process	BGP プロセス情報を表示します。
show ip route *ip-address* **detail vrf all | i bw**	リンク帯域幅の EXTCOMM フィールドを表示します。出力の bw：xx（bw：40 など）は、BGP ピアが帯域幅付きの BGP 拡張属性を送信していることを示します。
show {**ipv4**} **bgp** *options*	BGP のステータスと構成情報を表示します。
show running-configuration bgp	現在実行中の BGP コンフィギュレーションを表示します。

BGP 統計情報のモニタリング

BGP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
	BGP ルート フラップの統計情報を表示します。これらの統計情報をクリアするには、**clear bgp flap-statistics** コマンドを使用します。

	ルーティング テーブルに挿入されたルートを表示します。
show bgp sessions	すべてのピアの BGP セッションを表示します。これらの統計情報をクリアするには、**clear bgp sessions** コマンドを使用します。
show bgp statistics	BGP 統計情報を表示します。

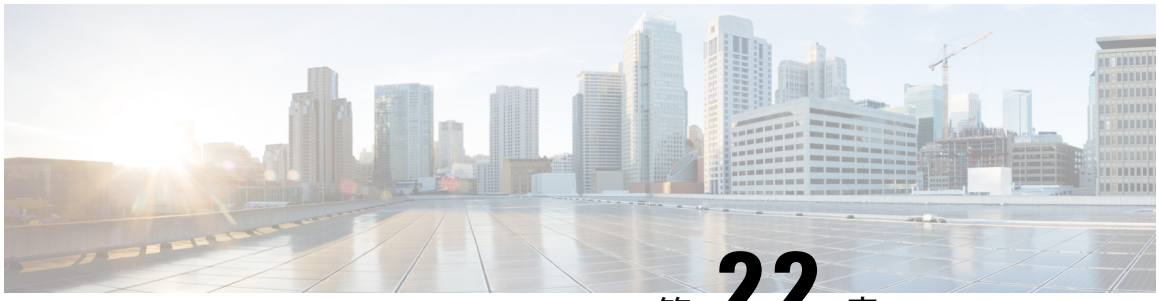
関連項目

BGP の詳細については、次の項目を参照してください。

- 基本的 BGP の設定 （301 ページ）

その他の参考資料

BGP の実装に関連する詳細情報については、次の項を参照してください。



第 22 章

スタティック ルーティングの設定

この章では、Cisco NX-OS デバイス上でスタティック ルーティング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。

スタティック ルーティングについて

ルータは、ユーザが手動で設定したルート テーブル エントリのルート情報を使用するか、またはダイナミック ルーティング アルゴリズムで計算されたルート情報を使用して、パケットを転送します。

スタティック ルートは、2 つのルータ間の明示パスを定義するものであり、自動的にはアップデートできません。ネットワークに変更が生じたときは、手動で再設定する必要があります。スタティック ルートは、ダイナミック ルートに比べて使用する帯域幅が少なくなります。ルーティング アップデートの計算や分析に CPU サイクルを使用しません。

必要に応じて、スタティック ルートでダイナミック ルートを補うことができます。スタティック ルートをダイナミック ルーティング アルゴリズムに再配布できますが、ダイナミック ルーティング アルゴリズムで計算されたルーティング情報をスタティック ルーティング テーブルに再配布できません。

スタティック ルートは、ネットワーク トラフィックが予測可能で、ネットワーク設計が単純な環境で使用します。スタティック ルートはネットワークの変化に対応できないので、大規模でたえず変化しているネットワークでは、スタティック ルートを使用すべきではありません。大部分のネットワークは、ルータ間の通信にダイナミック ルートを使用しますが、特殊な状況でスタティック ルートを 1 つか 2 つ設定する場合があります。スタティック ルートは、最終手段としてのゲートウェイ（ルーティング不能なすべてのパケットの送信先となるデフォルト ルータ）を指定する場合にも便利です。

アドミニストレーティブ ディスタンス

アドミニストレーティブディスタンスは、2つの異なるルーティング プロトコルから同じ宛先に、2 つ以上のルートが存在する場合に、最適なパスを選択するために、ルータが使用するメトリックです。複数のプロトコルがユニキャスト ルーティング テーブルに同じルートを追加した場合に、アドミニストレーティブ ディスタンスを手がかりに、他のルーティング プロトコル（またはスタティック ルート）ではなく、特定のルーティング プロトコル（またはスタティック ルート）が選択されます。各ルーティング プロトコルは、アドミニストレーティブ ディスタンス値を使用して、信頼性の高い順にプライオリティが与えられます。

スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。ルータは値の小さいルートが最短であると見なすので、スタティック ルートがダイナミック ルートより優先されます。ダイナミック ルートでスタティック ルートを上書きする場合は、スタティック ルートにアドミニストレーティブ ディスタンスを指定します。たとえば、アドミニストレーティブ ディスタンスが 120 のダイナミック ルートが 2 つある場合に、ダイナミック ルートでスタティック ルートを上書きするには、スタティック ルートに 120 より大きいアドミニストレーティブ ディスタンスを指定します。

直接接続のスタティック ルート

直接接続のスタティック ルートでは、出力インターフェイス（あらゆるパケットを宛先ネットワークに送り出すインターフェイス）のみを指定する必要があります。ルータは宛先が出力インターフェイスに直接接続されているものと見なし、パケットの宛先をネクストホップ アドレスとして使用します。ネクストホップは、ポイントツーポイントインターフェイスの場合に限り、インターフェイスにできます。ブロードキャスト インターフェイスの場合は、ネクストホップを IPv4 アドレスにする必要があります。

完全指定のスタティック ルート

完全指定のスタティック ルートでは、出力インターフェイス（あらゆるパケットを宛先ネットワークに送り出すインターフェイス）またはネクスト ホップ アドレスのどちらかを指定する必要があります。完全指定のスタティック ルートを使用できるのは、出力インターフェイスがマルチアクセス インターフェイスで、ネクストホップ アドレスを特定する必要がある場合です。ネクストホップアドレスは、指定された出力インターフェイスに直接接続する必要があります。

フローティング スタティック ルート

フローティング スタティック ルートは、ダイナミック ルートをバックアップするためにルータが使用するスタティック ルートです。フローティング スタティック ルートには、バックアップするダイナミック ルートより大きいアドミニストレーティブ ディスタンスを設定する必要があります。この場合、ルータはフローティング スタティック ルートよりダイナミック ルートを優先させます。フローティング スタティック ルートは、ダイナミック ルートが失われた場合の代用として使用できます。

（注） デフォルトでは、ルータはダイナミック ルートよりスタティック ルートを優先させます。スタティック ルートの方がダイナミック ルートより、アドミニストレーティブ ディスタンスが小さいからです。

スタティック ルートのリモート ネクスト ホップ

リモート（非直接接続）ネクスト ホップを指定したスタティック ルートの場合、ルータに直接接続されていない隣接ルータのネクストホップアドレスを指定できます。データ転送時に、スタティック ルートにリモート ネクストホップがあると、そのネクスト ホップがユニキャスト ルーティング テーブルで繰り返し使用され、リモート ネクストホップに到達可能な、対応する直接接続のネクストホップ（複数可）が特定されます。

スタティック ルーティングの前提条件

スタティック ルーティングの前提条件は、次のとおりです。

- スタティックルートのネクストホップアドレスが到達不能な場合、そのスタティック ルートはユニキャスト ルーティング テーブルに追加されません。

デフォルト設定

表にスタティック ルーティング パラメータのデフォルト設定を示します。

表 *20*：デフォルトのスタティック ルーティング パラメータ

パラメータ	デフォルト
アドミニストレーティブ ディスタンス	1
RIP 機能	ディセーブル

スタティック ルーティングの設定

（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。

スタティック ルーティングの設定

デバイスにスタティックルートを設定できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	次のコマンドを入力します。 例： `switch(config)# ip route 192.0.2.0/8 ethernet 1/2 192.0.2.4`	**ip route** {*ip-prefix* | *ip-addr*/*ip-mask*} {[*next-hop* | *nh-prefix*] | [*interface next-hop* | *nh-prefix*]} [**name** *nexthop-name*] [**tag** *tag-value*] [*preference*] スタティック ルートおよびこのスタティック ルート用のインターフェイスを設定します。サポートされているインターフェイスのリストを表示するには、**?** を使用します。**null 0** を使用すると、ヌル インターフェイスを指定できます。 任意でネクスト ホップ アドレスを設定できます。 *preference* 値でアドミニストレーティブ ディスタンスを設定します。範囲は1～255 です。デフォルトは 1 です。 （注） **no** {**ip**} **route** を使用する コマンドを使用すれば、スタティック ルートを削除できます。
ステップ 3	（任意） **show** {**ip**} **static-route** 例： `switch(config)# show ip static-route`	スタティックルート情報を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	この設定変更を保存します。

例

次に、ヌル インターフェイスのスタティック ルートを設定する例を示します。

```
switch# configure terminal
switch(config)# ip route 1.1.1.1/32 null 0
switch(config)# copy running-config startup-config
```

VLAN を介したスタティック ルートの設定

スタティック ルートは、VLAN を介したネクスト ホップのサポートなしで設定できます。

始める前に

アクセス ポートが VLAN の一部であることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**feature interface vlan** 例： `switch(config)# feature interface-vlan`	VLANインターフェイスモードをイネーブルにします。
ステップ 3	**interface-vlan** *vlan-id* 例： `switch(config)# interface-vlan 10`	SVIを作成して、インターフェイス設定モードを開始します。 **vlan-id** 引数の範囲は 1 ～ 4094 です。ただし、内部スイッチ用に予約されている VLAN は除きます。
ステップ 4	**ip address** *ip-addr*/*length* 例： `switch(config)# ip address 192.0.2.1/8`	VLAN の IP アドレスを設定します。
ステップ 5	[**no**] **ip route** *ip-addr*/*length vlan-id* 例： `switch(config)# ip route 209.165.200.224/27 vlan 10`	スイッチ仮想インターフェイス（SVI）上のネクストホップなしでインターフェイスのスタティック ルートを追加します。

	コマンドまたはアクション	目的
		IP アドレスは、スイッチに接続されたインターフェイスで設定されるアドレスです。 スタティック ルートを削除するには、**no** キーワードを使用します。
ステップ 6	（任意） **show ip route** **例：** `switch(config)# show ip route`	Unicast Route Information Base （URIB）からルートを表示します。
ステップ 7	（任意） **copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	この設定変更を保存します。

例

次に、SVI を介したネクスト ホップなしでスタティック ルートを設定する例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
swicth(config)# interface vlan 10
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# ip route 209.165.200.224/27 vlan 10  <===209,165.200.224 is the IP
address of the interface that is configured on the interface that is directly connected
 to
the switch.
switch(config-if)# copy running-config startup-config
```

スタティック ルーティングの設定確認

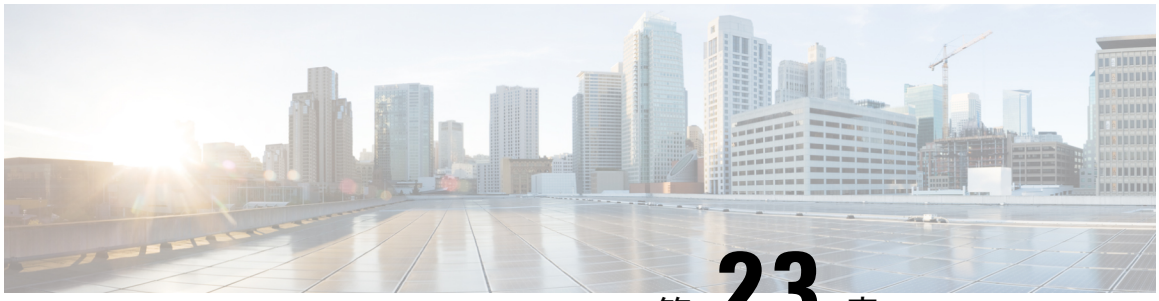
スタティック ルーティングの設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show {**ip**} **static-route**	設定されているスタティック ルートを表示します。
show {**ip**} **static-route track-table**	IPv4 static-route トラック テーブルに関する情報を表示します。

スタティック ルーティングの設定例

次に、スタティック ルーティングの設定例を示します。

```
configure terminal
ip route 192.0.2.0/8 192.0.2.10
copy running-config startup-config
```



第 23 章

VRRP の設定

この章は、次の項で構成されています。

VRRP について

VRRP を使用すると、仮想 IP アドレスを共有するルータ グループを設定することによって、ファーストホップ IP ルータで透過的フェールオーバーが可能になります。VRRP ではそのグループに許可されるルータが選択され、仮想 IP アドレスへのすべてのパケットが処理できるようになります。残りのルータはスタンバイになり、許可されるルータで障害が発生した場合に処理を引き継ぎます。

VRRP の動作

LAN クライアントは、ダイナミック プロセスまたはスタティック設定を使用することによって、特定のリモート宛先へのファーストホップにするルータを決定できます。ダイナミック ルータ ディスカバリの例を示します。

プロキシ ARP：クライアントはアドレス解決プロトコル（ARP）を使用して到達すべき宛先を取得します。ルータは独自の MAC アドレスで ARP 要求に応答します。

ルーティング プロトコル：クライアントはダイナミック ルーティング プロトコルのアップデートを（ルーティング情報プロトコル（RIP）などから）受信し、独自のルーティング テーブルを形成します。

ICMP Router Discovery Protocol（IRDP）クライアント：クライアントはインターネット制御メッセージ プロトコル（ICMP）ルータ ディスカバリ クライアントを実行します。

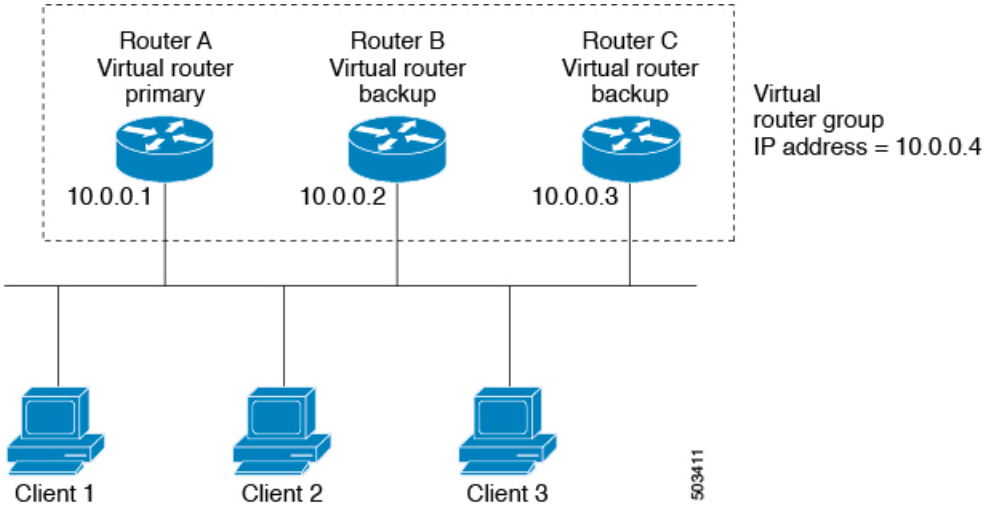
ダイナミック ディスカバリ プロトコルのデメリットは、LAN クライアントにある程度、設定および処理のオーバーヘッドが発生することです。また、ルータが故障した場合、他のルータに切り替えるプロセスも遅くなる場合があります。

ダイナミック ディスカバリ プロトコルの代わりに、クライアント上でデフォルト ルータをスタティックに設定することもできます。このアプローチでは、クライアントの設定および処理が簡素化されますが、シングルポイント障害が生じます。デフォルト ゲートウェイで障害が発生した場合、LAN クライアントの通信はローカル IP ネットワーク セグメントに限定され、ネットワークの他の部分から切り離されます。

VRRP では、ルータ グループ（VRRP グループ）が単一の仮想 IP アドレスを共有できるようにすることによって、スタティック設定に伴う問題を解決できます。さらに、デフォルト ゲートウェイとして仮想 IP アドレスを指定して、LAN クライアントを設定できます。

次の図は、基本的な VLANトポロジです。この例では、ルータ A、B、および C が VRRP グループを形成します。グループの IP アドレスは、ルータ A のインターフェイス インターフェイスに設定されているアドレス（10.0.0.1）と同じです。

図 *20*：基本的な *VRRP* トポロジ



仮想 IP アドレスにルータ A の物理イーサネット インターフェイスの IP アドレスが使用されるので、ルータ A がプライマリ（「IP アドレス オーナー」）になります。ルータ A はプライマリとして、VRRP グループの仮想 IP アドレスを所有し、送信されたパケットをこの IP アドレスに転送します。クライアント 1 ～ 3 には、デフォルト ゲートウェイの IP アドレス 10.0.0.1 が設定されています。

ルータ B および C の役割はバックアップです。プライマリで障害が発生すると、プライオリティが最も高いバックアップ ルータがプライマリになり、仮想 IP アドレスを引き継いで、LAN ホストへのサービスが途切れないようにします。ルータ A が回復すると、これが再びプライマリになります。

（注） ルーテッド ポートで受信した VRRP 仮想 IP アドレス宛のパケットは、ローカル ルータ上で終端します。そのルータがプライマリ VRRP ルータであるのかバックアップ VRRP ルータであるのかは関係ありません。これらのパケットには、ping トラフィックと Telnet トラフィックが含まれます。レイヤ 2（VLAN）インターフェイスで受信した、VRRP 仮想 IP アドレス宛のパケットは、プライマリ ルータに届きます。

VRRP の利点

VRRP の利点は、次のとおりです。

- 冗長性：複数のルータをデフォルト ゲートウェイ ルータとして設定できるので、ネットワークにシングル ポイント障害が発生する確率が下がります。
- ロード シェアリング：複数のルータで LAN クライアントとの間のトラフィックを分担できます。トラフィックの負荷が使用可能なルータ間でより公平に分担されます。
- マルチ VRRP グループ：プラットフォームが複数の MAC アドレスをサポートする場合、ルータの物理インターフェイス上で、複数の VRRP グループをサポートします。マルチ VRRP グループによって、LAN トポロジで冗長性およびロード シェアリングを実現できます。
- マルチ IP アドレス：セカンダリ IP アドレスを含めて、複数の IP アドレスを管理できます。イーサネット インターフェイス上で複数のサブネットを設定している場合は、各サブネットで VRRP を設定できます。
- プリエンプト：障害プライマリを引き継いでいたバックアップ ルータより、さらにプライオリティが高いバックアップ ルータが使用可能になったときに、プライオリティが高い方を優先させることができます。
- アドバタイズメント プロトコル：VRRP アドバタイズメントに、専用のインターネット割り当て番号局（IANA）規格マルチキャスト アドレス（224.0.0.18）を使用します。このアドレッシング方式によって、マルチキャストを提供するルータ数が最小限になり、テスト機器でセグメント上の VRRP パケットを正確に識別できるようになります。IANA は VRRP に IP プロトコル番号 112 を割り当てています。
- VRRP トラッキング：インターフェイスのステートに基づいて VRRP プライオリティを変更することによって、最適な VRRP ルータがグループのプライマリになることが保証されます。

複数の VRRP グループ

物理インターフェイス上で複数の VRRP グループを設定できます。サポートされる VRRP グループの数については、『*Cisco Nexus 3550 Series NX-OS* 検証済みの拡張性ガイド』を参照してください。

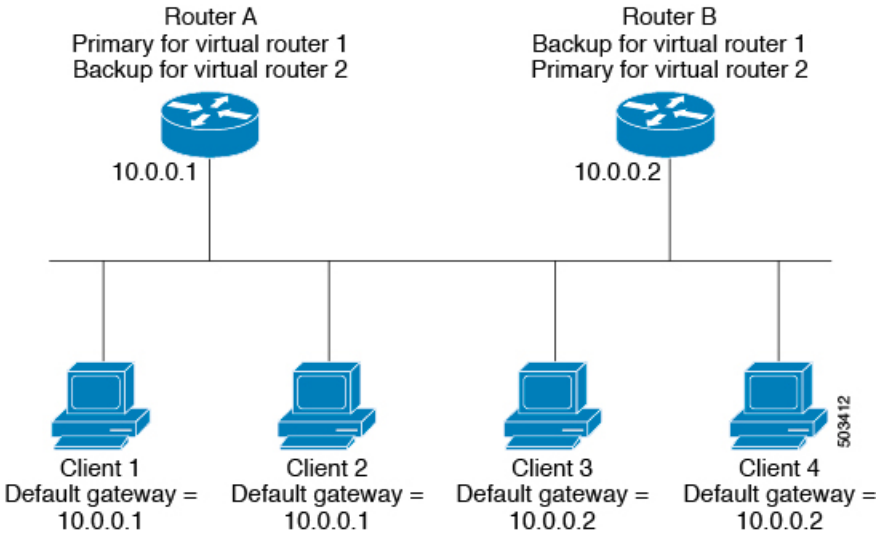
ルータ インターフェイスがサポートできる VRRP グループの数は、次の要因によって決まります。

- ルータの処理能力
- ルータのメモリの能力

ルータ インターフェイス上で複数の VRRP グループが設定されたトポロジでは、インターフェイスはある VRRP グループのプライマリ、および他の 1 つまたは複数の VRRP グループのバックアップとして動作可能です。

次の図の LAN トポロジでは、ルータ A と B がクライアント 1 ～ 4 のトラフィックを共有するように、VRRP が設定されています。ルータ A と B の一方で障害が発生した場合、もう一方がバックアップとして機能します。

図 *21* : ロード シェアリングおよび冗長 *VRRP* トポロジ



このトポロジには、オーバーラップする 2 つの VRRP グループに対応する 2 つの仮想 IP アドレスが含まれています。VRRP グループ 1 では、ルータ A が IP アドレス 10.0.0.1 のオーナーであり、プライマリです。ルータ B はルータ A をバックアップします。クライアント 1 と 2 には、デフォルト ゲートウェイの IP アドレス 10.0.0.1 が設定されています。

VRRP グループ 2 では、ルータ B が IP アドレス 10.0.0.2 のオーナーであり、プライマリです。ルータ A はルータ B をバックアップします。クライアント 3 と 4 には、デフォルト ゲートウェイの IP アドレス 10.0.0.2 が設定されています。

VRRP ルータのプライオリティおよびプリエンプション

VRRP 冗長構成の重要な側面は、VRRP ルータのプライオリティです。各 VRRP ルータが果たす役割やプライマリ ルータで障害が発生した場合のアクションは、プライオリティによって決まるからです。

VRRP ルータが仮想 IP アドレスおよび物理インターフェイスの IP アドレスを所有する場合、そのルータはプライマリとして機能します。プライマリのプライオリティは 255 です。

プライオリティによって、VRRPルータがバックアップルータとして動作するかどうかが決まり、さらに、プライマリで障害が発生した場合にプライマリになる順序も決まります。

たとえば、ルータ A が LAN トポロジにおけるプライマリであり、そのルータ A で障害が発生した場合、VRRP はバックアップ B が引き継ぐのか、バックアップ C が引き継ぐのかを判断する必要があります。ルータ B にプライオリティ 101 が設定されていて、ルータ C がデフォルトのプライオリティ 100 の場合、VRRP はルータ B をプライマリになるべきルータとして選択します。ルータ B の方がプライオリティが高いからです。ルータ B および C にデフォルトのプライオリティ 100 が設定されている場合は、VRRP は IP アドレスが大きい方のバックアップをプライマリになるべきルータとして選択します。

VRRP ではプリエンプションを使用して、VRRP バックアップ ルータがプライマリになってからのアクションを決定します。プリエンプションはデフォルトでイネーブルなので、VRRP は新しいプライマリよりプライオリティの高いバックアップがオンラインになると、バックアップに切り替えます。たとえば、ルータ A がプライマリであり、そのルータ A で障害が発生した場合、VRRP は（プライオリティの順位が次である）ルータ B を選択します。ルータ C がルータ B より高いプライオリティでオンラインになると、ルータ B で障害が発生していなくても、VRRP はルータ C を新しいプライマリとして選択します。

プリエンプションを無効にした場合、VRRP が切り替わるのは、元のプライマリが回復した場合、または新しいプライマリで障害が発生した場合に限られます。

VRRP のアドバタイズメント

VRRP プライマリは、同じグループ内の他の VRRP ルータに VRRP アドバタイズメントを送信します。アドバタイズメントは、プライマリのプライオリティと状態を伝えます。Cisco NX-OS は、VRRPアドバタイズメントを IP パケットにカプセル化し、VRRPグループに割り当てられた IP マルチキャストアドレスに送信します。デフォルトでは、Cisco NX-OS が 1 秒ごとにアドバタイズメントを送信しますが、異なるアドバタイズメント間隔を設定できます。

VRRP 認証

VRRP は、次の認証機能をサポートします。

- 認証なし
- プレーン テキスト認証

VRRP は次の場合に、パケットを拒否します。

- 認証方式がルータと着信パケットで異なる。
- テキスト認証文字列がルータと着信パケットで異なる。

VRRP トラッキング

VRRP は次のトラッキング オプションをサポートしています。

- ネイティブ インターフェイス トラッキング：インターフェイスのステートを追跡し、そのステートを使用してVRRPグループのVRRPルータのプライオリティを判別します。インターフェイスがダウンしている場合、またはインターフェイスにプライマリ IP アドレスがない場合、トラッキング対象ステートはダウンとなります。
- オブジェクト トラッキング：設定されたオブジェクトのステートを追跡し、そのステートを使用してVRRPグループのVRRPルータのプライオリティを判別します。オブジェクト トラッキングの詳細については、「オブジェクト トラッキングの構成」セクションを参照してください。

トラッキング対象ステート（インターフェイスまたはオブジェクト）がダウンになると、VRRPはユーザがトラッキング対象ステートに対して新しいプライオリティをどのように設定するかに基づいて、プライオリティをアップデートします。トラッキング対象ステートがオンラインになると、VRRP は仮想ルータ グループの元のプライオリティを復元します。

たとえば、ネットワークへのアップリンクがダウンした場合、別のグループ メンバーがVRRPグループのプライマリとして引き継げるように、VRRPグループ メンバーのプライオリティを引き下げなければならないことがあります。詳細については、VRRPインターフェイス ステート トラッキングの設定 （424 ページ）を参照してください。

（注） VRRP はレイヤ 2 インターフェイスのトラッキングをサポートしていません。

高可用性

VRRP は、ステートフル リスタートとステートフル スイッチオーバーを通して高可用性をサポートします。ステートフル リスタートは、VRRPが障害を処理してリスタートするときに行われます。ステートフル スイッチオーバーは、アクティブ スーパーバイザがスタンバイ スーパーバイザに切り替わるときに行われます。Cisco NX-OS は、スイッチオーバー後に実行コンフィギュレーションを適用します。

VRRP の注意事項と制約事項

VRRP には、次の注意事項および制限事項があります。

- 管理インターフェイス上で VRRP を設定できません。
- VRRPがイネーブルの場合は、ネットワーク上のデバイス全体でVRRP設定を複製する必要があります。
- 同一インターフェイス上では、複数のファーストホップ冗長プロトコルを設定しないことを推奨します。
- VRRP を設定するインターフェイスに IP アドレスを設定し、そのインターフェイスをイネーブルにしてからでなければ、VRRP はアクティブになりません。

- インターフェイス VRF メンバーシップまたはポート チャネル メンバーシップを変更した場合、またはポート モードをレイヤ 2 に変更した場合は、Cisco NX-OS によってインターフェイス上のすべてのレイヤ 3 設定が削除されます。
- VRRP でレイヤ 2 インターフェイスを追跡するよう設定した場合、レイヤ 2 をシャットダウンしてからインターフェイスを再度イネーブル化することにより、VRRP プライオリティを更新してレイヤ 2 インターフェイスのステートを反映させる必要があります。

VRRP パラメータのデフォルト設定

次の表に、VRRP パラメータのデフォルト設定を示します。

表 *21* : デフォルトの *VRRP* パラメータ

パラメータ	デフォルト
VRRP	ディセーブル
アドバタイズ インターバル	1 秒
認証	認証なし
プリエンプション	イネーブル
プライオリティ	100

VRRP の設定

（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。

VRRP のイネーブル化

VRRP グループを設定してイネーブルにするには、事前に VRRP 機能をグローバルにイネーブルにしておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	
ステップ 2	**[no] feature vrrp** 例： `switch(config)# feature vrrp`	VRRP をイネーブルにします。VRRP をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VRRP グループの設定

VRRP グループを作成し、仮想 IP アドレスを割り当て、グループを有効にすることができます。

VRRP グループに設定できる仮想 IPv4 アドレスは 1 つです。プライマリ VRRP ルータはデフォルトで、仮想 IP アドレスを直接の宛先とするパケットをドロップします。これは、VRRP プライマリがパケットを転送するネクストホップ ルータとしてのみ想定されているからです。アプリケーションによっては、Cisco NX-OS が仮想ルータ IP 宛のパケットを受け付けるようにする必要があります。仮想 IP アドレスに secondary オプションを使用すると、ローカル ルータが VRRP マスターの場合、これらのパケットを受け付けるようになります。

VRRP グループを設定した場合は、そのグループをアクティブにするために、グループを明示的に有効にする必要があります。

始める前に

インターフェイス上で IP アドレスを設定していることを確認します。IPv4 アドレス指定の設定 （241 ページ）を参照してください。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**vrrp** *number*
	例：
	`switch(config-if)# vrrp 250`
	`switch(config-if-vrrp)#`
		仮想ルータ グループを作成します。範囲は 1 ～ 255 です。

ステップ 4	**address** *ip-address* [**secondary**] 例： `switch(config-if-vrrp)# address 192.0.2.8`	指定の VRRP グループに仮想 IPv4 アドレスを設定します。このアドレスは、インターフェイスの IPv4 アドレスと同じサブネットになければなりません。 **secondary** オプションは、VRRP ルータが仮想ルータの IP アドレスに送信されたパケットを受け付けて、アプリケーションに配信することをアプリケーションが要求する場合に限られます。
ステップ 5	**no shutdown** 例： `switch(config-if-vrrp)# no shutdown`	VRRP グループを有効にします。デフォルトでは無効になっています。
ステップ 6	（任意） **show vrrp** 例： `switch(config-if-vrrp)# show vrrp`	VRRP 情報の要約を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config-if-vrrp)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VRRP プライオリティの設定

仮想ルータの有効なプライオリティ範囲は 1 ～ 254 です（1 が最下位、254 が最上位のプライオリティ）。バックアップのデフォルトのプライオリティ値は 100 です。インターフェイス アドレスがプライマリ仮想 IP アドレスと同じデバイス（プライマリ）の場合、デフォルト値は 255 です。

始める前に

インターフェイス上で IP アドレスを設定していることを確認します。IPv4 アドレス指定の設定 （241 ページ）を参照してください。

VRRP が有効になっていることを確認します。（「VRRP の設定 （417 ページ）」のセクションを参照してください）。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**vrrp** *number*
	例：
	`switch(config-if)# vrrp 250`
	`switch(config-if-vrrp)#`
		仮想ルータ グループを作成します。

ステップ 4	**shutdown** 例： `switch(config-if-vrrp)# shutdown`	VRRP グループを無効にします。
ステップ 5	**priority** *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*] 例： `switch(config-if-vrrp)# priority 60 forwarding-threshold lower 40 upper 50`	VRRP グループでのアクティブ ルータ選択に使用するプライオリティ レベルを設定します。レベルの範囲は 1 ー 254 です。バックアップの場合、デフォルトは 100 です。インターフェイス IP アドレスが仮想 IP アドレスと等しいプライマリの場合は 255 です。
ステップ 6	**no shutdown** 例： `switch(config-if-vrrp)# no shutdown`	VRRP グループを有効にします。
ステップ 7	（任意） **show vrrp** 例： `switch(config-if-vrrp)# show vrrp`	VRRP 情報の要約を表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config-if-vrrp)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VRRP 認証の設定

VRRP グループに単純なテキスト認証を設定できます。

始める前に

インターフェイス上で IP アドレスを設定していることを確認します（IPv4 アドレス指定の設定 （241 ページ）を参照）。

VRRP が有効になっていることを確認します（「VRRP の設定 （417 ページ）」セクションを参照）。

ネットワーク上のすべての VRRP デバイスで、認証設定が同じであることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**vrrp** *number*
	例：
	`switch(config-if)# vrrp 250`
	`switch(config-if-vrrp)#`
		仮想ルータ グループを作成します。

ステップ 4	**shutdown** 例： `switch(config-if-vrrp)# shutdown`	VRRP グループを無効にします。
ステップ 5	**authentication text** *password* 例： `switch(config-if-vrrp)# authentication text aPassword`	単純なテキスト認証オプションを指定し、キーネーム パスワードを指定します。キーネームの範囲は 1 ～ 255 文字です。16 文字以上を推奨します。テキスト パスワードは、英数字で最大 8 文字です。
ステップ 6	**no shutdown** 例： `switch(config-if-vrrp)# no shutdown`	VRRP グループを有効にします。デフォルトでは無効になっています。

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

アドバタイズメント パケットのタイム インターバルの設定

アドバタイズメント パケットのタイム インターバルを設定できます。

始める前に

インターフェイス上で IP アドレスを設定していることを確認します（IPv4 アドレス指定の設定 （241 ページ）を参照）。

VRRP が有効になっていることを確認します（「VRRP の設定 （417 ページ）」セクションを参照）。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**vrrp** *number*
	例：
	`switch(config-if)# vrrp 250`
	`switch(config-if-vrrp)#`
		仮想ルータ グループを作成します。

ステップ 4	**shutdown** 例： `switch(config-if-vrrp)# shutdown`	VRRP グループを無効にします。

	コマンドまたはアクション	目的
ステップ 5	**advertisement interval** *seconds* 例： `switch(config-if-vrrp)# advertisement-interval 15`	アドバタイズメント フレームの送信間隔を秒数で設定します。範囲は 1 ～ 255 です。デフォルト値は 1 秒です。
ステップ 6	**no shutdown** 例： `switch(config-if-vrrp)# no shutdown`	VRRP グループを有効にします。
ステップ 7	（任意） **show vrrp** 例： `switch(config-if-vrrp)# show vrrp`	VRRP 情報の要約を表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config-if-vrrp)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

プリエンプションのディセーブル化

VRRP グループ メンバーのプリエンプションをディセーブルにできます。プリエンプションをディセーブルにした場合は、プライオリティのより高いバックアップ ルータが、プライオリティのより低いプライマリ ルータを引き継ぐことはありません。プリエンプションはデフォルトでイネーブルです。

始める前に

インターフェイス上で IP アドレスを設定していることを確認します。IPv4 アドレス指定の設定 （241 ページ）を参照してください。

VRRP が有効になっていることを確認します。「VRRP の設定 （417 ページ）」の項を参照してください。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**vrrp** *number*
	例：
	`switch(config-if)# vrrp 250`
	`switch(config-if-vrrp)#`
		仮想ルータ グループを作成します。

ステップ 4	**shutdown** 例： `switch(config-if-vrrp)# shutdown`	VRRP グループを無効にします。
ステップ 5	**no preempt** 例： `switch(config-if-vrrp)# no preempt`	preempt オプションをディセーブルにして、プライオリティが上位のバックアップが使用されてもプライマリが変わらないようにします。
ステップ 6	**no shutdown** 例： `switch(config-if-vrrp)# no shutdown`	VRRP グループを有効にします。
ステップ 7	（任意） **show vrrp** 例： `switch(config-if-vrrp)# show vrrp`	VRRP 情報の要約を表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config-if-vrrp)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VRRP インターフェイス ステート トラッキングの設定

インターフェイス ステート トラッキングでは、デバイス内の他のインターフェイスのステートに基づいて、仮想ルータのプライオリティが変更されます。トラッキング対象のインターフェイスがダウンしたり、IPアドレスが削除されると、Cisco NX-OS はトラッキング プライオリティ値を仮想ルータに割り当てます。トラッキング対象のインターフェイスがオンライン状態になり、IP アドレスがこのインターフェイスに設定されると、Cisco NX-OS は仮想ルータに

設定されていたプライオリティを復元します（「VRRPプライオリティの設定 （419ページ）」セクションを参照）。

（注） VRRP はレイヤ 2 インターフェイスのトラッキングをサポートしていません。

始める前に

インターフェイス上で IP アドレスを設定していることを確認します（IPv4 アドレス指定の設定 （241 ページ）を参照）。

VRRP が有効になっていることを確認します（「VRRP の設定 （417 ページ）」セクションを参照）。

仮想ルータが有効になっていることを確認します（「VRRP グループの設定 （418 ページ）」を参照）。

インターフェイスでプリエンプションが有効になっていることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**vrrp** *number*
	例：
	`switch(config-if)# vrrp 250`
	`switch(config-if-vrrp)#`
		仮想ルータ グループを作成します。

ステップ 4	**shutdown** 例： `switch(config-if-vrrp)# shutdown`	VRRP グループを無効にします。
ステップ 5	**track interface** *type slot/port* **priority** *value* 例： `switch(config-if-vrrp)# track interface ethernet 1/10 priority 254`	VRRP グループのインターフェイス プライオリティ トラッキングをイネーブルにします。プライオリティの範囲は1 ～ 254 です。

	コマンドまたはアクション	目的
ステップ 6	**no shutdown** 例： `switch(config-if-vrrp)# no shutdown`	VRRP グループを有効にします。
ステップ 7	（任意） **show vrrp** 例： `switch(config-if-vrrp)# show vrrp`	VRRP 情報の要約を表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config-if-vrrp)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VRRP オブジェクト トラッキングの設定

VRRP を使用して IPv4 オブジェクトを追跡できます。

始める前に

VRRP が有効になっていることを確認します。

「オブジェクト トラッキングの設定」セクションのコマンドを使用して、オブジェクト トラッキングを構成します。

手順

	コマンドまたはアクション	目的

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

ステップ 3	**vrrp** *number* **address-family ipv4**
	例：
	`switch(config-if)# vrrp 5 address-family ipv4`
	`switch(config-if-vrrp-group)#`
		IPv4 用に VRRP グループを作成し、VRRP vrrp number address-family ipv4 グループ設定モードを開始します。範囲は 1 ～ 255 です。

	コマンドまたはアクション	目的
ステップ 4	**track** *object-number* **decrement** *number* 例： `switch(config-if-vrrp-group)# track 1 decrement 2`	仮想ルータ グループを作成します。範囲は 1 ～ 255 です。
ステップ 5	（任意） **show running-config vrrp** 例： `switch(config-if-vrrp-group)# show running-config vrrp`	VRRP の実行中の設定を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config-if-vrrp-group)# copy running-config startup-config`	この設定変更を保存します。

VRRP の設定の確認

VRRP 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show interface *interface-type*	インターフェイスの仮想ルータ設定を表示します。
show fhrp *interface-type interface-number*	ファーストホップ冗長性プロトコル（FHRP）の情報を表示します。
show vrrp [*group-number*]	すべてのグループまたは特定の VRRP グループについて、VRRP ステータスを表示します。

VRRP 統計情報のモニタリングとクリア

VRRP の統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show vrrp statistics	VRRP の統計情報を表示します。

デバイスのすべてのインターフェイスについて、すべての VRRP 統計情報を消去するには、**clear vrrp statistics** コマンドを使用します。

VRRP の設定例

この例では、ルータ A とルータ B はそれぞれ 3 つの VRRP グループに属しています。コンフィギュレーションにおいて、各グループのプロパティは次のとおりです。

- グループ 1：
  - 仮想 IP アドレスは 10.1.0.10 です。
  - ルータ A は優先順位 120 で、このグループのプライマリになります。
  - アドバタイズ インターバルは 3 秒です。
  - プリエンプションはイネーブルです。
- グループ 5：
  - ルータ B はプライオリティ 200 で、このグループのマスターになります。
  - アドバタイズ インターバルは 30 秒です。
  - プリエンプションはイネーブルです。
- グループ 100：
  - ルータ A は、IP アドレスが上位（10.1.0.2）なので、このグループのプライマリになります。
  - アドバタイズ インターバルはデフォルトの 1 秒です。
  - プリエンプションはディセーブルです。

ルータ A

```
switch (config)# interface ethernet 1/0
switch (config-if)# ip address 10.1.0.2/16
switch (config-if)# no shutdown
switch (config-if)# vrrp 1
switch (config-if-vrrp)# priority 120
switch (config-if-vrrp)# authentication text cisco
switch (config-if-vrrp)# advertisement-interval 3
switch (config-if-vrrp)# address 10.1.0.10
switch (config-if-vrrp)# no shutdown
switch (config-if-vrrp)# exit
switch (config-if)# vrrp 5
switch (config-if-vrrp)# priority 100
switch (config-if-vrrp)# advertisement-interval 30
switch (config-if-vrrp)# address 10.1.0.50
switch (config-if-vrrp)# no shutdown
switch (config-if-vrrp)# exit
switch (config-if)# vrrp 100
switch (config-if-vrrp)# no preempt
switch (config-if-vrrp)# address 10.1.0.100
switch (config-if-vrrp)# no shutdown
```

ルータ B

```
switch (config)# interface ethernet 1/0
switch (config-if)# ip address 10.2.0.1/2
switch (config-if)# no shutdown
switch (config-if)# vrrp 1
switch (config-if-vrrp)# priority 100
switch (config-if-vrrp)# authentication text cisco
switch (config-if-vrrp)# advertisement-interval 3
switch (config-if-vrrp)# address 10.2.0.10
switch (config-if-vrrp)# no shutdown
switch (config-if-vrrp)# exit
switch (config-if)# vrrp 5
switch (config-if-vrrp)# priority 200
switch (config-if-vrrp)# advertisement-interval 30
switch (config-if-vrrp)# address 10.2.0.50
switch (config-if-vrrp)# no shutdown
switch (config-if-vrrp)# exit
switch (config-if)# vrrp 100
switch (config-if-vrrp)# no preempt
switch (config-if-vrrp)# address 10.2.0.100
switch (config-if-vrrp)# no shutdown
```

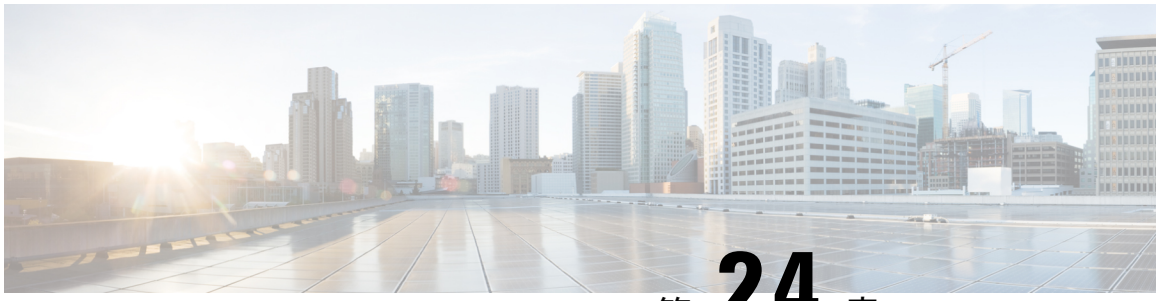
その他の参考資料

VRRP の関連資料

関連項目	マニュアル タイトル
高可用性の設定	*Cisco Nexus*® 高可用性および冗長性ガイド

第 VI 部

Cisco Nexus 3550-T レイヤ 2 スイッチング構成ガイド



第 24 章

『Layer 2 Switching Configuration Guide』

この前書きは、次の項で構成されています。

ライセンス要件

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

レイヤ 2 イーサネット スイッチングの概要

レイヤ 2 スイッチングについて

（注） インターフェイスの作成の詳細については、「*Cisco Nexus® 3550-T* インターフェイス構成」のセクションを参照してください。

レイヤ2スイッチングポートは、アクセスポートまたはトランクポートとして設定できます。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。レイヤ 2 スイッチング ポートはすべて、MAC アドレス テーブルを維持します。

レイヤ 2 イーサネット スイッチングの概要

このデバイスは、レイヤ2イーサネットセグメント間の同時パラレル接続をサポートします。イーサネット セグメント間のスイッチド コネクションは、パケットが伝送されている間だけ維持されます。次のパケットには、別のセグメント間に新しい接続が確立されます。

また、このデバイスでは、各デバイス（サーバなど）を独自のコリジョン ドメインに割り当てることによって、広帯域デバイスおよび多数のユーザによって発生する輻輳の問題を解決できます。各 LAN ポートが個別のイーサネット コリジョン ドメインに接続されるので、スイッチド環境のサーバは全帯域幅にアクセスできます。

イーサネット ネットワークではコリジョンによって深刻な輻輳が発生するため、全二重通信を使用することが有効な対処法の 1 つとなります。これらのインターフェイスを全二重モードに設定すると、2 つのステーション間で同時に送受信を実行できます。パケットを双方向へ同時に送ることができるので、有効なイーサネット帯域幅は 2 倍になります。

デバイス上の各LANポートは、単一のワークステーション、サーバ、またはワークステーションやサーバがネットワークへの接続時に経由する他のデバイスに接続できます。

信号の劣化を防ぐために、デバイスは各 LAN ポートを個々のセグメントとして処理します。異なる LAN ポートに接続しているステーションが相互に通信する必要がある場合、デバイスは、一方の LAN ポートから他方の LAN ポートにワイヤ速度でフレームを転送し、各セッションが全帯域幅を利用できるようにします。

デバイスは、LAN ポート間で効率的にフレームをスイッチングするために、アドレス テーブルを管理しています。デバイスは、フレームを受信すると、受信した LAN ポートに、送信側ネットワーク デバイスのメディア アクセス コントロール（MAC）アドレスを関連付けます。

デバイスは、受信したフレームの送信元MACアドレスを使用して、アドレス テーブルをダイナミックに構築します。自分のアドレス テーブルに登録されていない宛先 MAC アドレスを持つフレームを受信すると、デバイスは、そのフレームを同じ VLAN のすべての LAN ポート（受信したポートは除く）に送出します。宛先端末が応答を返してきたら、デバイスは、その応答パケットの送信元 MAC アドレスとポート ID をアドレス テーブルに追加します。以降、その宛先へのフレームを、すべての LAN ポートに送出せず、単一の LAN ポートだけに転送します。

スタティック MAC アドレスと呼ばれる、デバイス上の特定のインターフェイスだけをスタティックに示すMACアドレスを設定できます。スタティック MAC アドレスは、インターフェイス上でダイナミックに学習された MAC アドレスをすべて書き換えます。ブロードキャストのアドレスは、スタティック MAC アドレスとして設定できません。スタティック MAC エントリは、デバイスのリブート後も保持されます。

アドレス テーブルは、ハードウェアの I/O モジュールに応じて多数の MAC アドレス エントリを格納できます。デバイスは、設定可能なエージング タイマーによって定義されるエージング メカニズムを使用しているため、アドレスが非アクティブな状態のまま指定時間（秒）が経過すると、そのアドレスはアドレス テーブルから削除されます。

レイヤ 3 スタティック MAC アドレス

スタティック MAC アドレスは、次のレイヤ 3 インターフェイスに設定できます。

- レイヤ 3 インターフェイス

- レイヤ 3 ポート チャネル
- VLAN ネットワーク インターフェイス

レイヤ 3 インターフェイスの構成の詳細については、「*Cisco Nexus® 3550-T* インターフェイス構成」のセクションを参照してください。

VLANs

VLANは、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。

どのようなスイッチポートでもVLANに属すことができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN に属する端末だけに転送またはフラッディングされます。各 VLAN は 1 つの論理ネットワークであると見なされます。VLAN に属していないステーション宛てのパケットは、ブリッジまたはルータを経由して転送する必要があります。

デバイスの初回の起動時にすべてのポートがデフォルトの VLAN（VLAN1）に割り当てられます。VLAN インターフェイスまたはスイッチ仮想インターフェイス（SVI）は、VLAN 間の通信用として作成されるレイヤ 3 インターフェイスです。

このデバイスは、IEEE 802.1Q 規格に基づき、4095 の VLAN 範囲（255 の最大 VLAN をサポート）をサポートします。これらの VLAN はいくつかの範囲に分かれています。各範囲の使用法は少しずつ異なります。一部のVLANはデバイスの内部使用のために予約されているため、設定には使用できません。

Note Cisco NX-OS では、スイッチ間リンク（ISL）はサポートされません。

スパニングツリー

ここでは、ソフトウェア上でのスパニングツリープロトコル（STP）の実装について説明します。このマニュアルでは、IEEE 802.1wおよびIEEE 802.1s を指す用語として、「スパニングツリー」を使用します。このマニュアルでIEEE 802.1D 規格のスパニングツリープロトコルについて記す場合は、802.1D であることを明記します。

STP の概要

STP は、レイヤ 2 レベルで、ループのないネットワークを実現します。レイヤ 2 LAN ポートは STP フレーム（ブリッジ プロトコル データ ユニット（BPDU））を一定の時間間隔で送受信します。ネットワーク デバイスは、これらのフレームを転送せずに、フレームを使用してループフリー パスを構築します。

802.1D は、オリジナルの STP 規格です。基本的なループフリー STP から、多数の改善を経て拡張されました。また、機器の高速化に対応して、ループフリーコンバージェンス処理も高速化するために、規格全体が再構築されました。

さらに、802.1s 規格のマルチ スパニングツリー（MST）では、複数の VLAN を単一のスパニングツリー インスタンスにマッピングできます。各インスタンスは、独立したスパニングツリー トポロジで実行されます。

ソフトウェアは、従来の 802.1D システムで相互運用できますが、システムでは MST が実行されます。MST は、Cisco Nexus デバイス用のデフォルトの STP プロトコルです。

Note Cisco NX-OS では、拡張システム ID と MAC アドレス リダクションが使用されます。これらの機能はディセーブルにできません。

また、シスコはスパニングツリーの動作を拡張するための独自の機能をいくつか作成しました。

MST

MST は、ソフトウェアのデフォルトのスパニングツリー モードで、デフォルト VLAN および新規作成のすべての VLAN 上で、デフォルトで有効になります。

MST を使用した複数の独立したスパニングツリー トポロジにより、データ トラフィック用に複数の転送パスを提供し、ロード バランシングを有効にして、多数の VLAN をサポートするために必要な STP インスタンスの数を削減できます。

MST には RSTP が統合されているので、高速コンバージェンスもサポートされます。MST では、1 つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）に影響しないため、ネットワークのフォールト トレランスが向上します。

コマンドライン インターフェイスを使用すると、先行標準（標準ではない）の MST メッセージを指定インターフェイスで強制的に送信できます。

STP 拡張機能

このソフトウェアは、次に示すシスコ独自の機能をサポートしています。

- スパニングツリー ポート タイプ：デフォルトのスパニングツリー ポート タイプは、標準（normal）です。レイヤ 2 ホストに接続するインターフェイスをエッジ ポートとして、また、レイヤ 2 スイッチまたはブリッジに接続するインターフェイスをネットワーク ポートとして設定できます。
- BPDU ガード：BPDU ガードは、BPDU を受信したポートをシャットダウンします。
- BPDU フィルタ：BPDU フィルタは、ポート上での BPDU の送受信を抑制します。
- ループ ガード：ループ ガードを使用すると、ポイントツーポイント リンク上の単方向リンク障害によって発生することがあるブリッジング ループを防止できます。

- ルート ガード：STP ルート ガードを使用すると、ポートがルート ポートまたはブロッキングされたポートになることが防止されます。ルート ガードに設定されたポートが上位 BPDU を受信すると、このポートはただちにルートとして一貫性のない（ブロックされた）ステートになります。

トラフィック ストーム制御について

トラフィック ストーム制御しきい値の数値と期間の組み合わせにより、トラフィック ストーム制御アルゴリズムがさまざまな粒度で機能します。しきい値が高いほど、通過できるパケット数が多くなります。

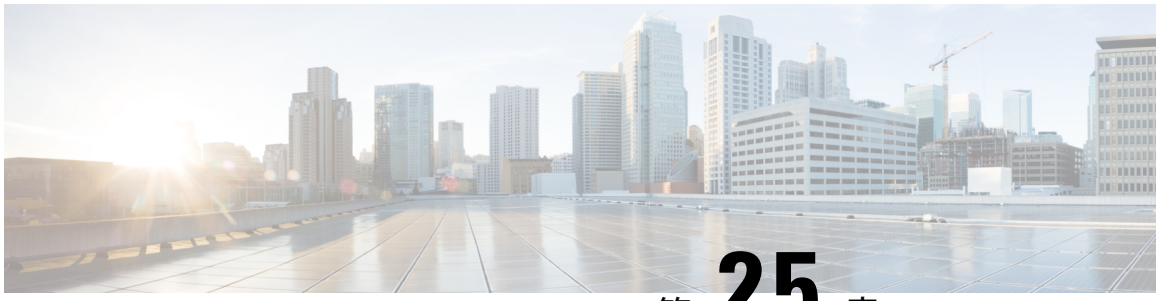
Cisco Nexus 3550-T デバイスのトラフィック ストーム制御はハードウェアに実装されています。トラフィック ストーム制御回路は、レイヤ 2 インターフェイスを通過してスイッチング バスに到着するパケットをモニタリングします。

関連項目

レイヤ 2 スイッチング機能に関連するマニュアルは、次のとおりです。

- *Cisco Nexus® 3550-T* インターフェイス構成セクション
- *Cisco Nexus® 3550-T* セキュリティ構成セクション
- *Cisco Nexus® 3550-T* システム管理構成セクション

関連項目



第 25 章

レイヤ 2 スイッチングの設定

レイヤ 2 スイッチングについて

（注） インターフェイスの作成の詳細については、『』を参照してください。

レイヤ2スイッチング ポートは、アクセス ポートまたはトランク ポートとして設定できます。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。レイヤ 2 スイッチング ポートはすべて、MAC アドレス テーブルを維持します。

レイヤ 2 イーサネット スイッチングの概要

このデバイスは、レイヤ2イーサネット セグメント間の同時パラレル接続をサポートします。イーサネット セグメント間のスイッチド コネクションは、パケットが伝送されている間だけ維持されます。次のパケットには、別のセグメント間に新しい接続が確立されます。

また、このデバイスでは、各デバイス（サーバなど）を独自のコリジョン ドメインに割り当てることによって、広帯域デバイスおよび多数のユーザによって発生する輻輳の問題を解決できます。各 LAN ポートが個別のイーサネット コリジョン ドメインに接続されるので、スイッチド環境のサーバは全帯域幅にアクセスできます。

イーサネット ネットワークではコリジョンによって深刻な輻輳が発生するため、全二重通信を使用することが有効な対処法の 1 つとなります。これらのインターフェイスを全二重モードに

設定すると、2 つのステーション間で同時に送受信を実行できます。パケットを双方向へ同時に送ることができるので、有効なイーサネット帯域幅は 2 倍になります。

セグメント間のフレーム スイッチング

デバイス上の各LANポートは、単一のワークステーション、サーバ、またはワークステーションやサーバがネットワークへの接続時に経由する他のデバイスに接続できます。

信号の劣化を防ぐために、デバイスは各 LAN ポートを個々のセグメントとして処理します。異なる LAN ポートに接続しているステーションが相互に通信する必要がある場合、デバイスは、一方のLANポートから他方のLANポートにワイヤ速度でフレームを転送し、各セッションが全帯域幅を利用できるようにします。

デバイスは、LAN ポート間で効率的にフレームをスイッチングするために、アドレス テーブルを管理しています。デバイスは、フレームを受信すると、受信した LAN ポートに、送信側ネットワーク デバイスのメディア アクセス コントロール（MAC）アドレスを関連付けます。

アドレス テーブルの構築およびアドレス テーブルの変更

デバイスは、受信したフレームの送信元MACアドレスを使用して、アドレス テーブルをダイナミックに構築します。自分のアドレス テーブルに登録されていない宛先MACアドレスを持つフレームを受信すると、デバイスは、そのフレームを同じ VLAN のすべての LAN ポート（受信したポートは除く）に送出します。宛先端末が応答を返してきたら、デバイスは、その応答パケットの送信元 MAC アドレスとポート ID をアドレス テーブルに追加します。以降、その宛先へのフレームを、すべてのLANポートに送出せず、単一のLANポートだけに転送します。

スタティック MAC アドレスと呼ばれる、デバイス上の特定のインターフェイスだけをスタティックに示すMACアドレスを設定できます。スタティックMACアドレスは、インターフェイス上でダイナミックに学習された MAC アドレスをすべて書き換えます。ブロードキャストのアドレスは、スタティック MAC アドレスとして設定できません。スタティック MAC エントリは、デバイスのリブート後も保持されます。

アドレス テーブルは、ハードウェアの I/O モジュールに応じて多数の MAC アドレス エントリを格納できます。デバイスは、設定可能なエージング タイマーによって定義されるエージング メカニズムを使用しているため、アドレスが非アクティブな状態のまま指定時間（秒）が経過すると、そのアドレスはアドレス テーブルから削除されます。

レイヤ 3 スタティック MAC アドレス

スタティック MAC アドレスは、次のレイヤ 3 インターフェイスに設定できます。

- レイヤ 3 インターフェイス
- レイヤ 3 ポート チャネル
- VLAN ネットワーク インターフェイス

（注） トンネル インターフェイスにはスタティック MAC アドレスを設定できません。

レイヤ3インターフェイスの構成の詳細については、『Cisco Nexus Series NX-OS インターフェイス構成ガイド』を参照してください。

MAC アドレス設定の前提条件

MAC アドレスには次の前提条件があります。

- デバイスにログインしていること。
- 必要に応じて、アドバンスド サービスのライセンスをインストールします。

レイヤ 2 スイッチングのデフォルト設定

次の表に、レイヤ 2 スイッチングのパラメータのデフォルト設定を示します。

表 *22:* レイヤ *2* スイッチング パラメータのデフォルト値

パラメータ	デフォルト
エージング タイム	1800 秒

レイヤ 2 スイッチングの設定手順

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

スタティック MAC アドレスの設定

スタティック MAC アドレスと呼ばれる、デバイス上の特定のインターフェイスだけをスタティックに示すMACアドレスを設定できます。スタティックMACアドレスは、インターフェイス上でダイナミックに学習された MAC アドレスをすべて書き換えます。ブロードキャストまたはマルチキャストのアドレスは、スタティック MAC アドレスとして設定できません。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**mac address-table static** *mac-address* **vlan** *vlan-id* {[**drop** | **interface** {*type slot/port*} | **port-channel** *number*]} **Example:** `switch(config)# mac address-table static 1.1.1 vlan 2 interface ethernet 1/2`	レイヤ 2 MAC アドレス テーブルに追加するスタティック MAC アドレスを指定します。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show mac address-table static** **Example:** `switch# show mac address-table static`	スタティック MAC アドレスを表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、レイヤ 2 MAC アドレス テーブルにスタティック エントリを入力する例を示します。

```
switch# config t
switch(config)# mac address-table static 1.1.1 vlan 2 interface ethernet 1/2
switch(config)#
```

レイヤ 3 インターフェイス上のスタティック MAC アドレスの設定

レイヤ 3 インターフェイスのスタティック MAC アドレスを設定できます。ブロードキャストまたはマルチキャストのアドレスは、スタティック MAC アドレスとして設定できません。

レイヤ 3 インターフェイスの構成の詳細については、「レイヤ *3* インターフェイスの構成」セクションを参照してください。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*] **Example:** `switch(config)# interface ethernet 1/3`	レイヤ3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。 **Note** スタティック MAC アドレスを割り当てる前に、レイヤ 3 インターフェイスを作成する必要があります。

ステップ 3	**mac-address** *mac-address*
	Example:
	`switch(config-if)# mac-address 22ab.47dd.ff89`
	`switch(config-if)#`
		レイヤ3インターフェイスに追加するスタティック MAC アドレスを指定します。

ステップ 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイスモードを終了します。

ステップ 5	(Optional) **show interface** [**ethernet** *slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*] **Example:** `switch# show interface ethernet 1/3`	レイヤ3インターフェイスに関する情報を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、スロット 1、ポート 3 上のレイヤ 3 インターフェイスに静的 MAC アドレスを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/3
switch(config-if)# mac-address 22ab.47dd.ff89
switch(config-if)#
```

MAC テーブルのエージング タイムの設定

MACアドレスエントリ（パケットの送信元MACアドレスおよびパケットを学習したポート）を、レイヤ 2 情報を含む MAC テーブルに格納しておく時間を設定できます。

Note MAC アドレスのエージング タイムアウトの最大時間は、設定された MAC アドレス テーブルのエージング タイムアウトの 2 倍です。

Note インターフェイス コンフィギュレーション モードまたはVLAN コンフィギュレーション モードで MAC エージング タイムを設定することもできます。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**mac address-table aging-time** *seconds* **Example:** `switch(config)# mac address-table aging-time 600`	エントリが期限切れになり、レイヤ 2 MACアドレステーブルから廃棄される前にエージング タイムを指定します。指定できる範囲は 120 ～ 918000 秒です。デフォルトは 1800 秒です。0 を入力すると、MAC エージングがディセーブルになります。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show mac address-table aging-time** **Example:** `switch# show mac address-table aging-time`	MACアドレスを保持するエージング タイム設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、レイヤ 2 MAC アドレス テーブルのエントリのエージング タイムを 600 秒（10 分）に設定する例を示します。

```
switch# config t
switch(config)# mac address-table aging-time 600
switch(config)#
```

MAC テーブルからのダイナミック アドレスのクリア

MAC アドレス テーブルにある、すべてのダイナミック レイヤ 2 エントリをクリアできます。（指定したインターフェイスまたは VLAN によりエントリをクリアすることもできます。）

Procedure

	Command or Action	Purpose
ステップ 1	**clear mac address-table dynamic** {**address** *mac_addr*} {**interface** [**ethernet** *slot/port* | **port-channel** *channel-number*]} {**vlan** *vlan_id*} **Example:** `switch# clear mac address-table dynamic`	レイヤ 2 の MAC アドレス テーブルから、ダイナミック アドレス エントリをクリアします。
ステップ 2	(Optional) **show mac address-table** **Example:** `switch# show mac address-table`	MAC Address Table を表示します。

Example

次に、レイヤ 2 MAC アドレス テーブルからダイナミック エントリをクリアする例を示します。

```
switch# clear mac address-table dynamic
switch#
```

レイヤ 2 スイッチング設定の確認

レイヤ 2 スイッチ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。

コマンド	目的
show mac address-table	MAC アドレス テーブルに関する情報を表示します。

コマンド	目的
show mac address-table aging-time	MACアドレステーブルに設定されているエージング タイムの情報を表示します。
show mac address-table static	MACアドレステーブルのスタティック エントリの情報を表示します。
show interface [*interface*] **mac-address**	インターフェイスのMACアドレスとバーンドインMACアドレスを表示します。

レイヤ 2 スイッチングの設定例

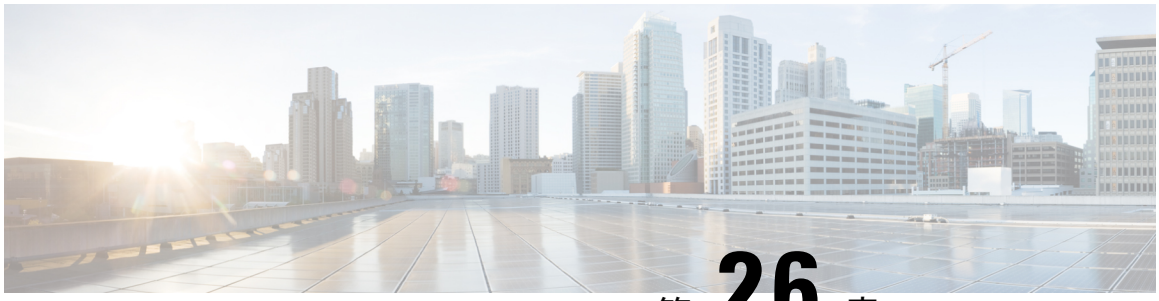
次に、スタティック MAC アドレスを追加し、MAC アドレスのデフォルトのグローバル エージング タイムを変更する例を示します。

```
switch# configure terminal
switch(config)# mac address-table static 0000.0000.1234 vlan 10 interface ethernet 1/15
switch(config)# mac address-table aging-time 120
```

レイヤ 2 スイッチングの追加情報（CLI バージョン）

関連資料

関連項目	マニュアル タイトル
スタティック MAC アドレス	「*Cisco Nexus® 3550-T* セキュリティの設定」セクション
インターフェイス	「*Cisco Nexus® 3550-T* インターフェイスの構成」セクション
システム管理	「*Cisco Cisco Nexus® 3550-T* システム管理構成」セクション



第 26 章

Cisco NX-OS を使用した MST の設定

MST について

Note レイヤ 2 インターフェイスの作成の詳細については、「*Cisco Nexus® 3550-T* インターフェイス構成」のセクションを参照してください。

IEEE 802.1s 標準の MST を使用すると、スパニングツリー インスタンスに複数の VLAN を割り当てることができます。MST は、デフォルトのスパニングツリー モードではありません。Rapid per VLAN Spanning Tree（Rapid PVST+）がデフォルト モードです。MST インスタンスは、同じ名前、リビジョン番号、VLAN からインスタンスへのマッピングと組み合わされて、MST 領域が形成されます。MST 領域は、領域外のスパニングツリー設定への単一のブリッジとして表示されます。MST がネイバー デバイスから IEEE 802.1D スパニングツリー プロトコル（STP）メッセージを受信すると、該当するインターフェイスとの境界が形成されます。

Note このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。このマニュアルで IEEE 802.1D スパニングツリー プロトコルに関して説明する場合は、具体的に 802.1D と表記されます。

MST の概要

Note MST はデフォルトのスパニングツリー モードです。

MST では、各 MST インスタンスで IEEE 802.1w 規格を採用することによって、明示的なハンドシェイクによる高速収束が可能なため、802.1D 転送遅延がなくなり、ルート ブリッジ ポートと指定ポートが迅速にフォワーディング ステートに変わります

デバイスでは常にMACアドレス リダクションがイネーブルです。この機能はディセーブルにはできません。

MST ではスパニング ツリーの動作が改善され、元の 802.1D スパニング ツリープロトコル STP バージョンとの後方互換性を維持しています。

Note

- IEEE 802.1 は、Rapid Spanning Tree Protocol（RSTP）で定義されて、IEEE 802.1D に組み込まれました。
- IEEE 802.1 は MST で定義され、IEEE 802.1Q に組み込まれました。

。

MST 領域

MST インスタンスにデバイスを参加させるには、常に同じ MST 設定情報を使用してデバイスを設定する必要があります。

同一の MST 設定を持つ、相互接続されたデバイスの集合を MST 領域といいます。MST リージョンは、同じ MST 設定で MST ブリッジのグループとリンクされます。

MST 設定により、各デバイスが属する MST 領域が制御されます。この設定には、領域名、リビジョン番号、VLAN/MST インスタンス割り当てマッピングが含まれます。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。各メンバには、802.1w Bridge Protocol Data Unit（BPDU：ブリッジ プロトコル データ ユニット）を処理する機能が必要です。ネットワーク内の MST リージョンには、数の制限はありません。

各デバイスは、単一の MST 領域内で、MST インスタンス（インスタンス 0）のみをサポート可能です。VLAN は、一度に 1 つの MST インスタンスに対してのみ割り当てることができます。

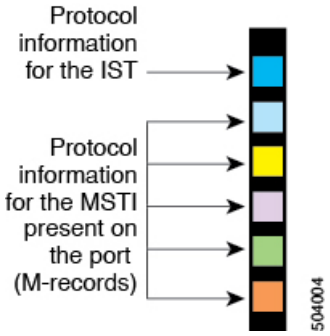
MST 領域は、隣接の MST 領域、他の 802.1D スパニングツリープロトコルへの単一のブリッジとして表示されます。

Note ネットワークを、非常に多数の領域に分けることは推奨しません。

MST BPDU

各デバイスで使用できる MST BPDU は、インターフェイスごとに 1 つだけです。この BPDU が、デバイス上の各 MSTI の M レコードを伝達します。IST だけが MST リージョンの BPDU を送信します。すべての M レコードは、IST が送信する 1 つの BPDU でカプセル化されています。MST BPDU にはすべてのインスタンスに関する情報が保持されるため、MST をサポートするために処理する必要がある BPDU の数は、非常に少なくなります。

Figure 22: MSTI の M レコードが含まれる MST BPDU



MST 設定情報

単一の MST 領域内にあるすべてのデバイスで MST 設定を同一にする必要がある場合は、ユーザ側で設定します。

MST 設定では、次の 3 つのパラメータを設定できます。

- 名前：32 文字の文字列。MST リージョンを指定します。ヌルで埋められ、ヌルで終了します。
- リビジョン番号：現在の MST 設定のリビジョンを指定する 16 ビットの符号なし数字。

Note MST 設定の一部として必要な場合、リビジョン番号を設定する必要があります。MST 設定をコミットするたびにリビジョン番号が自動的に増加することはありません。

- VLAN/MST インスタンス マッピング：要素が 4096 あるテーブルで、サポート対象の、存在する可能性のある各 VLAN が該当のインスタンスに関連付けられます。最初（0）と最後（4095）の要素は 0 に設定されています。要素番号 X の値は、VLAN X がマッピングされるインスタンスを表します。

Note VLAN/MSTI マッピングを変更すると、MST が再コンバージェンスされます。

MST BPDU には、これらの 3 つの設定パラメータが含まれています。MST ブリッジは、これら 3 つの設定パラメータが厳密に一致する場合、MST BPDU をそのリージョンに受け入れます。設定属性が 1 つでも異なっていると、MST ブリッジでは、BPDU が別の MST リージョンのものであると見なされます。

IST、CIST、CST

IST、CIST、CST の概要

MST は、次のように IST、CIST、および CST スパニング ツリーを確立および維持します。

- IST は、MST 領域で実行されるスパニングツリーです。

  MST は、それぞれの MST 領域内で追加のスパニングツリーを確立して維持します。このスパニングツリーは、Multiple Spanning Tree Instance（MSTI）と呼ばれます。

  インスタンス 0 は、IST という、領域の特殊インスタンスです。IST は、すべてのポートに必ず存在します。IST（インスタンス 0）は削除できません。デフォルトでは、すべての VLAN が IST に割り当てられます。その他すべての MSTI には、1 ～ 4094 の番号が付きます。

  IST は、BPDU の送受信を行う唯一の STP インスタンスです。他の MSTI 情報はすべて MST レコード（M レコード）に含まれ、MST BPDU 内でカプセル化されます。

  同じリージョン内のすべての MSTI は同じプロトコル タイマーを共有しますが、各 MSTI には、ルート ブリッジ ID やルート パス コストなど、それぞれ独自のトポロジ パラメータがあります。

  MSTI は、リージョンに対してローカルです。たとえば、リージョン A とリージョン B が相互接続されている場合でも、リージョン A にある MSTI 9 は、リージョン B にある MSTI 9 には依存しません。領域の境界をまたいで使用されるのは、CST 情報だけです。

- CST は、MST リージョンと、ネットワーク上で実行されている可能性がある 802.1D および 802.1w STP のインスタンスを相互接続します。CST は、ブリッジ型ネットワーク全体で 1 つ存在する STP インスタンスで、すべての MST リージョン、802.1w インスタンスおよび 802.1D インスタンスを含みます。

- CIST は、各 MST リージョンの IST の集合です。CIST は、MST リージョン内部の IST や、MST リージョン外部の CST と同じです。

MST 領域で計算されるスパニングツリーは、スイッチ ドメイン全体を含んだ CST 内のサブツリーとして認識されます。CIST は、802.1w、802.1s、802.1D 標準をサポートするデバイスで動作するスパニングツリーアルゴリズムによって形成されます。MST リージョン内の CIST は、リージョン外の CST と同じです。

MST 領域内でのスパニングツリーの動作

IST は領域内のすべての MST デバイスを接続します。IST が収束すると、IST のルートは CIST リージョナル ルートになります。ネットワークに領域が 1 つしかない場合、CIST リージョナル ルートは CIST ルートにもなります。CIST ルートが領域外にある場合、領域の境界にある MST デバイスの 1 つが CIST リージョナル ルートとして選択されます。

MST デバイスは、初期化されると、CIST のルートおよび CIST リージョナル ルートとして自分自身を識別する BPDU を送信します。BPDU では、CIST ルートのパス コストおよび CIST リージョナル ルートへのパス コストの両方がゼロに設定されます。このデバイスはすべての MSTI も初期化し、そのすべてのルートであることを申告します。このデバイスは、ポートで現在保存されている情報よりも優位の MSTI ルート情報（低いスイッチ ID や低いパス コストなど）を受信すると、CIST リージョナル ルートとしての申告を放棄します。

初期化中に、MST リージョン内に独自の CIST リージョナル ルートを持つ多くのサブ リージョンが形成される場合があります。デバイスは、同一領域のネイバーから優位 IST 情報を受信すると、古いサブ領域を離れ本来の CIST リージョナル ルートを含む新しいサブ領域に加わります。このようにして、真の CIST リージョナル ルートが含まれているサブ リージョン以外のサブ領域はすべて縮小します。

MST 領域内のすべてのデバイスは、同一 CIST リージョナル ルートで合意する必要があります。領域内の任意の 2 つのデバイスは、共通 CIST リージョナル ルートに収束する場合、MSTI のポート ロールのみを同期化します。

MST 領域間のスパニングツリー動作

領域または 802.1w か 802.1D の STP インスタンスがネットワーク内に複数ある場合、MST は CST を確立して維持します。これには、ネットワークのすべての MST 領域およびすべての 802.1w と 802.1D の STP デバイスが含まれます。MSTI は、リージョンの境界で IST と結合して CST になります。

IST は領域内のすべての MST デバイスを接続し、スイッチド ドメイン全体を網羅する CIST でサブツリーのように見えます。サブツリーのルートは CIST リージョナル ルートです。隣接する STP デバイスおよび MST 領域には、MST 領域が仮想デバイスのように見えます。

MST 用語

MST の命名規則には、内部パラメータまたはリージョナル パラメータの識別情報が含まれます。これらのパラメータは MST 領域内だけで使用され、ネットワーク全体で使用される外部パラメータと比較されます。CIST だけがネットワーク全体に広がるスパニングツリー インスタンスなので、CIST パラメータだけに外部修飾子が必要になり、修飾子またはリージョン修飾子は不要です。MST 用語を次に示します。

- CIST ルートは CIST のルート ブリッジで、ネットワーク全体にまたがる一意のインスタンスです。
- CIST 外部ルート パス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。CIST には、MST 領域が単一のデバイスのように見えます。CIST 外部

ルート パス コストは、この仮想デバイス、およびどの領域にも属さないデバイスの間で計算されるルート パス コストです。

- CIST ルートが領域内にある場合、CIST リージョナル ルートは CIST ルートです。CIST ルートが領域内にない場合、CIST リージョナル ルートは領域内の CIST ルートに最も近いデバイスです。CIST リージョナル ルートは、IST のルート ブリッジとして動作します。
- CIST 内部ルート パス コストは、領域内の CIST リージョナル ルートまでのコストです。このコストは、IST つまりインスタンス 0 だけに関連します。

ホップ カウント

MST リージョン内の STP トポロジを計算する場合、MST はコンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報は使用しません。代わりに、ルートへのパス コストと、IP の存続可能時間（TTL）メカニズムに類似したホップ カウント メカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用すると、領域内の最大ホップ数を設定し、IST およびその領域のすべての MSTI に適用できます。

ホップ カウントは、メッセージ エージ情報と同じ結果になります（再設定を開始）。インスタンスのルート ブリッジは、コストが 0 でホップ カウントが最大値に設定された BPDU（M レコード）を常に送信します。デバイスは、この BPDU を受信すると、受信した残存ホップ カウントから 1 を差し引き、生成する BPDU の残存ホップ カウントとしてこの値を伝播します。カウントがゼロに達すると、デバイスは BPDU を廃棄し、ポート用に維持されている情報をエージングします。

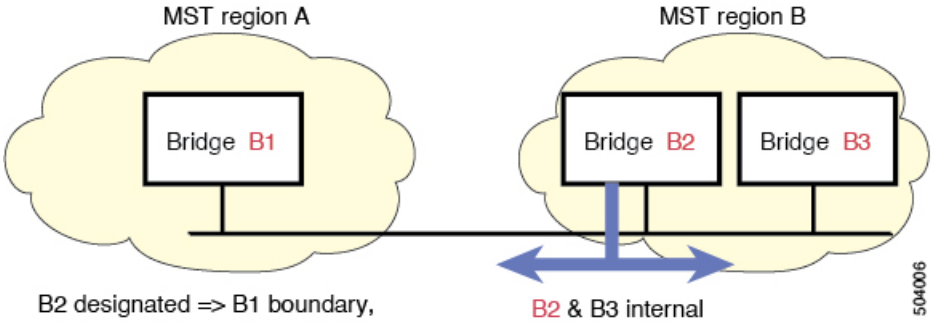
BPDU の 802.1w 部分に格納されているメッセージ有効期間および最大エージング タイムの情報は、領域全体で同じです（IST の場合のみ）。同じ値が、境界にある領域の指定ポートによって伝播されます。

最大エージング タイムは、デバイスがスパニングツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数です。

境界ポート

境界ポートは、LAN に接続されたポートで、その代表ブリッジは、MST 構成が異なるブリッジ（つまり、別の MST 領域）、802.1D STP ブリッジです。指定ポートは、STP ブリッジを検出するか、構成が異なる MST ブリッジから同意メッセージを受信すると、境界にあることを認識します。この定義では、領域内部の 2 つのポートが、別の領域に属するポートとセグメントを共有でき、そのため内部メッセージおよび外部メッセージの両方をポートで受信する可能性があります。

Figure 23: MST 境界ポート



境界では、MST ポートのロールは問題ではなく、そのステートは強制的に IST ポート ステートと同じに設定されます。境界フラグがポートに対してオンに設定されている場合、MST ポートのロールの選択処理では、ポートのロールが境界に割り当てられ、同じステートが IST ポートのステートとして割り当てられます。境界にある IST ポートでは、バックアップ ポートのロール以外のすべてのポートのロールを引き継ぐことができます。

ポート コストとポート プライオリティ

スパニングツリーはポート コストを使用して、指定ポートを決定します。値が低いほど、ポート コストは小さくなります。スパニングツリーでは、最小のコスト パスが選択されます。デフォルト ポート コストは、次のように、インターフェイス帯域幅から取得されます。

- 1 ギガビット イーサネット：20,000
- 10 ギガビット イーサネット：2,000
- 40 ギガビット イーサネット：500

ポート コストを設定すると、選択されるポートが影響を受けます。

Note MST では常にロング パスコスト計算方式が使用されるため、有効値は 1 ～ 200,000,000 です。

コストが同じポートを差別化するために、ポート プライオリティが使用されます。値が小さいほど、プライオリティが高いことを示します。デフォルトのポートの優先順位は 128 です。プライオリティは、0 ～ 224 の間の値に、32 ずつ増やして設定できます。

IEEE 802.1D との相互運用性

MST を実行するデバイスでは組み込みプロトコル移行機能がサポートされ、802.1D STP デバイスとの相互運用が可能になります。このデバイスで 802.1D コンフィギュレーション BPDU（プロトコル バージョンが 0 に設定されている BPDU）を受信する場合、そのポート上の 802.1D BPDU のみが送信されます。また、MST デバイスは、802.1D BPDU、別の領域に関連

する MST BPDU（バージョン 3）、802.1w BPDU（バージョン 2）のうちいずれかを受信すると、ポートが領域の境界にあることを検出できます。

ただし、このデバイスは、802.1D BPDU を受信しなくなっても、MST モードに自動的に戻りません。802.1D デバイスが指定デバイスでない場合、802.1D デバイスがリンクから削除されたかどうかを検出できないからです。このデバイスの接続先デバイスが領域に加わったとき、デバイスは境界ロールをポートに割り当て続けることもあります。

プロトコル移行プロセスを再開する（強制的に隣接デバイスと再ネゴシエーションさせる）には、**clear spanning-tree detected-protocols** コマンドを入力します。

リンク上にあるすべての 8021.D STP スイッチでは、MST BPDU を 802.1w BPDU の場合と同様に処理できます。MST デバイスは、バージョン 0 設定とトポロジ変更通知（TCN）BPDU、またはバージョン 3 MST BPDU のどちらかを境界ポートで送信できます。境界ポートは LAN に接続します。つまり、単一スパニングツリー デバイスまたは MST 設定が異なるデバイスのいずれかである指定デバイスに接続します。

MST は、MST ポート上で先行標準 MSTP を受信するたびに、シスコの先行標準 MSTP と相互に動作します。明示的な設定は必要ありません。

また、インターフェイスを設定して、先行標準の MSTP メッセージを事前に送信することもできます。

MST のハイ アベイラビリティ

ソフトウェアは MST に対してハイ アベイラビリティをサポートしています。ただし、MST を再起動した場合、統計情報およびタイマーは復元されません。タイマーは最初から開始され、統計情報は 0 にリセットされます。

MST の前提条件

MST には次の前提条件があります。

- デバイスにログインしていること。

MST の設定に関するガイドラインおよび制約事項

（注） VLAN/MSTI マッピングを変更すると、MST が再コンバージェンスされます。

MST 設定時のガイドラインと制約事項は次のとおりです。

- MST 構成制限については、『*Cisco Nexus® 3550-T* 検証済み拡張性ガイド』を参照してください。

- キーワードが付いている**show**コマンド**internal**はサポートされていません。
- MST はデフォルトのスパニングツリー モードです。
- VLAN は、Cisco Nexus® 3550-T スイッチの 1 つの MST インスタンスにのみ割り当てることができます。
- デフォルトでは、すべての VLAN が MSTI 0（IST）にマッピングされます。
- ロード バランスは、MST 領域の内部でのみ実行できます。
- MSTI にマッピングされたすべての VLAN が、トランクによって伝送されているか、または伝送から除外されていることを確認します。
- STP は常にイネーブルのままにしておきます。
- タイマーは変更しないでください。ネットワークの安定性が低下することがあります。
- ユーザ トラフィックを管理 VLAN から切り離し、管理 VLAN をユーザ データから分離します。
- プライマリおよびセカンダリ ルート スイッチの場所として、ディストリビューション レイヤおよびコア レイヤを選択します。
- ポート チャネリング：ポート チャネル バンドルは、単一ポートと見なされます。ポート コストは、そのチャネルに割り当てられている設定済みのすべてのポート コストの合計です。
- VLAN を MSTI にマッピングすると、この VLAN が以前の MSTI から自動的に削除されます。
- 1 つの MSTI に任意の個数の VLAN をマッピングできます。
- ネットワークを多数の領域に分割しないでください。ただしこの状況を避けられない場合は、レイヤ 2 デバイスによって相互接続された、より小さい LAN にスイッチド LAN を分割することを推奨します。
- MST 設定サブモードの場合、次の注意事項が適用されます。
  - 各コマンド参照行により、保留中のリージョン設定が作成されます。
  - 保留中のリージョン設定により、現在のリージョン設定が開始されます。
  - 変更をコミットすることなく MST コンフィギュレーション サブモードを終了するには、**abort** コマンドを入力します。
  - MST コンフィギュレーション サブモードを終了し、サブモードを終了する前に行ったすべての変更をコミットするには、**exit** または **end** コマンドを入力するか、または **Ctrl + Z** キーを押します。

MST のデフォルト設定

次の表に、MST パラメータのデフォルト設定を示します。

Table 23: デフォルトの ***MST*** パラメータ

パラメータ	デフォルト
スパニングツリー	有効（Enabled）
名前	空の文字列
VLAN マッピング	すべての VLAN を CIST インスタンスにマッピング
改定	0
[インスタンス ID（Instance ID）]	インスタンス 0。VLAN 1 ～ 3967 はデフォルトでインスタンス 0 にマッピングされます。
MST 領域ごとの MSTI	Cisco Nexus® 3550-T スイッチでは、MST の単一インスタンスのみが許可されます
ブリッジ プライオリティ（CIST ポート単位で設定可能）	32768
スパニングツリーポートプライオリティ（CIST ポート単位で設定可能）	128
スパニングツリー ポート コスト（CIST ポート単位で設定可能）	Auto デフォルトのポート コストは、次のように、ポート速度から判別されます。 • 1 ギガビット イーサネット：20,000 • 10 ギガビット イーサネット：2,000 • 40 ギガビット イーサネット：500
hello タイム	2 秒
転送遅延時間	15 秒
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

パラメータ	デフォルト
リンク タイプ	Auto デフォルト リンク タイプは、次のようにデュプレックスから判別されます。 • 全二重：ポイントツーポイント リンク • 半二重：共有リンク

MST の設定

Note Cisco IOS の CLI に慣れている場合、この機能のシスコ ソフトウェア コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

MST のイネーブル化（CLI バージョン）

MST はデフォルトのスパニング ツリー モードです。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mode mst**. **Example:** `switch(config)# spanning-tree mode mst`	• **spanning-tree mode mst** デバイスの MST をイネーブルにします。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show running-config spanning-tree all** **Example:** `switch# show running-config spanning-tree all`	現在稼働している STP コンフィギュレーションを表示します。

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

Example

次に、デバイス上で MST をイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree mode mst
switch(config)# exit
switch#
```

MST コンフィギュレーション モードの開始

デバイスに MST 名、VLAN/インスタンス マッピング、および MST リビジョン番号を設定するには、MST コンフィギュレーション モードを開始します。

複数のデバイスが同じ MST 領域内にある場合は、これらのデバイスの MST 名、VLAN/インスタンス マッピング、および MST リビジョン番号を同一にする必要があります。

Note 各コマンド参照行により、MST コンフィギュレーション モードで保留中の領域設定が作成されます。さらに、保留中の領域設定により、現在の領域設定が開始されます。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst configuration** または **no spanning-tree mst configuration**
	Example:
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		• **spanning-tree mst configuration**
		システム上で、MST 設定サブモードを開始します。次の MST 設定パラメータを割り当てるには、MST 設定サブモードを開始しておく必要があります。
		• MST 名

	Command or Action	Purpose
		• VLAN/MSTI マッピング • MST リビジョン番号 • **no spanning-tree mst configuration** MST リージョン設定を次のデフォルト値に戻します。 • 領域名は空の文字列になります。 • VLAN は MSTI にマッピングされません（すべての VLAN は CIST インスタンスにマッピングされます）。 • リビジョン番号は 0 です。

ステップ 3	**exit** または **abort**
	Example:
	`switch(config-mst)# exit`
	`switch(config)#`
		• **exit**
		すべての変更をコミットし、MST 設定サブモードを終了します。
		• **abort**
		いずれの変更もコミットすることなく、MST 設定サブモードを終了します。

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

Example

次に、デバイスでMST コンフィギュレーション サブモードを開始する例を示します。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)# exit
switch(config)#
```

MST の名前の指定

ブリッジに領域名を設定できます。複数のブリッジが同じ MST 領域内にある場合は、これらのブリッジの MST 名、VLAN/インスタンス マッピング、および MST リビジョン番号を同一にする必要があります。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst configuration**
	Example:
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

ステップ 3	**name** *name* **Example:** `switch(config-mst)# name accounting`	MST 領域の名前を指定します。*name* 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。デフォルトは空の文字列です。

ステップ 4	**exit** または **abort**
	Example:
	`switch(config-mst)# exit`
	`switch(config)#`
		• **exit**
		すべての変更をコミットし、MST 設定サブモードを終了します。
		• **abort**
		いずれの変更もコミットすることなく、MST 設定サブモードを終了します。

ステップ 5	(Optional) **show spanning-tree mst configuration** **Example:** `switch# show spanning-tree mst configuration`	MST の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、MST リージョンの名前の設定方法を示しています。

```
switch# config t
switch(config)#  spanning-tree mst configuration
switch(config-mst)# name accounting
switch(config-mst)# exit
switch(config)#
```

MST 設定のリビジョン番号の指定

リビジョン番号は、ブリッジ上に設定します。複数のブリッジが同じ MST 領域内にある場合は、これらのブリッジの MST 名、VLAN/インスタンス マッピング、および MST リビジョン番号を同一にする必要があります。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst configuration**
	Example:
	`switch(config)# spanning-tree mst configuration`
	`switch(config-mst)#`
		MST コンフィギュレーション サブモードを開始します。

ステップ 3	**revision** *version* **Example:** `switch(config-mst)# revision 5`	MST リージョンのリビジョン番号を指定します。範囲は 0 ～ 65535 で、デフォルト値は 0 です。

ステップ 4	**exit** または **abort**
	Example:
	`switch(config-mst)# exit`
	`switch(config)#`
		• **exit**
		すべての変更をコミットし、MST 設定サブモードを終了します。
		• **abort**
		いずれの変更もコミットすることなく、MST 設定サブモードを終了します。

ステップ 5	(Optional) **show spanning-tree mst configuration** **Example:**	MST の設定を表示します。

	Command or Action	Purpose
	`switch# show spanning-tree mst configuration`	
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、MSTI 領域のリビジョン番号を 5 に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst configuration
switch(config-mst)# revision 5
switch(config-mst)#
```

ルート ブリッジの設定

MST ルート ブリッジになるデバイスを設定できます。

spanning-tree vlan *vlan_ID* **primary root** ルート ブリッジになるために必要な値が 4096 より小さい場合は、このコマンドは機能しません。ソフトウェアでブリッジプライオリティをそれ以上低くできない場合、デバイスは次のメッセージを返します。

```
Error: Failed to set root bridge for VLAN 1
It may be possible to make the bridge root by setting the priority
for some (or all) of these instances to zero.
```

Note 各 MSTI のルート ブリッジは、バックボーンまたはディストリビューション デバイスである必要があります。アクセス デバイスは、スパニングツリーのプライマリ ルート ブリッジとして設定しないでください。

diameterを入力します レイヤ 2 ネットワークの直径（レイヤ 2 ネットワーク上の任意の 2 台の端末間における最大レイヤ 2 ホップ カウント）を指定するには、MSTI 0（IST）専用のキーワードを入力します。ネットワーク直径を指定すると、デバイスは、その直径のネットワークで最適な hello タイム、転送遅延時間、最大エージング タイムを自動的に設定し、これによって収束時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムをオーバーライドできます。

Note ルート ブリッジとして設定されたデバイスで、以下のコマンドを使用して、hello タイム、転送遅延時間、最大エージング タイムを手動で設定しないでください。**spanning-tree mst hello-timespanning-tree mst forward-time**、および **spanning-tree mst max-age** グローバル コンフィギュレーション コマンド。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]] or **no spanning-tree mst** *instance-id* **root** **Example:** `switch(config)# spanning-tree mst 5 root primary`	• **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia* [**hello-time** *hello-time*]] 次のようにルート ブリッジとしてデバイスを設定します。 • *instance-id* には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定します。範囲は 1 ～ 4094 です。 • **diameter** *net-diameter* には、任意の 2 つのエンド ステーション間にレイヤ 2 ホップの最大数を指定します。デフォルトは 7 です。このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • **hello-time** には *seconds* には、ルートブリッジが設定メッセージを生成するインターバルを秒単位で指定します。有効範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。 • **no spanning-tree mst** *instance-id* **root**

	Command or Action	Purpose
		スイッチのプライオリティ、範囲、hello タイムをデフォルト値に戻します。

ステップ 3	**exit** または **abort**
	Example:
	`switch(config)# exit`
	`switch#`
		• **exit**
		すべての変更をコミットし、MST 設定サブモードを終了します。
		• **abort**
		いずれの変更もコミットすることなく、MST 設定サブモードを終了します。

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

Example

次に、デバイスを MSTI 5 のルート スイッチに設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst 5 root primary
switch(config)# exit
switch(config)#
```

MST セカンダリ ルート ブリッジの設定

複数のバックアップ ルート ブリッジを設定するには、複数のデバイスでこのコマンドを使用します。**spanning-tree mst root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート ブリッジを設定したときに使用したのと同じネットワーク直径と hello タイムの値を入力します。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia*[**hello-time** *hello-time*]] or **no spanning-tree mst** *instance-id* **root** **Example:** `switch(config)# spanning-tree mst 0 root secondary`	• **spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *dia*[**hello-time** *hello-time*]] 次のようにセカンダリ ルート ブリッジとしてデバイスを設定します。 • *instance-id* には、単一の MSTI ID を指定します。 • **diameter** *net-diameter* には、任意の 2 つのエンド ステーション間にレイヤ 2 ホップの最大数を指定します。デフォルトは 7 です。このキーワードは、MSTI インスタンス 0 の場合にのみ使用できます。 • **hello-time** には *seconds* には、ルートブリッジが設定メッセージを生成するインターバルを秒単位で指定します。有効範囲は 1 ～ 10 秒で、デフォルトは 2 秒です。 • **no spanning-tree mst** *instance-id* **root** スイッチのプライオリティ、範囲、hello タイムをデフォルト値に戻します。

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

ステップ 4	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。

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

Example

次に、デバイスを MSTI 0 のセカンダリ ルートスイッチに設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst 0 root secondary
switch(config)# exit
switch#
```

MST スイッチ プライオリティの設定

MST インスタンスのスイッチ プライオリティを設定し、指定デバイスがルート ブリッジとして選択される可能性を高めることができます。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst** *instance-id* **priority** *priority-value* **Example:** `switch(config)# spanning-tree mst 0 priority 4096`	次のようにデバイス プライオリティを設定します。 • *instance-id* には、単一の MSTI ID を指定します。 • *priority-value* の範囲は 0 ～ 61440 で、4096 ずつ増加します。デフォルト値は32768 です。数値を小さくすると、ルート ブリッジとしてデバイスが選択される可能性が高くなります。 使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、

	Command or Action	Purpose
		61440 です。システムでは、他のすべての値が拒否されます。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、MSTI 0 のブリッジのプライオリティを 4096 に構成する方法を示しています。

```
switch# config t
switch(config)# spanning-tree mst 0 priority 4096
switch(config)# exit
switch#
```

MST ポート プライオリティの設定

ループが発生する場合、MST は、フォワーディング ステートにするインターフェイスを選択するとき、ポートプライオリティを使用します。最初に選択させるインターフェイスには低いプライオリティの値を割り当て、最後に選択させるインターフェイスには高いプライオリティの値を割り当てることができます。すべてのインターフェイスのプライオリティ値が同一である場合、MSTはインターフェイス番号が最も低いインターフェイスをフォワーディング ステートにして、その他のインターフェイスをブロックします。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	Command or Action	Purpose

ステップ 2	**interface** {{*type slot/port*} | {**port-channel** *number*}}
	Example:
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		設定する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	**spanning-tree mst** *instance-id* **port-priority** *priority* **Example:** `switch(config-if)# spanning-tree mst 0 port-priority 64`	次のように、ポートのプライオリティを設定します。 • *instance-id* には、単一の MSTI ID を指定します。 • *priority* の範囲は 0 ～ 224 で、32 ずつ増加します。デフォルト値は 128 です。値が小さいほど、プライオリティが高いことを示します。 プライオリティ値は、0、32、64、96、128、160、192、224 です。システムでは、他のすべての値が拒否されます。

ステップ 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイスモードを終了します。

ステップ 5	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、イーサネット ポート 1/1 で MSTI 0 の MST インターフェイス ポートの優先順位を 64 に設定する方法を示しています。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# spanning-tree mst 0 port-priority 64
switch(config-if)# exit
switch(config)#
```

MST ポート コストの設定

MST ポート コストのデフォルト値は、インターフェイスのメディア速度から抽出されます。ループが発生した場合、MST は、コストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択させるインターフェイスには小さいコストの値を割り当て、最後に選択させるインターフェイスの値には大きいコストを割り当てることができます。すべてのインターフェイスのコスト値が同一である場合、MST はインターフェイス番号が最も低いインターフェイスをフォワーディング ステートにして、その他のインターフェイスをブロックします。

Note MST はロング パスコスト計算方式を使用します。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** {{*type slot/port*} | {**port-channel** *number*}}
	Example:
	`switch# config t`
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		設定する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	**spanning-tree mst** *instance-id* **cost** {*cost* | *auto*} **Example:** `switch(config-if)# spanning-tree mst 0 cost 17031970`	コストを設定します。 ループが発生した場合、MST はパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストが小さいほど、送信速度が速いことを示します。 • *instance-id* には、単一の MSTI ID を指定します。 • *cost* の範囲は 1 ～ 200000000 です。デフォルト値は **auto** で、インターフェイスのメディア速度から取得されるものです。
ステップ 4	**exit** **Example:**	インターフェイスモードを終了します。

	Command or Action	Purpose
	`switch(config-if)# exit` `switch(config)#`	
ステップ 5	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、イーサネット ポート 1/1 で MSTI 0 の MST インターフェイス ポート コストを設定する方法を示しています。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# spanning-tree mst 0 cost 17031970
switch(config-if)# exit
switch(config)#
```

MST hello タイムの設定

デバイス上のすべてのインスタンスに対してルートブリッジが作成する設定メッセージの間隔を設定するには、hello タイムを変更します。

Note **spanning-tree mst hello-time** コマンドを使用するときは注意してください。ほとんどの場合、hello タイムを変更するには、**spanning-tree mst** *instance-id* **root primary** および **spanning-tree mst** *instance-id* **root secondary** のグローバル コンフィギュレーション コマンドの使用を推奨します。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst hello-time** *seconds* **Example:**	MST インスタンスについて、hello タイムを構成します。hello タイムは、ルー

	Command or Action	Purpose
	`switch(config)# spanning-tree mst hello-time 1`	トブリッジが設定メッセージを生成する時間です。これらのメッセージは、デバイスが動作していることを示します。*seconds* の範囲は 1 ～ 10 で、デフォルトは 2 秒です。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、デバイスの hello タイムを 1 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst hello-time 1
switch(config)# exit
switch#
```

MST 転送遅延時間の設定

デバイスの MST インスタンスの転送遅延時間を 1 つのコマンドで設定できます。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst forward-time** *seconds* **Example:**	MST インスタンスについて、転送時間を構成します。転送遅延は、スパニングツリー ブロッキング ステートとラーニ

	Command or Action	Purpose
	`switch(config)# spanning-tree mst forward-time 10`	ング ステートからフォワーディング ステートに変更する前に、ポートが待つ秒数です。*seconds* の範囲は 4 ～ 30 で、デフォルトは 15 秒です。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、デバイスの転送遅延時間を 10 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-time mst forward-time 10
switch(config)# exit
switch#
```

MST 最大エージング タイムの設定

デバイスの MST インスタンスの最大エージング タイマーを 1 つのコマンドで設定できます（最大エージング タイムが適用されるのは IST のみです）。

最大エージング タイマーは、デバイスがスパニングツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数です。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	Command or Action	Purpose
ステップ 2	**spanning-tree mst max-age** *seconds* **Example:** `switch(config)# spanning-tree mst max-age 40`	MST インスタンスについて、最大エージング タイムを構成します。最大エージング タイムは、デバイスがスパニングツリー設定メッセージを受信せずに再設定を試行するまで待機する秒数です。*seconds* の範囲は 6 ～ 40 で、デフォルトは 20 秒です。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、デバイスの最大エージング タイマーを 40 秒に設定する例を示します。

```
switch# config t
switch(config)# spanning-tree mst max-age 40
switch(config)# exit
switch#
```

MST 最大ホップ カウントの設定

領域内の最大ホップを構成し、それをその領域内にある IST およびす MST インスタンスに適用できます。MST では、IST リージョナル ルートへのパス コストと、IP の存続可能時間（TTL）メカニズムに類似したホップ カウント メカニズムが、使用されます。ホップ カウントを設定すると、メッセージエージ情報を設定するのと同様の結果が得られます（再構成の開始時期を決定します）。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree mst max-hops** *hop-count* **Example:** `switch(config)# spanning-tree mst max-hops 40`	BPDUが廃棄され、ポートに維持されていた情報が期限切れになるまでの、領域内でのホップ カウントを指定します。*hop-count* の範囲は 1 ～ 255 で、デフォルト値は 20 ホップです。

ステップ 3	**exit**
	Example:
	`switch(config-mst)# 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	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、最大ホップ カウントを 40 に設定する方法を示しています。

```
switch# config t
switch(config)# spanning-tree mst max-hops 40
switch(config)# exit
switch#
```

先行標準 MSTP メッセージを事前に送信するインターフェイスの設定（CLI バージョン）

デフォルトで、MST を実行中のデバイス上のインターフェイスは、別のインターフェイスから先行標準MSTPメッセージを受信したあと、標準ではなく先行標準のMSTPメッセージを送信します。インターフェイスを設定して、先行標準の MSTP メッセージを事前に送信できます。つまり、指定されたインターフェイスは、先行標準MSTPメッセージの受信を待機する必要がなく、この設定のインターフェイスは常に先行標準 MSTP メッセージを送信します。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree mst pre-standard** **Example:** `switch(config-if)# spanning-tree mst pre-standard`	インターフェイスが MSTP 標準形式ではなく、先行標準形式の MSTP メッセージを常に送信するように指定します。

ステップ 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイスモードを終了します。

ステップ 5	(Optional) **show spanning-tree mst** **Example:** `switch# show spanning-tree mst`	MST の設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、MSTP メッセージを常に先行標準形式で送信するように、MST インターフェイスを設定する例を示します。

```
switch# config t
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree mst pre-standard
switch(config-if)# exit
switch(config)#
```

MST のリンク タイプの指定（CLI バージョン）

Rapid の接続性（802.1w 規格）は、ポイントツーポイントのリンク上でのみ確立されます。リンク タイプは、デフォルトでは、インターフェイスのデュプレックス モードから制御されます。全二重ポートはポイントツーポイント接続であると見なされ、半二重ポートは共有接続であると見なされます。

リモートデバイスの単一ポートに、ポイントツーポイントで物理的に接続されている半二重リンクがある場合、リンク タイプのデフォルト設定を上書きして高速移行をイネーブルにできます。

リンクを共有に設定すると、STP は 802.1D にフォール バックします。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**spanning-tree link-type** {*auto* | *point-to-point* | *shared*} **Example:** `switch(config-if)# spanning-tree link-type point-to-point`	リンク タイプを、ポイントツーポイント インクまたは共有リンクに設定します。デフォルト値はデバイス接続から読み取られ、半二重リンクは共有、全二重リンクはポイントツーポイントです。リンク タイプが共有の場合、STP は 802.1D にフォール バックします。デフォルトは auto で、インターフェイスのデュプレックス設定に基づいてリンク タイプが設定されます。

ステップ 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	(Optional) **show spanning-tree** **Example:** `switch# show spanning-tree`	STP の設定を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次の例は、リンク タイプをポイントツーポイント リンクとして設定する方法を示しています。

```
switch# config t
switch (config)# interface ethernet 1/4
switch(config-if)# spanning-tree link-type point-to-point
switch(config-if)# exit
switch(config)#
```

MST 用のプロトコルの再初期化

MSTブリッジでは、レガシーBPDUまたは異なるリージョンに関連付けられているMSTBPDUを受信するときに、ポートがリージョンの境界にあることを検出できます。ただし、STPプロトコルを移行しても、レガシー デバイス（IEEE 802.1D だけが稼働するデバイス）が代表スイッチでないかぎり、レガシーデバイスがリンクから削除されたかどうかを判別することはできません。デバイス全体で、または指定されたインターフェイスでプロトコル ネゴシエーションを再初期化する（ネイバーデバイスとの再ネゴシエーションを強制的に行う）には、次のコマンドを入力します。

Procedure

	Command or Action	Purpose
ステップ 1	**clear spanning-tree detected-protocol** [**interface** *interface* [*interface-num* | *port-channel*]] **Example:** `switch# clear spanning-tree detected-protocol`	デバイス全体または指定されたインターフェイスで、MST を再初期化します。

Example

次に、スロット 1 のイーサネット インターフェイスのポート 8 で、MST を再初期化する例を示します。

```
switch# clear spanning-tree detected-protocol interface ethernet 1/8
```

MST の設定の確認

MST 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show running-config spanning-tree [**all**]	STP 情報を表示します。
show spanning-tree mst configuration	MST 情報を表示します。
show spanning-tree mst [**detail**]	MST インスタンスの情報を表示します。
show spanning-tree mst*instance-id* [**detail**]	指定された MST インスタンスに関する情報を表示します。
show spanning-tree mst *instance-id* **interface** {**ethernet** *slot/port* | **port-channel** *channel-number*} [**detail**]	指定したインターフェイスおよびインスタンスの MST 情報を表示します。
show spanning-tree summary	STP の概要を表示します。
show spanning-tree detail	STP の詳細を表示します。
show spanning-tree {**vlan** *vlan-id* | **interface** {[**ethernet** *slot/port*] | [**port-channel** *channel-number*]}} [**detail**]	VLAN またはインターフェイス単位の STP 情報を表示します。
show spanning-tree vlan *vlan-id* **bridge**	STP ブリッジの情報を表示します。

MST 統計情報の表示およびクリア（CLI バージョン）

MST 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
clear spanning-tree counters [**interface** *type slot/port* | **vlan***vlan-id*]	STP のカウンタをクリアします。
show spanning-tree {**vlan** *vlan-id* | **interface** {[**ethernet** *slot/port*] | [**port-channel***channel-number*]}} **detail**	送受信された BPDU などの STP 情報を、インターフェイスまたは VLAN 別に表示します。

MST の設定例

次に、MST を設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree mode mst
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# spanning-tree port type edge bpdufilter default
switch(config)# spanning-tree port type network default
switch(config)# spanning-tree mst 0 priority 24576
switch(config)# spanning-tree mst configuration
switch(config-mst)# name cisco_region_1
switch(config-mst)# revision 2
switch(config-mst)# instance 1 vlan 1-21
```

MST の追加情報（CLI バージョン）

関連資料

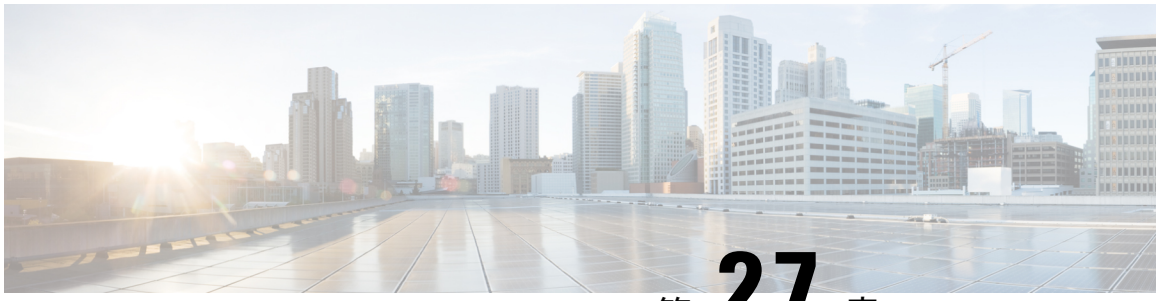
関連項目	マニュアル タイトル
レイヤ2インターフェイス	「*Cisco Nexus® 3550-T* インターフェイスの構成」セクション
NX-OS の基礎	*Cisco Nexus Series NX-OS Fundamentals* 構成ガイド
高可用性	『*Cisco Nexus Series* 高可用性および冗長性ガイド』
システム管理	「*Cisco Nexus® 3550-T* システム管理の構成」セクション

標準

標準	タイトル
IEEE 802.1Q-2006（旧称 IEEE 802.1s）、IEEE 802.1D-2004（旧称 IEEE 802.1w）、IEEE 802.1D、IEEE 802.1t	—

MIB

MIB	MIB のリンク
CISCO-STP-EXTENSION-MIB BRIDGE-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてくだ い。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.



第 27 章

Cisco NX-OS を使用した STP 拡張の設定

STP 拡張機能について

Note レイヤ 2 インターフェイスの作成の詳細については、『*Cisco Nexus® 3550-T* インターフェイス構成ガイド』を参照してください。

ループ回避を改善し、ユーザによる設定ミスを削減し、プロトコルパラメータの制御を向上するために、シスコは STP に拡張機能を追加しました。IEEE 802.1w 高速スパニングツリー プロトコル（RSTP）規格に同様の機能が統合されていることも考えられますが、ここで紹介する拡張機能を使用することを推奨します。PVST シミュレーションを除き、これらの拡張機能はすべて、MST で使用できます。PVST シミュレーションを使用できるのは、MST だけです。

使用できる拡張機能は、スパニングツリー エッジ ポート（従来の PortFast の機能を提供）、ブリッジ保証、BPDU ガード、BPDU フィルタリング、ループ ガード、ルート ガード、および PVT シミュレーションです。これらの機能の大部分は、グローバルに、または指定インターフェイスに適用できます。

Note このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。IEEE 802.1D STP について説明している箇所では、802.1D と明記します。

STP ポート タイプ

スパニングツリー ポートは、エッジ ポート、ネットワーク ポート、または標準ポートとして構成できます。ポートは、ある一時点において、これらのうちいずれか 1 つの状態をとります。デフォルトのスパニング ツリー ポート タイプは「標準」です。

レイヤ 2 ホストに接続するエッジ ポートは、アクセス ポートまたはトランク ポートのどちらかになります。

Note レイヤ 2 スイッチまたはブリッジに接続しているポートをエッジ ポートとして設定すると、ブリッジング ループが発生することがあります。

STP エッジ ポート

STP エッジ ポートは、レイヤ 2 ホストだけに接続します。エッジ ポート インターフェイスは、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します（この直接移行動作は、以前は、シスコ独自の機能 PortFast として設定していました）。

レイヤ 2 ホストに接続したインターフェイスでは、STP のブリッジ プロトコル データ ユニット（BPDU）を受信しないようにします。

BPDU ガード

BPDU ガードをイネーブルにすると、BPDU を受信したときにそのインターフェイスがシャットダウンされます。

BPDU ガードはインターフェイス レベルで設定できます。BPDU ガードをインターフェイス レベルで設定すると、そのポートはポート タイプ設定にかかわらず BPDU を受信するとすぐにシャットダウンされます。

BPDU ガードをグローバル単位で設定すると、動作中のスパニングツリー エッジ ポート上だけで有効となります。有効な設定では、レイヤ 2 LAN エッジ インターフェイスは BPDU を受信しません。レイヤ 2 LAN エッジ インターフェイスが BPDU を受信した場合、許可されていないデバイスの接続と同様に、無効な設定として通知されます。BPDU ガードをグローバル単位でイネーブルにすると、BPDU を受信したすべてのスパニングツリー エッジ ポートがシャットダウンされます。

BPDU ガードでは、無効な設定が通知された場合、レイヤ 2 LAN インターフェイスを手動で再起動させる必要があるので、無効な設定に対して安全に対応できます。

Note BPDU ガードをグローバル単位でイネーブルにすると、動作中のすべてのスパニングツリー エッジ インターフェイスに適用されます。

BPDU フィルタリング

BPDUフィルタリングを使用すると、デバイスの特定のポート上でBPDUが送信されないように、またはBPDU を受信しないように設定できます。

グローバルに設定された BPDU フィルタリングは、動作中のすべてのスパニングツリー エッジポートに適用されます。エッジポートはホストだけに接続してください。ホストでは通常、BPDU は破棄されます。動作中のスパニングツリー エッジ ポートが BPDU を受信すると、ただちに標準のスパニングツリー ポート タイプに戻り、通常のポート状態遷移が行われます。その場合、当該ポートで BPDU フィルタリングはディセーブルとなり、スパニングツリーによって、同ポートでの BPDU の送信が再開されます。

BPDU フィルタリングは、インターフェイスごとに設定することもできます。BPDU フィルタリングを特定のポートに明示的に設定すると、そのポートはBPDUを送出しなくなり、受信したBPDUをすべてドロップします。特定のインターフェイスを設定することによって、個々のポート上のグローバルなBPDUフィルタリングの設定を実質的に上書きできます。このようにインターフェイスに対して実行されたBPDUフィルタリングは、そのインターフェイスがトランキングであるか否かに関係なく、インターフェイス全体に適用されます。

Caution BPDUフィルタリングをインターフェイスごとに設定するときは注意が必要です。ホストに接続されていないポートに BPDU フィルタリングを明示的に設定すると、ブリッジング ループに陥る可能性があります。このようなポートは受信した BPDU をすべて無視して、フォワーディング ステートに移行するからです。

次の表に、すべての BPDU フィルタリングの組み合わせを示します。

***Table 24: BPDU* フィルタリングの設定**

ポート単位の BPDU フィルタリングの設定	グローバルな BPDU フィルタリングの設定	STP エッジ ポート設定	BPDU フィルタリングの状態
デフォルト [1]	有効	有効	イネーブル [2]
デフォルト	有効	無効	無効
デフォルト	無効	N/A	無効
無効	N/A	N/A	無効
有効	N/A	N/A	有効

1 明示的なポート設定はありません。
2 ポートは最低 10 個の BPDU を送信します。このポートは、BPDU を受信すると、スパニングツリー標準ポート状態に戻り、BPDU フィルタリングはディセーブルになります。

ループ ガード

ループ ガードを使用すると、ポイントツーポイント リンク上の単方向リンク障害によって発生することがあるブリッジング ループを防止できます。

STP ループは、冗長なトポロジにおいてブロッキング ポートが誤ってフォワーディング ステートに移行すると発生します。通常、BPDU の受信を停止する、物理的に冗長なトポロジ内のポート（ブロッキング ポートとは限らない）が原因で移行が発生します。

ループ ガードをグローバルにイネーブルにしても、デバイスがポイントツーポイント リンクで接続されているスイッチド ネットワークでしか使用できません。ポイントツーポイント リンクでは、下位 BPDU を送信するか、リンクをダウンしない限り、代表ブリッジは消えることはありません。ただし、共有リンク上のループ ガードはインターフェイス単位でイネーブルに設定できます。

ループ ガードを使用して、ルート ポートまたは代替/バックアップ ループ ポートが BPDU を受信するかどうかを確認できます。BPDU を受信していたポートで BPDU が受信されなくなると、ループ ガードは、ポート上で BPDU の受信が再開されるまで、そのポートを不整合（ブロッキング）ステートにします。これらのポートで BPDU の受信が再開されると、ポートおよびリンクは再び動作可能として認識されます。この回復は自動的に実行されるので、プロトコルによりポートからループ不整合が排除されると、STP によりポート ステートが判別されます。

ループ ガードは障害を分離し、STP は障害のあるリンクやブリッジを含まない安定したトポロジに収束できます。ループ ガードをディセーブルにすると、すべてのループ不整合ポートはリスニング ステートに移行します

ループ ガードはポート単位でイネーブルにできます。ループ ガードを特定のポートでイネーブルにすると、そのポートが属するすべてのアクティブ インスタンスまたは VLAN にループ ガードが自動的に適用されます。ループ ガードをディセーブルにすると、指定ポートでディセーブルになります。

ルート デバイス上でループ ガードをイネーブルにしても効果はありませんが、ルート デバイスが非ルート デバイスになった場合、保護が有効になります。

ルート ガード

特定のポートでルート ガードをイネーブルにすると、そのポートはルート ポートになることが禁じられます。受信した BPDU によって STP コンバージェンスが実行され、指定ポートがルート ポートになると、そのポートはルート不整合（ブロッキング）状態になります。このポートが優位 BPDU の受信を停止すると、ブロッキングが再度解除されます。次に、STP によって、フォワーディング ステートに移行します。リカバリは自動的に行われます。

インターフェイス上でルート ガードをイネーブルにすると、そのインターフェイスが属しているすべての VLAN にルート ガードが適用されます。

ルート ガードを使用すると、ネットワーク内にルート ブリッジを強制的に配置できます。ルート ガードは、ルート ガードがイネーブルにされたポートを指定ポートに選出します。通常、ルート ブリッジのポートはすべて指定ポートとなります（ただし、ルート ブリッジの 2 つ以

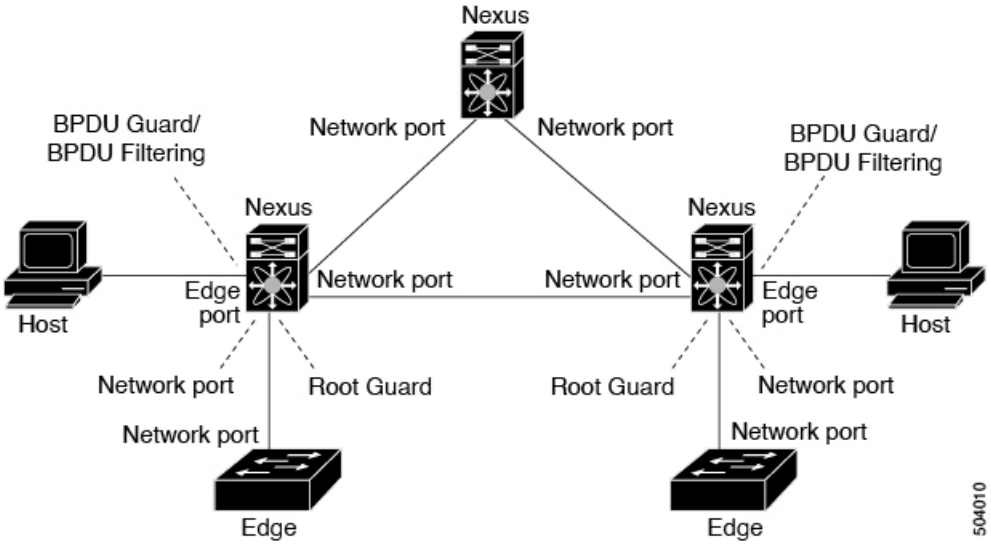
上のポートが接続されている場合はその限りではありません）。ルート ブリッジは、ルート ガードがイネーブルにされたポートで上位 BPDU を受信すると、そのポートをルート不整合 STP 状態に移行します。このように、ルートガードはルートブリッジの配置を適用します。

ルート ガードをグローバルには設定できません。

STP 拡張機能の適用

***Figure 24: STP* 拡張機能を適正に展開したネットワーク**

この図に示すように、ネットワーク上に各種の STP 拡張機能を設定することを推奨します。Bridge Assurance は、ネットワーク全体でイネーブルになります。ホスト インターフェイス上で、BPDU ガードと BPDU フィルタリングのいずれかをイネーブルにすることをお勧めします。



PVST シミュレーション

MST の運用では、ユーザ構成は不要です。この相互運用性を提供するのが、PVST シミュレーション機能です。

Note MST をイネーブルにすると、PVST シミュレーションがデフォルトでイネーブルになります。デフォルトでは、デバイス上のすべてのインターフェイスが MST で運用します。

すべての STP インスタンスのルート ブリッジはすべて、MST 領域内に存在します。すべての STP インスタンスのルート ブリッジが MST 上に存在しない場合、ポートは PVST シミュレーション不整合ステートになります。

Note STP インスタンスのルート ブリッジを、MST 側に配置することを推奨します。デフォルトの STP インスタンスのみが Cisco Nexus® 3550-T でサポートされています。

STP のハイ アベイラビリティ

ソフトウェアは STP に対してハイ アベイラビリティをサポートしています。ただし、STP を再起動した場合、統計情報およびタイマーは復元されません。タイマーは最初から開始され、統計情報は 0 にリセットされます。

Note 高可用性機能の詳細については、『*Cisco Nexus Series NX-OS* 高可用性および冗長性ガイド』を参照してください。

STP 拡張機能の前提条件

STP には次の前提条件があります。

- デバイスにログインしていること。
- STP を設定しておく必要があります。

STP 拡張機能の設定に関するガイドラインおよび制約事項

STP 拡張機能の設定に関するガイドラインと制約事項は次のとおりです。

- **show** コマンド（**internal** キーワード付き）はサポートされていません。
- STP ネットワーク ポートは、スイッチだけに接続してください。
- ホスト ポートは、ネットワーク ポートではなく STP エッジ ポートとして設定する必要があります。
- レイヤ 2 ホストに接続しているすべてのアクセス ポートおよびトランク ポートを、エッジ ポートとして設定する必要があります。
- すべてのエッジ ポートで BPDU ガードをイネーブルにすることを推奨します。
- グローバルにイネーブルにしたループ ガードは、ポイントツーポイント リンク上でのみ動作します。

- インターフェイス単位でイネーブルにしたループ ガードは、共有リンクおよびポイントツーポイント リンクの両方で動作します。
- ルート ガードを適用したポートは強制的に指定ポートになりますが、ルート ポートにはなりません。ループ ガードは、ポートがルート ポートまたは代替ポートの場合にのみ有効です。ポート上でループ ガードとルート ガードの両方を同時にイネーブルにすることはできません。
- ディセーブル化されたスパニングツリー インスタンスまたは VLAN 上では、ループ ガードは無効です。
- スパニングツリーは、BPDUを送信するチャネル内で最初に動作するポートを常に選択します。このリンクが単方向になると、チャネル内の他のリンクが正常に動作していても、ループ ガードによりチャネルがブロックされます。
- ループ ガードによってブロックされている一連のポートをグループ化してチャネルを形成すると、これらのポートのステート情報はスパニングツリーからすべて削除され、新しいチャネルのポートは指定ロールによりフォワーディング ステートに移行できます。
- チャネルがループ ガードによりブロックされ、チャネルのメンバーが個々のリンク ステータスに戻ると、スパニングツリーからすべてのステート情報が削除されます。チャネルを形成する 1 つまたは複数のリンクが単一方向リンクである場合も、各物理ポートは指定されたロールを使用して、フォワーディング ステートに移行できます。
- 物理ループのあるスイッチ ネットワーク上では、ループ ガードをグローバルにイネーブルにする必要があります。
- 直接の管理制御下にないネットワーク デバイスに接続しているポート上では、ルート ガードをイネーブルにする必要があります。

STP 拡張機能のデフォルト設定

次の表に、STP 拡張機能のデフォルト設定を示します。

***Table 25: STP* 拡張機能パラメータのデフォルト設定**

パラメータ	デフォルト
ポート タイプ	標準
グローバル BPDU ガード	ディセーブル
インターフェイス単位の BPDU ガード	ディセーブル
グローバル BPDU フィルタリング	ディセーブル

パラメータ	デフォルト
インターフェイス単位の BPDU フィルタリング	ディセーブル
グローバル ループ ガード	ディセーブル
インターフェイス単位のループ ガード	ディセーブル
インターフェイス単位のルート ガード	ディセーブル

STP 拡張機能の設定手順

Note Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

ループ ガードは、共有リンクまたはポイントツーポイント リンク上のインターフェイス単位でイネーブルに設定できます。

スパニングツリー ポート タイプのグローバルな設定

スパニングツリー ポート タイプの指定は、次のように、ポートの接続先デバイスによって異なります。

- エッジ：エッジ ポートは、レイヤ 2 ホストに接続するアクセス ポートです。
- 標準：標準ポートはエッジ ポートでもネットワーク ポートでもない、標準のスパニングツリー ポートです。これらのポートは、どのデバイスにも接続できます。

ポート タイプは、グローバル単位でもインターフェイス単位でも設定できます。デフォルトのスパニングツリー ポート タイプは「標準」です。

Before you begin

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree port type edge default** or **spanning-tree port type network default** **Example:** `switch(config)# spanning-tree port type edge default`	• **spanning-tree port type edge default** レイヤ2ホストに接続しているすべてのアクセス ポートをエッジ ポートとして設定します。エッジ ポートは、リンクアップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。デフォルトのスパニングツリー ポート タイプは「標準」です。 • **spanning-tree port type network default** レイヤ2スイッチおよびブリッジに接続しているすべてのインターフェイスを、スパニングツリー ネットワーク ポートとして設定します。Bridge Assurance をイネーブルにすると、各ネットワーク ポート上で Bridge Assurance が自動的に実行されます。デフォルトのスパニングツリー ポート タイプは「標準」です。 **Note** レイヤ 2 ホストに接続しているインターフェイスをネットワーク ポートとして設定すると、これらのポートは自動的にブロッキング ステートに移行します。

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

	Command or Action	Purpose
ステップ 4	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	設定した STP ポート タイプを含む STP コンフィギュレーションを表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、レイヤ 2 ホストに接続しているすべてのアクセス ポートをスパニングツリー エッジ ポートとして設定する例を示します。

```
switch# config t
switch(config)# spanning-tree port type edge default
switch(config)# exit
switch#
```

指定インターフェイスでのスパニングツリー エッジ ポートの設定

指定インターフェイスにスパニングツリー エッジ ポートを設定できます。スパニングツリー エッジポートとして設定されたインターフェイスは、リンクアップ時に、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。

このコマンドには次の 4 つの状態があります。

- **spanning-tree port type edge**: このコマンドはアクセス ポートでのエッジ動作を明示的にイネーブルにします。
- **spanning-tree port type edge trunk**: このコマンドはトランク ポートでのエッジ動作を明示的にイネーブルにします。

Note **spanning-tree port type edge trunk** を入力すると、 コマンド、そのポートは、アクセス モードであってもエッジ ポートとして設定されます。

- **spanning-tree port type normal**：このコマンドは、ポートを標準スパニングツリー ポートとして明示的に設定しますが、フォワーディング ステートへの直接移行はイネーブルにしません。
- **no spanning-tree port type**：このコマンドは、**spanning-tree port type edge default** コマンドをグローバル コンフィギュレーション モードで定義した場合に、エッジ動作を暗黙的に

イネーブルにします。エッジポートをグローバルに設定していない場合、**no spanning-tree port type** コマンドは、**spanning-tree port type normal** コマンドと同じです。

Before you begin

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定する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	**spanning-tree port type edge** **Example:** `switch(config-if)# spanning-tree port type edge`	指定したアクセス インターフェイスをスパニング エッジ ポートに設定します。エッジ ポートは、リンク アップすると、ブロッキング ステートやラーニング ステートを経由することなく、フォワーディング ステートに直接移行します。デフォルトのスパニングツリーポート タイプは「標準」です。

ステップ 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	(Optional) **show spanning-tree interface** *type slot/port* **ethernet** *x/y* **Example:** `switch# show spanning-tree ethernet 1/4`	設定した STP ポート タイプを含む STP コンフィギュレーションを表示します。

	Command or Action	Purpose
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、アクセス インターフェイス Ethernet 1/4 をスパニングツリー エッジ ポートとして設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit
switch(config)#
```

BPDU ガードのグローバルなイネーブル化

BPDU ガードをデフォルトでグローバルにイネーブルにできます。BPDU ガードがグローバルにイネーブルにされると、システムは、BPDU を受信したエッジ ポートをシャット ダウンします。

Note すべてのエッジ ポートで BPDU ガードをイネーブルにすることを推奨します。

Before you begin

スパニングツリー ポート タイプを設定する前に、次の点を確認してください。

- STP が設定されていること。
- ポートの接続先デバイスに応じて、ポートを正しく設定していること。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree port type edge bpduguard default** **Example:**	すべてのスパニングツリー エッジ ポートで、BPDUガードを、デフォルトでイネーブルにします。デフォルトでは、グ

	Command or Action	Purpose
	`switch(config)# spanning-tree port type edge bpduguard default`	ローバルな BPDU ガードはディセーブルです。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	STP の概要を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、すべてのスパニングツリー エッジ ポートで BPDU ガードをイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# exit
switch#
```

指定インターフェイスでの BPDU ガードのイネーブル化

指定インターフェイスで、BPDU ガードをイネーブルにできます。BPDU ガードがイネーブルにされたポートは、BPDU を受信すると、シャットダウンされます。

BPDU ガードは、指定インターフェイスで次のように設定にできます。

- **spanning-tree bpduguard enable** : インターフェイス上で、BPDU ガードが無条件にイネーブルになります。
- **spanning-tree bpduguard disable** : インターフェイス上で、BPDU ガードが無条件にディセーブルになります。
- **no spanning-tree bpduguard** ：動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpduguard default** コマンドが設定されている場合、そのインターフェイスで BPDU ガードをイネーブルにします。

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定する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	**spanning-tree bpduguard** {**enable** | **disable**} or **no spanning-tree bpduguard** **Example:** `switch(config-if)# spanning-tree bpduguard enable`	• **spanning-tree bpduguard** {**enable** | **disable**} 指定したスパニングツリー エッジ インターフェイスの BPDU ガードをイネーブルまたはディセーブルにします。デフォルトでは、インターフェイス上の BPDU ガードはディセーブルです。 • **no spanning-tree bpduguard** **spanning-tree port type edge bpduguard default** コマンドの入力により、インターフェイスに設定されたデフォルトのグローバル BPDU ガード設定に戻します。

ステップ 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	(Optional) **show spanning-tree interface** *type slot/port* **detail** **Example:** `switch# show spanning-tree interface ethernet detail`	STP の概要を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、エッジ ポート Ethernet 1/4 で BPDU ガードを明示的にイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpduguard enable
switch(config-if)# exit
switch(config)#
```

BPDU フィルタリングのグローバルなイネーブル化

スパニングツリーエッジポートで、BPDUフィルタリングをデフォルトでグローバルにイネーブルにできます。

BPDU フィルタリングがイネーブルであるエッジ ポートは、BPDU を受信するとエッジ ポートとしての稼働ステータスが失われ、通常の STP ステート移行を再開します。ただし、このポートは、エッジ ポートとしての設定は保持したままです。

Caution このコマンドを使用するときは注意してください。このコマンドを誤って使用すると、ブリッジング ループに陥る可能性があります。

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。
- 少なくとも一部のスパニングツリー エッジ ポートが設定済みであること。

Note グローバルにイネーブルにされた BPDU フィルタリングは、動作中のエッジ ポートにだけ適用されます。ポートは数個の BPDU をリンクアップ時に送出してから、実際に、発信 BPDU のフィルタリングを開始します。エッジ ポートは、BPDU を受信すると、動作中のエッジポート ステータスを失い、BPDUフィルタリングはディセーブルになります。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree port type edge bpdufilter default** **Example:** `switch(config)# spanning-tree port type edge bpdufilter default`	すべてのスパニングツリー エッジ ポートで、BPDUフィルタリングを、デフォルトでイネーブルにします。デフォルトでは、グローバルな BPDU フィルタリングはディセーブルです。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	STP の概要を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、すべての動作中のスパニングツリー エッジ ポートで BPDU フィルタリングをイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree port type edge bpdufilter default
switch(config)# exit
switch#
```

指定インターフェイスでの BPDU フィルタリングのイネーブル化

指定インターフェイスにBPDUフィルタリングを適用できます。BPDUフィルタリングを特定のインターフェイス上でイネーブルにすると、そのインターフェイスはBPDUを送信しなくなり、受信した BPDU をすべてドロップするようになります。この BPDU フィルタリング機能は、トランキングインターフェイスであるかどうかに関係なく、すべてのインターフェイスに適用されます。

Caution **spanning-tree bpdufilter enable** を入力する場合は、慎重に行ってください。 指定されたインターフェイスでコマンドを入力します。ホストに接続していないポートにBPDUフィルタリングを設定すると、そのポートは受信した BPDU をすべて無視してフォワーディングに移行するので、ブリッジング ループが発生することがあります。

このコマンドを入力すると、指定インターフェイスのポート設定が上書きされます。

このコマンドには次の 3 つの状態があります。

- **spanning-tree bpdufilter enable** : インターフェイス上で、BPDU フィルタ処理が無条件にイネーブルになります。
- **spanning-tree bpdufilter disable** : インターフェイス上で、BPDU フィルタ処理が無条件にディセーブルになります。
- **no spanning-tree bpdufilter** :動作中のエッジ ポート インターフェイスに **spanning-tree port type edge bpdufilter default** コマンドが設定されている場合、そのインターフェイスで BPDU フィルタリングをイネーブルにします。コマンドを使用します。

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。

Note 特定のポートだけでBPDUフィルタリングをイネーブルにすると、そのポートでのBPDUの送受信が禁止されます。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定する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	{| }または **spanning-tree bpdufilter enable disable no spanning-tree bpdufilter** **Example:**	• **spanning-tree bpdufilter** {**enable** | **disable**}

	Command or Action	Purpose
	`switch(config-if)# spanning-tree bpdufilter enable`	指定したスパニングツリー エッジ インターフェイスの BPDU フィルタリングをイネーブルまたはディセーブルにします。デフォルトでは、BPDU フィルタリングはディセーブルです。 • **no spanning-tree bpdufilter** 動作中のスパニングツリー エッジ ポート インターフェイスに **spanning-tree port type edge bpdufilter default** コマンドが設定されている場合、そのインターフェイスで BPDU フィルタリングをイネーブルにします。

ステップ 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイスモードを終了します。

ステップ 5	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	STP の概要を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、スパニング ツリー エッジ ポート Ethernet 1/4 で BPDU フィルタリングを明示的にイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree bpdufilter enable
switch(config-if)# exit
switch(config)#
```

ループ ガードのグローバルなイネーブル化

ループ ガードは、デフォルトの設定により、すべてのポイントツーポイント スパニングツリーの標準およびネットワーク ポートで、グローバルにイネーブルにできます。ループ ガードは、エッジ ポートでは動作しません。

ループ ガードを使用すると、ブリッジネットワークのセキュリティを高めることができます。ループ ガードは、単方向リンクを引き起こす可能性のある障害が原因で、代替ポートまたはルート ポートが指定ポートになるのを防ぎます。

Note 指定インターフェイスでループ ガード コマンドを入力すると、グローバルなループ ガード コマンドが上書きされます。

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。
- スパニングツリー標準ポートが存在し、少なくとも一部のネットワーク ポートが設定済みであること。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**spanning-tree loopguard default** **Example:** `switch(config)# spanning-tree loopguard default`	スパニングツリーのすべての標準およびネットワーク ポートで、ループ ガードを、デフォルトでイネーブルにします。デフォルトでは、グローバルなループ ガードはディセーブルです。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show spanning-tree summary** **Example:** `switch# show spanning-tree summary`	STP の概要を表示します。

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

Example

次に、スパニングツリーのすべての標準およびネットワーク ポートでループ ガードをイネーブルにする例を示します。

```
switch# config t
switch(config)# spanning-tree loopguard default
switch(config)# exit
switch#
```

指定インターフェイスでのループガードまたはルートガードのイネーブル化

Note ループ ガードは、スパニングツリーの標準またはネットワーク ポート上で実行できます。ルート ガードは、すべてのスパニングツリー ポート（標準、エッジ、ネットワーク）上で実行できます。

ループ ガードまたはルート ガードは、指定インターフェイスでイネーブルにできます。

ポート上でルート ガードをイネーブルにすることは、そのポートをルート ポートにできないことを意味します。ループ ガードは、単方向リンクの障害発生時に、代替ポートまたはルート ポートが指定ポートになるのを防止します。

特定のインターフェイスでループ ガードおよびルート ガードの両機能をイネーブルにすると、そのインターフェイスが属するすべての VLAN に両機能が適用されます。

Note 指定インターフェイスでループ ガード コマンドを入力すると、グローバルなループ ガード コマンドが上書きされます。

Before you begin

この機能を設定する前に、次の点を確認してください。

- STP が設定されていること。

- ループ ガードが、スパニングツリーの標準またはネットワーク ポート上で設定されていること。

Procedure

	Command or Action	Purpose

ステップ 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定する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	**spanning-tree guard** {**loop** | **root** | **none**} **Example:** `switch(config-if)# spanning-tree guard loop`	ループ ガードまたはルート ガードを、指定インターフェイスでイネーブルまたはディセーブルにします。ルート ガードはデフォルトでディセーブル、ループ ガードも指定ポートでディセーブルになります。 **Note** ループ ガードは、スパニングツリーの標準およびネットワーク インターフェイスだけで動作します。この例では、指定したインターフェイス上でループ ガードをイネーブルにしています。

ステップ 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイスモードを終了します。

ステップ 5	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 1/10`
	`switch(config-if)#`
		設定する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 6	**spanning-tree guard** {**loop** | **root** | **none**} **Example:** `switch(config-if)# spanning-tree guard root`	ループ ガードまたはルート ガードを、指定インターフェイスでイネーブルまたはディセーブルにします。ルート ガードはデフォルトでディセーブル、ループ ガードも指定ポートでディセーブルになります。

	Command or Action	Purpose
		この例では、別のインターフェイス上でルート ガードをイネーブルにしています。

ステップ 7	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイスモードを終了します。

ステップ 8	(Optional) **show spanning-tree interface** *type slot/port* **detail** **Example:** `switch# show spanning-tree interface ethernet 1/4 detail`	STP の概要を表示します。
ステップ 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、Ethernet ポート 1/4 で、ルート ガードをイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree guard root
switch(config-if)# exit
switch(config)#
```

STP 拡張機能の設定の確認

STP 拡張機能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 spanning-tree [**all**]	STP に関する情報を表示します。
show spanning-tree summary	STP 情報の要約を表示します。
show spanning-tree mst*instance-id* **interface** {**ethernet** *slot/port* | **port-channel** *channel-number*} [**detail**]	指定したインターフェイスおよびインスタンスの MST 情報を表示します。

STP 拡張機能の設定例

次に、STP 拡張機能を設定する例を示します。

```
switch# configure terminal
switch(config)# spanning-tree port type network default
switch(config)# spanning-tree port type edge bpduguard default
switch(config)# spanning-tree port type edge bpdufilter default

switch(config)# interface ethernet 1/1
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit

switch(config)# interface ethernet 1/2
switch(config-if)# spanning-tree port type edge
switch(config-if)# exit
switch(config)#
```

STP 拡張機能の追加情報（CLI バージョン）

関連資料

関連項目	マニュアル タイトル
レイヤ2インターフェイス	「*Cisco Nexus® 3550-T* インターフェイスの構成」セクション
NX-OS の基礎	「*Cisco Nexus® 3550-T* の基本設定」セクション
システム管理	「*Cisco Nexus® 3550-T* システム管理の構成ガイド」セクション
	『*Cisco NX-OS Licensing Guide*』

標準

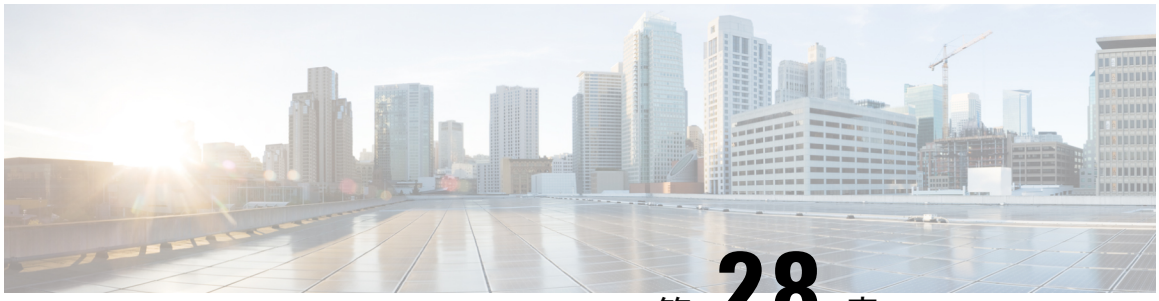
標準	タイトル
IEEE 802.1Q-2006（旧称 IEEE 802.1s）、IEEE 802.1D-2004（旧称 IEEE 802.1w）、IEEE 802.1D、IEEE 802.1t	—

MIB

MIB	MIB のリンク
• CISCO-STP-EXTENSION-MIB • BRIDGE-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

第 VII 部

Cisco Nexus 3550-T インターフェイス構成ガイド



第 28 章

『Interfaces Configuration Guide』

この前書きは、次の項で構成されています。

ライセンス要件

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

インターフェイスについて

Cisco NX-OS は、サポート対象の各インターフェイス タイプの複数の設定パラメータをサポートします。ほとんどのパラメータはこのマニュアルで説明しますが、一部は他のマニュアルで説明します。

以下の表に、インターフェイスに設定できるパラメータの情報の入手先を示します。

表 *26*：インターフェイスのパラメータ

機能	パラメータ	解説場所
基本パラメータ	説明、デュプレックス、エラー無効化、フロー制御、ビーコン	基本インターフェイス パラメータの設定
レイヤ 3	メディア、IPv4 アドレス	レイヤ 3 インターフェイスの設定

機能	パラメータ	解説場所
レイヤ 3	帯域幅、遅延、IP ルーティング、VRF	「*Cisco Nexus® 3550-T* ユニキャスト ルーティング構成」セクション 「*Cisco Nexus® 3550-T* マルチキャスト ルーティング構成」セクション
ポート チャネル	チャネル グループ、LACP	ポート チャネルの設定
セキュリティ	EOU	「*Cisco Nexus® 3550-T* セキュリティの設定」セクション

イーサネット インターフェイス

イーサネット インターフェイスには、ルーテッド ポートが含まれます。

Cisco Nexus® 3550-T スイッチには、次の注意事項と制限事項があります。

- Cisco Nexus® 3550-T は、10G の速度のみをサポートします。

アクセス ポート

アクセス ポートは 1 つの VLAN のトラフィックを送受信します。このポートのタイプはレイヤ 2 インターフェイスだけです。

アクセス ポートの詳細については、「アクセス インターフェイスとトランク インターフェイスについて」の項を参照してください。

トランク ポート

トランク ポートは、1 つの VLAN の非タグ付きパケットと、複数の VLAN のカプセル化されたタグ付きパケットを伝送します。（カプセル化については、「IEEE 802.1Q カプセル化」のセクションを参照してください）。

レイヤ2スイッチングポートは、アクセスポートまたはトランク ポートとして設定できます。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。レイヤ 2 スイッチング ポートはすべて、MAC アドレス テーブルを維持します。

ルーテッド ポート

ルーテッドポートは、IP トラフィックを他のデバイスにルーティングできる物理ポートです。ルーテッド ポートはレイヤ 3 インターフェイスだけです。

ルーテッド ポートの詳細については、「ルーテッド インターフェイス」のセクションを参照してください。

管理インターフェイス

管理イーサネットインターフェイスを使用して、Telnet クライアント、簡易ネットワーク管理プロトコル（SNMP）、その他の管理エージェントを使用するリモート管理用ネットワークにデバイスを接続できます。管理ポート（mgmt0）は、自動検知であり、10/100/1000 Mb/s の速度の全二重モードで動作します。

管理インターフェイスの詳細については、『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』を参照してください。このマニュアルにも、管理インターフェイスの IP アドレスとデフォルト IP ルーティング設定に関する情報を記載しています。

ポートチャネル インターフェイス

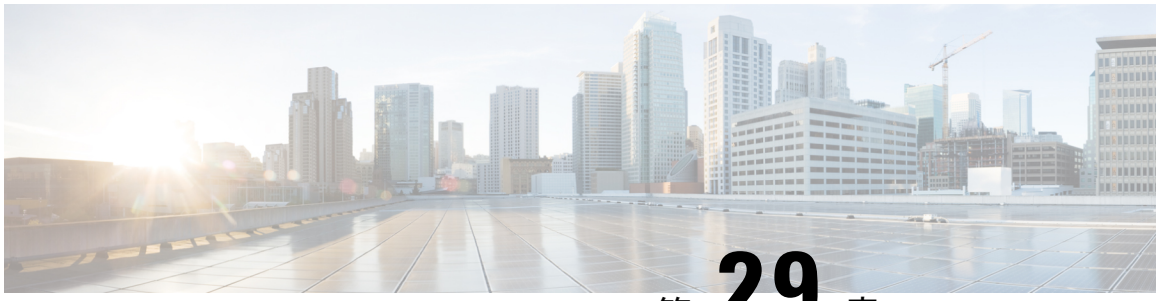
ポートチャネルは、複数の物理インターフェイスを集約した論理インターフェイスです。最大 4 の物理ポートへの個別リンクを 1 つのポート チャネルにバンドルして、帯域幅と冗長性を向上させることができます。ポート チャネリングにより、これらの物理インターフェイス チャネルのトラフィックをロード バランスさせることもできます。ポート チャネル インターフェイスの詳細については、「ポート チャネルの構成」のセクションを参照してください。

ループバック インターフェイス

仮想ループバック インターフェイスは、常にアップ状態にあるシングル エンドポイントを持つ仮想インターフェイスです。パケットが仮想ループバック インターフェイスを通じて送信されると、仮想ループバック インターフェイスですぐに受信されます。ループバック インターフェイスは物理インターフェイスをエミュレートします。

インターフェイスのハイ アベイラビリティ

インターフェイスは、ステートフル再起動とステートレス再起動をサポートします。



第 29 章

静的 NAT 変換の構成

ネットワーク アドレス変換の概要

ネットワークアドレス変換（NAT）は、登録されていないIPアドレスを使用してインターネットへ接続するプライベート IP インターネットワークをイネーブルにします。NAT はデバイス（通常、2 つのネットワークを接続するもの）で動作し、パケットを別のネットワークに転送する前に、社内ネットワークの（グローバルに一意のアドレスではなく）プライベート IP アドレスを正規の IP アドレスに変換します。NAT は、ネットワーク全体に対して 1 つの IP アドレスだけを外部にアドバタイズするように設定できます。この機能により、1 つの IP アドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

NAT が設定されたデバイスには、内部ネットワークと外部ネットワークのそれぞれに接続するインターフェイスが少なくとも 1 つずつあります。標準的な環境では、NAT はスタブ ドメインとバックボーンの間の出口ルータに設定されます。パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元 アドレスをグローバルで一意の アドレスに変換します。パケットがドメインに入ってくる際は、NAT はグローバルに一意な宛先アドレスをローカル アドレスに変換します。出口点が複数存在する場合、個々の NAT は同じ変換テーブルを持っている必要があります。

NAT は RFC 1631 に記述されています。

スタティック NAT に関する情報

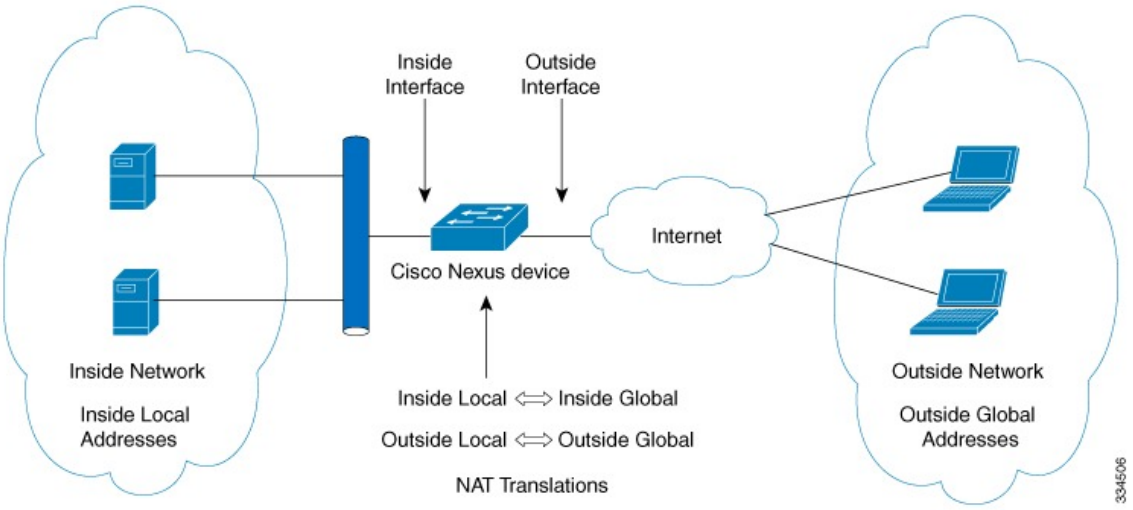
スタティック ネットワーク アドレス変換（NAT）を使用すると、ユーザは内部ローカル アドレスから外部グローバル アドレスへの 1 対 1 変換を設定することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへの IP アドレスとポート番号の両

方の変換が可能になります。Cisco Nexus デバイスはヒットレス NAT をサポートします。これは、既存の NAT トラフィック フローに影響を与えずに NAT 構成で NAT 変換を追加または削除できることを意味します。

スタティック NAT では、プライベート アドレスからパブリック アドレスへの固定変換が作成されます。スタティック NAT では 1 対 1 ベースでアドレスが割り当てられるため、プライベート アドレスと同じ数のパブリック アドレスが必要です。スタティック NAT では、パブリック アドレスは連続する各接続で同じであり、永続的な変換規則が存在するため、宛先ネットワークのホストは変換済みのホストへのトラフィックを開始できます（そのトラフィックを許可するアクセス リストがある場合）。

次の図に、一般的なスタティック NAT のシナリオを示します。変換は常にアクティブであるため、変換対象ホストとリモート ホストの両方で接続を生成でき、マップ アドレスは **static** コマンドによって静的に割り当てられます。

図 *25 :* スタティック *NAT*



次に、スタティック NAT を理解するのに役立つ主な用語を示します。

- NAT の内部インターフェイス：プライベート ネットワークに面するレイヤ 3 インターフェイス。
- NAT の外部インターフェイス：パブリック ネットワークに面するレイヤ 3 インターフェイス。
- ローカル アドレス：ネットワークの内部（プライベート）部分に表示される任意のアドレス。
- グローバル アドレス：ネットワークの外部（パブリック）部分に表示される任意のアドレス。
- 正規の IP アドレス：Network Information Center（NIC）やサービス プロバイダーにより割り当てられたアドレス。

- 内部ローカル アドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは正規の IP アドレスである必要はありません。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。これは、内部ネットワークのルーティング可能なアドレス空間から割り当てられるため、正規のアドレスである必要はありません。
- 内部グローバルアドレス：1 つ以上の内部ローカル IP アドレスを外部に対して表すために使用できる正規の IP アドレス。
- 外部グローバル アドレス：ホスト所有者が外部ネットワーク上のホストに割り当てる IP アドレス。このアドレスは、ルート可能なアドレスまたはネットワーク空間から割り当てられた正規のアドレスです。

NAT の内部アドレスおよび外部アドレス

NAT 内部とは、変換を必要とする組織が所有するネットワークを指します。NAT が設定されている場合、このネットワーク内のホストは、別の空間（グローバル アドレス空間として知られている）にあるものとしてネットワークの外側に現れる 1 つ空間（ローカル アドレス空間として知られている）内のアドレスを持つことになります。

同様に、NAT 外部とは、スタブ ネットワークが接続するネットワークを指します。通常、組織の管理下にはありません。外部ネットワーク内のホストを変換の対象にすることもできるため、これらのホストもローカル アドレスとグローバル アドレスを持つことができます。

NAT では、次の定義が使用されます。

- ローカル アドレス：ネットワークの内側部分に表示されるローカルな IP アドレスです。
- グローバル アドレス：ネットワークの外側部分に表示されるグローバルな IP アドレスです。
- 内部ローカル アドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは、多くの場合、インターネット ネットワーク情報センター（InterNIC）やサービス プロバイダーにより割り当てられた正規の IP アドレスではありません。
- 内部グローバル アドレス：外部に向けて、1 つ以上の内部ローカル IP アドレスを表現した正規の IP アドレス（InterNIC またはサービス プロバイダーにより割り当てられたもの）。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。必ずしも正規のアドレスでありません。内部でルート可能なアドレス空間から割り当てられたものです。
- 外部グローバルアドレス：外部ネットワークに存在するホストに対して、ホストの所有者により割り当てられた IP アドレス。このアドレスは、グローバルにルート可能なアドレス、またはネットワーク空間から割り当てられたものです。

スタティック NAT の注意事項および制約事項

スタティック NAT 設定時の注意事項および制約事項は、次のとおりです。

- キーワードが付いている**show**コマンド**internal**はサポートされていません。
- 変換された IP が、外部インターフェイス サブネットの一部である場合、NAT の外部インターフェイスで **ip proxy-arp** コマンドを使用します。**add-route** キーワードを使用する場合は、**ip proxy-arp** を有効にする必要があります。
- Cisco Nexus デバイスは、次のインターフェイスタイプで NAT をサポートします。
  - ルーテッド ポート
- NAT はデフォルトの仮想ルーティングおよびフォワーディング（VRF）テーブルのみでサポートされます。
- NAT は、IPv4 ユニキャストだけでサポートされています。
- Cisco Nexusデバイスは次をサポートしていません。
  - ソフトウェアの変換。すべての変換はハードウェアで行われます。
  - NAT ルーティング
  - アプリケーション層の変換。レイヤ 4 およびその他の組み込み IP は変換されません（FTP、ICMP の障害、IPSec、HTTPS など）。
  - インターフェイス上で同時に設定された NAT および VLAN アクセス コントロール リスト（VACL）。
  - フラグメント化された IP パケットの PAT 変換。
  - ソフトウェア転送パケットの NAT 変換。たとえば、IP オプションを持つパケットは NAT 変換されません。
- IP アドレスがスタティック NAT 変換または PAT 変換に使用される場合、他の目的には使用できません。たとえば、インターフェイスに割り当てることはできません。
- スタティック NAT の場合は、外部グローバル IP アドレスが外部インターフェイス IP アドレスと異なる必要があります。
- （100 を超える）多数の変換を設定する場合、変換を設定してから NAT インターフェイスを設定する方が迅速に設定できます。
- ECMP NAT は Cisco Nexus® 3550-T スイッチではサポートされません。

スタティック NAT の設定

スタティック NAT のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **feature nat**	デバイス上でスタティック NAT 機能をイネーブルにします。
ステップ 3	switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

インターフェイスでのスタティック NAT の設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*	設定する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	switch(config-if)# **ip nat** {**inside** | **outside**}	内部または外部としてインターフェイスを指定します。 （注） マーク付きインターフェイスに到着したパケットだけが変換できます。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、スタティック NAT を使用して内部のインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# ip nat inside
```

内部送信元アドレスのスタティック NAT のイネーブル化

内部送信元変換の場合、トラフィックは内部インターフェイスから外部インターフェイスに流れます。NAT は、内部ローカル IP アドレスを内部グローバル IP アドレスに変換します。リターン トラフィックでは、宛先の内部グローバル IP アドレスが内部ローカル IP アドレスに変換されて戻されます。

（注） が、内部送信元 IP アドレス（Src:ip1）を外部送信元 IP アドレス（newSrc:ip2）に変換するように設定されている場合、は内部宛先 IP アドレス（newDst: ip1）への外部宛先 IP アドレス（Dst: ip2）の変換をCisco Nexus デバイス暗黙的に追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat inside source static** *local-ip-address global-ip-address* [**group** *group-id*]	内部グローバル アドレスを内部ローカル アドレスに、またはその逆に（内部ローカル トラフィックを内部ローカル（local）トラフィックに）変換するようにスタティック NAT を設定します。**group** を指定することにより、スタティック Twice NAT でこの変換が属するグループが指定されます。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、内部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.1 5.5.5.5
switch(config)# copy running-config startup-config
```

外部送信元アドレスのスタティック NAT のイネーブル化

外部送信元変換の場合、トラフィックは外部インターフェイスから内部インターフェイスに流れます。NAT は、外部グローバル IP アドレスを外部ローカル IP アドレスに変換します。リターン トラフィックでは、宛先の外部ローカル IP アドレスが外部グローバル IP アドレスに変換されて戻されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat outside source static** *outsideGlobalIP outsideLocalIP* [**dynamic**] [**add-route**]]	外部グローバル アドレスを外部ローカル アドレスに、またはその逆に（外部ローカル トラフィックを外部グローバル トラフィックに）変換するようにスタティック NAT を設定します。ポートなしで内部変換が設定されると、暗黙的な追加ルートが実行されます。外部変換の設定中、最初の追加ルート機能はオプションです。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、外部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source static 2.2.2.2 6.6.6.6
switch(config)# copy running-config startup-config
```

内部送信元アドレスのスタティック PAT の設定

ポート アドレス変換（PAT）を使用して、特定の内部ホストにサービスをマッピングできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat inside source static** {*inside-local-address inside-global-address* | {**tcp**| **udp**} *inside-local-address* {*local-tcp-port* | *local-udp-port*} *inside-global-address* {*global-tcp-port* | *global-udp-port*}}	スタティック NAT を内部ローカル ポート、内部グローバル ポートにマッピングします。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、UDP サービスを特定の内部送信元アドレスおよび UDP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)#  ip nat inside source static udp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

外部送信元アドレスのスタティック PAT の設定

ポート アドレス変換（PAT）を使用して、サービスを特定の外部ホストにマッピングできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat outside source static** {*outside-global-address outside-local-address* | {**tcp** | **udp**} *outside-global-address* {*global-tcp-port* |	スタティック NAT を、外部グローバル ポート、外部ローカル ポートにマッピングします。

	コマンドまたはアクション	目的
	global-udp-port} *outside-local-address* {*global-tcp-port* | *global-udp-port*}} {**add-route**}	
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、TCP サービスを特定の外部送信元アドレスおよび TCP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)#  ip nat outside source static tcp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

no-alias 設定の有効化と無効化

NAT デバイスは内部グローバル（IG）アドレスと外部ローカル（OL）アドレスを所有し、これらのアドレス宛ての ARP 要求に応答します。IG/OL アドレス サブネットがローカル インターフェイス サブネットと一致すると、NAT は IP エイリアスと ARP エントリをインストールします。この場合、デバイスは local-proxy-arp を使用して ARP 要求に応答します。

no-alias 機能は、アドレス範囲が外部インターフェイスの同じサブネットにある場合、特定の NAT プール アドレス範囲からのすべての変換された IP の ARP 要求に応答します。

NAT が設定されたインターフェイスで no-alias が有効になっている場合、外部インターフェイスはサブネット内の ARP 要求に応答しません。no-alias を無効にすると、外部インターフェイスと同じサブネット内の IP に対する ARP 要求が処理されます。

（注） この機能をサポートしていない古いリリースにダウングレードすると、*no-alias* オプションの設定が削除されることがあります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **feature nat**	デバイス上でスタティック NAT 機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **show run nat**	NAT の設定を表示します。
ステップ 4	switch(config)# **show ip nat-alias**	エイリアスが作成されたかどうかの情報を表示します。 （注） デフォルトでは、エイリアスが作成されます。エイリアスを無効にするには、*no-alias* キーワードをコマンドに追加する必要があります。
ステップ 5	switch(config)# **clear ip nat-alias** *ip address*/*all*	エイリアス リストからエントリを削除します。特定のエントリを削除するには、削除する IP アドレスを指定する必要があります。すべてのエントリを削除するには、すべてのキーワードを使用します。

例

次に、すべてのインターフェイスの情報を表示する例を示します。

```
switch# configure terminal
switch(config)# show ip int b
IP Interface Status for VRF "default"(1)
Interface            IP Address      Interface Status
Lo0                  100.1.1.1       protocol-up/link-up/admin-up
Eth1/1               7.7.7.1         protocol-up/link-up/admin-up
Eth1/3               8.8.8.1         protocol-up/link-up/admin-up
```

次に、実行コンフィギュレーションの例を示します。

```
switch# configure terminal
switch(config)# show running-config nat
!Command: show running-config nat
!Running configuration last done at: Thu Aug 23 11:57:01 2018
!Time: Thu Aug 23 11:58:13 2018

version 9.2(2) Bios:version 07.64
feature nat
interface Ethernet1/1
  ip nat inside
interface Ethernet1/3
  ip nat outside
switch(config)#
```

この例は、エイリアスを設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool p1 7.7.7.2 7.7.7.20 prefix-length 24
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3
switch(config)# show ip nat-alias
Alias Information for Context: default
```

```
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#
```

次に、*show ip nat-alias* の出力例を示します。デフォルトでは、エイリアスが作成されます。

```
switch# configure terminal
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#
```

この例は、エイリアスを無効にする方法を示します。

```
switch# configure terminal
switch(config)# ip nat pool p1 7.7.7.2 7.7.7.20 prefix-length 24 no-alias
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3 no-alias
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3 no-alias
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#

** None of the entry got appended as alias is disabled for above CLIs.
switch(config)#
```

この例は、エイリアスをクリアする方法を示します。エイリアス リストからエントリを削除するには、*clear ip nat-alias* を使用します。IP アドレスを指定して 1 つのエントリを削除することも、すべてのエイリアス エントリを削除することもできます。

```
switch# configure terminal
switch(config)# clear ip nat-alias address 7.7.7.2
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
8.8.8.2          Ethernet1/3
switch(config)#
switch(config)# clear ip nat-alias all
switch(config)# show ip nat-alias
switch(config)#
```

スタティック NAT および PAT の設定例

次に、スタティック NAT の設定例を示します。

```
ip nat inside source static 103.1.1.1 11.3.1.1
ip nat inside source static 139.1.1.1 11.39.1.1
ip nat inside source static 141.1.1.1 11.41.1.1
ip nat inside source static 149.1.1.1 95.1.1.1
ip nat inside source static 149.2.1.1 96.1.1.1
ip nat outside source static 95.3.1.1 95.4.1.1
ip nat outside source static 96.3.1.1 96.4.1.1
ip nat outside source static 102.1.2.1 51.1.2.1
```

```
ip nat outside source static 104.1.1.1 51.3.1.1
ip nat outside source static 140.1.1.1 51.40.1.1
```

次に、スタティック PAT の設定例を示します。

```
ip nat inside source static tcp 10.11.1.1 1 210.11.1.1 101
ip nat inside source static tcp 10.11.1.1 2 210.11.1.1 201
ip nat inside source static tcp 10.11.1.1 3 210.11.1.1 301
ip nat inside source static tcp 10.11.1.1 4 210.11.1.1 401
ip nat inside source static tcp 10.11.1.1 5 210.11.1.1 501
ip nat inside source static tcp 10.11.1.1 6 210.11.1.1 601
ip nat inside source static tcp 10.11.1.1 7 210.11.1.1 701
ip nat inside source static tcp 10.11.1.1 8 210.11.1.1 801
ip nat inside source static tcp 10.11.1.1 9 210.11.1.1 901
ip nat inside source static tcp 10.11.1.1 10 210.11.1.1 1001
ip nat inside source static tcp 10.11.1.1 11 210.11.1.1 1101
ip nat inside source static tcp 10.11.1.1 12 210.11.1.1 1201
```

スタティック NAT の設定の確認

スタティック NAT の設定を表示するには、次の作業を行います。

手順

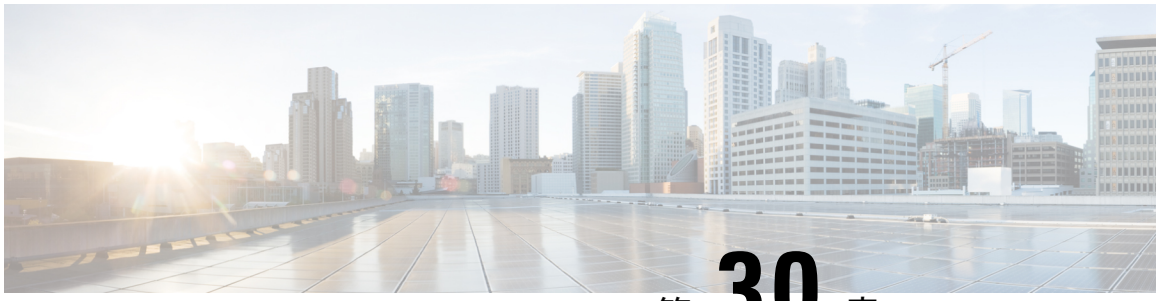
	コマンドまたはアクション	目的
ステップ 1	switch# **show ip nat translations**	内部グローバル、内部ローカル、外部ローカル、および外部グローバルの各 IP アドレスを示します。

例

次に、スタティック NAT の設定を表示する例を示します。

```
switch# sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global

--- ---                ---                51.3.1.1           104.1.1.1
--- ---                ---                95.4.1.1           95.3.1.1
--- ---                ---                96.4.1.1           96.3.1.1
--- ---                ---                51.40.1.1          140.1.1.1
--- ---                ---                51.42.1.1          142.1.2.1
--- ---                ---                51.1.2.1           102.1.2.1
--- 11.1.1.1           101.1.1.1          ---                ---
--- 11.3.1.1           103.1.1.1          ---                ---
--- 11.39.1.1          139.1.1.1          ---                ---
--- 11.41.1.1          141.1.1.1          ---                ---
--- 95.1.1.1           149.1.1.1          ---                ---
--- 96.1.1.1           149.2.1.1          ---                ---
    130.1.1.1:590      30.1.1.100:5000    ---                ---
    130.2.1.1:590      30.2.1.100:5000    ---                ---
    130.3.1.1:590      30.3.1.100:5000    ---                ---
    130.4.1.1:590      30.4.1.100:5000    ---                ---
    130.1.1.1:591      30.1.1.101:5000    ---                ---
```

```
switch# sh ip nat translations verbose
Pro Inside global      Inside local       Outside local      Outside global
any ---                ---                22.1.1.3           22.1.1.2
    Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.130         11.1.1.3           ---                ---
    Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:0
any 11.1.1.133         11.1.1.33          ---                ---
    Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.133         11.1.1.33          22.1.1.3           22.1.1.2
    Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:0
tcp 10.1.1.100:64490   10.1.1.2:0         20.1.1.2:0         20.1.1.2:0
    Flags:0x82 time-left(secs):43192 id:31 state:0x3 grp_id:0 vrf: default
N3550T-1#
```



第 30 章

レイヤ 2 インターフェイスの設定

この章では、レイヤ 2 スイッチング ポートを、Cisco NX-OS デバイスでのアクセス ポートまたはトランク ポートとして構成する方法について説明します。

（注） レイヤ 2 ポートは、次のいずれかとして機能できます。

- トランク ポート
- アクセス ポート

（注） SPAN 宛先インターフェイスについては、システム管理の概要 （139 ページ）を参照してください。

レイヤ 2 スイッチング ポートは、アクセス ポートまたはトランク ポートとして設定できます。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。すべてのレイヤ 2 スイッチング ポートは、メディア アクセス コントロール（MAC）アドレス テーブルを維持します。

（注） VLAN、MAC アドレス テーブル、プライベート VLAN、およびスパニングツリー プロトコルの詳細については、『Layer 2 Switching Configuration Guide』 （433 ページ）を参照してください。

アクセス インターフェイスとトランク インターフェイスについて

（注） このデバイスは、IEEE 802.1Q タイプ VLAN トランク カプセル化だけをサポートします。

アクセス インターフェイスとトランク インターフェイスの概要

レイヤ 2 ポートは、アクセスまたはトランク ポートとして次のように設定できます。

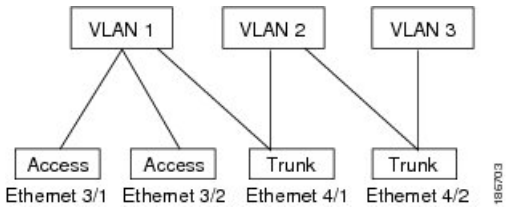
- アクセス ポートでは VLAN を 1 つだけ設定でき、1 つの VLAN のトラフィックだけを伝送できます。
- トランク ポートには複数の VLAN を設定でき、複数の VLAN のトラフィックを同時に伝送できます。

デフォルトでは、Cisco Nexus® 3550-T スイッチのすべてのポートはレイヤ 3 ポート/レイヤ 2 ポートです。

セットアップ スクリプトを使用するか、**system default switchport** コマンドを入力して、すべてのポートをレイヤ 2 ポートにできますすべてのポートをレイヤ 2 ポートにできます。セットアップ スクリプトを使用する詳細については、「*Cisco Nexus® 3550-T Fundamentals* 構成」のセクションを参照してください。CLI を使用して、ポートをレイヤ 2 ポートとして設定するには、**switchport** コマンドを使用します。

次の図は、ネットワークにおけるトランク ポートの使い方を示したものです。トランク ポートは、2 つ以上の VLAN のトラフィックを伝送します。

図 *26 :* トランクおよびアクセス ポートと *VLAN* トラフィック



（注） VLAN については、「*Cisco Nexus® 3550-T Layer 2 Switching* 構成」のセクションを参照してください。

複数の VLAN に接続するトランク ポートのトラフィックを正しく伝送するために、デバイスは IEEE 802.1Q カプセル化（タギング方式）を使用します（詳細については、「IEEE 802.1Q カプセル化」の項を参照）。

アクセス ポートでのパフォーマンスを最適化するには、そのポートをホスト ポートとして設定します。ホスト ポートとして設定されたポートは、自動的にアクセス ポートとして設定され、チャネル グループ化はディセーブルになります。ホストを割り当てると、割り当てたポートがパケット転送を開始する時間が短縮されます。

ホスト ポートとして設定できるのは端末だけです。端末以外のポートをホストとして設定しようとするとエラーになります。

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

レイヤ 2 インターフェイスはアクセス ポートまたはトランク ポートとして機能できますが、両方のポート タイプとして同時に機能できません。

レイヤ 2 インターフェイスをレイヤ 3 インターフェイスに戻すと、このインターフェイスはレイヤ 2 の設定をすべて失い、デフォルト VLAN 設定に戻ります。

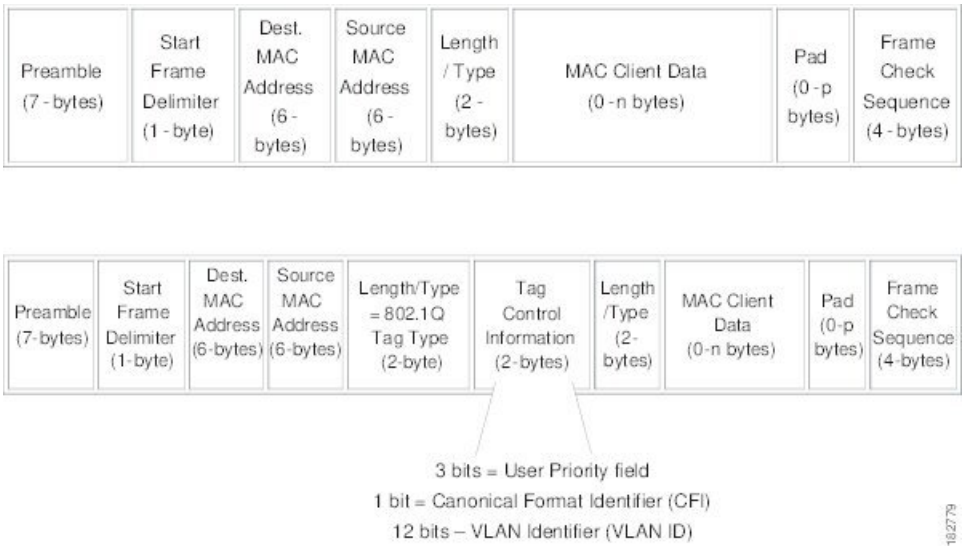
IEEE 802.1Q カプセル化

（注） VLAN については、「*Cisco Nexus® 3550-T Layer 2 Switching* 構成」のセクションを参照してください。

トランクとは、スイッチと他のネットワーキングデバイス間のポイントツーポイントリンクです。トランクは 1 つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。

複数の VLAN に接続するトランク ポートのトラフィックを正しく配信するために、デバイスは IEEE 802.1Q カプセル化（タギング方式）を使用します。この方式では、フレーム ヘッダーに挿入したタグが使用されます。このタグには、そのフレームおよびパケットが属する特定の VLAN に関する情報が含まれます。タグ方式を使用すると、複数の異なる VLAN 用にカプセル化されたパケットが、同じポートを通過しても、各 VLAN のトラフィックを区別することができます。また、カプセル化された VLAN タグにより、トランクは同じ VLAN 上のネットワークの端から端までトラフィックを移動させます。

図 *27 : 802.1Q* タグなしヘッダーと *802.1Q* タグ付きヘッダー



アクセス VLAN

アクセス モードでポートを設定すると、そのインターフェイスのトラフィックを伝送する VLAN を指定できます。アクセス モードのポート（アクセス ポート）用に VLAN を設定しないと、そのインターフェイスはデフォルトの VLAN（VLAN1）のトラフィックだけを伝送します。

VLAN のアクセス ポート メンバーシップを変更するには、新しい VLAN を指定します。VLAN をアクセス ポートのアクセス VLAN として割り当てるには、まず、VLAN を作成する必要があります。アクセス ポートのアクセス VLAN をまだ作成していない VLAN に変更すると、アクセス ポートがシャットダウンされます。

アクセス ポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

トランク ポートのネイティブ VLAN ID

トランク ポートは、タグなしパケットと 802.1Q タグ付きパケットを同時に伝送できます。デフォルトのポート VLAN ID をトランク ポートに割り当てると、すべてのタグなしトラフィックが、そのトランク ポートのデフォルトのポート VLAN ID で伝送され、タグなしトラフィックはすべてこの VLAN に属するものと見なされます。この VLAN のことを、トランク ポートのネイティブ VLAN ID といいます。つまり、トランク ポートでタグなしトラフィックを伝送する VLAN がネイティブ VLAN ID となります。

（注） ネイティブ VLAN ID 番号は、トランクの両端で一致していなければなりません。

トランク ポートは、デフォルトのポート VLAN ID と同じ VLAN が設定された出力パケットをタグなしで送信します。他のすべての出力パケットは、トランク ポートによってタグ付けされます。ネイティブ VLAN ID を設定しないと、トランク ポートはデフォルト VLAN を使用します。

ネイティブ VLAN トラフィックのタギング

シスコのソフトウェアは、トランク ポートで IEEE 802.1Q 標準をサポートします。タグなしトラフィックがトランク ポートを通過するには、パケットにタグがない VLAN を作成する必要があります（またはデフォルト VLAN を使用することもできます）。タグなしパケットはトランク ポートとアクセス ポートを通過できます。

ただし、デバイスを通過するすべてのパケットに 802.1Q タグがあり、トランクのネイティブ VLAN の値と一致する場合はタギングが取り除かれ、タグなしパケットとしてトランク ポートから出力されます。トランク ポートのネイティブ VLAN でパケットのタギングを保持したい場合は、この点が問題になります。

Allowed VLANs

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランク上では、すべての VLAN ID が許可されます。この包括的なリストから VLAN を削除することによって、特定の VLAN からのトラフィックが、そのトランクを通過するのを禁止できます。後ほど、トラフィックを伝送するトランクの VLAN を指定してリストに追加し直すこともできます。

デフォルト VLAN のスパニングツリープロトコル（STP）トポロジを区切るには、許容 VLAN のリストから VLAN1 を削除します。この分割を行わないと、VLAN1（デフォルトでは、すべてのポートでイネーブル）が非常に大きな STP トポロジを形成し、STP のコンバージェンス中に問題が発生する可能性があります。VLAN1 を削除すると、そのポート上で VLAN1 のデータ トラフィックはすべてブロックされますが、制御トラフィックは通過し続けます。

（注） STP の詳細については、「*Cisco Nexus® 3550-T Layer 2 Switching* 構成」のセクションを参照してください。

デフォルト インターフェイス

デフォルト インターフェイス機能を使用して、イーサネット、ループバック、VLAN ネットワーク、およびポートチャネル インターフェイスなどの物理インターフェイスおよび論理インターフェイスの両方に対する構成済みパラメータを消去できます。

（注） すべての 48 ポートがデフォルト インターフェイスに選択できます。

スイッチ仮想インターフェイスおよび自動ステート動作

Cisco NX-OS では、スイッチ仮想インターフェイス（SVI）は、デバイスの VLAN のブリッジング機能とルーティング機能間の論理インターフェイスを表します。

このインターフェイスの動作状態は、その対応する VLAN 内のさまざまなポートの状態によって決まります。VLAN の SVI インターフェイスは、その VLAN 内の少なくとも 1 個のポートがスパニングツリー プロトコル（STP）のフォワーディング ステートにある場合に稼働します。同様に、このインターフェイスは最後の STP 転送ポートがダウンするか、別の STP 状態になったとき、ダウンします。

高可用性

ソフトウェアは、レイヤ 2 ポートのハイ アベイラビリティをサポートします。

（注） 高可用性機能の詳細については、『*Cisco Nexus® 3550-T* 高可用性および冗長性ガイド』を参照してください。

レイヤ 2 インターフェイスの前提条件

レイヤ 2 インターフェイスには次の前提条件があります。

- デバイスにログインしている。
- デフォルトでは、Cisco NX-OS はレイヤ 3 パラメータを設定します。レイヤ 2 パラメータを設定するには、ポート モードをレイヤ 2 に切り替える必要があります。**switchport** コマンドを使用すれば、ポート モードを変更できます。
- **switchport mode** コマンドを使用する前に、ポートをレイヤ 2 ポートとして設定する必要があります。デフォルトでは、デバイスのポートはすべてレイヤ 3 ポートです。デフォルトでは、Cisco Nexus® 3550-T デバイスのすべてのポートはレイヤ 2 ポートです。

レイヤ 2 インターフェイスのガイドラインおよび制約事項

VLAN トランキングには次の設定上のガイドラインと制限事項があります。

- ポートはレイヤ 2 またはレイヤ 3 インターフェイスのいずれかです。両方が同時に成立することはありません。
- レイヤ 3 ポートをレイヤ 2 ポートに変更する場合またはレイヤ 2 ポートをレイヤ 3 ポートに変更する場合は、レイヤに依存するすべての設定は失われます。アクセスまたはトラン

ク ポートをレイヤ 3 ポートに変更すると、アクセス VLAN、ネイティブ VLAN、許容 VLAN などの情報はすべて失われます。

- アクセス リンクを持つデバイスには接続しないでください。アクセス リンクにより VLAN が区分されることがあります。
- 802.1Q トランクを介してシスコ デバイスを接続するときは、802.1Q トランクのネイティブ VLAN がトランク リンクの両端で同じであることを確認してください。トランクの一端のネイティブ VLAN と反対側の端のネイティブ VLAN が異なると、スパニングツリー ループの原因になります。
- ネットワーク上のすべてのネイティブ VLAN についてスパニングツリーをディセーブルにせずに、802.1Q トランクの VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。802.1Q トランクのネイティブ VLAN のスパニングツリーはイネーブルのままにしておく必要があります。スパニングツリーをイネーブルにしておけない場合は、ネットワークの各 VLAN のスパニングツリーをディセーブルにする必要があります。スパニングツリーをディセーブルにする前に、ネットワークに物理ループがないことを確認してください。
- 802.1Q トランクを介して 2 台のシスコ デバイスを接続すると、トランク上で許容される VLAN ごとにスパニングツリー ブリッジ プロトコル データ ユニット（BPDU）が交換されます。トランクのネイティブ VLAN 上の BPDU は、タグなしの状態で予約済み IEEE 802.1D スパニングツリー マルチキャスト MAC アドレス（01-80-C2-00-00-00）に送信されます。トランクの他のすべての VLAN 上の BPDU は、タグ付きの状態で、予約済み Cisco Shared Spanning Tree（SSTP）マルチキャスト MAC アドレス（01-00-0c-cc-cc-cd）に送信されます。
- 他社製の 802.1Q デバイスでは、すべての VLAN に対してスパニングツリー トポロジを定義するスパニングツリーのインスタンス（Mono Spanning Tree）が 1 つしか維持されません。802.1Q トランクを介してシスコ製スイッチを他社製のスイッチに接続すると、他社製のスイッチの Mono Spanning Tree とシスコ製スイッチのネイティブ VLAN スパニングツリーが組み合わされて、Common Spanning Tree（CST）と呼ばれる単一のスパニングツリー トポロジが形成されます。
- シスコ デバイスは、トランクのネイティブ VLAN 以外の VLAN にある SSTP マルチキャスト MAC アドレスに BPDU を伝送します。したがって、他社製のデバイスではこれらのフレームが BPDU として認識されず、対応する VLAN のすべてのポート上でフラッディングされます。他社製の 802.1Q クラウドに接続された他のシスコ デバイスは、フラッディングされたこれらの BPDU を受信します。BPDU を受信すると、Cisco スイッチは、他社製の 802.1Q デバイス クラウドにわたって、VLAN 別のスパニングツリー トポロジを維持できます。シスコ デバイスを隔てている他社製の 802.1Q クラウドは、802.1Q トランクを介して他社製の 802.1Q クラウドに接続されたすべてのデバイス間の単一のブロードキャスト セグメントとして処理されます。
- シスコ デバイスを他社製の 802.1Q クラウドに接続するすべての 802.1Q トランク上で、ネイティブ VLAN が同じであることを確認します。
- 他社製の特定の 802.1Q クラウドに複数のシスコ デバイスを接続する場合は、すべての接続に 802.1Q トランクを使用する必要があります。シスコ デバイスを他社製の 802.1Q クラ

ウドにアクセス ポート経由で接続することはできません。この場合、シスコ製のアクセス ポートはスパニングツリー「ポート不一致」状態になり、トラフィックはポートを通過しません。

- トランク ポートをポートチャネル グループに含めることができますが、そのグループのトランクはすべて同じ設定にする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。パラメータの設定を変更すると、許容 VLAN やトランク ステータスなど、デバイスのグループのすべてのポートにその設定を伝えます。たとえば、ポート グループのあるポートがトランクになるのを中止すると、すべてのポートがトランクになるのを中止します。
- clear mac address-table dynamicコマンドを使用してVLANのMACアドレスをクリアすると、そのVLANのダイナミックARP（Address Resolution Protocol）エントリが更新されます。
- VLAN上にスタティックARPエントリが存在し、MACアドレスからポートへのマッピングが存在しない場合、スーパーバイザはARP要求を生成してMACアドレスを学習できます。MACアドレスを学習すると、隣接エントリは正しい物理ポートをポイントします。
- Cisco NX-OSは、SVIの1つがBIA MAC（バーンドインMACアドレス）を使用してCisco Nexus 9000上にある場合、2つのVLAN間のトランスペアレントブリッジングをサポートしません。これは、BIA MACがSVI / VLAN間で共有される場合に発生します。BIA MACとは異なるMACを、トランスペアレントブリッジングが正しく動作するようにSVIで設定できます。
- インターフェイス モードをトランク VLAN とトランク VLAN に同時に設定しようとすると、エラー メッセージが表示されることがあります。Cisco NX-OS インターフェイスでは、インターフェイス モードのデフォルト値は access です。トランク関連の設定を実装するには、最初にインターフェイス モードを trunk に変更してから、トランク VLAN 範囲を設定する必要があります。
- ***Cisco Nexus 3550-T - 10.1(2t)* リリース** のスイッチはカットスルー転送を行います。したがって、MTU チェックは導入されていません。

  ハードウェア バッファリングはジャンボ パケット用に設計されておらず、通常の mtu サイズ 1516 を超えるパケットはサポートされていません。

レイヤ 2 インターフェイスのデフォルト設定

次の表に、デバイスのアクセスおよびトランク ポート モード パラメータのデフォルト設定を示します。

アクセスインターフェイスとトランク インターフェイスの設定

（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。

レイヤ 2 アクセス ポートとしての VLAN インターフェイスの設定

レイヤ 2 ポートをアクセス ポートとして設定できます。アクセス ポートは、パケットを、1 つのタグなし VLAN 上だけで送信します。インターフェイスが伝送する VLAN トラフィックを指定します。これがアクセス VLAN になります。アクセス ポートの VLAN を指定しない場合、そのインターフェイスはデフォルト VLAN のトラフィックだけを伝送します。デフォルトの VLAN は VLAN 1 です。

VLAN をアクセス VLAN として指定するには、その VLAN が存在しなければなりません。システムは、存在しないアクセス VLAN に割り当てられたアクセス ポートをシャット ダウンします。

始める前に

レイヤ 2 インターフェイスを設定することを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet** {{*type slot/port*} | {**port-channel** *number*}}
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		設定する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	**switchport mode** [**access** | **trunk**] 例： `switch(config-if)# switchport mode access`	インターフェイスを、非トランキング、タグなし、シングル VLAN レイヤ 2 インターフェイスとして設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。デフォル

	コマンドまたはアクション	目的
		トでは、アクセス ポートはVLAN1 のトラフィックを伝送します。異なるVLAN のトラフィックを伝送するようにアクセス ポートを設定するには、**switchport access vlan** を使用します コマンドを使用します。
ステップ 4	**switchport access vlan** *vlan-id* 例： `switch(config-if)# switchport access vlan 5`	このアクセス ポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しないと、アクセス ポートはVLAN1 だけのトラフィックを伝送します。このコマンドを使用して、アクセス ポートがトラフィックを伝送する VLAN を変更できます。

ステップ 5	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 6	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 7	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

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。

例

次に、イーサネット 1/1 をレイヤ 2 アクセス ポートとして設定し、VLAN5 のトラフィックだけを伝送する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
```

```
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

アクセス ホスト ポートの設定

（注） switchport host コマンドは、端末に接続するインターフェイスだけに使用します。

端末に接続されたアクセス ポートでのパフォーマンスを最適化するには、そのポートをホスト ポートとしても設定します。アクセス ホスト ポートはエッジ ポートと同様に STP を処理し、ブロッキング ステートおよびラーニング ステートを通過することなくただちにフォワーディング ステートに移行します。インターフェイスをアクセス ホスト ポートとして設定すると、そのインターフェイス上でポート チャネル動作がディセーブルになります。

（注） ポートチャネル インターフェイスについては、「ポート チャネルの構成」のセクションおよび「*Cisco Nexus® 3550-T Layer 2 Switching* の構成 」のセクションを参照してください。

始める前に

エンドステーションのインターフェイスに接続された適切なインターフェイスを設定することを確認してください。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface ethernet** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		設定する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	**switchport host** 例： `switch(config-if)# switchport host`	インターフェイスをアクセス ホスト ポートとして設定します。このポートはただちに、スパニングツリー フォワーディング ステートに移行し、このインターフェイスのポート チャネル動作をディセーブルにします。

	コマンドまたはアクション	目的
		（注） このコマンドは端末だけに適用します。

ステップ 4	**exit**
	例：
	`switch(config-if-range)# exit`
	`switch(config)#`
		インターフェイスモードを終了します。

ステップ 5	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 6	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、イーサネット 1/1 をレイヤ 2 アクセス ポートとして設定し、PortFast を有効化してポート チャネルを無効化にする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport host
switch(config-if)#
```

トランク ポートの設定

レイヤ 2 ポートをトランク ポートとして設定できます。トランク ポートは、1 つの VLAN の非タグ付きパケットと、複数のVLANのカプセル化されたタグ付きパケットを伝送します（カプセル化については、「*IEEE 802.1Q* カプセル化」のセクションを参照してください）。

（注） デバイスは 802.1Q カプセル化だけをサポートします。

始める前に

トランク ポートを設定する前に、レイヤ 2 インターフェイスを設定することを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** {*type slot/port* | **port-channel** *number*}
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		設定する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	**switchport mode** [**access** | **trunk**] 例： `switch(config-if)# switchport mode trunk`	インターフェイスをレイヤ 2 トランク ポートとして設定します。トランク ポートは、同じ物理リンクで 1 つ以上の VLAN内のトラフィックを伝送できます（各 VLAN はトランキングが許可された VLAN リストに基づいています）。デフォルトでは、トランク インターフェイスはすべての VLAN のトラフィックを伝送できます。指定したトランクで特定の VLAN のみが許可されるように指定するには、**switchport trunk allowed vlan** コマンドを使用します。

ステップ 4	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。
ステップ 6	**no shutdown** 例：	（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび

	コマンドまたはアクション	目的
	switch# **configure terminal** switch(config)# **int e1/1** switch(config-if)# **no shutdown**	VLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 7	**copy running-config startup-config** 例： switch(config)# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、イーサネット 1/1 をレイヤ 2 トランク ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode trunk
switch(config-if)#
```

802.1Q トランク ポートのネイティブ VLAN の設定

ネイティブ VLAN を 802.1Q トランク ポートに設定できます。このパラメータを設定しないと、トランク ポートは、デフォルト VLAN をネイティブ VLAN ID として使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 slot/port*} | {**port-channel** *number*}} 例： switch(config)# **interface ethernet 1/1** switch(config-if)#	設定する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	**switchport trunk native vlan** *vlan-id* 例： switch(config-if)# switchport trunk native vlan 5	802.1Q トランクのネイティブ VLAN を設定します。指定できる範囲は1～4094です（ただし、内部使用に予約されてい

	コマンドまたはアクション	目的
		る VLAN は除きます）。デフォルト値は VLAN 1 です。

ステップ 4	**exit**
	例：
	`switch(config-if-range)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show vlan** 例： `switch# show vlan`	（任意）VLANのステータスと内容を表示します。

ステップ 6	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、ネイティブ VLAN をイーサネット 1/1 に設定し、レイヤ 2 トランク ポートを VLAN5 に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport trunk native vlan 5
switch(config-if)#
```

トランキング ポートの許可 VLAN の設定

特定のトランク ポートで許可されている VLAN の ID を指定できます。

（注） **switchport trunk allowed vlan** *vlan-list* コマンドは、指定されたポートの現在のVLANリストを新しいリストに置き換えます。新しいリストが適用される前に確認を求められます。

大規模な設定のコピー アンド ペーストをしている場合は、CLI が他のコマンドを受け入れる前に確認のため待機しているので障害が発生する場合があります。この問題を回避するため、**terminal dont-ask** を使用してプロンプトを無効にできます。 コマンドを入力してから、設定を貼り付けます。

始める前に

指定トランク ポートの許可 VLAN を設定する前に、正しいインターフェイスを設定していること、およびそのインターフェイスがトランクであることを確認してください。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** {**ethernet** *slot/port* | **port-channel** *number*} 例： `switch(config)# interface ethernet 1/1`	設定する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	**switchport trunk allowed vlan** {*vlan-list* **add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*} 例： `switch(config-if)# switchport trunk allowed vlan add 15-20#`	トランク インターフェイスの許可VLANを設定します。デフォルトでは、トランク インターフェイス上のすべてのVLAN（1 ～ 3967 および 4048 ～ 4094）が許可されます。

ステップ 4	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了します。

ステップ 5	**show vlan** 例： `switch# show vlan`	（任意）VLANのステータスと内容を表示します。
ステップ 6	**no shutdown** 例：	（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび

	コマンドまたはアクション	目的

	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		VLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、VLAN 15 ～ 20 をイーサネット 1/1、レイヤ 2 トランク ポートの許容 VLAN リストに追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport trunk allowed vlan 15-20
switch(config-if)#
```

デフォルト インターフェイスの設定

デフォルトインターフェイス機能によって、イーサネット、ループバック、VLANネットワーク、ポートチャネル、およびトンネルインターフェイスなどの複数インターフェイスの既存コンフィギュレーションを消去できます。特定のインターフェイスでのすべてのユーザコンフィギュレーションは削除されます。後で削除したコンフィギュレーションを復元できるように、任意でチェックポイントを作成してからインターフェイスのコンフィギュレーションを消去できます。

（注） デフォルトのインターフェイス機能は、管理インターフェイスに対しサポートされていません。それはデバイスが到達不能な状態になる可能性があるためです。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
ステップ 2	**default interface** *int-if* [**checkpoint** *name*] 例： `switch(config)# default interface ethernet 1/1 checkpoint test8`	インターフェイスの設定を削除しデフォルトの設定を復元します。**?** キーワードを使用して、サポートされるインターフェイスを表示します。 **checkpoint** コマンドを使用し、キーワードを使用して、設定を消し去ってしまう前にインターフェイスの実行コンフィギュレーションを保存します。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch(config)#`
		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 interface** 例： `switch# show interface`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 5	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

例

次に、ロールバック目的で実行コンフィギュレーションのチェックポイントを保存する際にイーサネット インターフェイスの設定を削除する例を示します。

```
switch# configure terminal
switch(config)# default interface ethernet 1/1 checkpoint test8
.......Done
switch(config)#
```

システムのデフォルト ポート モードをレイヤ 2 に変更

システムのデフォルト ポート モードをレイヤ 2 アクセス ポートに設定できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**system default switchport** [**shutdown**] 例： switch(config-if)# **system default switchport**	システムのすべてのインターフェイスに対するデフォルトのポート モードをレイヤ 2 アクセス ポート モードに設定し、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。デフォルトでは、すべてのインターフェイスがレイヤ 3 です。 （注） クライアントが **system default switchport shutdown** コマンドが発行されます。 • **no shutdown** で明示的に設定されていないレイヤ 2 ポートはシャットダウンされます。シャットダウンを回避するには、**no shut** でレイヤ 2 ポートを設定します。

ステップ 3	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 4	**show interface brief** 例： `switch# show interface brief`	（任意）インターフェイスのステータスと内容を表示します。

ステップ 5	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

	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。

例

次に、システム ポートをデフォルトでレイヤ 2 アクセス ポートに設定する例を示します。

```
switch# configure terminal
switch(config-if)# system default switchport
switch(config-if)#
```

インターフェイス コンフィギュレーションの確認

アクセスおよびトランク インターフェイス設定情報を表示するには、次のタスクのいずれかを行います。

コマンド	目的
show interface ethernet *slot/port* [**brief** | | **counters** | **debounce** | **description** | **flowcontrol** | **mac-address** | **status** | **transceiver**]	インターフェイスの設定を表示します。
show interface brief	インターフェイス設定情報を、モードも含めて表示します。
show interface switchport	アクセスおよびトランク インターフェイスも含めて、すべてのレイヤ 2 インターフェイスの情報を表示します。
show interface trunk [**module** *module-number* | **vlan** *vlan-id*]	トランク設定情報を表示します。
show interface capabilities	インターフェイスの機能に関する情報を表示します。
show running-config [**all**]	現在の設定に関する情報を表示します。 **all** コマンドを使用すると、デフォルトの設定と現在の設定が表示されます。
show running-config interface ethernet *slot/port*	指定されたインターフェイスに関する設定情報を表示します。

コマンド	目的
show running-config interface port-channel *slot/port*	指定されたポートチャネル インターフェイスに関するコンフィギュレーション情報を表示します。
show running-config interface vlan *vlan-id*	指定された VLAN インターフェイスに関するコンフィギュレーション情報を表示します。

レイヤ 2 インターフェイスのモニタリング

レイヤ 2 インターフェイスを表示するには、次のコマンドを使用します。

コマンド	目的
clear counters interface [**interface**]	カウンタをクリアします。
show interface counters [**module** *module*]	入力および出力オクテット ユニキャスト パケット、マルチキャスト パケット、ブロードキャスト パケットを表示します。
show interface counters detailed [**all**]	入力パケット、バイト、マルチキャストを、出力パケットおよびバイトとともに表示します。
show interface counters errors [**module** *module*]	エラー パケットの数を表示します。

アクセス ポートおよびトランク ポートの設定例

次に、レイヤ2アクセスインターフェイスを設定し、このインターフェイスにアクセスVLANモードを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/30
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

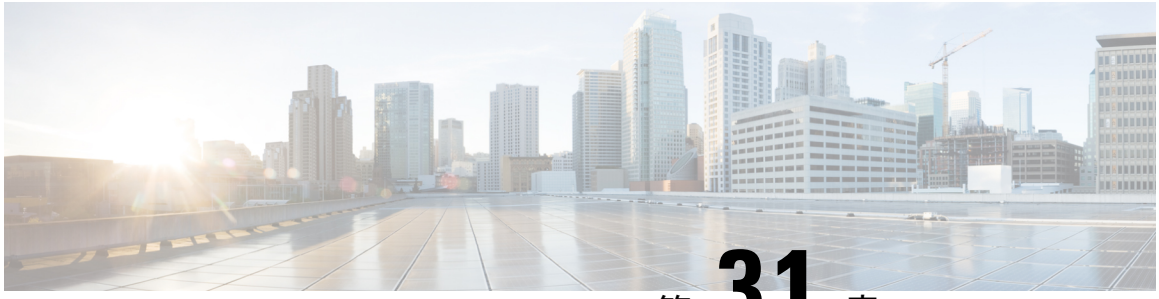
次に、レイヤ 2 トランク インターフェイスを設定してネイティブ VLAN および許容 VLAN を割り当て、デバイスにトランク インターフェイスのネイティブ VLAN トラフィックのタグを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/35
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 10
switch(config-if)# switchport trunk allowed vlan 5, 10
```

```
switch(config-if)# exit
switch(config)#
```

関連資料

関連資料	マニュアル タイトル
レイヤ 3 インターフェイスの設定	「レイヤ*2*インターフェイスの構成」セクション
ポート チャネル	「ポート チャネルの構成」セクション
VLAN、および STP	「*Cisco Nexus® 3550-T* レイヤ *2* スイッチング構成」章
システム管理	「*Cisco Nexus® 3550-T* システム管理構成」章
高可用性	『*Cisco Nexus Series* 高可用性および冗長性ガイド』
ライセンス	『*Cisco NX-OS Licensing Guide*』
リリース ノート	『*Cisco Nexus® Series NX-OS* リリース ノート』



第 31 章

ポート チャネルの設定

ポート チャネルについて

ポートチャネルは複数の物理インターフェイスの集合体で、論理インターフェイスを作成します。1つのポートチャネルに最大4つの個別アクティブ リンクをバンドルして、帯域幅と冗長性を向上させることができます。これらの集約された各物理インターフェイス間でトラフィックのロード バランシングも行います。ポート チャネルの物理インターフェイスが少なくとも1つ動作していれば、そのポート チャネルは動作しています。

レイヤ 2 ポート チャネルに適合するレイヤ 2 インターフェイスをバンドルすれば、レイヤ 2 ポート チャネルを作成できます。レイヤ 3 ポート チャネルに適合するレイヤ 3 インターフェイスをバンドルすれば、レイヤ3ポートチャネルを作成できます。レイヤ2インターフェイスとレイヤ 3 インターフェイスを同一のポート チャネルで組み合わせることはできません。

ポートチャネルをレイヤ3からレイヤ2に変更することもできます。レイヤ2インターフェイスの作成については、「レイヤ *2* インターフェイスの構成」の章を参照してください。

レイヤ 2 ポート チャネル インターフェイスとそのメンバー ポートは、異なる STP パラメータを持つことができます。ポート チャネルの STP パラメータを変更しても、メンバー ポートがバンドルされている場合はポートチャネルインターフェイスが優先されるため、メンバーポートの STP パラメータには影響しません。

（注） メンバーは、同じ**クワッド**に属している場合にのみ、ポート チャネルにバンドルできます。

（注） レイヤ 2 ポートがポート チャネルの一部になった後に、すべてのスイッチポートの設定をポート チャネルで実行する必要があります。スイッチポートの設定を各ポート チャネル メンバに適用できません。レイヤ 3 の設定を各ポート チャネル メンバに適用できません。設定をポート チャネル全体に適用する必要があります。

集約プロトコルが関連付けられていない場合でもスタティック ポート チャネルを使用して設定を簡略化できます。

柔軟性を高めたい場合は LACP を使用できます。Link Aggregation Control Protocol（LACP）は IEEE 802.3ad で定義されています。LACP を使用すると、リンクによってプロトコル パケットが渡されます。共有インターフェイスでは LACP を設定できません。

LACP については、「*LACP* の概要」のセクションを参照してください。

ポート チャネル

ポート チャネルは、物理リンクをまとめて 1 つのチャネル グループに入れ、最大 4 の物理リンクの帯域幅を集約した単一の論理リンクを作ります。ポート チャネル内のメンバー ポートに障害が発生すると、障害が発生したリンクで伝送されていたトラフィックはポート チャネル内のその他のメンバー ポートに切り替わります。

ただし、LACP をイネーブルにすればポート チャネルをより柔軟に使用できます。LACP を使ってポート チャネルを設定する場合と静的ポート チャネルを使って設定する場合では、手順が多少異なります（「ポート チャネルの構成」のセクションを参照してください）。

（注） デバイスはポート チャネルに対するポート集約プロトコル（PAgP）をサポートしません。

各ポートにはポート チャネルが 1 つだけあります。ポート チャネルのすべてのポートには互換性があり、同じ速度とデュプレックス モードを使用します（「互換性要件」のセクションを参照してください）。集約プロトコルを使わずに静的ポート チャネルを実行する場合、物理リンクはすべて on チャネル モードです。このモードは、LACP を有効化しない限り変更できません（「ポート チャネル モード」のセクションを参照してください）。

ポート チャネル インターフェイスを作成すると、ポート チャネルを直接作成できます。またはチャネル グループを作成して個別ポートをバンドルに集約させることができます。インターフェイスをチャネル グループに関連付けると、ポート チャネルがない場合は対応するポート チャネルが自動的に作成されます。この場合、ポート チャネルは最初のインターフェイスのレ

イヤ2またはレイヤ3設定を行います。最初にポート チャネルを作成することもできます。この場合は、Cisco NX-OS ソフトウェアがポート チャネルと同じチャネル番号の空のチャネル グループを作成してデフォルト レイヤ2またはレイヤ3設定を行い、互換性も構成します（「互換性要件」のセクションを参照してください）。

（注） 少なくともメンバ ポートの 1 つがアップしており、かつそのポートのチャネルが有効であれば、ポート チャネルは動作上アップ状態にあります。メンバー ポートがすべてダウンしていれば、ポート チャネルはダウンしています。

ポートチャネル インターフェイス

次に、ポートチャネル インターフェイスを示します。

ポート チャネル インターフェイスは、レイヤ 2 またはレイヤ 3 インターフェイスとして分類できます。さらに、レイヤ 2 ポート チャネルはアクセス モードまたはトランク モードに設定できます。レイヤ 3 ポート チャネル インターフェイスのチャネル メンバにはルーテッド ポートがあます。

レイヤ3 ポート チャネルにスタティック MAC アドレスを設定できます。この値を設定しない場合、レイヤ 3 ポート チャネルは、最初にアップになるチャネル メンバのルータ MAC を使用します。レイヤ3 ポート チャネルで静的 MAC アドレスを構成するための詳細については、「*Cisco Nexus® 3550-T* レイヤ *2* スイッチング構成」のセクションを参照してください。

アクセス モードまたはトランク モードでのレイヤ 2 ポートの構成について詳細は、「 *Cisco Nexus® 3550-T* レイヤ *2* インターフェイスの構成」の章を、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の構成については、「レイヤ*3*インターフェイスの構成」の章を参照してください。

基本設定

ポート チャネル インターフェイスには次の基本設定ができます。

- 帯域幅：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 遅延：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 説明
- IP アドレス
- シャットダウン

互換性要件

チャネル グループにインターフェイスを追加する場合、そのインターフェイスにチャネル グループとの互換性があるかどうかを確認するために、特定のインターフェイス属性がチェックされます。たとえば、レイヤ 2 チャネル グループにレイヤ 3 インターフェイスを追加できません。また Cisco NX-OS ソフトウェアは、インターフェイスがポート チャネル集約に参加することを許可する前に、そのインターフェイスの多数の動作属性もチェックします。

互換性チェックの対象となる動作属性は次のとおりです。

- ネットワーク層
- ポート モード
- アクセス VLAN
- トランク ネイティブ VLAN
- タグ付きまたは非タグ付き
- 許可 VLAN リスト
- フロー制御性能
- フロー制御設定
- メディア タイプ、銅線またはファイバ

show port-channel compatibility-parameters を使用します Cisco NX-OS で使用される互換性チェックの全リストを表示するは、コマンドを使用します。

チャネル モードが on に設定されているインターフェイスは、スタティックなポート チャネルにだけ追加できます。また、チャネル モードが active または passive に設定されているインターフェイスは、LACP が実行されているポート チャネルにだけ追加できます。これらのアトリビュートは個別のメンバ ポートに設定できます。設定するメンバ ポートの属性に互換性がない場合、ソフトウェアはこのポートをポート チャネルで一時停止させます。

または、次のパラメータが同じ場合、パラメータに互換性がないポートを強制的にポート チャネルに参加させることもできます。

- フロー制御性能
- フロー制御設定

インターフェイスがポート チャネルに参加すると、一部のパラメータが削除され、ポート チャネルの値が次のように置き換わります。

- 帯域幅
- 遅延
- IP アドレス

- MAC アドレス
- スパニングツリー プロトコル

インターフェイスがポートチャネルに参加または脱退しても、次に示す多くのインターフェイス パラメータは影響を受けません。

- ビーコン
- 説明
- CDP
- LACP ポート プライオリティ
- Debounce
- シャットダウン
- SNMP トラップ

（注） ポートチャネルを削除すると、すべてのメンバインターフェイスはポートチャネルから削除されたかのように設定されます。

ポートチャネルモードについては、「LACPマーカー レスポンダ」の項を参照してください。

ポート チャネルを使ったロード バランシング

Cisco NX-OS ソフトウェアは、ポートチャネルにおけるすべての動作インターフェイス間のトラフィックをロード バランシングします。その際、フレーム内のアドレスをハッシュして、チャネル内の 1 つのリンクを選択する数値にします。ポート チャネルはデフォルトでロード バランシングを備えています。ポートチャネル ロードバランシングでは、MACアドレス、IP アドレス、またはレイヤ 4 ポート番号を使用してリンクを選択します。ポート チャネル ロードバランシングは、送信元または宛先アドレスおよびポートの両方またはどちらか一方を使用します。

ロード バランシング モードを設定して、デバイス全体に設定したすべてのポート チャネルに適用することができます。デバイス全体で1つのロードバランシング モードを設定できます。ポート チャネルごとにロード バランシング方式を設定することはできません。

使用するロード バランシング アルゴリズムのタイプを設定できます。ロード バランシング アルゴリズムを指定し、フレームのフィールドを見て出力トラフィックに選択するメンバ ポートを決定します。

レイヤ 3 インターフェイスのデフォルト ロード バランシング モードは、発信元および宛先 IP L4 ポートです。非 IP トラフィックのデフォルト ロード バランシング モードは、送信元および宛先 MAC アドレスです。**port-channel load-balance** コマンドを使用し、 して、チャネル グループ バンドルのインターフェイス間のロード バランシング方式を設定します。レイヤ 2 パ

ケットのデフォルト方式は src-dst-mac です。レイヤ 3 パケットのデフォルトの方式は src-dst ip-l4 です。

次のいずれかの方式を使用するデバイスを設定し、ポート チャネル全体をロード バランシングできます。

- 宛先 MAC アドレス
- 送信元 MAC アドレス
- 送信元および宛先 MAC アドレス
- 宛先 IP アドレス
- 送信元 IP アドレス
- 送信元および宛先 IP アドレス

非 IP およびレイヤ 3 ポート チャネルはどちらも設定したロード バランシング方式に従い、発信元、宛先、または発信元および宛先パラメータを使用します。たとえば、発信元 IP アドレスを使用するロード バランシングを設定すると、すべての非 IP トラフィックは発信元 MAC アドレスを使用してトラフィックをロードバランシングしますが、レイヤ3トラフィックは発信元 IP アドレスを使用してトラフィックをロード バランシングします。同様に、宛先 MAC アドレスをロードバランシング方式として設定すると、すべてのレイヤ3トラフィックは宛先 IP アドレスを使用しますが、非 IP トラフィックは宛先 MAC アドレスを使用してロード バランシングします。

ユニキャストおよびマルチキャスト トラフィックは、**show port-channel load-balancing**コマンド出力に表示される設定済みのロードバランシングアルゴリズムに基づいて、ポートチャネル リンク間でロードバランシングが行われます。

マルチキャスト トラフィックは、次の方式を使用してポート チャネルのロード バランシングを行います。

- レイヤ 4 情報を持たないマルチキャスト トラフィック：発信元 IP アドレス、宛先 IP アドレス
- 非 IP マルチキャスト トラフィック：発信元 MAC アドレス、宛先 MAC アドレス

（注） Cisco IOS を実行するデバイスは、port-channel hash-distribution コマンドによって単一のメンバーに障害が発生した場合、メンバー ポート ASIC の動作を最適化できます。Cisco Nexus 3550-T のデバイスはこの最適化をデフォルトで実行し、このコマンドを必要とせず、またサポートしません。Cisco NX-OS は、デバイス全体に対して、port-channel load-balance コマンドによるポート チャネル上のロードバランシング基準のカスタマイズをサポートします。

LACP

LACP では、最大 4 のインターフェイスを 1 つのポート チャネルに設定できます。

LACP の概要

イーサネットのリンク アグリゲーション制御プロトコル（LACP）は、IEEE 802.1AX および IEEE 802.3ad で定義されています。このプロトコルは、物理ポートをまとめて 1 つの論理チャネルを形成する方法を制御します。

（注） LCAP は、使用する前にイネーブルにする必要があります。デフォルトでは、LACP はディセーブルです。LACP の有効化については、「*LACP* の有効化」のセクションを参照してください。

システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックおよびチェックポイントについては、『*Cisco Nexus® 3550-T* システム管理構成』のセクションを参照してください。

個別リンクを LACP ポート チャネルおよびチャネル グループに組み込み、個別リンクとして機能させることが可能です。

LACP では、最大 4 つのインターフェイスを 1 つのチャネル グループにまとめることができます。

（注） ポート チャネルを削除すると、ソフトウェアは関連付けられたチャネル グループを自動的に削除します。すべてのメンバ インターフェイスはオリジナルの設定に戻ります。

LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

ポートチャネル モード

ポートチャネルの個別インターフェイスは、チャネルモードで設定します。スタティック ポート チャネルを集約プロトコルを使用せずに実行すると、チャネル モードは常に **on** に設定されます。デバイス上で LACP をグローバルにイネーブルにした後、各チャネルの LACP をイネーブルにします。それには、各インターフェイスのチャネル モードを **active** または **passive** に設定します。チャネル グループにリンクを追加すると、LACP チャネル グループの個別リンクにチャネル モードを設定できます。

（注） **active** または **passive** のチャネル モードで、個々のインターフェイスを設定するには、まず、LACP をグローバルにイネーブルにする必要があります。

次の図は、チャネル モードをまとめたものです。

表 *27*: ポート チャネルの個別リンクのチャネル モード

チャネル モード	説明
passive	LACP はこのポート チャネルでイネーブルになっており、ポートはパッシブ ネゴシエーション状態になっています。ポートは受信した LACP パケットに応答しますが、LACP ネゴシエーションは開始しません。
active	LACP はこのポートチャネルでイネーブルになっており、ポートはアクティブ ネゴシエーション状態です。アクティブモードでは、ポートは LACP パケットを送信することによって他のポートとのネゴシエーションを開始します。
on	LACP はこのポート チャネルでディセーブルであり、ポートは非ネゴシエーション状態です。ポートチャネルが **on** 状態であることは、スタティック モードであることを表します。 ポートはポート チャネル メンバーシップの確認またはネゴシエートを行いません。LACP をイネーブルにする前にチャネル モードをアクティブまたはパッシブにしようとすると、デバイス表示はエラー メッセージを表示します。LACP は、**on** 状態のインターフェイスとネゴシエートする場合、LACP パケットを受信しないため、そのインターフェイスと個別のリンクを形成します。つまり、LACP チャネル グループには参加しません。**on** 状態が、デフォルト ポート チャネル モードです。

LACP は、パッシブおよびアクティブ モードの両方でポート間をネゴシエートして、ポート速度やトランキング ステートなどを基準にしてポート チャネルを形成できるかどうかを決定します。パッシブ モードは、リモート システムやパートナーが LACP をサポートするかどうか不明の場合に役に立ちます。

次の例のようにモードに互換性がある場合、ポートの LACP モードが異なれば、2 つのデバイスは LACP ポート チャネルを形成できます。

表 *28 :* チャネルモードの互換性

デバイス 1 > ポート-1	デバイス 2 > ポート-2	結果
アクティブ	アクティブ	ポート チャネルを形成できます。
Active	Passive	ポート チャネルを形成できます。
パッシブ	パッシブ	ネゴシエーションを開始できるポートがないため、ポート チャネルを形成できません。
点灯	アクティブ	LACPが片側でのみ有効になっているため、ポート チャネルを形成できません。
点灯	パッシブ	LACP が有効になっていないため、ポート チャネルを形成できません。

LACP ID パラメータ

ここでは、LACP パラメータについて説明します。

LACP システム プライオリティ

LACP を実行するどのシステムにも LACP システム プライオリティ値があります。このパラメータのデフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。LACP は、このシステム プライオリティと MAC アドレスを組み合わせてシステム ID を生成します。また、システム プライオリティを他のデバイスとのネゴシエーションにも使用します。システム プライオリティ値が大きいほど、プライオリティは低くなります。

（注） LACP システム ID は、LACP システム プライオリティ値と MAC アドレスを組み合わせたものです。

LACP ポート プライオリティ

LACP を使用するように設定されたポートにはそれぞれ LACP ポート プライオリティがあります。デフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。LACP では、ポート プライオリティおよびポート番号によりポート ID が構成されます。

また、互換性のあるポートのうち一部を束ねることができない場合に、どのポートをスタンバイ モードにし、どのポートをアクティブ モードにするかを決定するのに、ポート プライオリティを使用します。LACP では、ポート プライオリティ値が大きいほど、プライオリティは低くなります。指定ポートが、より低い LACP プライオリティを持ち、ホット スタンバイ リンクではなくアクティブ リンクとして選択される可能性が最も高くなるように、ポート プライオリティを設定できます。

LACP 管理キー

LACP は、LACP を使用するように設定されたポートごとに、チャネルグループ番号と同じ管理キー値を自動的に設定します。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。他のポートとともに集約されるポートの機能は、次の要因によって決まります。

- ポートの物理特性。データ レートやデュプレックス性能などです。
- ユーザが作成した設定に関する制約事項

LACP マーカー レスポンダ

ポート チャネルを使用すればデータ トラフィックを動的に再配布できます。この再配布により、リンクが削除または追加されたり、ロード バランシング スキームが変更されることもあります。トラフィック フローの途中でトラフィックが再配布されると、フレームの秩序が乱れる可能性があります。

LACP は Marker Protocol を使って、再配布によってフレームが重複したり順番が入れ替わらないようにします。Marker Protocol は、所定のトラフィック フローのすべてのフレームがリモートエンドで正しく受信すると検出します。LACP はポート チャネル リンクごとに Marker PDUS を送信します。リモート システムは、Marker PDU よりも先にこのリンクで受信されたすべてのフレームを受信すると、Marker PDU に応答します。リモート システムは次に Marker Responder を送信します。ポート チャネルのすべてのメンバ リンクの Marker Responder を受信したローカル システムは、トラフィック フローのフレームを正しい順序で再配分します。ソフトウェアは Marker Responder だけをサポートします。

LACP がイネーブルのポート チャネルとスタティック ポート チャネルの相違点

次の表に、LACP がイネーブルのポート チャネルとスタティック ポート チャネルの主な相違点を示します。

表 *29 : LACP* がイネーブルのポート チャネルとスタティック ポート チャネル

構成	LACP がイネーブルのポート チャネル	スタティック ポート チャネル
適用されるプロトコル	グローバルにイネーブル	N/A
リンクのチャネル モード	次のいずれか • Active • Passive	On だけ

構成	LACP がイネーブルのポート チャネル	スタティック ポート チャネル
チャネルを構成する最大リンク数	4	4

LACP 互換性の拡張

Cisco Nexus 3550-T のデバイスが非 Nexus ピアに接続されている場合、そのグレースフル フェールオーバーのデフォルトが、無効にされたポートがダウンになるための時間を遅らせる可能性があります。また、ピアからのトラフィックを喪失する原因にもなります。これらの条件に対処するため、 **lacp graceful-convergence** コマンドが追加されました。

デフォルトで、ピアから LACP PDU を受信しない場合、ポートは一時停止状態に設定されます。 **lacp suspend-individual** は Cisco Nexus® 3550-T スイッチではデフォルト構成です。このコマンドは、LACP PDU を受信しない場合、ポートを中断状態にします。場合によっては、この機能は誤設定によって作成されるループの防止に役立ちますが、サーバが LACP にポートを論理的アップにするように要求するため、サーバの起動に失敗する原因になることがあります。 **no lacp suspend-individual** コマンドを使用して、ポートを個別の状態に設定できます。個々に設定されているポートは、ポート設定に基づいて個々のポートの属性を取得します。

LACP ポートチャネルは、サーバとスイッチを接続すると、リンクの迅速なバンドルのために LACP PDU を交換します。ただし、PDU が受信されない場合は、リンクが中断状態になります。

delayed LACP 機能により、LACP PDU の受信前に 1 つのポートチャネル メンバー（遅延 LACP ポート）がまず通常のポートチャネルのメンバーとしてアップできます。このメンバーが LACP モードで接続した後に、他のメンバー（補助 LACP ポート）がアップします。これにより、PDU が受信されない場合にリンクが中断状態になることが回避されます。

ポート チャネルのどのポートが最初に起動するかは、ポートのポート プライオリティ値によって決まります。プライオリティ値が最も低いポート チャネルのメンバー リンクが、LACP 遅延ポートとして最初に起動します。リンクの動作ステータスに関係なく、LACP ポートに設定されたプライオリティが使用され、遅延 lacp ポートが選択されます。

この機能は、レイヤ 2 ポート チャネル、トランク モード スパニング ツリーをサポートします。

- 同じポートチャネルで **no lacp suspend-individuallacp mode delay** を使用することは、非 lacp 遅延ポートを個別の状態にする可能性があるため、推奨されません。ベスト プラクティスとして、これら 2 つの設定を組み合わせないようにする必要があります。
- レイヤ 3 ポート チャネルではサポートされません。

LACP ポート チャネルの最小リンクおよび MaxBundle

ポートチャネルは、同様のポートを集約し、単一の管理可能なインターフェイスの帯域幅を増加させます。

最小リンクおよびmaxbundle機能の導入により、LACP ポート チャネル動作を改善し、単一の管理可能なインターフェイスの帯域幅を増加させます。

LACP ポート チャネルの最小リンク機能は次の処理を実行します。

- LACP ポート チャネルにリンク アップし、バンドルする必要があるポートの最小数を設定します。
- 低帯域幅の LACP ポート チャネルがアクティブにならないようにします。
- 必要な最小帯域幅を提供するアクティブ メンバー ポートが少数の場合、LACPポートチャネルが非アクティブになります。

LACP MaxBundle は、LACP ポート チャネルで許可されるバンドル ポートの最大数を定義します。

LACP MaxBundle 機能では、次の処理が行われます。

- LACP ポート チャネルのバンドル ポートの上限数を定義します。
- バンドル ポートがより少ない場合のホット スタンバイ ポートを可能にします。（たとえば、4 つのポートを含む LACP ポート チャネルにおいて、ホット スタンバイ ポートとしてそれらのポートの 2 つを指定できます）。

（注） 最小リンクおよびmaxbundle機能は、LACPポートチャネルだけで動作します。ただし、デバイスでは非 LACP ポート チャネルでこの機能を設定できますが、機能は動作しません。

LACP 高速タイマー

LACP タイマー レートを変更することにより、LACP タイムアウトの時間を変更することができます。lacp rate コマンドを使用すれば、LACP がサポートされているインターフェイスに LACP制御パケットを送信する際のレートを設定できます。タイムアウト レートは、デフォルトのレート（30 秒）から高速レート（1 秒）に変更することができます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。LACP 高速タイマー レートを構成するには、「*LACP* 高速タイマー レートの構成」のセクションを参照してください。

高可用性

ポート チャネルは、複数のポートのトラフィックをロード バランシングすることでハイ アベイラビリティを実現します。物理ポートが故障した場合、ポートチャネルのメンバがアクティブであればポートチャネルは引き続き動作します。モジュール間の設定が共通しているため、異なるモジュールのポートをバンドルして、モジュール故障時にも動作するポートチャネルを作成できます。

ポート チャネルは、ステートフル再起動とステートレス再起動をサポートします。

動作しているポート数が設定された最小リンク数を下回った場合、ポートチャネルはダウンします。

（注） 高可用性機能の詳細については、『*Cisco Nexus* 高可用性および冗長性ガイド』を参照してください。

ポート チャネリングの前提条件

ポート チャネリングには次の前提条件があります。

- デバイスにログインしていること。
- シングル ポート チャネルのすべてのポートは、レイヤ 2 またはレイヤ 3 ポートであること。
- シングル ポート チャネルのすべてのポートが、互換性の要件を満たしていること。互換性の要件の詳細については、互換性要件 （550ページ） セクションを参照してください。

ガイドラインと制約事項

ポート チャネル設定時のガイドラインおよび制約事項は、次のとおりです。

- キーワードが付いている**show**コマンド**internal**はサポートされていません。
- LACP ポートチャネルの最小リンクおよび maxbundle 機能は、ホスト インターフェイス ポート チャネルではサポートされていません。
- この機能を使用する前に LACP をイネーブルにする必要があります。
- デバイスに複数のポート チャネルを設定できます。
- 共有および専用ポートは同じポート チャネルに設定できません（共有ポートおよび専用ポートについては、「基本インターフェイス パラメータの構成」のセクションを参照してください。）

- レイヤ 2 ポート チャネルでは、ポートに互換性が設定されていれば、STP ポート パス コストが異なる場合でもポート チャネルを形成できます。互換性の要件の詳細については、互換性要件 （550 ページ） セクションを参照してください。
-
- STP では、ポートチャネルのコストはポート メンバーの集約帯域幅に基づきます。
- ポートチャネルを設定した場合、ポートチャネルインターフェイスに適用した設定はポートチャネル メンバ ポートに影響を与えます。メンバ ポートに適用した設定は、設定を適用したメンバ ポートにだけ影響します。
- LACP は半二重モードをサポートしません。LACP ポート チャネルの半二重ポートは中断ステートになります。
- Cisco Nexus 3550-T スイッチは、システム全体で最大 12 個のポート チャネルをサポートできます。

デフォルト設定

次の表に、ポートチャネル パラメータのデフォルト設定を示します。

表 *30*: デフォルト ポート チャネル パラメータ

パラメータ	デフォルト
ポート チャネル	管理アップ
レイヤ 3 インターフェイスのロード バランシング方式	送信元および宛先 IP アドレス
レイヤ 2 インターフェイスのロード バランシング方式	送信元および宛先 MAC アドレス
モジュールごとのロード バランシング	ディセーブル
LACP	ディセーブル
チャンネル モード	on
LACP システム プライオリティ	32768
LACP ポート プライオリティ	32768
LACP 用最少リンク数	1
Maxbundle	4

ポート チャネルの設定

（注） ポート チャネル インターフェイスに IPv4 アドレスを構成する手順については、「レイヤ *3* インターフェイスの構成」の章を参照してください。

（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。

ポート チャネルの作成

チャネル グループを作成する前に、ポート チャネルを作成します。関連するチャネル グループは自動的に作成されます。

（注） ポート チャネルがチャネル グループの前に作成されると、ポート チャネルは、メンバー インターフェイスが設定されるインターフェイス属性のすべてを使用して設定される必要があります。**switchport mode trunk** {*allowed vlan vlan-id* | *native vlan-id*} コマンドを使用して、 メンバーを設定します。

これは、チャネル グループのメンバがレイヤ 2 ポート（switchport）およびトランク（switchport mode trunk）の場合にのみ必要です。

（注） **no interface port-channel** コマンドを使用して、ポート チャネルを削除し、関連するチャネル グループを削除します。

コマンド	目的
no interface port-channel *channel-number* 例： `switch(config)# no interface port-channel 1`	ポートチャネルを削除し、関連するチャネル グループを削除します。

始める前に

LACP ベースのポート チャネルにする場合は LACP をイネーブルにします。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *channel-number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)`
		設定するポート チャネル 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。範囲は 1 ～ 4096 です。Cisco NX-OS ソフトウェアは、チャネル グループがない場合はそれを自動的に作成します。

ステップ 3	**show port-channel summary** 例： `switch(config-router)# show port-channel summary`	（任意）ポート チャネルに関する情報を表示します。

ステップ 4	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

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。

例

次の例は、ポート チャネルの作成方法を示しています。

```
switch# configure terminal
switch (config)# interface port-channel 1
```

ポート チャネルを削除したときのインターフェイス構成の変化について詳しくは、互換性要件 （550 ページ） のセクションを参照してください。

レイヤ 2 ポートをポート チャネルに追加

新しいチャネル グループまたはすでにレイヤ2ポートを含むチャネル グループにレイヤ2ポートを追加できます。ポート チャネルがない場合は、このチャネル グループに関連付けられたポート チャネルが作成されます。

（注） **no channel-group** コマンドを使用して、チャネル グループからポートを削除します。

コマンド	目的
no channel-group 例： `switch(config)# no channel-group`	チャネル グループからポートを削除します。

始める前に

LACP ベースのポート チャネルにする場合は LACP をイネーブルにします。

すべてのレイヤ 2 メンバ ポートは、全二重モードで同じ速度で実行されている必要があります。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加する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	**switchport** 例： `switch(config)# switchport`	インターフェイスをレイヤ 2 アクセス ポートとして設定します。
ステップ 4	**switchport mode trunk** 例： `switch(config)# switchport mode trunk`	（任意）インターフェイスをレイヤ2 トランク ポートとして設定します。

	コマンドまたはアクション	目的

ステップ 5	**switchport trunk** {**allowed vlan** *vlan-id* | **native** *vlan-id*}
	例：
	`switch(config)# switchport trunk native 3`
	`switch(config-if)#`
		（任意）レイヤ 2 トランク ポートに必要なパラメータを設定します。

ステップ 6	**channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}] 例： • `switch(config-if)# channel-group 5` • `switch(config-if)# channel-group 5 force`	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 4096 です。ポート チャネルがない場合は、このチャネル グループに関連付けられたポート チャネルが作成されます。すべてのスタティック ポート チャネル インターフェイスは、**on** モードに設定されます。すべての LACP 対応ポート チャネルインターフェイスを **active** または **passive** に設定する必要があります。デフォルト モードは **on** です。 （任意）一部の設定に互換性がないインターフェイスをチャネルに追加します。強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。
ステップ 7	**show interface** *type slot/port* 例： `switch# show interface port channel 5`	（任意）インターフェイスの内容を表示します。

ステップ 8	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 9	**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。

例

次に、レイヤ 2 イーサネット インターフェイス 1/4 をチャネル グループ 5 に追加する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# switchport
switch(config-if)# channel-group 5
```

レイヤ 3 ポートをポート チャネルに追加

新しいチャネル グループまたはすでにレイヤ 3 ポートが設定されているチャネル グループにレイヤ 3 ポートを追加できます。ポート チャネルがない場合は、このチャネル グループに関連付けられたポート チャネルが作成されます。

追加するレイヤ 3 ポートに IP アドレスが設定されている場合、ポートがポート チャネルに追加される前にその IP アドレスは削除されます。レイヤ 3 ポート チャネルを作成したら、ポート チャネル インターフェイスに IP アドレスを割り当てることができます。

（注） **no channel-group** コマンドを使用して、チャネル グループからポートを削除します。チャネル グループから削除されたポートは元の設定に戻ります。このポートの IP アドレスを再設定する必要があります。

コマンド	目的
no channel-group 例： `switch(config)# no channel-group`	チャネル グループからポートを削除します。

始める前に

LACP ベースのポート チャネルにする場合は LACP をイネーブルにします。

レイヤ 3 インターフェイスに設定した IP アドレスがあれば、この IP アドレスを削除します。

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的

ステップ 2	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加する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	**no switchport** 例： `switch(config-if)# no switchport`	インターフェイスをレイヤ 3 ポートとして設定します。
ステップ 4	**channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}] 例： • `switch(config-if)# channel-group 5` • `switch(config-if)# channel-group 5 force`	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 4096 です。ポート チャネルがない場合は、このチャネル グループに関連付けられたポート チャネルが作成されます。 （任意）一部の設定に互換性がないインターフェイスをチャネルに追加します。強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。
ステップ 5	**show interface** *type slot/port* 例： `switch# show interface ethernet 1/4`	（任意）インターフェイスの内容を表示します。

ステップ 6	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、レイヤ 3 イーサネット インターフェイス 1/5 を on モードのチャネル グループ 6 に追加する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# switchport
switch(config-if)# channel-group 6
```

次の例では、レイヤ3ポートチャネルインターフェイスを作成し、IPアドレスを割り当てる方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 4
switch(config-if)# ip address 192.0.2.1/8
```

情報目的としての帯域幅および遅延の設定

ポートチャネルの帯域幅は、チャネル内のアクティブリンクの合計数によって決定されます。

情報目的でポート チャネル インターフェイスに帯域幅および遅延を設定します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *channel-number*
	例：
	`switch(config)# interface port-channel 2`
	`switch(config-if)#`
		設定するポート チャネル 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	**bandwidth** *value*
	例：
	`switch(config-if)# bandwidth 60000000`
	`switch(config-if)#`
		情報目的で使用される帯域幅を指定します。有効な範囲は 1 ～ 3,200,000,000 kbs です。デフォルト値はチャネル グループのアクティブ インターフェイスの合計によって異なります。

ステップ 4	**delay** *value*
	例：
	`switch(config-if)# delay 10000`
	`switch(config-if)#`
		情報目的で使用されるスループット遅延を指定します。範囲は、1 ～ 16,777,215（10 マイクロ秒単位）です。デフォルト値は 10 マイクロ秒です。

	コマンドまたはアクション	目的

ステップ 5	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 6	**show interface port-channel** *channel-number* 例： `switch# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、ポート チャネル 5 の帯域幅および遅延の情報パラメータを設定する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 5
switch(config-if)# bandwidth 60000000
switch(config-if)# delay 10000
switch(config-if)#
```

ポート チャネル インターフェイスのシャットダウンと再起動

ポート チャネル インターフェイスをシャットダウンして再起動できます。ポート チャネル インターフェイスをシャットダウンすると、トラフィックは通過しなくなりインターフェイスは管理ダウンします。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *channel-number* 例：	設定するポート チャネル インターフェイスを指定し、インターフェイス コン

	コマンドまたはアクション	目的
	`switch(config)# interface port-channel 2` `switch(config-if)#`	フィギュレーション モードを開始します。

ステップ 3	**shutdown**
	例：
	`switch(config-if)# shutdown`
	`switch(config-if)#`
		インターフェイスをシャットダウンします。トラフィックは通過せず、インターフェイスは管理ダウン状態になります。デフォルトはシャットダウンなしです。
		（注） インターフェイスを開くには、 **no shutdown** コマンドを使用します。
		インターフェイスは管理アップとなります。操作上の問題がなければ、トラフィックが通過します。デフォルトはシャットダウンなしです。

ステップ 4	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 5	**show interface port-channel** *channel-number* 例： `switch(config-router)# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。

ステップ 6	**no shutdown**
	例：
	`switch# configure terminal`
	`switch(config)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、ポート チャネル 2 のインターフェイスをアップする例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# no shutdown
```

ポート チャネルの説明の設定

ポート チャネルの説明を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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 port-channel** *channel-number*
	例：
	`switch(config)# interface port-channel 2`
	`switch(config-if)#`
		設定するポート チャネル 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	**description**
	例：
	`switch(config-if)# description engineering`
	`switch(config-if)#`
		ポート チャネル インターフェイスに説明を追加できます。説明に 80 文字まで使用できます。デフォルトでは、説明は表示されません。このパラメータを設定してから、出力に説明を表示する必要があります。

ステップ 4	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 5	**show interface port-channel** *channel-number* 例： `switch# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**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。

例

次に、ポート チャネル 2 に説明を追加する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# description engineering
```

ポート チャネル インターフェイスへの速度とデュプレックスの設定

ポート チャネル インターフェイスに速度とデュプレックスを設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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 port-channel** *channel-number*
	例：
	`switch(config)# interface port-channel 2`
	`switch(config-if)#`
		設定するポート チャネル 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	**speed** {**auto**}
	例：
	`switch(config-if)# speed auto`
	`switch(config-if)#`
		ポートチャネル インターフェイスの速度を設定します。デフォルトの自動ネゴシエーションは自動です。

ステップ 4	**duplex** {**auto** | **full** | **half**}
	例：
	`switch(config-if)# speed auto`
	`switch(config-if)#`
		ポート チャネル インターフェイスのデュプレックスを設定します。デフォルトの自動ネゴシエーションは自動です。

	コマンドまたはアクション	目的

ステップ 5	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。

ステップ 6	**show interface port-channel** *channel-number* 例： `switch# show interface port-channel 2`	（任意）指定したポート チャネルのインターフェイス情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、ポート チャネル 2 に 100 Mb/s を設定する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# speed 100
```

ポート チャネルを使ったロード バランシングの設定

VDC アソシエーションにかかわらず、ポート チャネルのロードバランシング アルゴリズムを設定し、デバイス全体または 1 つのモジュールだけに適用できます。

（注） デフォルトのロードバランシング アルゴリズムである、非 IP トラフィック用の source-dest-mac、および IP トラフィック用の source-dest-ip を復元するには、**no port-channel load-balance** コマンドを使用します。

コマンド	目的
no port-channel load-balance 例： `switch(config)# no port-channel load-balance`	デフォルトのロードバランシング アルゴリズムを復元します。

始める前に

LACP ベースのポート チャネルにする場合は LACP をイネーブルにします。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**port-channel load-balance** *method* {**dst ip** | **dst ip-l4port** | **dst ip-l4port-vlan** | **dst ip-vlan** | **dst l4port** | **dst mac** | **src ip** | **src ip-l4port** | **src ip-l4port-vlan** | **src ip-vlan** | **src l4port** | **src mac** | **src-dst ip** | **src-dst ip-l4port** [**symmetric**] | **src-dst ip-l4port-vlan** | **src-dst ip-vlan** | **src-dst l4port** | **src-dst mac**} [{*all*}] [**rotate** *rotate*] 例： • `switch(config)# port-channel load-balance src-dst mac` `switch(config)#` • `switch(config)# no port-channel load-balance src-dst mac` `switch(config)#`	デバイスのロード バランシング アルゴリズムを指定します。指定可能なアルゴリズムはデバイスによって異なります。レイヤ 3 のデフォルトは IPv4 で **src-dst ip-l4port** で、非 IP のデフォルトは **src-dst mac** です。 （注） 次のロードバランシング アルゴリズムがシンメトリック ハッシングをサポートします。 • src-dst ip • src-dst ip-l4port
ステップ 3	**show port-channel load-balance** 例： `switch(config-router)# show port-channel load-balance`	（任意）ポート チャネル ロード バランシング アルゴリズムを表示します。
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。

LACP のイネーブル化

LACP はデフォルトではディセーブルです。LACP の設定を開始するには、LACP をイネーブルにする必要があります。LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

LACP は、LAN ポート グループの機能を動的に学習し、残りの LAN ポートに通知します。LACP は、正確に一致しているイーサネット リンクを識別すると、リンクを 1 つのポート チャネルとしてまとめます。次に、ポート チャネルは単一ブリッジ ポートとしてスパニング ツリーに追加されます。

LACP を設定する手順は次のとおりです。

- LACP をグローバルにイネーブルにするには、**feature lacp** コマンドを使用します。
- LACP をイネーブルにした同一ポート チャネルでは、異なるインターフェイスに異なるモードを使用できます。指定したチャネル グループに割り当てられた唯一のインターフェイスである場合に限り、モードを **active** と **passive** で切り替えることができます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**feature lacp** 例： `switch(config)# feature lacp`	デバイスの LACP をイネーブルにします。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、LACP をイネーブルにする例を示します。

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

LACP ポート チャネル ポート モードの設定

LACP をイネーブルにしたら、LACP ポート チャネルのそれぞれのリンクのチャネル モードを **active** または **passive** に設定できます。このチャネル コンフィギュレーション モードを使用すると、リンクは LACP で動作可能になります。

関連する集約プロトコルを使用せずにポート チャネルを設定すると、リンク両端のすべてのインターフェイスは **on** チャネル モードを維持します。

手順

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

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加する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	**channel-group** *number* **mode** {**active** | **on** | **passive**} 例： `switch(config-if)# channel-group 5 mode active`	ポート チャネルのリンクのポート モードを指定します。LACP をイネーブルにしたら、各リンクまたはチャネル全体を active または passive に設定します。 関連する集約プロトコルを使用せずにポート チャネルを実行する場合、ポートチャネル モードは常に on です。 デフォルト ポート チャネル モードは **on** です。
ステップ 4	**show port-channel summary** 例： `switch(config-if)# show port-channel summary`	（任意）ポート チャネルの概要を表示します。
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。

例

次に、LACP をイネーブルにしたインターフェイスを、チャネル グループ 5 のイーサネット インターフェイス 1/4 のアクティブ ポートチャネル モードに設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# channel-group 5 mode active
```

LACP ポート チャネル最少リンク数の設定

LACP の最小リンク機能を設定できます。最小リンクと maxbundles は LACP でのみ動作します。ただし、非 LACP ポート チャネルに対してこれらの機能の CLI コマンドを入力できますが、これらのコマンドは動作不能です。

（注） **no lacp min-links** コマンドを使用して、デフォルト ポートチャネル最小リンクの設定を復元します。

コマンド	目的
no lacp min-links 例： `switch(config)# no lacp min-links`	デフォルトのポートチャネル最小リンク設定を復元します。

始める前に

正しいポートチャネル インターフェイスであることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	例：
	`switch(config)# interface port-channel 3`
	`switch(config-if)#`
		設定する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	**lacp min-links** *number* 例： `switch(config-if)# lacp min-links 3`	ポート チャネル インターフェイスを指定して、最小リンクの数を設定します。指定できる範囲は 1 ～ 4 です。
ステップ 4	**show running-config interface port-channel** *number* 例： `switch(config-if)# show running-config interface port-channel 3`	（任意）ポート チャネル最小リンク設定を表示します。

例

次に、アップ/アクティブにするポート チャネルに関して、アップ/アクティブにするポート チャネル メンバー インターフェイスの最小数を設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 3
switch(config-if)# lacp min-links 3
```

LACP ポートチャネル MaxBundle の設定

LACP の maxbundle 機能を設定できます。最小リンクと maxbundles は LACP でのみ動作します。ただし、非 LACP ポート チャネルに対してこれらの機能の CLI コマンドを入力できますが、これらのコマンドは動作不能です。

（注） デフォルトのポートチャネル max-bundle 設定を復元するには、**no lacp max-bundle** コマンドを使用します。

コマンド	目的
no lacp max-bundle 例： `switch(config)# no lacp max-bundle`	デフォルトのポートチャネル max-bundle 設定を復元します。

始める前に

正しいポート チャネル インターフェイスを使用していることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	例：
	`switch(config)# interface port-channel 3`
	`switch(config-if)#`
		設定する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	**lacp max-bundle** *number* 例： `switch(config-if)# lacp max-bundle`	max-bundle を設定するポートチャネル インターフェイスを指定します。 ポート チャネルの max-bundle のデフォルト値は 4 です。指定できる範囲は 1 ～ 4 です。

	コマンドまたはアクション	目的
		（注） デフォルト値は 4 ですが、ポート チャネルのアクティブ メンバ数は、pc_max_links_config およびポートチャネルで許可されている pc_max_active_members の最小数です。
ステップ 4	**show running-config interface port-channel** *number* 例： `switch(config-if)# show running-config interface port-channel 3`	（任意）ポートチャネル max-bundle 設定を表示します。

例

次に、ポート チャネル インターフェイスの max-bundle を設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 3
switch(config-if)# lacp max-bundle 3
```

LACP 高速タイマー レートの設定

LACP タイマー レートを変更することにより、LACP タイムアウトの時間を変更することができます。**lacp rate** コマンドを使用し、コマンドを使用すれば、LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートを設定できます。タイムアウトレートは、デフォルトのレート（30秒）から高速レート（1秒）に変更することができます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。

（注） LACP タイマー レートの変更は推奨しません。HA および SSO は、LACP 高速レートのタイマーが設定されている場合はサポートされません。

始める前に

LACP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		設定する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	**lacp rate fast** 例： `switch(config-if)# lacp rate fast`	LACP がサポートされているインターフェイスにLACP制御パケットを送信する際のレートとして高速レート（1秒）を設定します。 タイムアウト レートをデフォルトにリセットするには、コマンドの **no** 形式を使用します。

例

次の例は、イーサネット インターフェイス 1/4 に対して LACP 高速レートを設定する方法を示したものです。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# lacp rate fast
```

次の例は、イーサネット インターフェイス 1/4 の LACP レートをデフォルトのレート（30 秒）に戻す方法を示したものです。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# no lacp rate fast
```

LACP システム プライオリティの設定

LACP システム ID は、LACP システム プライオリティ値と MAC アドレスを組み合わせたものです。

始める前に

LACP をイネーブルにします。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**lacp system-priority** *priority* 例： `switch(config)# lacp system-priority 40000`	LACP で使用するシステム プライオリティを設定します。指定できる範囲は1～65535で、値が大きいほどプライオリティは低くなります。デフォルト値は32768 です。
ステップ 3	**show lacp system-identifier** 例： `switch(config-if)# show lacp system-identifier`	（任意）LACP システム識別子を表示します。
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。

例

次に、LACP システム プライオリティを 2500 に設定する例を示します。

```
switch# configure terminal
switch(config)# lacp system-priority 2500
```

LACP ポート プライオリティの設定

LACP をイネーブルにしたら、ポート プライオリティの LACP ポート チャネルにそれぞれのリンクを設定できます。

始める前に

LACP をイネーブルにします。

手順

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

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**interface** *type slot/port*
	例：
	`switch(config)# interface ethernet 1/4`
	`switch(config-if)#`
		チャネル グループに追加する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	**lacp port-priority** *priority* 例： `switch(config-if)# lacp port-priority 40000`	LACP で使用するポート プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。
ステップ 4	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、イーサネット インターフェイス 1/4 の LACP ポート プライオリティを 40000 に設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# lacp port-priority 40000
```

LACP システム MAC およびロールの設定

プロトコル交換用の LACP で使用される MAC アドレスとオプションのロールを設定できます。デフォルトでは、ロールはプライマリです。

この手順は、Cisco Nexus 3550-T スイッチでサポートされています。

始める前に

LACP を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル 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	**lacp system-mac** *mac-address* **role** *role-value*
	例：
	`switch(config)# lacp system-mac 000a.000b.000c role primary`
	`switch(config)# lacp system-mac 000a.000b.000c role secondary`
		LACP プロトコル交換で使用する MAC アドレスを指定します。ロールはオプションです。プライマリがデフォルトです。

ステップ 3	（任意） **show lacp system-identifier** 例： `switch(config)# show lacp system-identifier`	設定されている MAC アドレスを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、スイッチのロールをプライマリとして設定する例を示します。

```
Switch1# sh lacp system-identifier
32768,0-b-0-b-0-b
Switch1# sh run  | grep lacp
feature lacp
lacp system-mac 000b.000b.000b role primary
```

セカンダリとしてスイッチのロールを設定する例を示します。

```
Switch2# sh lacp system-identifier
32768,0-b-0-b-0-b
Switch2# sh run | grep lacp
feature lacp
lacp system-mac 000b.000b.000b role secondary
```

LACP グレースフル コンバージェンスのディセーブル化

デフォルトで、LACP グレースフル コンバージェンスはイネーブルになっています。あるデバイスとの LACP 相互運用性をサポートする必要がある場合、コンバージェンスをディセーブルにできます。そのデバイスとは、グレースフル フェールオーバーのデフォルトが、ディセーブルにされたポートがダウンになるための時間を遅らせる可能性がある、または、ピアからのトラフィックを喪失する原因にもなるデバイスです。ダウンストリーム アクセス スイッチが Cisco Nexus デバイスでない場合は、LACP グレースフル コンバージェンス オプションをディセーブルにします。

（注） このコマンドを使用する前に、ポート チャネルが管理ダウン状態である必要があります。

始める前に

LACP をイネーブルにします。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)#`
		設定するポート チャネル 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	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**no lacp graceful-convergence** 例： `switch(config-if)# no lacp graceful-convergence`	ポート チャネルの LACP グレースフル コンバージェンスをディセーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
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。

例

次に、ポート チャネルの LACP グレースフル コンバージェンスをディセーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# no lacp graceful-convergence
switch(config-if)# no shutdown
```

LACP グレースフル コンバージェンスの再イネーブル化

デフォルトの LACP グレースフル コンバージェンスが再度必要になった場合、コンバージェンスを再度イネーブルにできます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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 port-channel** *number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)#`
		設定するポート チャネル 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	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**lacp graceful-convergence** 例： `switch(config-if)# lacp graceful-convergence`	ポート チャネルの LACP グレースフル コンバージェンスをイネーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
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。

例

次に、ポートチャネルのLACPグレースフル コンバージェンスをイネーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# lacp graceful-convergence
switch(config-if)# no shutdown
```

LACP の個別一時停止のディセーブル化

ポートがピアから LACP PDU を受信しない場合、LACP はポートを中断ステートに設定します。このプロセスは、サーバがLACPにポートを論理的アップにするように要求するときに、サーバの起動に失敗する原因になることがあります。

（注） **lacp suspend-individual** のみを入力する必要がありますエッジポートのコマンド。このコマンドを使用する前に、ポート チャネルが管理上のダウン状態である必要があります。

始める前に

LACP をイネーブルにします。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface port-channel** *number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)#`
		設定するポート チャネル 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	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。
ステップ 4	**no lacp suspend-individual** 例：	ポート チャネルで LACP 個別ポートの一時停止動作をディセーブルにします。

	コマンドまたはアクション	目的
	`switch(config-if)# no lacp suspend-individual`	
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
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。

例

次に、ポート チャネルで LACP 個別ポートの一時停止をディセーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# no lacp suspend-individual
switch(config-if)# no shutdown
```

LACP の個別一時停止の再イネーブル化

デフォルトの LACP 個別ポートの一時停止を再度イネーブルにできます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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 port-channel** *number*
	例：
	`switch(config)# interface port-channel 1`
	`switch(config-if)#`
		設定するポート チャネル 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	**shutdown** 例： `switch(config-if) shutdown`	ポート チャネルを管理シャットダウンします。

	コマンドまたはアクション	目的
ステップ 4	**lacp suspend-individual** 例： `switch(config-if)# lacp suspend-individual`	ポート チャネルで LACP 個別ポートの一時停止動作をイネーブルにします。
ステップ 5	**no shutdown** 例： `switch(config-if) no shutdown`	ポート チャネルを管理アップします。
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。

例

次に、ポート チャネルで LACP 個別ポートの一時停止を再度イネーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# lacp suspend-individual
switch(config-if)# no shutdown
```

遅延 LACP の設定

遅延 LACP 機能により、LACP PDU の受信前に 1 つのポートチャネル メンバー（遅延 LACP ポート）がまず通常のポート チャネルのメンバーとしてアップできます。遅延 LACP 機能を設定するには、ポートチャネルでコマンドを使用してから、ポートチャネルの 1 つのメンバーポートで LACP ポート プライオリティを設定します。**lacp mode delay**

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *number*	設定するポート チャネル 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	**lacp mode delay**	遅延 LACP を有効化します。

	コマンドまたはアクション	目的
		（注） 遅延 LACP を無効にするには、 **no lacp mode delay** コマンドを使用します。 LACP ポート プライオリティを設定して、遅延LACPの設定を完了します。詳細については、「LACPポートプライオリティの設定」を参照してください。 LACP ポートのプライオリティによって、遅延LACPポートの選択が決まります。プライオリティの数値が最小のポートが選択されます。 遅延LACP機能を設定し、ポートチャネルフラップで有効にすると、遅延LACPポートは通常のポートチャネルのメンバーとして動作し、サーバとスイッチ間でデータを交換できるようになります。最初の LACP PDU を受信すると、遅延LACPポートは通常のポート メンバーからLACPポートメンバーに移行します。 （注） 遅延 LACP ポートの選択は、ポートチャネルがスイッチまたはリモート サーバでフラップするまで完了または有効になりません。

例

次に、遅延 LACP を設定する例を示します。

```
switch# config terminal
switch(config)# interface po 1
switch(config-if)# lacp mode delay


switch# config terminal
switch(config)# interface ethernet 1/1
switch(config-if)# lacp port-priority 1
switch(config-if)# channel-group 1 mode active
```

次に、遅延 LACP をディセーブルにする例を示します。

```
switch# config terminal
```

```
switch(config)# interface po 1
switch(config-if)# no lacp mode delay
```

ポートチャネル設定の確認

ポート チャネル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 interface port-channel *channel-number*	ポートチャネルインターフェイスのステータスを表示します。
show feature	イネーブルにされた機能を表示します。
load- interval {**interval** *seconds* {**1** | **2** | **3**}}	ビットレートとパケットレートの統計情報に対して 3 つの異なるサンプリング間隔を設定します。
show port-channel compatibility-parameters	ポート チャネルに追加するためにメンバー ポート間で同じにするパラメータを表示します。
show port-channel database [**interface port-channel** *channel-number*]	1 つ以上のポート チャネル インターフェイスの集約状態を表示します。
show port-channel load-balance	ポートチャネルで使用するロードバランシングのタイプを表示します。
show port-channel summary	ポートチャネルインターフェイスのサマリーを表示します。
show port-channel traffic	ポート チャネルのトラフィック統計情報を表示します。
show port-channel usage	使用済みおよび未使用のチャネル番号の範囲を表示します。
show lacp {**counters** [**interface port-channel** *channel-number*] | [**interface** *type/slot*] | **neighbor** [**interface port-channel** *channel-number*] | **port-channel** [**interface port-channel** *channel-number*] | **system-identifier**]]}	LACP に関する情報を表示します。
show running-config interface port-channel *channel-number*	ポート チャネルの実行コンフィギュレーションに関する情報を表示します。

ポート チャネル インターフェイス コンフィギュレーションのモニタリング

次のコマンドを使用すると、ポート チャネル インターフェイス構成情報を表示することができます。

コマンド	目的
clear counters interface port-channel *channel-number*	カウンタをクリアします。
clear lacp counters [**interface port-channel** *channel-number*]	LACP カウンタをクリアします。
load- interval {**interval** *seconds* {**1** | **2** | **3**}}	ビットレートとパケットレートの統計情報に対して 3 つの異なるサンプリング間隔を設定します。
show interface counters [**module** *module*]	入力および出力オクテット ユニキャスト パケット、マルチキャスト パケット、ブロードキャスト パケットを表示します。
show interface counters detailed [**all**]	入力パケット、バイト、マルチキャストおよび出力パケット、バイトを表示します。
show interface counters errors [**module** *module*]	エラー パケットの数を表示します。
show lacp counters	LACP の統計情報を表示します。

ポート チャネルの設定例

次に、LACP ポート チャネルを作成し、そのポート チャネルに 2 つのレイヤ 2 インターフェイスを追加する例を示します。

```
switch# configure terminal
switch (config)# feature lacp
switch (config)# interface port-channel 5
switch (config-if)# interface ethernet 1/4
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode active
switch(config-if)# lacp port priority 40000
switch(config-if)# interface ethernet 1/7
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode
```

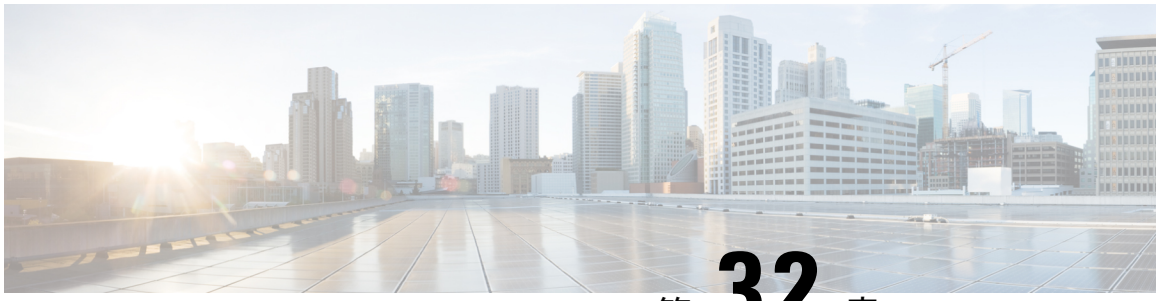
次に、チャネル グループに 2 つのレイヤ 3 インターフェイスを追加する例を示します。Cisco NX-OS ソフトウェアはポート チャネルを自動的に作成します。

```
switch# configure terminal
```

```
switch (config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch (config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch (config)# interface port-channel 6
switch(config-if)# ip address 192.0.2.1/8
```

関連資料

関連項目	マニュアル タイトル
システム管理	「*Cisco Nexus 3550-T NX-OS* システム管理構成」セクション
ライセンス	『*Cisco NX-OS Licensing Guide*』



第 32 章

レイヤ 3 インターフェイスの設定

レイヤ 3 インターフェイスについて

レイヤ 3 インターフェイスは、IPv4 パケットを静的またはダイナミック ルーティング プロトコルを使って別のデバイスに転送します。レイヤ 2 トラフィックの IP ルーティングおよび内部 Virtual Local Area Network（VLAN）ルーティングにはレイヤ 3 インターフェイスが使用できます。

ルーテッド インターフェイス

ポートをレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスとして設定できます。ルーテッド インターフェイスは、IP トラフィックを他のデバイスにルーティングできる物理ポートです。ルーテッド インターフェイスはレイヤ 3 インターフェイスだけで、スパニング ツリー プロトコル（STP）などのレイヤ 2 プロトコルはサポートしません。

すべてのイーサネット ポートは、デフォルトでルーテッド インターフェイスです。CLI セットアップ スクリプトでこのデフォルトの動作を変更できます。

（注） Cisco Nexus® 3550-T スイッチ インターフェイスのデフォルト モードはレイヤ 3 です。

ポートに IP アドレスを割り当て、ルーティングをイネーブルにし、このルーテッド インターフェイスにルーティング プロトコル特性を割り当てることができます。

ルーテッド インターフェイスからレイヤ 3 ポート チャネルも作成できます。ポート チャネルの詳細については、「ポート チャネルの構成」のセクションを参照してください。

ルーテッド インターフェイス は、指数関数的に減少するレート カウンタをサポートします。Cisco NX-OS はこれらの平均カウンタを用いて次の統計情報を追跡します。

- 入力パケット数/秒
- 出力パケット数/秒

（注） レイヤ 3 サブインターフェイスは、Cisco Nexus® 3550-T 10.1(2t) リリースではサポートされていません。

VLAN インターフェイス

VLAN インターフェイス、またはスイッチ仮想インターフェイス（SVI）、は、デバイス上の VLAN を同じデバイス上のレイヤ 3 ルータ エンジンに接続する仮想ルーテッド インターフェイスです。VLAN には 1 つの VLAN インターフェイスだけを関連付けることができますが、VLAN に VLAN インターフェイスを構成する必要があるのは、VLAN 間でルーティングする場合か、または IP ホスト接続する場合だけです。VLAN インターフェイスの作成を有効にすると、Cisco NX-OS によってデフォルト VLAN（VLAN 1）に VLAN インターフェイスが作成され、リモート スイッチ管理が許可されます。

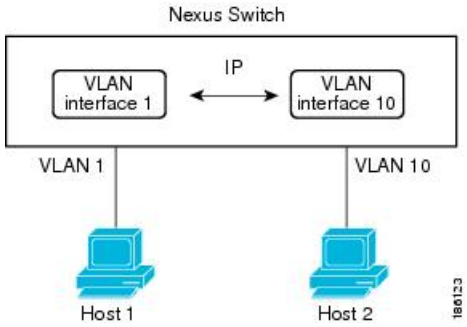
設定の前に VLAN ネットワーク インターフェイス機能をイネーブルにする必要があります。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックおよびチェックポイントについては、「*Cisco Nexus® 3550-T* システム管理構成」のセクションを参照してください。

（注） VLAN 1 の VLAN インターフェイスは削除できません。

VLAN インターフェイスをルーティングするには、トラフィックをルーティングする VLAN ごとに VLAN インターフェイスを作成し、その VLAN インターフェイスに IP アドレスを割り当ててレイヤ 3 内部 VLAN ルーティングを実現します。IP アドレスおよび IP ルーティングの詳細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」セクションを参照してください。

次の図に、デバイス上の 2 つの VLAN に接続されている 2 つのホストを示します。VLAN ごとに VLAN インターフェイスを設定し、VLAN 間の IP ルーティングを使ってホスト 1 とホスト 2 を通信させることができます。VLAN 1 は VLAN インターフェイス 1 のレイヤ 3 で、VLAN 10 は VLAN インターフェイス 10 のレイヤ 3 で通信します。

図 *28 : VLAN* インターフェイスによる *2* つの *VLAN* の接続



（注） Cisco Nexus® 3550-T 10.1(2t) リリースでは、SVI インターフェイスはデフォルトの VRF インスタンスでのみサポートされます。

ループバック インターフェイス

ループバック インターフェイスは、常にアップ状態にある単独のエンドポイントを持つ仮想インターフェイスです。ループバック インターフェイスを通過するパケットはこのインターフェイスでただちに受信されます。ループバック インターフェイスは物理インターフェイスをエミュレートします。0 ～ 1023 の番号のループバック インターフェイスを最大 1024 個の設定できます。

ループバック インターフェイスを使用すると、パフォーマンスの分析、テスト、ローカル通信が実行できます。ループバック インターフェイスは、ルーティング プロトコル セッションの終端アドレスとして設定することができます。ループバックをこのように設定すると、アウトバウンドインターフェイスの一部がダウンしている場合でもルーティングプロトコルセッションはアップしたままです。

レイヤ 3 インターフェイスの前提条件

レイヤ 3 インターフェイスには次の前提条件があります。

- IP アドレッシングおよび基本設定を熟知している。IP アドレッシングの詳細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」のセクションを参照してください。

レイヤ 3 インターフェイスの注意事項および制約事項

レイヤ 3 インターフェイスの設定には次の注意事項と制約事項があります。

- キーワードが付いている **show** コマンドはサポートされていません。 **internal**

- Dynamic Host Configuration Protocol（DHCP）オプションは、***Cisco Nexus 3550-T - 10.1(2t)* リリース** ではサポートされていません。
- レイヤ 3 サブインターフェイスは、***Cisco Nexus 3550-T - 10.1(2t)* リリース** ではサポートされていません。
- SVI インターフェイスは、***Cisco Nexus 3550-T - 10.1(2t)* リリース** のデフォルト VRF インスタンスでのみサポートされます。
- MTU チェックは ***Cisco Nexus 3550-T - 10.1(2t)* リリース** ではサポートされておらず、MTU CLI は有効になりません。ピアリング デバイスが 1518 バイトを超えるパケットを送信すると、コントロール プレーンの隣接関係は形成されません。
- ***Cisco Nexus 3550-T - 10.1(2t)* リリース** のスイッチはカットスルー転送を行います。したがって、MTU チェックは導入されていません。

  ハードウェア バッファリングはジャンボ パケット用に設計されておらず、通常の MTU サイズ 1516 を超えるパケットはサポートされていません。
- ***Cisco Nexus 3550-T - 10.1(2t)* リリース** では、VLAN パケットおよびバイト カウンタはサポートされていません。
- ***Cisco Nexus 3550-T - 10.1(2t)* リリース** リリースは、どのインターフェイスでもバイト カウンタをサポートしていません。これらのカウンタはすべて 0 として表示されます。

（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。

デフォルト設定

次の表に、レイヤ 3 インターフェイス パラメータのデフォルト設定を示します。

表 *31* : レイヤ *3* インターフェイスのデフォルト パラメータ

パラメータ	デフォルト
管理ステート	閉じる

レイヤ 3 インターフェイスの設定

ルーテッド インターフェイスの設定

任意のイーサネット ポートをルーテッド インターフェイスとして設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	**no switchport** 例： `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ3インターフェイスとして設定します。
ステップ 4	[**ip address**] 例： `switch(config-if)# ip address 192.0.2.1/8`	• このインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」のセクションを参照してください。
ステップ 5	**show interfaces** 例： `switch(config-if)# show interfaces ethernet 1/1`	（任意）レイヤ3インターフェイスの統計情報を表示します。

ステップ 6	**no shutdown**
	例：
	`switch#`
	`switch(config-if)# int e1/1`
	`switch(config-if)# no shutdown`
		（任意）ポリシーがハードウェア ポリシーに対応するインターフェイスのエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。

ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

- **medium** コマンドを使用し、 コマンドを使用します。

コマンド	目的
switchport 例： `switch(config-if)# switchport`	インターフェイスをレイヤ 2 インターフェイスとして設定し、このインターフェイス上のレイヤ 3 固有の設定を削除します。

- 次に、ルーテッド インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

インターフェイスのデフォルト設定がルーテッドされます。レイヤ 2 にインターフェイスを設定するには、**switchport** を入力します コマンドを使用します。レイヤ 2 インターフェイスをルーテッド インターフェイスに変更する場合は、**no switchport** コマンドを入力します。

VLAN インターフェイスの設定

VLAN インターフェイスを作成して内部 VLAN ルーティングを行うことができます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**feature interface-vlan** 例： `switch(config)# feature interface-vlan`	VLANインターフェイス モードをイネーブルにします。

ステップ 3	**interface vlan** *number*
	例：
	`switch(config)# interface vlan 10`
	`switch(config-if)#`
		VLANインターフェイスを作成します。number の範囲は 1 ～ 4094 です。

ステップ 4	[**ip address** *ip-address/length*] 例： `switch(config-if)# ip address 192.0.2.1/8`	• この VLAN インターフェイスの IP アドレスを設定します。IP アドレスの詳細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」のセクション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 5	**show interface vlan** *number* 例： `switch(config-if)# show interface vlan 10`	（任意）レイヤ3インターフェイスの統計情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

次に、VLAN インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 10
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

ループバック インターフェイスの設定

ループバック インターフェイスを設定して、常にアップ状態にある仮想インターフェイスを作成できます。

始める前に

ループバック インターフェイスの IP アドレスが、ネットワークの全ルータで一意であることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface loopback** *instance*
	例：
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		ループバック インターフェイスを作成します。範囲は 0 ー 1023 です。

ステップ 3	[**ip address** *ip-address/length*]	• このインターフェイスの IP アドレスを設定します。IP アドレスの詳

	コマンドまたはアクション	目的
	例： `switch(config-if)# ip address 192.0.2.1/8`	細については、「*Cisco Nexus® 3550-T* ユニキャスト ルーティングの構成」のセクションを参照してください。
ステップ 4	**show interface loopback** *instance* 例： `switch(config-if)# show interface loopback 0`	（任意）ループバック インターフェイスの統計情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）この設定の変更を保存します。

例

次に、ループバック インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

インターフェイスでの DHCP クライアントの設定

SVI、管理インターフェイス、または物理イーサネット インターフェイスで DHCP クライアントの IPv4 アドレスを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** | **mgmt** *0* | **vlan** *vlan id*	管理インターフェイスを選択します。
ステップ 3	switch(config-if)# [**no**] [**ip** | **ipv4] address dhcp**	DHCP サーバに IPv4 アドレスを要求します。 取得されたいずれかのアドレスを削除するには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
ステップ 4	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。

例

次に、SVI で DHCP クライアントの IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# ip address dhcp
```

レイヤ 3 インターフェイス設定の確認

レイヤ 3 の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 interface ethernet *slot/port*	レイヤ3インターフェイスの構成情報、ステータス、カウンタ（インバウンドおよびアウトバウンドパケット レートが 5 分間に指数関数的に減少した平均値を含む）を表示します。
show interface ethernet *slot/port* **brief**	レイヤ 3 インターフェイスの動作ステータスを表示します。
show interface ethernet *slot/port* **capabilities**	レイヤ 3 インターフェイスの機能（ポート タイプ、速度、およびデュプレックスを含む）を表示します。
show interface ethernet *slot/port* **description**	レイヤ 3 インターフェイスの説明を表示します。
show interface ethernet *slot/port* **status**	レイヤ3インターフェイスの管理ステータス、ポート モード、速度、およびデュプレックスを表示します。
show interface loopback *number*	ループバック インターフェイスの設定情報、ステータス、カウンタを表示します。
show interface loopback *number* **brief**	ループバック インターフェイスの動作ステータスを表示します。
show interface loopback *number* **description**	ループバック インターフェイスの説明を表示します。

コマンド	目的
show interface loopback *number* **status**	ループバック インターフェイスの管理ステータスおよびプロトコル ステータスを表示します。
show interface vlan *number*	VLAN インターフェイスの設定情報、ステータス、カウンタを表示します。
show interface vlan *number* **brief**	VLAN インターフェイスの動作ステータスを表示します。
show interface vlan *number* **description**	VLANインターフェイスの説明を表示します。
show interface vlan *number* **status**	VLAN インターフェイスの管理ステータスおよびプロトコル ステータスを表示します。

レイヤ 3 インターフェイスのモニタリング

レイヤ 3 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
load- interval {**interval** *seconds* {**1** | **2** | **3**}}	Cisco Nexus® 3550-T デバイスは、パケットレートの統計に 3 種類のサンプリング インターバルを設定します。 VLAN ネットワーク インターフェイスでの範囲は 60 ～ 300 秒であり、レイヤ インターフェイスでの範囲は 30 ～ 300 秒です。
show interface ethernet *slot/port* **counters**	レイヤ 3 インターフェイスの統計情報を表示します（ユニキャスト、マルチキャスト、ブロードキャスト）。
show interface ethernet *slot/port* **counters brief**	レイヤ 3 インターフェイスの入力および出力カウンタを表示します。
show interface ethernet errors *slot/port* **detailed** [**all**]	レイヤ 3 インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイト カウンタ（エラーを含む）をすべて含めることができます。
show interface ethernet errors *slot/port* **counters errors**	レイヤ 3 インターフェイスの入力および出力エラーを表示します。

コマンド	目的
show interface ethernet errors *slot/port* **counters snmp**	SNMP MIB から報告されたレイヤ 3 インターフェイス カウンタを表示します。
show interface loopback *number* **counters**	ループバック インターフェイスの入力および出力カウンタ（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface loopback *number* **detailed** [**all**]	ループバック インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイト カウンタ（エラーを含む）をすべて含めることができます。
show interface loopback *number* **counters errors**	ループバック インターフェイスの入力および出力エラーを表示します。

レイヤ 3 インターフェイスの設定例

次に、イーサネット サブインターフェイスを設定する例を示します。

```
interface ethernet 1/1.10
description Layer 3
ip address 192.0.2.1/8
```

次に、ループバック インターフェイスを設定する例を示します。

```
interface loopback 3
ip address 192.0.2.2/32
```

関連資料

関連資料	マニュアル タイトル
IP	「*Cisco Nexus® 3550-T* ユニキャスト ルーティング構成」セクション
VLAN	「*Cisco Nexus® 3550-T* レイヤ *2* スイッチング構成」セクション

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

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