Cisco Catalyst 1300 スイッチ シリーズ CLI ガイド

初版：2023 年 1 月 10 日

最終更新：2023 年 7 月 11 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/

はじめに

この章は、次の項で構成されています。

- 概要 （2 ページ）
- ユーザ特権レベル （3 ページ）
- CLI コマンド モード （5 ページ）
- デバッグアクセス用のインターフェイス （8 ページ）
- CLI のアクセス （9 ページ）
- CLI コマンドの表記法 （11 ページ）
- 機能の編集 （12 ページ）
- インターフェイス命名規則 （15 ページ）
- IPv6z アドレスの表記法 （17 ページ）
- ループバック インターフェイス （18 ページ）
- CLI によるポートの管理 （20 ページ）
- リモート IP アドレスと OOB ポート （21 ページ）
- PHY 診断 （22 ページ）
- CLI 出力修飾子 （23 ページ）

概要

CLIはさまざまなコマンドモードに分けられます。各モードには、コマンドのグループが含まれます。

これらのモードについては、CLI コマンド モード （5 ページ）で説明します。

ユーザには、特権レベルが割り当てられます。各ユーザ権限レベルで特定のCLIモードにアクセスできます。

次の項では、ユーザ レベルについて説明します。

ユーザ特権レベル

ユーザは、次のいずれかのユーザ レベルを使用して作成できます。

- レベル 1：このレベルのユーザは、ユーザ EXEC モード コマンドのみを実行できます。このレベルのユーザは、web GUI またはコマンドに特権 EXEC モードでアクセスできません。
- レベル 7：このレベルのユーザは、コマンドをユーザ EXEC モードで実行したり、コマンドのサブセットを特権 EXEC モードで実行したりできます。このレベルのユーザは web GUI にアクセスできません。
- レベル 15：このレベルのユーザはすべてのコマンドを実行できます。このレベルのユーザのみが web GUI にアクセスできます。

システム管理者（レベル 15 のユーザ）は、低レベルのユーザが高レベルのユーザに一時的に昇格できるパスワードを作成できます。たとえば、ユーザのレベルを 1 から 7 に、1 から 15 に、7 から 15 などに昇格できます。

各レベルのパスワードは、次のコマンドを使用して（管理者が）設定します。

enable password [level privilege-level]{password|encrypted encrypted-password}

このパスワードを使用すると、enable コマンドとレベル 7 または 15 のパスワードを入力してユーザ レベルを昇格できます。レベル 1 からレベル 7 に、またはレベル 15 に直接昇格できます。高レベルは現在のセッションでのみ保持されます。

disable コマンドにより、ユーザは低レベルに戻されます。

ユーザを作成してユーザ レベルを割り当てるには、username コマンドを使用します。このレベルのユーザを作成できるのはコマンド レベル 15 のユーザのみです。

例：（管理者が）レベル 7 および 15 のパスワードを作成します。

```
switchxxxxxx#configure
switchxxxxxx<conf># enable password level 7 level7@aBc
switchxxxxxx<conf># enable password level 15 level15@aBc
switchxxxxxx<conf>#
```

ユーザ レベル 1 のユーザを作成します。

```
switchxxxxxx#configure
switchxxxxxx<conf> username john password John1234 privilege 1
switchxxxxxx<conf>
```

例 2：レベル 1 とレベル 15 を切り替えます。ユーザにはパスワードが必要です。

```
switchxxxxxx#
switchxxxxxx# enable
Enter Password: ****** (this is the password for level 15
- Level15@abc)
switchxxxxxx#
```

（注） パスワードの認証が RADIUS または TACACS+ サーバで実行される場合、ユーザ レベル 7 およびユーザ レベル 15 に割り当てるパスワードは外部サーバで設定し、$enable7$ と $enable15$ のユーザ名に個別に関連付ける必要があります。

CLI コマンド モード

CLI は 4 つのコマンド モードに分けられます。コマンド モードは次のとおりです（アクセス順）。

- ユーザ EXEC モード
- 特権 EXEC モード
- グローバル コンフィギュレーション モード

各コマンド モードには、独自の固有なコンソール プロンプトおよび CLI コマンド セットがあります。コンソールプロンプトで疑問符を入力すると、現在のモードとユーザのレベルで利用可能なコマンドのリストが表示されます。特定のコマンドは、モードを切り替えるために使用します。

ユーザには、モードとそこで利用可能なコマンドを決定する権限レベルが割り当てられます。

ユーザ EXEC モード

レベル 1 のユーザは、最初にユーザ EXEC モードにログインします。ユーザ EXEC モードは、基本的なテストの実行やシステム情報の表示などの設定を変更しないタスクで使用されます。

ユーザ レベル プロンプトでは、スイッチ ホスト名の後に # が続きます。デフォルト ホスト名は switchxxxxxx で、xxxxxx は次に示すようにデバイスの MAC アドレスの最後の 6 桁を示します

switchxxxxxx#

デフォルトのホスト名は、hostname コマンドを介してグローバル コンフィギュレーション モードで変更できます。

特権 EXEC モード

レベル 7 または 15 のユーザは特権 EXEC モードに自動的にログインします。

レベル 1 のユーザは、enable コマンドを入力してプロンプトが表示されたらレベル 15 のパスワードを入力すると、特権 EXEC モードを開始できます。

特権 EXEC モードからユーザ EXEC モードに戻るには、desable コマンドを使用します。

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 モードを使用すると、インターフェイス レベルではなく、システム レベルで機能を設定するコマンドを実行できます。

コマンド レベル 7 または 15 のユーザだけがこのモードでアクセスできます。

グローバル コンフィギュレーション モードを特権 EXEC モードからアクセスするには、configure コマンドを特権 EXEC モード プロンプトで入力して Enter を押します。グローバル コンフィ

ギュレーション モード プロンプトには、デバイス ホスト名の後に (config)# が続けて表示されます。

switchxxxxxx(config)#

グローバル コンフィギュレーション モードから特権 EXEC モードに戻るには、次のいずれかのコマンドを使用します。

- exit
- end
- Ctrl+Z

次の例では、グローバル コンフィギュレーション モードにアクセスして特権 EXEC モードに戻る方法を示します。

```
switchxxxxxx#
switchxxxxxx# configure
switchxxxxxx(config)# exit
switchxxxxxx#
```

インターフェイスまたは回線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 モードからさまざまなサブモードを入力できます。これらのサブモードは、

インターフェイスまたは回線のグループでコマンドを実行できるようにします。

たとえば、特定のポートまたはポートの範囲でいくつかの操作を実行する場合は、

そのインターフェイスのインターフェイス コンフィギュレーション モードを開始できます。

次に、vlan1 でインターフェイス コンフィギュレーション モードを開始し、

速度を設定する例を示します。

グローバル コンフィギュレーション モードに戻るには exit コマンドを使用します。

```
switchxxxxxx#
switchxxxxxx# configure
switchxxxxxx(config)# interface range vlan1
switchxxxxxx(config-if)#speed 10
switchxxxxxx(config-if)#exit
switchxxxxxx(config)#
```

次に、使用可能ないくつかのサブモードの例を示します。

- インターフェイス：特定のインターフェイス（ポート、VLAN、ポート チャネル、またはトンネル）またはインターフェイス範囲を設定するコマンドが含まれます。グローバル コンフィギュレーション モード コマンド インターフェイスを使用すると、インターフェイス コンフィギュレーション モードを開始できます。interface 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、このモードを開始できます。
- 回線インターフェイス：コンソール、Telnet、SSH の管理接続の設定に使用するコマンドが含まれます。回線タイムアウト設定などのコマンドが含まれます。line 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、回線設定コマンド モードを開始できます。

- VLAN データベース：VLAN 全体の設定に使用するコマンドが含まれます。vlan database グローバル コンフィギュレーション モード コマンドを使用すると、VLAN データベース インターフェイス コンフィギュレーション モードを開始できます。
- 管理アクセス リスト：管理アクセス リストの定義に使用するコマンドが含まれます。management access-list グローバル コンフィギュレーション モード コマンドを使用すると、管理アクセス リスト コンフィギュレーション モードを開始できます。
- MAC アクセスリスト、IPv6 アクセスリスト、IP アクセスリスト：MAC アドレス、IPv6 アドレス、および IPv4 アドレスのそれぞれに基づいてトラフィックを許可するために必要な条件を設定します。これらのコンフィギュレーション モードを開始するには、mac access-list、ipv6 access-list、および ip access-list グローバル コンフィギュレーション モード コマンドを使用します。

インターフェイス コンフィギュレーション モードからグローバル コンフィギュレーション モードに戻るには、exit コマンドを使用します。

デバッグアクセス用のインターフェイス

上述の標準CLIインターフェイスモードに加えて、デバイスはデバイスデバッグアクセス用の追加インターフェイスをサポートしています。これらのインターレースは、デバイスの動作をデバッグする必要がある場合に、シスコサポートチームの担当者が使用することを目的としています。これらのインターフェイスはパスワードで保護されています。

デバイスは、次のデバッグインターフェイスをサポートしています。

- ブートシーケンス時のU-BOOTアクセス（シリアルコンソール端末経由でのみアクセス可能）
- ブートシーケンス時のLinuxカーネルアクセス（シリアルコンソール端末からのみアクセス可能）
- 実行時デバッグモード：シスコサポートチームの担当者がデバイス設定を表示し、プロトコルとレイヤ1のデバッグコマンドと設定を適用できます（シリアル、Telnet、またはSSHコンソール経由でアクセス可能）

これらのインターフェイスのパスワードは、次のように生成されます。

- デバッグインターフェイスにアクセスすると、デバイスはランダムなハッシュ値を生成し、画面に表示します。
- ハッシュ値は、秘密キーを使用してセキュアなシスコサーバーで署名するために、デバイス管理者とシスコのサポート担当者によって送信されます。
- この操作の出力は、デバッグ インターフェイス アクセスのパスワードとして使用されます。
- このパスワードは現在のセッションに適しています。次回デバッグインターフェイスに入ろうとする時、またはデバイスの再起動後には、デバイスは新しいランダムハッシュを生成します。

CLI のアクセス

CLI には、次のタスクのいずれかを実行して端末またはコンピュータからアクセスできます。

- HyperTerminal などの端末アプリケーションをスイッチのコンソールポートに直接接続されているコンピュータの COM ポートで実行するか、

  または

- スイッチとネットワークで接続されたコンピュータでコマンドプロンプトから Telnet セッションを実行する。
- スイッチへのネットワーク接続があるコンピュータで実行している SSH クライアントをサポートするアプリケーションから SSH を使用する。

（注） デフォルトでは、スイッチの Telnet および SSH は無効です。

Telnet 接続または SSH 接続でアクセスする場合、CLI コマンドを使用する前に次の条件を満たしていることを確認します。

- スイッチには IP アドレスが定義されている
- 対応する管理アクセスが有効になっている
- コンピュータとスイッチが相互に接続できるように IP パスがある

コンソールインターフェイスを介した端末の使用

デバイスは、デュアルコンソール管理インターフェイス（Type-C USB インターフェイスと RJ45 ポート）をサポートしています。Type-C USB と RJ45 の両方が接続されている場合は、Type-C USB インターフェイスが優先されます。Type-C インターフェイスをサポートするために、管理ステーションへのドライバのインストールが必要になる場合があります。

（注） Type-C USB インターフェイスは、デバイスの電源がオン/リブートされてから数秒後にアクティブになります。

コンピュータとスイッチを接続したら、CLI にアクセスするための端末アプリケーションを実行します。ターミナル エミュレータは、databits=8 と parity=none になるように設定する必要があります。

[Enter] を 2 回クリックし、デバイスで PC のシリアル ポート速度に対応するシリアル ポート速度を設定します。

CLI が表示されたら、[User Name] プロンプトに cisco と入力し、[Password] プロンプトに cisco と入力します。

（注） デフォルトのユーザ名とパスワードを使用して初めてログインすると、デバイスにはユーザ名とパスワードを変更するプロンプトが表示されます。新しいパスワードは、パスワードの複雑さのルールを順守する必要があります。

switchxxxxxx# のプロンプトが表示されます。

CLI コマンドを入力してスイッチを管理できるようになりました。CLI コマンドの詳細については、このリファレンス ガイドの該当する章を参照してください。

イーサネット インターフェイス上で Telnet を使用する

Telnet は、IP ネットワークを介して CLI に接続する方法を提供します。

コマンドプロンプトから telnet セッションを確立するには、次の手順を実行します。

ステップ 1 [Start] をクリックし、[All Programs] > [Accessories] > [Command Prompt] を選択してコマンドプロンプトを開きます。

ステップ 2 プロンプトに **telnet 1<IP address of switch>** と入力し、[Enter] を押します。

ステップ 3 CLI が表示されます。

ステップ 4 CLIが表示されたら、[UserName]プロンプトで定義したユーザ名を入力し、定義したパスワードを[Password]プロンプトに入力します。

（注） デフォルトのユーザ名とパスワードを使用して初めてログインすると、デバイスにはユーザ名とパスワードを変更するプロンプトが表示されます。新しいパスワードは、パスワードの複雑さのルールを順守する必要があります。

switchxxxxxx# のプロンプトが表示されます。CLI コマンドを入力してスイッチを管理できるようになりました。CLI コマンドの詳細については、このリファレンス ガイドの該当する章を参照してください。

CLI コマンドの表記法

コマンドを入力する場合、すべてのコマンドに適用される特定のコマンド入力標準があります。次の表では、コマンド表記法について説明します。

表記法	説明
[ ]	コマンド ラインで、角カッコはオプション入力のことを示します。
{ }	コマンド ラインで、中カッコは必須パラメータを区切る | 文字の選択範囲を示します。オプションを 1 つ選択する必要があります。たとえば、**flowcontrol {auto|on|off}** は flowcontrol コマンドを指し、auto、on、または off のいずれかを選択する必要があります。
""（反転カンマ）	入力文字列にスペースや予約語（つまり VLAN）が含まれている場合、文字列を反転カンマ内に配置します。
parameter	斜体はパラメータを示します。
押すキー	押すキーの名前は太字で表示されます。
Ctrl+F4	+ 文字で区切られたキーはキーボードで同時に押します
画面表示	固定長フォントは、CLI プロンプト、ユーザが入力した CLI コマンド、およびコンソールに表示されるシステム メッセージです。
all	ポートまたはパラメータの範囲の定義でパラメータが必要で、all がオプションにある場合、パラメータが定義されていないと、コマンドのデフォルト値は all になります。たとえば、interface range port-channel コマンドでは、チャネルの範囲を入力するオプションまたは all を選択するオプションのいずれかを指定します。パラメータを指定せずにコマンドを入力すると、デフォルト値は自動的に all になります。
text	テキストが空白で区切られた複数の文字で構成される場合（snmp-server contact コマンドの場合など）、コマンドのパラメータとしてテキストを自由に入力するには、文字列全体を二重引用符で囲んで表示する必要があります。例：**snmp-server contact** "QA on floor 8"

機能の編集

コマンドの入力

CLI コマンドは一連のキーワードと引数で構成されます。キーワードはコマンドを特定し、引数は設定パラメータを指定します。たとえば、show interfaces status Gigabitethernet 1 コマンドでは、show、interfaces、および status はキーワードで、Gigabitethernet はインターフェイス タイプを指定する引数、1 はポートを指定します。

パラメータが必要なコマンドを入力するには、コマンドキーワードの後に必要なパラメータを入力します。たとえば、管理者のパスワードを設定するには次のように入力します。

switchxxxxxx(config)# username admin password Alansmith1

CLI を使用する場合、コマンドオプションは表示されません。ヘルプを要求するための標準コマンドは ? です。

ヘルプ情報が表示される 2 つのインスタンスがあります。

- キーワードルックアップ：?文字をコマンドの代わりに入力します。すべての有効なコマンドと対応するヘルプメッセージのリストが表示されます。
- 部分的なキーワードルックアップ：コマンドが不完全な場合にパラメータの代わりに?文字を入力すると、このコマンドに一致するキーワードまたはパラメータが表示されます。

端末のコマンド バッファ

CLI でコマンドを入力するたびに、内部的に管理されているコマンド履歴バッファに記録されます。バッファに記録されているコマンドは先入れ先出し（FIFO）で保持されます。このコマンドは、呼び出し、確認、変更、および再発行を行うことができます。このバッファは、デバイスがリセットされると保持されません。

キーワード	説明
↑キー	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
↓キー	↑キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。

デフォルトでは、履歴バッファ システムは有効ですが、いつでも無効にすることができます。履歴バッファの有効と無効の切り替えに関する詳細については、history コマンドを参照してください。

デフォルトでは、バッファには標準的な数のコマンドが保存されています。標準的な 10 個のコマンドを 216 個に増やすことができます。0 に設定すると、履歴バッファ システムを無効に

した場合と同じ効果が得られます。コマンド履歴バッファの設定に関する詳細については、**history size** コマンドを参照してください。

履歴バッファを表示する場合は、**show history** コマンドを参照してください。

コマンドの影響を無効にする

多くの設定コマンドでは、プレフィックス キーワード no を入力すると、コマンドの影響を取り消したり、デフォルト値に対する設定をリセットしたりできます。このリファレンス ガイドでは、各 CLI コマンドの無効効果について説明します。

コマンドの補完

入力したコマンドが不完全な場合、無効な場合、パラメータが欠けているまたは無効な場合、適切なエラー メッセージが表示されます。このため、正しいコマンドを入力できます。不完全なコマンドを入力した後に Tab を押すと、コマンドを特定して完全なものにしようとします。すでに入力した文字が足りずに、システムが一致するコマンドを 1 つも特定できない場合は、? を押すと、すでに入力した文字と一致する利用可能なコマンドが表示されます。

キーボードのショートカット

CLI には、CLI コマンドの編集に役立つ一連のキーボード ショートカットが指定されています。次の表では、CLI ショートカットについて説明します。

キーボードのキー	説明
↑	履歴バッファからコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
↓	↑キーでコマンドを呼び出した後で、履歴バッファ内の最新のコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。
Ctrl+A	コマンドラインの先頭にカーソルを移動します。
Ctrl+E	カーソルをコマンド ラインの末尾に移動します。
Ctrl+Z/End	コンフィギュレーション モードから特権 EXEC モードに戻ります。
Back Space	カーソル位置の左にある 1 つの文字を削除します。

テキストのコピー アンド ペースト

デバイスには、最大 1000 行のテキスト（またはコマンド）をコピー アンド ペーストできます。

（注） ユーザの責任において、デバイスにコピーしたテキストが適切なコマンドのみで構成されるようにします。

設定ファイルからコマンドをコピー アンド ペーストする場合は、次の条件を確認してください。

- デバイスのコンフィギュレーション モードにアクセスできる。

コマンドには、暗号化パスワードやキーなどの暗号化データを含めない。暗号化データの前に暗号化キーワードが使用される場合の暗号化パスワードを除いて、暗号化データをデバイスにコピー アンド ペーストすることはできません（enable password コマンドの場合など）。

インターフェイス命名規則

デバイスのインターフェイスは、次のタイプのいずれかにすることができます。

- ギガビットイーサネット（10/100/1000 キロビット）ポート：これらは GigabitEthernet、または gi、あるいは GE と記述されます。
- 2.5 ギガビットイーサネット（10/100/1000/25000 キロビット）ポート：これらは TwoPointFiveGigabitEthernet または tw と記述されます。
- 5 ギガビットイーサネット（10/100/1000/25000/50000 キロビット）ポート：これらは FiveGigabitEthernet または fi のいずれかで記述されます。
- LAG（ポートチャネル）：Port-Channel または po のいずれかで記述されます。
- VLAN：VLAN と記述されます。
- トンネル：tunnel または tu と記述されます。
- OOB：OutOfBand または oob と記述されます。

CLI で内では、インターフェイスは次の要素を連結して表されます。

- インターフェイスのタイプ：前述のとおり。
- ユニット番号：スタック内のユニット。
- スロット番号：スロット番号は常に 0 です。
- スタッキング モードでのインターフェイス名の構文は次のとおりです。

  {<port-type>[ ][<unit-number>/]<slot-number>/<port-number>} | {port-channel | po |

  }[ ]<port-channel-number> |

  {tunnel | tu}[ ]<tunnel-number> | vlan[ ]<vlan-id>
- インターフェイス番号：ポート、LAG、トンネル、または VLAN 番号。

次に、これらのさまざまなオプションの例を示します。

```
switchxxxxxx(config)#interface GigabitEthernet 1
switchxxxxxx(config)#interface GE 1
switchxxxxxx(config)#interface TwoPointFiveGigabitEthernet
switchxxxxxx(config)#interface po1
switchxxxxxx(config)# interface vlan 1
```

インターフェイス範囲

インターフェイスは、個別にまたは範囲内で説明されています。インターフェイス範囲のコマンドは次のような構文になります。

<interface-range> ::=

{<port-type>[

][<unit-number>/]<slot-number>/<first-port-number>[-
<last-port-number]} |
port-channel[ ]<first-port-channel-number>[-
<last-port-channel-number>] |
tunnel[ ]<first-tunnel-number>[- <last-tunnel-number>] |
vlan[ ]<first-vlan-id>[- <last-vlan-id>]

このコマンドのサンプルを、次の例で示します。

```
switchxxxxxx#configure
switchxxxxxx(config-if)#interface range gi1-5g
```

複数のインターフェイスタイプのリスト

インターフェイス タイプの組み合わせは、interface range コマンドで次の形式で指定できます。

<range-list> ::= <interface-range> | <range-list>, <interface-range>

最大 5 つの範囲を含めることができます。

（注） 範囲リストには、ポートとポート チャネルまたは VLAN のいずれかを含められます。ポート/ポートチャネルと VLAN の組み合わせは使用できません。

カンマの後のスペースは省略可能です。

範囲リストを定義する場合、最初の入力後とカンマ（,）前にスペースを入力する必要があります。

このコマンドのサンプルを、次の例で示します。

```
switchxxxxxx#configure
switchxxxxxx(config)#interface range gi1-5, vlan 1-2
```

IPv6z アドレスの表記法

次に、リンク ローカルの IPv6 アドレスである IPv6z アドレスを記述する方法について説明します。

形式：<ipv6-link-local-address>%<egress-interface>

値は次のとおりです。

egress-interface (also known as zone) = vlan<vlan-id> | po<number> | tunnel<number> | port<number> | 0

出力インターフェイスが指定されていない場合、デフォルトのインターフェイスが選択されます。出力インターフェイス = 0 に指定することは、出力インターフェイスを定義しているわけではありません。

次の組み合わせを使用できます。

- ipv6_address%egress-interface：指定したインターフェイスの IPv6 アドレスを参照します。
- ipv6_address%0：IPv6 アドレスが定義される単一インターフェイスの IPv6 アドレスを参照します。
- ipv6_address：IPv6 アドレスが定義される単一インターフェイスの IPv6 アドレスを参照します。

ループバック インターフェイス

ルータ上の IP アプリケーションがリモート IP アプリケーションと通信する必要がある場合、その IP アドレスとして使用するローカル IP アドレスを選択する必要があります。ルータで定義された任意の IP アドレスを使用できますが、このリンクに障害が発生した場合、これらの IP アプリケーション間に別の IP ルートが用意されていても、通信が中断されます。

ループバック インターフェイスは仮想インターフェイスで、動作状態は常に稼働しています。この仮想インターフェイスで設定されている IP アドレスを、リモート IP アプリケーションと通信するときにローカル アドレスとして使用する場合、リモート アプリケーションへの実際のルートが変更されていても、通信は中断されません。

ループバック インターフェイスの名前は loopback1 です。

ループバック インターフェイスはブリッジをサポートしていません。いかなる VLAN のメンバーになることもできません。有効にできる レイヤ 2 プロトコルはありません。

レイヤ 3 の指定

IP インターフェイス

IPv4 および IPv6 アドレスはループバック インターフェイスに割り当てることができます。

IPv6 リンク ローカルのインターフェイス識別子は 1 です。

ルーティング プロトコル

スイッチで実行されているルーティング プロトコルは、ルーティング プロトコルの再配布メカニズムを使用してループバック インターフェイスで定義された IP プレフィックスの通知をサポートしています。

設定例

スタティック ルーティング

次の例で、スタティック ルーティングを使用するスイッチの IP を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 10.10.10.2 /24
Switch(config-if)# ipv6 address 2001:DB8:2222:7270::2312/64
Switch(config-if)# exit
Switch(config)# interface vlan 2
Switch(config-if)# ip address 10.11.11.2 /24
Switch(config-if)# ipv6 address 2001:DB8:3333:7271::2312/64
Switch(config-if)# exit
Switch(config)# interface loopback 1
Switch(config-if)# ip address 172.25.13.2 /32
Switch(config-if)# ipv6 address 2001:DB8:2222:7272::72/128
Switch(config-if)# exit
Switch(config)# ip route 0.0.0.0/0 10.10.11.1
Switch(config)# ip route 10.11.0.0 /16 10.11.11.1
Switch(config)# ipv6 route 0::/0 2001:DB8:2222:7270::1
```

```
Switch(config)# ipv6 route 2001:DB8:3333::/48
2001:DB8:3333:7271::1
```

ネイバー ルータ 10.10.11.1 は、次のスタティック ルートを使用して設定する必要があります：ip ルート 172.25.13.2/32 10.10.10.2。

ネイバー ルータ 10.11.11.1 は、次のスタティック ルートを使用して設定する必要があります：ip ルート 172.25.13.2/32 10.11.11.2。

VLAN 1 に接続されたネイバー ルータ 2001:DB8:2222:7270::1 は、次のスタティック ルートを使用して設定する必要があります。

ipv6 route 2001:DB8:2222:7272::72/128 2001:DB8:2222:7270::2312

VLAN 1 に接続されたネイバー ルータ 2001:DB8:3333:7271::1 は、直下のスタティック ルートを使用して設定する必要があります。

IPv6 Route 2001:DB8:2222:7272::72/128 2001:DB8:3333:7271::2312

CLI によるポートの管理

スタッキングをサポートするユニットのポートインターフェイスにアクセスするには、「interfaceGigabitEthernetX/0/Z（1gig インターフェイスの場合）」または「interface TenGigabitEthernetX/0/Y（10gig ポートの場合）」と入力します。X（1 ～ 4）はスタック ID、Y はアップリンクポート番号（1 ～ 4）、Z はダウンリンクポート番号で、Z はポート数が 48 未満のユニットでも 1 ～ 48 になります。

光ファイバケーブルとトランシーバ

シスコブランドはSFPモジュール一式を提供します。シスコのスイッチは他のサードパーティをサポートしていますが、特定のSFPモジュールと組み合わせて使用する光ファイバケーブルのタイプに注意することが重要です。

光ファイバケーブルは、シングルモードとマルチモードの2つのタイプに分類できます。主な違いは、カバーできる距離と直径です。シングルモードファイバは、マルチモードよりも長い距離をカバーし、直径が小さい（約9マイクロメートル）です。マルチモードファイバの直径は 50 ー 62.5 マイクロメートルです。

一方で、直接接続銅ケーブルの DAC ケーブルは、短距離に使用できます。カバーできる最大距離が 15 m であるため、主にマルチモード標準タイプのトランシーバを基準としています。ただし、AOC（アクティブ光ケーブル）は別です。

光ファイバ接続関連の問題をトラブルシューティングする場合は、SMF（シングルモードファイバ ケーブル）と MMF（マルチモード ファイバ ケーブル）、および特定の光ファイバがサポートできる対応する SFP トランシーバを区別することが重要です。

シスコには、正しいペアリングを判断しようとする際に参照できるマトリックスがあります。次のリンクでは、Cisco 10gig SFP に関するインサイトを提供しています。

例：

Cisco SFP-10G-SR は直径 62.5 マイクロメートルの MMF タイプのケーブルでのみ動作し、Cisco SFP-10G-LR は SMF タイプのケーブルでのみ動作します。MMF の範囲は OM1 ～ OM5 です。OM とは光マルチモードのことです。OM1 タイプのケーブルの直径は 62.5 マイクロメートルですが、他のタイプ（OM2 ～ OM5）はすべて直径が 50 マイクロメートルです。

したがって、それらが混在しないようにするには、何が行われているかを知ることが重要です。

リモート IP アドレスと 00B ポート

スイッチでは、OutOfBand（OOB）ポートで IP スタックがサポートされます。この IP スタックは ASIC ポートで実行している IP スタックとは切り離されており、特定のルートテーブルを設定する必要があります。

スイッチが複数の IP インターフェイスをサポートする場合、リモート IP アドレスまたは DNS 名を指定するときに、参照される IP スタックを指定する必要もあります。

PHY 診断

次の例外が利用できます。

- 銅線ポート：PHY 診断は銅線ポートでのみサポートされます。
- 10 G ポート：動作ポートの速度が 10 G の場合、TDR テストがサポートされます。ケーブル長の分解能は 20 m です。

CLI 出力修飾子

すべての **show** コマンドと **more** コマンド（**show technical support** を除く）では、出力修飾子が次のように追加されます。

```
<show/more command> | <output-modifier> <regular-expression-pattern>
```

出力修飾子は次のとおりです。

- **begin**：指定した正規表現パターンに一致する文字列を含む最初の行から出力を開始します。
- **include**：指定した正規表現パターンに一致する文字列を含む行のみを含めます。
- **exclude**：指定した正規表現パターンに一致する文字列を含むすべての行を除外します。
- **count**：指定した正規表現パターンに一致する文字列を含むすべての行をカウントし、結果を表示します（他の出力は表示されません）。

（注） 各コマンドで使用できる出力修飾子は1つのみです。入力したテキストの残りの部分は、正規表現パターンの一部になります。

正規表現は、パターン（フレーズ、番号、またはより複雑なパターン）です。CLI 文字列検索機能は、show コマンドまたは more コマンドの出力に正規表現を照合します。正規表現では、大文字と小文字が区別され、複雑な一致要件を指定することが可能です。

正規表現は、単一文字パターンか複数文字パターンです。つまり、正規表現は、コマンド出力中の同じ 1 文字に一致する 1 つの文字か、コマンド出力中の同じ複数の文字に一致する複数の文字です。コマンド出力中のパターンをストリングと呼びます。この項では、単一文字パターンと複数文字パターンの作成について説明します。また、量指定子、論理和指定子、位置指定子、カッコを使用した、より複雑な正規表現についても説明します。

単一文字パターン

最も単純な正規表現は、コマンド出力内の同じ1つの文字と一致する単一文字です。任意の文字（A ～ Z、a ～ z）または数字（0 ～ 9）を 1 文字のパターンとして使用できます。また、その他のキーボード文字（「!」や「~」など）も 1 文字のパターンとして使用できますが、一部のキーボード文字は正規表現では特別な意味を持ちます。次の表に、特殊な意味を持つキーボード文字のリストを示します。

文字	意味
.	スペースを含む任意の単一文字と一致します。
*	0 個以上のパターンのシーケンスと一致します。
+	1 個以上のパターンのシーケンスと一致します。

文字	意味
?	0 または 1 回のパターンと一致します。
^	ストリングの先頭と一致します。
$	ストリングの末尾と一致します。

これらの特殊文字を単一文字パターンとして使用するときは、各文字の前にバックスラッシュ（\）を置いて特別な意味を除外してください。

次の例は、それぞれドル記号、アンダースコア、プラス記号に一致する単一文字パターンマッチングの例です。

\$ _ \+

単一文字パターンを範囲指定して、コマンド出力とのマッチングを行うことができます。たとえば、文字 a、e、i、o、u のいずれかを含むストリングに一致する正規表現を作成できます。パターンマッチングが成功するためには、これらの文字のいずれかだけがストリング中に存在する必要があります。1 文字のパターンの範囲を指定するには、1 文字のパターンを角カッコ（[ ]）で囲みます。たとえば、[aeiou] は小文字アルファベットの 5 つの母音のうちの任意の 1 文字と一致しますが、[abcdABCD] は小文字または大文字アルファベットの最初の 4 つの文字のうちの任意の 1 文字と一致します。

ダッシュ（-）で区切って範囲の終点だけを入力することにより範囲を簡略化することができます。

上の範囲は次のように単純化されます。

[a-dA-D]

ダッシュを範囲内の単一文字パターンとして追加するには、ダッシュをもう 1 つ追加し、その前にバックスラッシュを入力します。

[a-dA-D\-]

次に示すように、右角カッコ（]）を、範囲内の単一文字パターンとして追加することもできます。

[a-dA-D\-\]]

上の例は、大文字または小文字のアルファベットの最初の 4 文字、ダッシュ、右角カッコのいずれかに一致します。範囲の先頭にキャレット（^）を追加することで、範囲の一致を反転させることができます。次の例は、その中の文字以外の文字に一致します。

[^a-dqsv]

次の例は、右角カッコ（]）または文字 d 以外のすべてと一致します。

[^\]d]

複数文字のパターン

正規表現を作成するとき、複数の文字を含むパターンを指定することもできます。複数文字正規表現は、文字、数字、特別な意味のないキーボード文字を組み合わせて作成します。たとえば、a4% は複数文字の正規表現です。

複数文字パターンでは、順序が大切です。a4% という正規表現は、a という文字のあとに 4 が続き、そのあとに % 記号が続く文字と一致します。ストリングの中に a4% という文字がその順序で含まれていないと、パターン マッチングは失敗します。複数文字の正規表現 a. ではピリオド文字に特殊な意味があり、文字 a の後に続く 1 文字に相当します。この例では、ab、a!、または a2 というストリングはすべてこの正規表現と一致します。

ピリオド文字の特別な意味を無効にするには、その前にバックスラッシュを挿入します。たとえば、表現 a\. がコマンド構文で使用されている場合、ストリング a. だけが一致します。

すべての文字、すべての数字、すべてのキーボード文字、文字と数字とその他のキーボード文字の組み合わせを含む複数文字正規表現を作成できます。たとえば、telebit 3107 v32bis は有効な正規表現です。

量指定子

指定した複数表現の出現を複数回一致させるようにシステムに指示する、より複雑な正規表現を作成できます。これを行うには、1 文字パターンと複数文字のパターンを使用していくつかの特殊文字を使用します。表 1 に、正規表現の出現回数を指定する特殊文字のリストを示します。

表 *1*：表 *1*：量指定子として使用する特殊文字

文字	説明
*	0 以上の単一文字パターンまたは複数文字パターンと一致します。
+	1 以上の単一文字パターンまたは複数文字パターンと一致します。
?	1 以上の単一文字パターンまたは複数文字パターンの 0 回または 1 回の出現と一致します。

次の例は、空文字を含む文字 a の任意の回数の出現と一致します。

a*

次のパターンでは、ストリングが一致するためには、文字 a が少なくとも 1 文字含まれていることが必要です。

a+

次のパターンは、ストリング bb または bab と一致します。

ba?b

次のストリングは、任意の数のアスタリスク（*）と一致します。

**

乗算子を複数文字パターンと共に使用するには、パターンをカッコで囲みます。次の例で、パターンは複数文字ストリング ab の任意の回数の出現と一致します。

(ab)*

次のパターンは、英数字ペアの 1 つ以上のインスタンスに一致しますが、存在しない場合には一致しません（空の文字列とは一致しません）。

([A-Za-z][0-9])+

量指定子（*、+、または?）を使用した一致の順序は、最長構造優先です。ネストした構造は、外側から内側に一致します。連結された構造は、構造の左側から一致します。したがって、上記の正規表現は A9b3 と一致しますが、数字の前に文字が指定されているため 9Ab3 とは一致しません。

代替

選択を使用すると、ストリングに対して一致する代替パターンを指定できます。選択パターンは垂直線（|）で区切ります。選択肢のいずれか 1 つだけがストリングと一致します。たとえば、正規表現 codex|telebit は文字列 codex または文字列 telebit のいずれかに一致しますが、codex と telebit の両方には一致しません。

位置指定

正規表現パターンを文字列の先頭または末尾と一致させるようにシステムに指示することができます。文字列の一部にこれらの正規表現を位置指定するには、表 2 に示す特殊文字を使用します。

表 *2:* 表 *2*：位置指定子として使用する特殊文字

文字	説明
^	ストリングの先頭と一致します。
$	ストリングの末尾と一致します。

たとえば、正規表現 ^con は con で始まるストリングに一致し、$sole は sole で終わるストリングに一致します。

文字列の先頭を示すのに加えて、^ 記号は角カッコの中で使用された場合は論理関数 not を示すものとして使用できます。たとえば、正規表現 [^abcd] は、a、b、c、または d 以外の任意の単一文字に一致する範囲を示します。

802-1x コマンド

この章は、次の項で構成されています。

- aaa authentication dot1x （29 ページ）
- authentication open （30 ページ）
- clear dot1x statistics （31 ページ）
- data （32 ページ）
- description 802.1x （33 ページ）
- dot1x auth-not-req （34 ページ）
- dot1x authentication （35 ページ）
- dot1x credentials （37 ページ）
- dot1x eap-max-retrans （38 ページ）
- dot1x guest-vlan （39 ページ）
- dot1x guest-vlan enable （40 ページ）
- dot1x guest-vlan timeout （41 ページ）
- dot1x host-mode （42 ページ）
- dot1x mac-auth （45 ページ）
- dot1x mac-auth password （47 ページ）
- dot1x max-hosts （48 ページ）
- dot1x max-login-attempts （49 ページ）
- dot1x max-req （50 ページ）
- dot1x page customization （51 ページ）
- dot1x port-control （52 ページ）
- dot1x radius-attributes vlan （54 ページ）
- dot1x re-authenticate （56 ページ）
- dot1x reauthentication （57 ページ）
- dot1x supplicant （58 ページ）
- dot1x supplicant traps authentication failure （60 ページ）
- dot1x supplicant traps authentication success （61 ページ）
- dot1x system-auth-control （62 ページ）
- dot1x timeout eap-timeout （63 ページ）

- dot1x timeout quiet-period （64 ページ）
- dot1x timeout reauth-period （65 ページ）
- dot1x timeout server-timeout （66 ページ）
- dot1x timeout silence-period （67 ページ）
- dot1x timeout supp-timeout （68 ページ）
- dot1x timeout supplicant-held-period （69 ページ）
- dot1x timeout tx-period （70 ページ）
- dot1x traps authentication failure （71 ページ）
- dot1x traps authentication quiet （72 ページ）
- dot1x traps authentication success （73 ページ）
- dot1x unlock client （74 ページ）
- dot1x violation-mode （75 ページ）
- password （76 ページ）
- show dot1x （77 ページ）
- show dot1x credentials （82 ページ）
- show dot1x locked clients （83 ページ）
- show dot1x statistics （84 ページ）
- show dot1x users （86 ページ）
- username（dot1x ログイン情報） （87 ページ）

aaa authentication dot1x

802.1X 認証の有効時の認証に使用するサーバを指定するには、グローバル コンフィギュレーション モードで **aaa authentication dot1x** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

aaa authentication dot1x default {**radius** | **none** | {**radius none**}}

no aaa authentication dot1x default

パラメータ

- **radius**：すべての RADIUS サーバのリストを認証に使用します。
- **none**：認証を使用しません。

デフォルト設定

RADIUS サーバ.

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

RADIUS サーバによる認証、認証なし（**none**）、または両方の方式を選択できます。

RADIUS サーバ応答が受信されなかったときにも認証を成功させる必要がある場合は、コマンド ラインで最後の方式として **none** を指定します。

例

次の例では、RADIUS サーバ認証に 802.1X 認証モードを設定しています。応答が受信されなかった場合でも、認証が成功します。

```
switchxxxxxx(config)# aaa authentication dot1x default radius none
```

authentication open

このポートでオープン アクセス（モニタリング モード）を有効にするには、インターフェイス コンフィギュレーション モードで **authentication open** コマンドを使用します。このポートでオープン アクセスを無効にするには、このコマンドの **no** 形式を使用します。

構文

authentication open

no authentication open

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

無効

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

オープン アクセス モードまたはモニタリング モードでは、認証が実行される前にクライアントまたはデバイスがネットワーク アクセスを取得できます。このモードでは、スイッチは RADIUS サーバから受信した失敗応答を、成功として実行します。

例

次に、インターフェイス gi1/0/1 でオープンモードを有効にする例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# authentication open
```

clear dot1x statistics

802.1X 統計情報をクリアするには、特権 EXEC モードで **clear dot1x statistics** コマンドを使用します。

構文

clear dot1x statistics [*interface-id*]

パラメータ

- ***interface-id***：イーサネット ポート ID を指定します。

デフォルト設定

すべてのポートの統計がクリアされます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドにより、**show dot1x** および **show dot1x statistics** コマンドに表示されるすべてのカウンタがクリアされます。

例

```
switchxxxxxx# clear dot1x statistics
```

data

Web ベース ページ カスタマイズを指定するには、Web ベース ページ カスタマイズ コンフィギュレーション モードで **data** コマンドを使用します。

構文

data *value*

パラメータ

- ***value***：最大 320 文字の、16 進数文字列。

デフォルト設定

ユーザのカスタマイズは未設定です。

コマンド モード

Web ベースのページ カスタマイズ コンフィギュレーション モード

使用上のガイドライン

このコマンドは、（コピーして貼り付けを使用しない限り）手動で入力または編集しないでください。スイッチが生成する設定ファイルの一部です。

ユーザは、Web インターフェイスを使用して、Web ベースの認証ページのみをカスタマイズできます。

例 1：次の例は、Web ベースのページ カスタマイズ コンフィギュレーションの一部を示しています。

```
switchxxxxxx(config)# dot1x page customization
switchxxxxxx(config-web-page)# data 1feabcde
switchxxxxxx(config-web-page)# data 17645874
switchxxxxxx(config-web-page)# exit
```

例 2：次に、**show running-config** コマンドの実行時に Web ベースのカスタマイズがどのように表示されるかの例を示します。

```
switchxxxxxx# show running-config
dot1x page customization
data ********
exit
```

description 802.1x

802.1X ログイン情報の構造体の説明を指定するには、Dot1x ログイン情報コンフィギュレーション モードで **description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

構文

description *text*

no description

パラメータ

- ***text***：テキストの説明。説明は最大 80 文字です。

デフォルト設定

説明が指定されていません。

コマンド モード

Dot1x ログイン情報コンフィギュレーション モード。

使用上のガイドライン

スイッチをサプリカント（クライアント）として設定する場合は、802.1X ログイン情報の構造体が必要です。このログイン情報の構造体には、ユーザ名とパスワードを含める必要があり、説明を含めることができます。

例

次に、802.1X ログイン情報の構造体を設定する例を示します。

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password 6f3c576n8
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
 connected to site-A
```

dot1x auth-not-req

許可されていないデバイスが VLAN にアクセスできるようにするには、インターフェイス（VLAN）コンフィギュレーション モードで **dot1x auth-not-req** を使用します。VLAN へのアクセスを無効にするには、このコマンドの **no** 形式を使用します。

構文

dot1x auth-not-req

no dot1x auth-not-req

デフォルト設定

アクセスが有効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

ゲスト VLAN は、許可されていない VLAN として設定できません。

例

次の例では、許可されていないデバイスが VLAN 5 にアクセスできるようにしています。

```
switchxxxxxx(config)# interface vlan 5
switchxxxxxx(config-if)# dot1x auth-not-req
```

dot1x authentication

ポートで認証方式を有効にするには、インターフェイス コンフィギュレーション モードで **dot1x authentication** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x authentication [**802.1x**] [**mac**] [**web**]

no dot1x authentication

パラメータ

- **802.1x**：802.1X に基づく認証（802.1X ベース認証）を有効にします。
- **mac**：ステーションの MAC アドレスに基づく認証（MAC ベース認証）を有効にします。
- **web**：Web ベース認証を有効にします。

デフォルト設定

802.1X ベース認証が有効になっています。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

スタティック MAC アドレスは、MAC ベースの方式で許可できません。

MAC アドレスが MAC ベース認証によって許可されている場合は、ダイナミック MAC アドレスをスタティック MAC アドレスに変更することや、MAC アドレスを削除することは推奨しません。

1. MAC ベースの認証で認証されたダイナミック MAC アドレスが静的 MAC アドレスに変更された場合は、手動では再認証されません。
2. MAC ベースの認証で認証されたダイナミック MAC アドレスを削除すると、再認証が行われます。

ポートチャネルに関連付けられたポートで有効になっている 802.1X には、次の制限があります。

- 802.1X ベースの認証のみがサポートされます。
- マルチホスト（レガシー 802.1X モード）モードのみがサポートされます。

例

次に、ポート gi1/0/1 の 802.1x とステーションの MAC アドレスに基づく認証を有効にする例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x authentication 802.1x mac
```

dot1x credentials

802.1X ログイン情報の構造体の名前を定義して Dot1x ログイン情報のコンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **dot1x credentials** コマンドを使用します。ログイン情報の構造体を削除するには、このコマンドの **no** 形式を使用します。

構文

dot1x credentials *name*

no dot1x credentials *name*

パラメータ

- ***name***：最大 32 文字のログイン情報の構造体名。

デフォルト設定

ログイン情報の構造体が指定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ログイン情報の構造体の設定を開始するには、**dot1x credentials** コマンドを使用します。ログイン情報の構造体にはサプリカント（クライアント）のパラメータが含まれており、インターフェイスで 802.1x サプリカントが有効になっている場合に使用されます。

ログイン情報の設定は、ログイン情報コンテキストの終了後にのみ行われます。

使用されているログイン情報の設定を変更すると、サプリカントのログオフとログオンが行われます。

スイッチは最大 24 個のログイン情報をサポートします。

ログイン情報を削除するには、**no dot1x credentials** コマンドを使用します。使用済みのログイン情報は削除できません。

例

次に、802.1X ログイン情報の構造体を設定する例を示します。

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password agrcx5642
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
 connected to site-A
```

dot1x eap-max-retrans

EAP の最大再送信回数を設定するには、インターフェイス コンフィギュレーション モードで **dot1x eap-max-retrans** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x eap-max-retrans *count*

no dot1x eap-max-retrans

パラメータ

- ***count***：EAP クライアント（EAP ピア）からの応答を受信しなかった場合に、EAP サーバ（EAP オーセンティケータ）が EAP 要求を再送信する最大回数を指定します。（範囲：1 ～ 10）。

デフォルト設定

デフォルトの最大試行回数は 2 回です。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対応する場合にのみ、変更する必要があります。

パラメータは 802.1x サプリカントで使用されます。

例

次に、EAP 最大再送信回数を 6 に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x eap-max-retrans 6
```

dot1x guest-vlan

ゲスト VLAN を定義するには、インターフェイス（VLAN）コンフィギュレーション モードで **dot1x guest-vlan** モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x guest-vlan

no dot1x guest-vlan

デフォルト設定

ゲスト VLAN として定義されている VLAN はありません。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

デバイスが持つことができるグローバル ゲスト VLAN は 1 つのみです。

ゲスト VLAN はスタティック VLAN である必要があり、削除することはできません。

未承認 VLAN はゲスト VLAN に設定できません。

例

次の例では、ゲスト VLAN として VLAN 2 を定義しています。

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# dot1x guest-vlan
```

dot1x guest-vlan enable

ゲストVLANへのアクセスインターフェイスで未承認ユーザを有効にするには、インターフェイス コンフィギュレーション モードで **dot1x guest-vlan enable** コマンドを使用します。アクセスを無効にするには、このコマンドの **no** 形式を使用します。

構文

dot1x guest-vlan enable

no dot1x guest-vlan enable

デフォルト設定

デフォルト設定では無効になっています。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

ゲスト VLAN と Web ベース認証は、ポートへの同時設定はできません。

モニタリング VLAN がインターフェイスで有効になっている場合、このコマンドを設定できません。

ポートがゲスト VLAN に属していない場合、ゲスト VLAN にタグなし出力ポートとして追加されます。

認証モードがシングルホストまたはマルチホストの場合、PVID の値はゲスト VLAN_ID に設定されます。

認証モードがマルチセッション モードの場合、PVID は変更されず、許可されていないホストからの非認証VLANに属していないすべてのタグなしトラフィックおよびタグ付きトラフィックが、ゲスト VLAN にマッピングされます。

802.1X が無効になっている場合は、ポートのスタティック設定がリセットされます。

例

次の例では、gi1/0/1 の未承認ユーザがゲスト VLAN にアクセスできるようにします。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x guest-vlan enable
```

dot1x guest-vlan timeout

802.1X の有効化（またはポートのアップ）とポートのゲスト VLAN への追加の間の遅延を設定するには、グローバル コンフィギュレーション モードで **dot1x guest-vlan timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x guest-vlan timeout *timeout*

no dot1x guest-vlan timeout

パラメータ

- ***timeout***：802.1X を有効にしてから（またはポートがアップ状態になってから）ゲスト VLANにポートが追加されるまでの時間遅延を秒単位で指定します。（範囲：30～180）。

デフォルト設定

ゲスト VLAN がただちに適用されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、ポート上でゲスト VLAN が有効になっている場合に関係します。タイムアウトを設定すると、802.1X を有効にしてから（またはポートがアップ状態になってから）デバイスによりゲスト VLAN にポートが追加されるまでの遅延が追加されます。

例

次の例では、802.1X を有効にしてからゲスト VLAN にポートが追加されるまでの遅延を 60 秒に設定しています。

```
switchxxxxxx(config)# dot1x guest-vlan timeout 60
```

dot1x host-mode

IEEE 802.1X 承認済みポートでシングルホスト（クライアント）またはマルチホストを許可するには、インターフェイス コンフィギュレーション モードで **dot1x host-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x host-mode {multi-host | single-host | multi-sessions}

パラメータ

- **multi-host**：マルチホスト モードを有効にします。
- **single-host**：シングルホスト モードを有効にします。
- **multi-sessions**：マルチセッション モードを有効にします。

デフォルト設定

デフォルトのモードはマルチホストです。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

シングルホスト モード

シングルホスト モードでは、ポートの認証ステータスが管理されます。許可ホストがある場合、ポートが許可されます。このモードでは、単一のホストのみをポートで許可できます。

ポートが未承認で、ゲスト VLAN が有効な場合、タグなしトラフィックはゲスト VLAN に再マップされます。VLAN タグがゲスト VLAN または未認証 VLAN ではない場合、タグ付きトラフィックはドロップされます。ゲスト VLAN がポートで有効になっていない場合、未認証 VLAN に属するタグ付きトラフィックのみがブリッジされます。

ポートが許可されると、許可ホストからのタグなしトラフィックおよびタグ付きトラフィックが、ポートで設定されたスタティック VLAN メンバーシップに基づいてブリッジされます。他のホストからのトラフィックはドロップされます。

許可ホストからのタグなしトラフィックが、認証プロセス中にRADIUSサーバによって割り当てられた VLAN に再マッピングされるようにユーザが指定できます。この場合、VLAN タグが RADIUS によって割り当てられた VLAN または認証されていない VLAN である場合を除いて、タグ付きトラフィックはドロップされます。

スイッチは、認証ステータスが許可から無許可に変更されたときに、ポートで学習されたすべての MAC アドレスを FDB から削除します。

マルチホスト モード

マルチホストモードでは、ポートの認証ステータスが管理されます。少なくとも1つのホストが許可された後に、ポートが許可されます。

ポートが未承認で、ゲスト VLAN が有効な場合、タグなしトラフィックはゲスト VLAN に再マップされます。VLAN タグがゲスト VLAN または未認証 VLAN ではない場合、タグ付きトラフィックはドロップされます。ゲスト VLAN がポートで有効になっていない場合、未認証 VLAN に属するタグ付きトラフィックのみがブリッジされます。

ポートが許可されると、ポートに接続されたすべてのホストからのタグなしトラフィックおよびタグ付きトラフィックが、ポートで設定されたスタティック VLAN メンバーシップに基づいてブリッジされます。

許可ポートからのタグなしトラフィックが、認証プロセス中にRADIUSサーバによって割り当てられた VLAN に再マッピングされるようにユーザが指定できます。この場合、VLAN タグが RADIUS によって割り当てられた VLAN または認証されていない VLAN である場合を除いて、タグ付きトラフィックはドロップされます。

スイッチは、認証ステータスが許可から無許可に変更されたときに、ポートで学習されたすべての MAC アドレスを FDB から削除します。

マルチセッション モード

シングルホストモードやマルチホストモード（ポートベース モード）とは異なり、マルチセッションモードでは、ポートに接続された各ホストの認証ステータスが管理されます（セッションベース モード）。ポートでマルチセッション モードが設定されている場合、ポートには認証ステータスがあります。任意の数のホストをポートで許可できます。dot1x max-hosts コマンドでは、ポートで許可される承認済みホストの最大数を制限できます。

各承認済みクライアントには、TCAM ルールが必要です。TCAM に使用可能な領域がない場合、認証は拒否されます。

認証が有効になっているときに **dot1x host-mode** コマンドを使用してポート モードを **single-host** または **multi-host** に変更すると、ポート ステートが無許可に設定されます。

認証が有効になっているときに **dot1x host-mode** コマンドでポート モードを **multi-session** に変更すると、接続されているすべてのホストのステートが無許可に設定されます。

ポート モードを single-host または multi-host に変更するには、ポートを force-unauthorized に設定し（**dot1x port-control**）、ポート モードを single-host または multi-host に変更して、ポートを authorization auto に設定します。

マルチセッション モードと、次のコマンドで設定されるポリシー ベース VLAN を同時に同じインターフェイスに設定することはできません。

- switchport general map protocol-group vlans
- switchport general map macs-group vlans

未認証 VLAN に属するタグ付きトラフィックは、ホストが承認済みかどうかに関わらず、常にブリッジされます。

ゲスト VLAN が有効になっている場合、認証されていない VLAN に属していない許可されていないホストからのタグなしトラフィックおよびタグ付きトラフィックは、ゲスト VLAN を介してブリッジされます。

許可ホストからのトラフィックは、ポートのスタティック設定に従ってブリッジされます。認証されていない VLAN に属していない許可ホストからのタグなしトラフィックおよびタグ付きトラフィックが、認証プロセス中に RADIUS サーバによって割り当てられた VLAN に再マッピングされるようにユーザが指定できます。

スイッチは、認証ステータスが許可から無許可に変更されたときに、ポートで学習されたホスト MAC アドレスを FDB から削除しません。エージング タイムアウトになると、MAC アドレスが削除されます。

ポートチャネルに関連付けられたポートで有効になっている 802.1X には、次の制限があります。

- 802.1X ベースの認証のみがサポートされます。
- マルチホスト（レガシー 802.1X モード）モードのみがサポートされます。

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x host-mode multi-host
```

dot1x mac-auth

MAC ベースの認証で使用するタイプ（EAP または RADIUS）と MAC ベースのユーザ名形式を指定するには、グローバル コンフィギュレーション モードで **dot1x mac-auth** コマンドを使用します。デフォルトの設定をリセットするには、このコマンドの **no** 形式を使用します。

構文

dot1x mac-auth {**eap** | **radius**} [**username groupsize** {**1**|**2**|**4**|**12**} **separator** {**-** | **:** |**.** } [**lowercase** | **uppercase**]]

no dot1x mac-auth

パラメータ

- **eap**：EAP MD5 チャレンジ認証を使用するように指定します。
- **radius**：サービスタイプ属性が Call-Check(10) の RADIUS（EAP なし）認証のみを使用するように指定します。
- **username**：ユーザ名の形式を指定します。キーワードを設定していない場合、小文字で区切り文字がない形式が適用されます。

username groupsize 12 separator - lowercase

- **groupsize**：デリミタ間の ASCII 文字の数を指定します。
- **separator**：デリミタを指定します。
- **lowercase**：ユーザ名を小文字でコーディングするように指定します。引数は、case 引数を設定していない場合に適用されます。
- **uppercase**：ユーザ名を大文字でコーディングするように指定します。

デフォルト設定

EAP MD5 チャレンジ認証

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

スイッチは、ユーザ名とパスワードとしてホスト MAC アドレスを使用する次の 2 種類の MAC ベースの認証をサポートしています。

- EAP MD5 チャレンジ認証。
- Call-Check(10) に相当するサービスタイプ属性と ASCII 形式のユーザ名とパスワードを使用した純粋な RADIUS 認証。

EAP MD5 チャレンジ認証タイプを指定するには、**eap** キーワードを使用します。

純粋な RADIUS 認証タイプを指定するには、**radius** キーワードを使用します。純粋な RADIUS 認証は次の RADIUS 属性を使用します。

- User-Name：ホスト MAC アドレス
- Password
- Service-Type：Call-Check(10)
- Frame-MTU
- Called-Station-Id：スイッチの MAC アドレス
- Calling-Station-Id：ホストの MAC アドレス
- Message-Authentication
- NAS-Port-Type：Ethernet(15)
- NAS-Port：ホストが接続されているポートの ifIndex
- NAS-Port-Id：ホストが接続されているポートの完全な CLI 名（GigabitEthernet2/0/2 など）
- NAS-IP-Address：スイッチの IP アドレス

ユーザ名属性の形式を指定するには、**username** キーワードを使用します。次の表に、MAC アドレス 08002b8619de のユーザ名コーディングの例を示します。

表 *3:* ユーザ名コーディングの例

Size	区切り文字（Separator）	ユーザ名
1	-	0-8-0-0-2-b-8-6-1-9-d-e
2	:	08:00:2b:86:19:de
4	.	0800.2b86.19de
12	該当なし	08002b8619de

ユーザ名の形式または認証タイプ（EAP または RADIUS）を変更すると、再認証が行われます。

例 1。次に、MAC ベースの認証で純粋な RADIUS 認証を使用するように指定し、ステーションの MAC アドレスに基づいてユーザ名に使用する属性を指定します。

switchxxxxxx(config)# dot1x mac-auth radius username groupsize 2 separator : uppercase

例 2。次に、MAC ベースの認証で EAP MD5 チャレンジ認証を使用するように指定する例を示します。ユーザ名の形式は、区切り文字なしの形式で小文字に設定されます。

```
switchxxxxxx(config)# dot1x mac-auth eap
```

dot1x mac-auth password

MAC ベースの認証のグローバルパスワードを指定するには、グローバル コンフィギュレーション モードで **dot1x mac-auth password** コマンドを使用します。パスワードを削除するには、このコマンドの **no** 形式を使用します。

構文

encrypted dot1x mac-auth password *encrypted-password*

dot1x mac-auth password *password*

no dot1x mac-auth password

パラメータ

- ***encrypted-password***：暗号化形式のパスワード。
- ***password***：最大 32 文字のパスワード。

デフォルト設定

ユーザー名。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用して、ホスト MAC アドレスの代わりに MAC ベースの認証に使用するパスワードを指定します。

パスワードまたはその形式を変更すると、再認証が行われます。

例

次に、MAC ベースの認証のグローバルパスワードを設定する例を示します。

```
switchxxxxxx(config)# dot1x mac-auth password 87b$#9hv5*
```

dot1x max-hosts

インターフェイスに許可される承認済みホストの最大数を設定するには、インターフェイス コンフィギュレーション モードで **dot1x max-hosts** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x max-hosts *count*

no dot1x max-hosts

パラメータ

- ***count***：インターフェイスで許可される許可ホストの最大数を指定します。32 ビットの正の数を使用できます。

デフォルト設定

制限されていません。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

デフォルトでは、インターフェイス上で許可される許可ホストの数は制限されていません。インターフェイス上で許可される許可ホストの数を制限するには、**dot1x max-hosts** コマンドを使用します。

このコマンドは、マルチセッション モードにのみ関係します。

例

次に、イーサネット ポート gi1/0/1 上の許可ホストの最大数を 6 に制限する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x max-hosts 6
```

dot1x max-login-attempts

許可されるログイン試行の最大数を設定するには、インターフェイス コンフィギュレーション モードで **dot1x max-login-attempts** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x max-login-attempts *count*

no dot1x max-login-attempts

パラメータ

- ***count***：許可されるログイン試行の最大回数を指定します。0 の値は、試行回数に制限がないことを意味します。有効な範囲は 3 ～ 10 です。

デフォルト設定

無制限

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

デフォルトでは、スイッチは失敗したログイン試行の回数を制限しません。ログイン試行の失敗が許可される回数を指定するには、このコマンドを使用します。

このコマンドは Web ベースの認証にのみ適用されます。

例

次の例では、許可されるログイン試行の最大回数を 5 回に設定しています。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x max-login-attempts 5
```

dot1x max-req

（応答がない場合）認証プロセスが再起動されるまでに、デバイスが Extensible Authentication Protocol（EAP）request/identity フレームをクライアントに送信する最大回数を設定するには、インターフェイス コンフィギュレーション モードで **dot1x max-req** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x max-req *count*

no dot1x max-req

パラメータ

- ***count***：デバイスが、認証プロセスを再始動する前に、EAP-Request/Identity フレームを送信する最大回数を設定します。（範囲：1 ～ 10）。

デフォルト設定

デフォルトの最大試行回数は 2 回です。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対応する場合にのみ、変更する必要があります。

例

次の例では、デバイスが EAP Request/Identity フレームを送信する最大回数を 6 回に設定しています。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x max-req 6
```

dot1x page customization

Web ベース ページ カスタマイズ コンフィギュレーション モードにするには、グローバル コンフィギュレーション モードで **dot1x page customization** コマンドを使用します。

構文

dot1x page customization

デフォルト設定

ユーザのカスタマイズは未設定です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、（コピーして貼り付けを使用しない限り）手動で入力または編集しないでください。スイッチが生成する設定ファイルの一部です。

ユーザは、ブラウザ インターフェイスを使用して、Web ベースの認証ページをカスタマイズする必要があります。

例

次の例は、Webベースのページカスタマイズコンフィギュレーションの一部を示しています。

```
switchxxxxxx(config)# dot1x page customization
switchxxxxxx(config-web-page)# data 1feabcde
switchxxxxxx(config-web-page)# data 17645874
switchxxxxxx(config-web-page)# exit
```

dot1x port-control

ポートの承認状態の手動コントロールを有効にするには、インターフェイス コンフィギュレーション モードで **dot1x port-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x port-control {auto | **force-authorized** | **force-unauthorized**} [**time-range** *time-range-name*]

no dot1x port-control

パラメータ

- **auto**：ポートで 802.1X 認証を有効にし、デバイスおよびクライアント間の 802.1X 認証交換に基づきポートを許可ステートまたは無許可ステートに移行します。
- **force-authorized**：インターフェイスで 802.1X 認証を無効にし、認証交換を必要とせずにポートを許可ステートに移行します。ポートは 802.1X ベースのクライアント認証なしでトラフィックを送受信します。
- **force-unauthorized**：ポートを強制的に無許可ステートに移行し、クライアントからの認証試行をすべて無視して、このポート経由のすべてのアクセスを拒否します。デバイスはこのポートを介してクライアントに認証サービスを提供できません。
- **time-range** *time-range-name*：時間範囲を指定します。時間範囲が有効でない場合、ポートは無許可ステートになります。（範囲：1 ～ 32 文字）。

デフォルト設定

ポートは force-authorized ステートです。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

同じインターフェイスでポートセキュリティ機能がすでに有効になっている場合は、インターフェイスで 802.1X 認証を有効にすることはできません。

スイッチは、認証制御が **force-authorized** から別のものに変更されたときに、ポートで学習されたすべての MAC アドレスを削除します。

（注） 認証が成功したらただちにフォワーディング ステートに進むことができるように、エンド ステーションに接続されている **auto** ステートの 802.1X エッジ ポートでスパニング ツリーを無効にするか、スパニング ツリー PortFast モードを有効にすることを推奨します。

例

次に、gi1/0/1 の 802.1X 認証を auto モードに設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x port-control auto
```

dot1x radius-attributes vlan

RADIUS ベース VLAN 割り当てを有効にするには、インターフェイス コンフィギュレーション モードで **dot1x radius-attributes vlan** コマンドを使用します。RADIUS ベース VLAN 割り当てを無効にするには、このコマンドの **no** 形式を使用します。

構文

dot1x radius-attributes vlan [**reject** | **static**]

no dot1x radius-attributes vlan

パラメータ

- **reject**：RADIUS サーバがサプリカントを許可し、サプリカント VLAN を提供しなかった場合、サプリカントは拒否されます。このパラメータを省略すると、このオプションがデフォルトで適用されます。
- **static**：RADIUS サーバがサプリカントを許可し、サプリカント VLAN を提供しなかった場合、サプリカントは承認されます。

デフォルト設定

reject

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

RADIUS が無効な VLAN 情報を提供した場合、認証は拒否されます。

RADIUS サーバが存在しない VLAN をクライアントに割り当てた場合は、スイッチが VLAN を作成します。この VLAN は使用されなくなった時点で削除されます。

RADIUS が有効な VLAN 情報を提供し、そのポートが RADIUS から受信した VLAN に属していない場合は、タグなし出力ポートとして VLAN に追加されます。VLAN に割り当てられている最後に許可されたクライアントが無許可になった場合、またはポート上で 802.1x が無効になっている場合、そのポートは VLAN から除外されます。

認証モードがシングルホストまたはマルチホストの場合、PVID の値は VLAN_ID に設定されます。

シングルホスト モードまたはマルチホスト モードの許可ポートのステータスが無許可に変更されると、ポートのスタティック設定がリセットされます。

認証モードがマルチセッション モードの場合、PVID は変更されず、非認証 VLAN に属していないすべてのタグなしトラフィックおよびタグ付きトラフィックが、TCAM を使用して VLAN にマッピングされます。

マルチセッション モードでポートに接続されている RADIUS から受信した VLAN に割り当てられている最後に許可されたホストのステータスが無許可に変更されると、ポートがスタティック設定でない場合は、VLAN から削除されます。

詳細については、**dot1x host-mode** コマンドのユーザ ガイドラインを参照してください。

802.1X が無効になっている場合は、ポートのスタティック設定がリセットされます。

reject キーワードが設定されていて、RADIUS サーバがホストを許可し、RADIUS 承認メッセージがサプリカントに VLAN を割り当てない場合、認証は拒否されます。

static キーワードが設定されていて、RADIUS サーバがホストを許可した場合は、RADIUS 受け入れメッセージでサプリカントに VLAN が割り当てられなくても、認証が承認され、ホストからのトラフィックがポートのスタティック設定に従ってブリッジされます。

許可ポートまたはホストがある場合にこのコマンドを使用すると、それ以降の認証で有効になります。手動で再認証するには、**dot1x re-authenticate** コマンドを使用します。

例 1。この例では、ユーザベース VLAN 割り当てを有効にします。RADIUS サーバがサプリカントを許可し、サプリカント VLAN を提供しなかった場合、サプリカントは拒否されます。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x radius-attributes vlan
switchxxxxxx(config-if)# exit
```

例 2。この例では、ユーザベース VLAN 割り当てを有効にします。RADIUS サーバがサプリカントを許可し、サプリカント VLAN を提供しなかった場合、サプリカントは承認され、スタティック VLAN 設定が使用されます。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x radius-attributes static
switchxxxxxx(config-if)# exit
```

dot1x re-authenticate

すべての 802.1X 対応ポートまたは指定した 802.1X 対応ポートの再認証を手動で開始するには、特権 EXEC モードで **dot1x re-authenticate** コマンドを使用します。

構文

dot1x re-authenticate [*interface-id*]

パラメータ

- ***interface-id***：イーサネット ポートまたは OOB ポートを指定します。

デフォルト設定

ポートが指定されていない場合は、すべてのポートにコマンドが適用されます。

コマンド モード

特権 EXEC モード

例

次に、802.1X 対応の gi1/0/1 の再認証を手動で開始するコマンドを示します。

```
switchxxxxxx# dot1x re-authenticate gi1/0/1
```

dot1x reauthentication

クライアントの定期的な再認証を有効にするには、インターフェイス コンフィギュレーション モードで **dot1x reauthentication** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x reauthentication

no dot1x reauthentication

デフォルト設定

定期的な再認証は無効です。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x reauthentication
```

dot1x supplicant

特定のインターフェイスの dot1x サプリカントロールを有効にするには、インターフェイス コンフィギュレーション モードで **dot1x supplicant** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x supplicant *name*

no dot1x supplicant

パラメータ

- ***name***：インターフェイスに適用するログイン情報の構造体の名前。

デフォルト設定

サプリカントロールは無効です。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

特定のインターフェイスで dot1x サプリカントを有効にするには、**dot1x supplicant** コマンドを使用します。サプリカントがインターフェイスで有効になっている場合、そのインターフェイスは未承認のインターフェイスになります。802.1X 認証が成功すると、インターフェイスの状態が承認済みに変更されます。

name 引数が未定義か、または完全に定義されていない（パスワードまたはユーザ名が設定されていない）802.1X ログイン情報の構造体を指定している場合、コマンドは拒否されます。

同じインターフェイス上でオーセンティケータとサプリカントを同時に有効にすることはできません。

同じポートでコマンドを複数回設定することはできません。設定したログイン情報を置き換えるには、新しいログイン情報を設定する前に、このコマンドの **no** 形式を使用します。

未承認のオーセンティケータ インターフェイスとは異なり、未承認のサプリカントインターフェイスは通過するトラフィックを制限しません。

次のイベントにより、ポートで 802.1X サプリカント認証が開始されます。

- **dot1x supplicant** コマンドは、UP ステータスのポートでサプリカントを有効にします。
- ポートのステータスが UP に変更され、そのポートでサプリカントが有効になります。
- EAP 識別子要求メッセージをポートで受信すると、そのポートでサプリカントが有効になります。

例

次に、ポート gi1/0/1 で 802.1X サプリカントを設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x supplicant upstream-port
```

dot1x supplicant traps authentication failure

802.1X サプリカント認証が失敗した場合にトラップの送信を有効にするには、グローバル コンフィギュレーション モードで **dot1x supplicant traps authentication failure** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x supplicant traps authentication failure

no dot1x supplicant traps authentication failure

デフォルト設定

トラップが無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

トラップには次のようにレート制限が適用されます。このタイプでは、10秒間に複数のトラップを送信できません。

例

次に、802.1Xサプリカント認証が失敗した場合にトラップの送信を有効にする例を示します。

```
switchxxxxxx(config)# dot1x supplicant traps authentication failure
```

dot1x supplicant traps authentication success

802.1X サプリカント認証が成功した場合にトラップの送信を有効にするには、グローバル コンフィギュレーション モードで **dot1x supplicant traps authentication success** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x supplicant traps authentication success

no dot1x supplicant traps authentication success

デフォルト設定

トラップが無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

トラップには次のようにレート制限が適用されます。このタイプでは、10秒間に複数のトラップを送信できません。

例

次に、802.1Xサプリカント認証が成功した場合にトラップの送信を有効にする例を示します。

```
switchxxxxxx(config)# dot1x supplicant traps authentication success
```

dot1x system-auth-control

802.1X をグローバルに有効にするには、グローバル コンフィギュレーション モードで **dot1x system-auth-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x system-auth-control

no dot1x system-auth-control

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、802.1X をグローバルに有効にしています。

```
switchxxxxxx(config)# dot1x system-auth-control
```

dot1x timeout eap-timeout

EAP タイムアウトを設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout eap-timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x timeout eap-timeout *seconds*

no dot1x timeout eap-timeout

パラメータ

- ***seconds***：要求が再転送されるまで EAP サーバ（EAP オーセンティケータ）が EAP クライアント（EAP ピア）からの応答を待つ時間間隔を指定します（秒単位）。（範囲：1 ～ 65535 秒）。

デフォルト設定

デフォルトのタイムアウト期間は 30 秒です。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対応する場合にのみ、変更する必要があります。

パラメータは 802.1x サプリカントで使用されます。

例

次に、EAP タイムアウトを 45 秒に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout eap-timeout 45
```

dot1x timeout quiet-period

デバイスが、認証交換に失敗した後に待機状態になる時間間隔を設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout quiet-period** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

パラメータ

- ***seconds***：クライアントとの認証交換が失敗した後にデバイスが待機状態を維持する時間間隔を秒単位で指定します。（範囲：10 ～ 65535 秒）。

デフォルト設定

デフォルトの待機時間は 60 秒です。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

待機時間中は、デバイスが認証要求を受け入れることも開始することもありません。

このコマンドのデフォルト値は、リンクの信頼性が低い場合や、特定のクライアントまたは認証サーバに特定の動作上の問題がある場合など、異常な状況に適応する場合にのみ変更するようにしてください。

より高速な応答時間をユーザに提供するには、デフォルト値よりも小さい数値を入力する必要があります。

802.1x および MAC ベースの認証の場合、失敗したログインの回数は 1 回です。

Web ベースの認証では、試行が複数回失敗した後に、待機時間が適用されます。

802.1x ベースおよび MAC ベースの認証方式では、試行が失敗するたびに待機時間が適用されます。

例

次の例では、認証交換に失敗した後にデバイスが待機状態を維持する時間間隔を、120 秒に設定しています。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout quiet-period 120
```

dot1x timeout reauth-period

再認証の試行間隔を秒単位で指定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout reauth-period** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x timeout reauth-period seconds

no dot1x timeout reauth-period

パラメータ

- **reauth-period** seconds：再認証試行間の秒数。（範囲：300 ～ 4294967295）。

デフォルト設定

3600

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

このコマンドは、802.1x 認証方式のみに適用されます。

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout reauth-period 5000
```

dot1x timeout server-timeout

デバイスが認証サーバからの応答を待つ時間間隔を設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout server-timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

パラメータ

- **server-timeout** *seconds*：デバイスが認証サーバからの応答を待機する時間間隔を秒単位で指定します。（範囲：1 ～ 65535 秒）。

デフォルト設定

デフォルトのタイムアウト期間は 30 秒です。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

実際のタイムアウト期間は、このコマンドによって指定した値と、radius-server transmit コマンドによって指定したタイムアウト期間で radius-server retransmit コマンドによって指定した再試行回数を乗算した結果と比較し、この 2 つの値の低い方を選択することで決定されます。

例

次の例では、認証サーバへのパケットの再送信の時間間隔を 3600 秒に設定しています。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout server-timeout 3600
```

dot1x timeout silence-period

認証サイレンス時間を設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout silence-period** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x timeout silence-period *seconds*

no dot1x timeout silence-period

パラメータ

- ***seconds***：サイレンス間隔を秒単位で指定します。有効な範囲は 60 ～ 65535 です。

デフォルト設定

サイレンス期間は制限されていません。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

サイレンス時間は、承認済みクライアントがこの期間にトラフィックを送信しないと、未承認に変更になる期間（秒単位）です。

承認済みクライアントが、このコマンドで指定したサイレンス期間にトラフィックを送信しないと、クライアントの状態が未承認に変更されます。

このコマンドは、Web ベース認証にのみ適用されます。

例

次の例では、認証のサイレンス時間を 100 秒に設定しています。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout silence-period 100
```

dot1x timeout supp-timeout

デバイスが要求を再送信するまでに、Extensible Authentication Protocol（EAP）request フレームに対するクライアントの応答を待つ時間間隔を設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout supp-timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

パラメータ

- **supp-timeout** *seconds*：要求を再送信する前にクライアントからの EAP Request フレームへの応答をデバイスが待機する時間間隔を秒単位で指定します。（範囲：1 ～ 65535 秒）。

デフォルト設定

デフォルトのタイムアウト期間は 30 秒です。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対応する場合にのみ、変更する必要があります。

このコマンドは、802.1x 認証方式のみに適用されます。

例

次の例では、要求を再送信する前にクライアントからの EAP Request フレームへの応答をデバイスが待機する時間間隔を、3600 秒に設定しています。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout supp-timeout 3600
```

dot1x timeout supplicant-held-period

RADIUS サーバから FAIL 応答を受信した後に認証を再開するまでサプリカントが待機する期間を設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout supplicant-held-period** コマンドを使用します。デフォルト設定を復元するには、このコマンドの **no** 形式を使用します。

構文

dot1x timeout supplicant-held-period *seconds*

no dot1x timeout supplicant-held-period

パラメータ

- ***seconds***：RADIUS サーバから FAIL 応答を受信した後に認証を再開するまでサプリカントが待機する期間を指定します。（範囲：1 ～ 65535 秒）。

デフォルト設定

デフォルトのタイムアウト期間は 60 秒です。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対応する場合にのみ、変更する必要があります。

例

次に、RADIUS サーバから FAIL 応答を受信した後に認証を再開するまでサプリカントが待機する期間を 70 秒に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout supplicant-held-period 70
```

dot1x timeout tx-period

デバイスが要求を再送信するまでに、Extensible Authentication Protocol（EAP）request/identity フレームに対するクライアントの応答を待つ時間間隔を設定するには、インターフェイス コンフィギュレーション モードで **dot1x timeout tx-period** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

パラメータ

- ***seconds***：要求を再送信する前にクライアントからの EAP-Request/Identity フレームへの応答をデバイスが待機する時間間隔を秒単位で指定します。（範囲：30 ～ 65535 秒）。

デフォルト設定

デフォルトのタイムアウト期間は 30 秒です。

コマンド モード

インターフェイス（イーサネット、OOB）コンフィギュレーション モード

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対応する場合にのみ、変更する必要があります。

このコマンドは、802.1x 認証方式のみに適用されます。

例

次のコマンドでは、EAP Request/Identity フレームへの応答をデバイスが待機する時間間隔を、60 秒に設定しています。

```
switchxxxxxx(config)# interface gi1/0/1:
switchxxxxxx(config-if)# dot1x timeout tx-period 60
```

dot1x traps authentication failure

802.1X認証方式の失敗時のトラップ送信を有効にするには、グローバル コンフィギュレーション モードで **dot1x traps authentication failure** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x traps authentication failure {[**802.1x**] [**mac**] [**web**]}

no dot1x traps authentication failure

パラメータ

- **802.1x**：802.1X ベース認証のトラップを有効にします。
- **mac**：MAC ベース認証のトラップを有効にします。
- **web**：WEB ベース認証のトラップを有効にします。

デフォルト設定

すべてのトラップが無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

キーワードの組み合わせに制限はありません。少なくとも1つのキーワードを設定する必要があります。

トラップには次のようにレート制限が適用されます。このタイプでは、10秒間に複数のトラップを送信できません。

例

次の例では、802.1X MAC 認証アクセス コントロールによる MAC アドレスの許可に失敗した場合のトラップ送信を有効にしています。

```
switchxxxxxx(config)# dot1x traps authentication failure 802.1x
```

dot1x traps authentication quiet

ログイン試行に最大連続回数失敗した後、ホスト状態が待機状態に設定された場合にトラップ送信を有効にするには、グローバル コンフィギュレーション モードで **dot1x traps authentication quiet** コマンドを使用します。このトラップを無効にするには、このコマンドの **no** 形式を使用します。

構文

dot1x traps authentication quiet

no dot1x traps authentication quiet

デフォルト設定

待機トラップが無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

トラップは、ログインの最大連続試行回数の後に、クライアントが待機状態に設定されると送信されます。

トラップには次のようにレート制限が適用されます。このタイプでは、10秒間に複数のトラップを送信できません。

例

次の例では、ホストが待機状態に設定されたときのトラップ送信を有効にしています。

```
switchxxxxxx(config)# dot1x traps authentication quiet
```

dot1x traps authentication success

ホストが802.1X認証方式によって正常に承認された場合にトラップの送信を有効にするには、グローバル コンフィギュレーション モードで **dot1x traps authentication success** コマンドを使用します。このトラップを無効にするには、このコマンドの **no** 形式を使用します。

構文

dot1x traps authentication success {[**802.1x**] [**mac**] [**web**]}

no dot1x traps authentication success

パラメータ

- **802.1x**：802.1X ベース認証のトラップを有効にします。
- **mac**：MAC ベース認証のトラップを有効にします。
- **web**：WEB ベース認証のトラップを有効にします。

デフォルト設定

成功トラップが無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

キーワードの組み合わせに制限はありません。少なくとも1つのキーワードを設定する必要があります。

トラップには次のようにレート制限が適用されます。このタイプでは、10秒間に複数のトラップを送信できません。

例

次の例では、802.1X MAC 認証アクセス コントロールにより MAC アドレスが正常に許可された場合のトラップ送信を有効にしています。

```
switchxxxxxx(config)# dot1x traps authentication success mac
```

dot1x unlock client

ロックされた（待機期間中の）クライアントをロック解除するには、特権EXECモードで**dot1x unlock client** コマンドを使用します。

構文

dot1x unlock client *interface-id mac-address*

パラメータ

- ***interface-id***：クライアントが接続されているインターフェイス ID。
- ***mac-address***：クライアント MAC アドレス。

デフォルト設定

クライアントは、待機時間が終わるまでロックされています。

コマンド モード

特権 EXEC モード

使用上のガイドライン

許可された認証の最大失敗試行回数の後でロックされたクライアントのロックを解除し、待機時間を終了するには、このコマンドを使用します。クライアントが待機時間でない場合、このコマンドは影響を与えません。

例

```
switchxxxxxx# dot1x unlock client gi1/0/1 00:01:12:af:00:56
```

dot1x violation-mode

シングルホストモードの承認済みポートの未承認ホストがインターフェイスへのアクセスを試行する場合のアクションを設定するには、インターフェイス コンフィギュレーション モードで **dot1x violation-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

dot1x violation-mode {restrict | protect | shutdown} [**traps** *seconds*]

no dot1x violation-mode

パラメータ

- **restrict**：MAC アドレスがサプリカント MAC アドレスではないステーションがインターフェイスへのアクセスを試みると、トラップを生成します。トラップ間の最小時間は1秒です。これらのフレームは転送されますが、送信元アドレスは学習されません。
- **protect**：サプリカント アドレスではない送信元アドレスを持つフレームを廃棄します。
- **shutdown**：サプリカントアドレスではない送信元アドレスを持つフレームを廃棄し、ポートをシャットダウンします。
- **trap** *seconds*：SNMP トラップを送信し、連続するトラップ間の最小時間を指定します。seconds を 0 にした場合、トラップは無効になります。このパラメータを指定しない場合、デフォルトは制限モードでは 1 秒になり、その他のモードでは 0 になります。

デフォルト設定

protect

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

このコマンドは、シングルホスト モードにのみ関係します。

保護モードでは、MAC アドレスがサプリカント MAC アドレスではない BPDU メッセージが廃棄されません。

シャットダウンモードでは、MACアドレスがサプリカントMACアドレスではないBPDUメッセージによりシャットダウンが行われます。

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x violation-mode protect
```

password

802.1X ログイン情報の構造体のパスワードを指定するには、Dot1x ログイン情報コンフィギュレーション モードで **password** コマンドを使用します。パスワードを削除するには、このコマンドの **no** 形式を使用します。

構文

encrypted password *encrypted-password*

password *password*

no password

パラメータ

- ***encrypted-password***：暗号化形式のパスワード。
- ***password***：最大 64 文字のパスワード。

デフォルト設定

パスワードが指定されていません。

コマンド モード

Dot1x ログイン情報コンフィギュレーション モード。

使用上のガイドライン

サプリカント（クライアント）として設定する場合は、802.1X ログイン情報の構造体が必要です。このログイン情報の構造体には、ユーザ名とパスワードが含まれている必要があり、説明が含まれている場合があります。

例

次に、802.1X ログイン情報の構造体を設定する例を示します。

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password 87b$#9hv5*
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
 connect to site-A.
```

show dot1x

802.1Xインターフェイスまたは指定したインターフェイスのステータスを表示するには、特権EXEC モードで **show dot1x** コマンドを使用します。

構文

show dot1x [interface interface-id **| detailed]**

パラメータ

- ***interface-id***：イーサネット ポートまたは OOB ポートを指定します。
- **detailed**：現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのポートについて表示します。**detailed** を使用しない場合、現在のポートだけが表示されます。

コマンド モード

特権 EXEC モード

例

次に、802.1x が有効になっているすべてのインターフェイスの認証情報を表示する例を示します。

```
switchxxxxxx# show dot1x
Authentication is enabled
Authenticator Global Configuration:
Authenticating Servers: Radius, None
MAC-Based Authentication:
  Type: Radius
  Username Groupsize: 2
  Username Separator: -
  Username case: Lowercase
  Password: MD5 checksum 1238af77aaca17568f12988601fcabed
Unathenticated VLANs: 100, 1000, 1021
Guest VLAN: VLAN 11, timeout 30 sec
Authentication failure traps are enabled for 802.1x+mac
Authentication success traps are enabled for 802.1x
Authentication quiet traps are enabled for 802.1x
Supplicant Global Configuration:
Supplicant Authentication failure traps are enabled
Supplicant Authentication success traps are enabled
gi1/0/1
  Authenticator is enabled
  Supplicant is disabled
  Authenticator Configuration:
  Host mode: multi-sessions
  Authentication methods: 802.1x+mac
  Port Adminstrated status: auto
  Guest VLAN: enabled
```

```
  VLAN Radius Attribute: enabled, static
  Open access: disabled
  Time range name: work_hours (Active now)
  Server-timeout: 30 sec
  Maximum Hosts: unlimited
  Maximum Login Attempts: 3
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
    max-req: 2
  Authentication success: 9
  Authentication fails: 1
  Number of Authorized Hosts: 10
  Supplicant Configuration:
  retry-max: 2
  EAP time period: 15 sec
  Supplicant Held Period: 30 sec
gi1/0/2
  Authenticator is enabled
  Supplicant is disabled
  Authenticator Configuration:
  Host mode: single-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: auto
  Port Operational status: authorized
  Guest VLAN: disabled
  VLAN Radius Attribute: enabled
  Open access: enabled
  Time range name: work_hours (Active now)
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
    Mode: restrict
    Trap: enabled
    Trap Min Interval: 20 sec
    Violations were detected: 9
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
    max-req: 2
  Authentication success: 2
  Authentication fails: 0
gi1/0/3
  Authenticator is enabled
  Supplicant is disabled
  Authenticator Configuration:
  Host mode: multi-host
  Authentication methods: 802.1x+mac
```

```
  Port Adminstrated status: auto
  Port Operational status: authorized
  Guest VLAN: disabled
  VLAN Radius Attribute: disabled
  Time range name: work_hours (Active now)
  Open access: disabled
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
    Mode: restrict
    Trap: enabled
    Trap Min Interval: 20 sec
    Violations were detected: 0
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
    max-req: 2
  Authentication success: 20
  Authentication fails: 0
  Supplicant Configuration:
  retry-max: 2
  EAP time period: 15 sec
  Supplicant Held Period: 30 sec
gi1/0/4
  Authenticator is disabled
  Supplicant is enabled
  Authenticator Configuration:
  Host mode: multi-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: force-auto
  Guest VLAN: disabled
  VLAN Radius Attribute: disabled
  Time range name: work_hours (Active now)
  Open access: disabled
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
    Mode: restrict
    Trap: enabled
    Trap Min Interval: 20 sec
    Violations were detected: 0
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
```

```
  max-req: 2
Authentication success: 0
Authentication fails: 0
Supplicant Configuration:
retry-max: 2
EAP time period: 15 sec
Supplicant Held Period: 30 sec
Credentials Name: Basic-User
Supplicant Operational status: authorized
```

次に、この出力で表示される重要なフィールドについて説明します。

- **Port**：ポートのインターフェイス ID。
- **Host mode**：ポート認証の設定されたモード。使用される値は、single-host、multi-host、multi-sessions です。
  - single-host
  - multi-host
  - multi-sessions
- **Authentication methods**：ポートで設定されている認証方式。使用される値は、次の方式の組み合わせです。
  - 802.1x
  - mac
  - wba
- **Port Administrated status**：ポートの管理（設定済み）モード。使用可能な値：**force-auth**、**force-unauth**、**auto**。
- **Port Operational status**：ポートの動作（実際の）モード。使用可能な値：**authorized** または **unauthorized**。
- **Username**：サプリカントアイデンティティを表すユーザ名。ポート制御が自動の場合は、このフィールドにユーザ名が表示されます。ポートが許可されている場合は、現在のユーザのユーザ名が表示されます。ポートが許可されていない場合は、最後に正常に認証されたユーザが表示されます。
- **Quiet period**：クライアントが無効なパスワードを提供した場合など、認証交換が失敗した後にデバイスが待機状態を維持する秒数。
- **Silence period**：このコマンドにより指定されたサイレンス期間中に許可クライアントがトラフィックを送信しなかった場合、そのクライアントが無許可ステートに変更される秒数。
- **EAP timeout**：要求が再送信されるまで EAP サーバ（EAP オーセンティケータ）が EAP クライアント（EAP ピア）からの応答を待つ時間間隔（秒単位）。
- **EAP Max Retrans**：EAP クライアント（EAP ピア）からの応答がない場合に、EAP サーバ（EAP オーセンティケータ）が EAP 要求を再送信する最大回数。

- **Tx period**：デバイスが Extensible Authentication Protocol（EAP）Request/Identity フレームに対するクライアントからの応答を待機し、要求を再送信するまでの秒数。
- **Max req**：（クライアントから応答が得られなかった場合に）デバイスが認証プロセスを再起動する前に、クライアントに EAP Request フレームを送信する最大回数。
- **Server timeout**：デバイスが認証サーバからの応答を待機し、要求を再送信するまでの秒数。
- **Session Time**：ユーザがログインしている時間の長さ（HH:MM:SS）。
- **MAC address**：サプリカント MAC アドレス。
- **Authentication success**：ステート マシンが認証サーバから成功メッセージを受信した回数。
- **Authentication fails**：ステート マシンが認証サーバから失敗メッセージを受信した回数。

show dot1x credentials

802.1X ログイン情報を表示するには、特権 EXEC モードで **show dot1x credentials mode** コマンドを使用します。

構文

show dot1x credentials

コマンド モード

特権 EXEC モード

例

次に、dot1x ログイン情報を表示する例を示します。

```
switchxxxxxx# show dot1x credentials
downstream-interface
 description: should be used for downstream ports
 username: downstream
 password's MD5: 1238af77aaca17568f12988601fcabed
upstream-interface
 description: should be used for connection to ISP
 username: up2isp
 password's MD5: 1238bbff75431230965394466ac76549
```

show dot1x locked clients

ロックされ、待機期間中のすべてのクライアントを表示するには、特権 EXEC モードで **show dot1x locked clients** コマンドを使用します。

構文

show dot1x locked clients

コマンド モード

特権 EXEC モード

使用上のガイドライン

ロックされている（待機時間中の）すべてのクライアントを表示するには、**show dot1x locked clients** コマンドを使用します。

例

次の例では、ロックされているクライアントを表示しています。

```
switchxxxxxx# show dot1x locked clients
```

Port	MAC Address	Remaining Time
-------	--------------	--------------
gi1/0/1	0008.3b79.8787	20
gi1/0/1	0008.3b89.3128	40
gi1/0/2	0008.3b89.3129	10

show dot1x statistics

指定したポートの 802.1X 統計情報を表示するには、特権 EXEC モードで **show dot1x statistics** コマンドを使用します。

構文

show dot1x statistics interface *interface-id*

パラメータ

- ***interface-id***：イーサネット ポートまたは OOB ポートを指定します。

コマンド モード

特権 EXEC モード

例

次に、gi1/0/1 の 802.1X 統計情報を表示する例を示します。

```
switchxxxxxx# show dot1x statistics interface gi1/0/1
EapolEapFramesRx: 10
EapolStartFramesRx: 0
EapolLogoffFramesRx: 1
EapolAnnouncementFramesRx: 0
EapolAnnouncementReqFramesRx: 0
EapolInvalidFramesRx: 0
EapolEapLengthErrorFramesRx: 0
EapolMkNoCknFramesRx: 0
EapolMkInvalidFramesRx: 0
EapolLastRxFrameVersion: 3
EapolLastRxFrameSource: 00:08:78:32:98:78
EapolSuppEapFramesTx: 0
EapolStartFramesTx: 1
EapolLogoffFramesTx: 0
EapolAnnouncementFramesTx: 0
EapolAnnouncementReqFramesTx: 0
EapolAuthEapFramesTx: 9
EapolMkaFramesTx: 0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

フィールド	説明
EapolInvalidFramesRx	この PAE で受信したすべてのタイプの無効な EAPOL フレームの数。
EapolEapLengthErrorFramesRx	パケット本文の長さがこの PAE で受信した EAPOL MPDU のオクテット内に含まれているパケット本文と一致しない EAPOL フレームの数。
EapolAnnouncementFramesRx	この PAE で受信した EAPOL-Announcement フレームの数。

フィールド	説明
EapolAnnouncementReqFramesRx	この PAE で受信した EAPOL-Announcement-Req フレームの数。
EapolStartFramesRx	この PAE で受信した EAPOL-Start フレームの数。
EapolEapFramesRx	この PAE で受信した EAPOL-EAP フレームの数。
EapolLogoffFramesRx	この PAE で受信した EAPOL-Logoff フレームの数。
EapolMkNoCknFramesRx	この PAE で MKA が有効になっていないか、CKN が認識されない状態で受信した MKPDU の数。
EapolMkInvalidFramesRx	この PAE の受信プロセスでメッセージ認証が失敗した MKPDU の数。
EapolLastRxFrameVersion	この PAE で最後に受信した EAPOL フレームのバージョン。
EapolLastRxFrameSource	この PAE で最後に受信した EAPOL フレームの送信元 MAC アドレス。
EapolSuppEapFramesTx	この PAE のサプリカントで送信した EAPOL-EAP フレームの数。
EapolLogoffFramesTx	この PAE で送信した EAPOL-Logoff フレームの数。
EapolAnnouncementFramesTx	この PAE で送信した EAPOL-Announcement フレームの数。
EapolAnnouncementReqFramesTx	この PAE で送信した EAPOL-Announcement-Req フレームの数。
EapolStartFramesTx	この PAE で受信した EAPOL-Start フレームの数。
EapolAuthEapFramesTx	この PAE の認証で送信した EAPOL-EAP フレームの数。
EapolMkaFramesTx	この PAE で送信した CKN 情報のない EAPOL-MKA フレームの数。

show dot1x users

デバイスのアクティブな 802.1X 承認済みユーザを表示するには、特権 EXEC モードで **show dot1x users** コマンドを使用します。

構文

show dot1x users [username *username*]

パラメータ

- **username username**：サプリカントユーザ名（長さ：1 ～ 160 文字）を指定します。

デフォルト設定

すべてのユーザを表示します。

コマンド モード

特権 EXEC モード

例 1。次のコマンドは、すべての 802.1x ユーザを表示します。

```
show dot1x users
```

Port	ユーザ名	MAC Address	Auth Method	Auth Server	Session Time	VLAN
gi1/0/1	Bob	0008.3b71.1111	802.1x	Remote	09:01:00	1020
gi1/0/2	00083b798787	0008.3b79.8787	MAC	Remote	00:11:12	
gi1/0/2	John	0008.3baa.0022	WBA	Remote	00:27:16	

例 2。次の例では、サプリカント ユーザ名が Bob の 802.1X ユーザを表示します。

```
switchxxxxxx# show dot1x users username Bob
```

Port	ユーザ名	MAC Address	Auth Method	Auth Server	Session Time	VLAN
gi1/0/1	Bob	0008.3b71.1111	802.1x	Remote	09:01:00	1020

username（dot1x ログイン情報）

802.1X ログイン情報の構造体のユーザ名を指定するには、Dot1x ログイン情報コンフィギュレーション モードで **username** コマンドを使用します。ユーザ名を削除するには、このコマンドの **no** 形式を使用します。

構文

username *username*

no username

パラメータ

- ***username***：最大 32 文字のユーザ名。

デフォルト設定

ユーザ名が指定されていません。

コマンド モード

Dot1x ログイン情報コンフィギュレーション モード。

使用上のガイドライン

サプリカント（クライアント）として設定する場合は、802.1X ログイン情報の構造体が必要です。このログイン情報の構造体には、ユーザ名、パスワード、および説明を含めることができます。

例

次に、802.1X ログイン情報の構造体を設定する例を示します。

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password 87%$#bgd98^
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
 connected to site-A
```

ACL コマンド

この章は、次の項で構成されています。

- ip access-list（IP 拡張） （90 ページ）
- permit (IP) （91 ページ）
- deny（IP） （94 ページ）
- ipv6 access-list（IPv6 拡張） （97 ページ）
- permit（IPv6） （98 ページ）
- deny（IPv6） （101 ページ）
- mac access-list （104 ページ）
- permit（MAC） （105 ページ）
- deny（MAC） （107 ページ）
- service-acl input （109 ページ）
- service-acl output （111 ページ）
- time-range （113 ページ）
- absolute （115 ページ）
- periodic （116 ページ）
- show time-range （117 ページ）
- show access-lists （118 ページ）
- clear access-lists counters （119 ページ）
- show interfaces access-lists trapped packets （120 ページ）
- ip access-list（IP 標準） （121 ページ）
- ipv6 access-list（IP 標準） （123 ページ）

ip access-list（IP 拡張）

IPv4 アクセス リスト（ACL）に名前を付けてデバイスを IPv4 アクセス リスト コンフィギュレーション モードにするには、**ip access-list extended** グローバル コンフィギュレーション モードコマンドを使用します。このコマンドに続くすべてのコマンドは、この ACL を参照します。この ACL のルール（ACE）は、permit (IP) （91 ページ） および deny（IP） （94 ページ） コマンドで定義されます。service-acl input （109 ページ） コマンドは、この ACL をインターフェイスに適用する場合に使用します。

アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

構文

ip access-list extended *acl-name*

no ip access-list extended *acl-name*

パラメータ

- **acl-name**：IPv4 アクセス リストの名前。（範囲：1 ～ 32 文字）

デフォルト設定

定義されている IPv4 アクセス リストはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

IPv4 ACL は一意の名前で定義されます。IPv4 ACL、IPv6 ACL、MAC ACL または ポリシー マップには、同じ名前を使用できません。

例

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)#
```

permit (IP)

IPv4 アクセス リスト（ACL）の許可条件を設定するには、**permit** IP アクセス リスト コンフィギュレーション モード コマンドを使用します。許可条件は、アクセス コントロール エントリ（ACE）とも呼ばれます。アクセス コントロール エントリを削除するには、コマンドの no 形式を使用します。

構文

permit *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

permit *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]] [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

permit *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*] [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

permit tcp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*}{**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]**

permit udp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*} {**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard}* [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit tcp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*}{**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]**

no permit udp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*} {**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

パラメータ

- ***protocol***：IP プロトコルの名前または番号。利用可能なプロトコル名は、icmp、igmp、ip、tcp、egp、igp、udp、hmp、rdp、idpr、ipv6、ipv6:rout、ipv6:frag、idrp、rsvp、gre、esp、ah、ipv6:icmp、eigrp、ospf、ipinip、pim、l2tp、isis です。任意のプロトコルを照合するには、**ip** キーワードを使用します（範囲：0 ～ 255）。
- ***source***：パケットの送信元 IP アドレス。

- ***source-wildcard***：送信元 IP アドレスに適用されるワイルドカードビット。無視するビット位置に使用します。
- ***destination***：パケットの宛先 IP アドレス。
- ***destination-wildcard***：宛先 IP アドレスに適用されるワイルドカードビット。無視するビット位置に使用します。
- ***priority***：アクセスコントロールリスト（ACL）内のアクセスコントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- **dscp** *number*：DSCP 値を指定します。
- **precedence** *number*：IP プレシデンス値を指定します。
- ***icmp-type***：ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。番号または次の値のいずれかを入力します。echo-reply、destination-unreachable、source-quench、redirect、alternate-host-address、echo-request、router-advertisement、router-solicitation、time-exceeded、parameter-problem、timestamp、timestamp-reply、information-request、information-reply、address-mask-request、address-mask-reply、traceroute、datagram-conversion-error、mobile-host-redirect、mobile-registration-request、mobile-registration-reply、domain-name-request、domain-name-reply、skip、photuris。（範囲：0 ～ 255）
- ***icmp-code***：ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。（範囲：0 ～ 255）
- ***igmp-type***：IGMP パケットは、IGMP メッセージ タイプでフィルタ処理できます。番号または次の値のいずれかを入力します。host-query、host-report、dvmrp、pim、cisco-trace、host-report-v2、host-leave-v2、host-report-v3。（範囲：0 ～ 255）
- ***destination-port***：UDP/TCP 宛先ポートを指定します。ポートの範囲を入力するには、ハイフンを使用します。例：20-21。TCP の場合は番号か次の値のいずれかを入力します。bgp (179)、chargen (19)、daytime (13)、discard (9)、domain (53)、drip (3949)、echo (7)、finger (79)、ftp (21)、ftp-data (20)、gopher (70)、hostname (42)、irc (194)、klogin (543)、kshell (544)、lpd (515)、nntp (119)、pop2 (109)、pop3 (110)、smtp (25)、sunrpc (1110)、syslog (514)、tacacs-ds (49)、talk (517)、telnet (23)、time (37)、uucp (117)、whois (43)、www (80)。UDP の場合は、番号または次の値の 1 つを入力します：biff (512)、bootpc (68)、bootps (67)、discard (9)、dnsix (90)、domain (53)、echo (7)、mobile-ip (434)、nameserver (42)、netbios-dgm (138)、netbios-ns (137)、on500-isakmp (4500)、ntp (123)、rip (520)、snmp (161)、snmptrap (162)、sunrpc (111)、syslog (514)、tacacs-ds (49)、talk (517)、tftp (69)、time (37)、who (513)、xdmcp (177)。（範囲：0 ～ 65535）。
- ***source-port***：UDP/TCP 送信元ポートを指定します。定義済みポート名は、destination-port パラメータで定義されます。（範囲：0 ～ 65535）
- **match-all** *list-of-flags*：発生する必要のある TCP フラグのリスト。フラグを設定する場合は「+」を前に付けます。フラグを設定しない場合は「-」を前に付けます。使用可能なオプ

ションは +urg、+ack、+psh、+rst、+syn、+fin、-urg、-ack、-psh、-rst、-syn および -fin です。フラグは、1 つの文字列に連結されます。例：+fin-ack。

- **time-range-name**：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- **log-input**：エントリに一致するパケットに関する情報 SYSLOG メッセージを送信することを指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

デフォルト設定

定義されている IPv4 アクセス リストはありません。

コマンド モード

IP アクセスリスト コンフィギュレーション モード

使用上のガイドライン

ある範囲のポートが ACE の送信元ポートに使用されている場合、別の ACE の送信元ポートにも使用されていれば再びカウントされません。ポートの範囲が ACE の宛先ポートに使用される場合、別の ACE の宛先ポートに使用されていても、再カウントはされません。

ポートの範囲が送信元ポートに使用される場合、宛先ポートにも使用されていると、再カウントされます。

ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

例

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# permit ip 176.212.0.0 00.255.255 any
```

deny（IP）

IPv4 アクセス リストの拒否条件を設定するには、**deny** IP アクセス リスト コンフィギュレーション モード コマンドを使用します。拒否条件は、アクセス コントロール エントリ（ACE）とも呼ばれます。アクセス コントロール エントリを削除するには、コマンドの no 形式を使用します。

構文

deny *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port**|**log-input**]

deny *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]][**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

deny *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*][**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

deny tcp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*}{**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**match-all** *list-of-flags*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

deny udp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*} {**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input** *]*

no deny *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

no deny *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

no deny *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input** *]*

no deny tcp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*}{**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**dscp** *number* | **precedence** *number*][**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**disable-port** |**log-input**]

no deny udp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*} {**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

パラメータ

- ***protocol***：IP プロトコルの名前または番号。利用可能なプロトコル名は、icmp、igmp、ip、tcp、egp、igp、udp、hmp、rdp、idpr、ipv6、ipv6:rout、ipv6:frag、idrp、rsvp、gre、esp、ah、ipv6:icmp、eigrp、ospf、ipinip、pim、l2tp、isis です。任意のプロトコルを照合するには、Ip キーワードを使用します。（範囲：0 ～ 255）

- ***source***：パケットの送信元 IP アドレス。
- ***source-wildcard***：送信元 IP アドレスに適用されるワイルドカードビット。無視するビット位置に使用します。
- ***destination***：パケットの宛先 IP アドレス。
- ***destination-wildcard***：宛先 IP アドレスに適用されるワイルドカードビット。無視するビット位置に使用します。
- ***priority***：アクセスコントロールリスト（ACL）内のアクセスコントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- **dscp** *number*：DSCP 値を指定します。
- **precedence** *number*：IP プレシデンス値を指定します。
- ***icmp-type***：ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。番号または次の値のいずれかを入力します。echo-reply、destination-unreachable、source-quench、redirect、alternate-host-address、echo-request、router-advertisement、router-solicitation、time-exceeded、parameter-problem、timestamp、timestamp-reply、information-request、information-reply、address-mask-request、address-mask-reply、traceroute、datagram-conversion-error、mobile-host-redirect、mobile-registration-request、mobile-registration-reply、domain-name-request、domain-name-reply、skip、photuris。（範囲：0 ～ 255）
- ***icmp-code***：ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。（範囲：0 ～ 255）
- ***igmp-type***：IGMP パケットは、IGMP メッセージ タイプでフィルタ処理できます。番号または次の値のいずれかを入力します。host-query、host-report、dvmrp、pim、cisco-trace、host-report-v2、host-leave-v2、host-report-v3。（範囲：0 ～ 255）
- ***destination-port***：UDP/TCP 宛先ポートを指定します。ポートの範囲を入力するには、ハイフンを使用します。例：20-21。TCP の場合は番号か次の値のいずれかを入力します。bgp (179)、chargen (19)、daytime (13)、discard (9)、domain (53)、drip (3949)、echo (7)、finger (79)、ftp (21)、ftp-data (20)、gopher (70)、hostname (42)、irc (194)、klogin (543)、kshell (544)、lpd (515)、nntp (119)、pop2 (109)、pop3 (110)、smtp (25)、sunrpc (1110)、syslog (514)、tacacs-ds (49)、talk (517)、telnet (23)、time (37)、uucp (117)、whois (43)、www (80)。UDP の場合は、番号または次の値の 1 つを入力します：biff (512)、bootpc (68)、bootps (67)、discard (9)、dnsix (90)、domain (53)、echo (7)、mobile-ip (434)、nameserver (42)、netbios-dgm (138)、netbios-ns (137)、non500-isakmp (4500)、ntp (123)、rip (520)、snmp (161)、snmptrap (162)、sunrpc (111)、syslog (514)、tacacs-ds (49)、talk (517)、tftp (69)、time (37)、who (513)、xdmcp (177)。（範囲：0 ～ 65535）
- ***source-port***：UDP/TCP 送信元ポートを指定します。定義済みポート名は、destination-port パラメータで定義されます。（範囲：0 ～ 65535）

- **match-all** *list-of-flags*：発生する必要のある TCP フラグのリスト。フラグのセットが必要な場合は、「+」を先頭に付けます。フラグのセット解除が必要な場合は、「-」を先頭に付けます。使用可能なオプションは+urg、+ack、+psh、+rst、+syn、+fin、-urg、-ack、-psh、-rst、-syn および -fin です。フラグは、1 つの文字列に連結されます。例：+fin-ack。
- **time-range-name**：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- **disable-port**：この条件に一致する場合、イーサネット インターフェイスは無効になります。
- **log-input**：エントリに一致するパケットに関する情報 syslog メッセージを送信するように指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

デフォルト設定

定義されている IPv4 アクセス リストはありません。

コマンド モード

IP アクセスリスト コンフィギュレーション モード

使用上のガイドライン

ACL で定義可能な TCP/UDP 範囲の数は制限されています。ある範囲のポートが ACE の送信元ポートに使用されている場合、別の ACE の送信元ポートにも使用されていれば再びカウントされません。ポートの範囲が ACE の宛先ポートに使用される場合、別の ACE の宛先ポートに使用されていても、再カウントはされません。

ある範囲のポートが送信元ポートに使用されている場合、宛先ポートにも使用されていれば再びカウントされます。

ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

例

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# deny ip 176.212.0.0 00.255.255 any
```

ipv6 access-list（IPv6 拡張）

IPv6 アクセス リスト（ACL）を定義して、デバイスを IPv6 アクセス リスト コンフィギュレーション モードにするには、**ipv6 access-list** グローバル コンフィギュレーション モード コマンドを使用します。このコマンドに続くすべてのコマンドは、この ACL を参照します。

アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 access-list [*acl-name]*

no ipv6 access-list *[acl-name]*

パラメータ

acl-name：IPv6 アクセス リストの名前。範囲：1 ～ 32 文字。

デフォルト設定

IPv6 アクセス リストは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

IPv6 ACL は一意の名前で定義されます。IPv4 ACL、IPv6 ACL、MAC ACL または ポリシー マップには、同じ名前を使用できません。

すべての IPv6 ACL には最後の一致条件として、暗黙の **permit icmp any any nd-ns any**、**permit icmp any any nd-na any**、および **deny ipv6 any any** ステートメントがあります（前の 2 つの一致条件は、ICMPv6 ネイバー探索を許可します）。

IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを使用します。したがって、デフォルトでは IPv6 ACL により、IPv6 ネイバー探索パケットのインターフェイス上での送受信が暗黙的に許可されます。IPv4 では、IPv6 ネイバー探索プロセスと同等のアドレス解決プロトコル（ARP）は、別のデータリンク層プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

例

```
switchxxxxxx(config)#  ipv6 access-list acl1
switchxxxxxx(config-ip-al)#  permit tcp 2001:0DB8:0300:0201::/64 any any 80
```

permit（IPv6）

IPv6 ACL の許可条件（ACE）を設定するには、Ipv6 アクセス リスト コンフィギュレーション モードで **permit** コマンドを使用します。アクセス コントロール エントリを削除するには、コマンドの **no** 形式を使用します。

構文

permit *protocol* {**any** |{*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input**] [**flow-label** *flow-label-value*]

permit icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

permit tcp {**any** | {*source-prefix*/*length*} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any** | *destination-port*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

permit udp {any | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any** | *destination-port*} [**ace-priority** *priority*][**dscp** *number* | precedence *number*][**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit *protocol* {**any** |{*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit tcp {**any** | {*source-prefix*/*length*} {**any** | source-port}}{**any** | destination- prefix/length} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit udp {**any** | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

パラメータ

- ***protocol***：IP プロトコルの名前または番号。使用可能なプロトコル名は、icmp (58)、tcp (6) および udp (17) です。任意のプロトコルに一致させるには、ipv6 キーワードを使用します。（範囲：0 ～ 255）
- ***source-prefix / lenght***：許可条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。この引数は、RFC 3513 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
- ***destination-prefix / lenght***：許可条件を設定する宛先 IPv6 ネットワークまたはネットワークのクラス。この引数は、RFC 3513 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。

- ***priority***：アクセスコントロールリスト（ACL）内のアクセスコントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- ***dscp number***：DSCP 値を指定します。(範囲：0 ～ 63)
- ***precedence number***：IP プレシデンス値を指定します。
- ***icmp-type***：ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。番号または次の値のいずれかを入力します。destination-unreachable (1)、packet-too-big (2)、time-exceeded (3)、parameter-problem (4)、echo-request (128)、echo-reply (129)、mld-query (130)、mld-report (131)、mldv2-report (143)、mld-done (132)、router-solicitation (133)、router-advertisement (134)、nd-ns (135)、nd-na (136)。（範囲：0 ～ 255）
- ***icmp-code***：ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。（範囲：0 ～ 255）
- ***destination-port***：UDP/TCP宛先ポートを指定します。TCP の場合は番号か次の値のいずれかを入力します。bgp (179)、chargen (19)、daytime (13)、discard (9)、domain (53)、drip (3949)、echo (7)、finger (79)、ftp (21)、ftp-data (20)、gopher (70)、hostname (42)、irc (194)、klogin (543)、kshell (544)、lpd (515)、nntp (119)、pop2 (109)、pop3 (110)、smtp (25)、sunrpc (1110)、syslog (514)、tacacs-ds (49)、talk (517)、telnet (23)、time (37)、uucp (117)、whois (43)、www (80)。UDP の場合は番号か次の値のいずれかを入力します。biff (512)、bootpc (68)、bootps (67)、discard (9)、dnsix (90)、domain (53)、echo (7)、mobile-ip (434)、nameserver (42)、netbios-dgm (138)、netbios-ns (137)、non500-isakmp (4500)、ntp (123)、rip (520)、snmp (161)、snmptrap (162)、sunrpc (111)、syslog (514)、tacacs (49)、talk (517)、tftp (69)、time (37)、who (513)、xdmcp (177)。（範囲：0 ～ 65535）
- ***source-port***：UDP/TCP 送信元ポートを指定します。定義済みポート名は、destination-port パラメータで定義されます。（範囲：0 ～ 65535）
- ***match-all list-of-flag***：発生するはずの TCP フラグのリスト。フラグのセットが必要な場合は、「+」を先頭に付けます。フラグのセット解除が必要な場合は、「-」を先頭に付けます。使用可能なオプションは+urg、+ack、+psh、+rst、+syn、+fin、-urg、-ack、-psh、-rst、-syn および -fin です。フラグは、1 つの文字列に連結されます。例：+fin-ack。
- ***time-range-name***：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- **log-input**：エントリに一致するパケットに関する情報 syslog メッセージを送信するように指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。
- **flow-label** *flow-label-value*：IPv6 フローラベル値を指定します。これらの引数の値は、0 ー 1048575 の範囲にする必要があります。

デフォルト設定

IPv6 アクセス リストは定義されていません。

コマンド モード

Ipv6 アクセス リスト コンフィギュレーション モード

使用上のガイドライン

ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

フローラベルとポート範囲を同時に設定することはできません。

フローラベルは出力 ACL には設定できません。

例 1。この例では、サーバの名前で ACL を定義し、tcp パケット用のルール（ACE）を入力しています。

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# permit tcp 3001::2/64 any any 80
```

例 2。次に、**flow-label** キーワードを指定して ACL を定義する例を示します。

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# permit ipv6 any any flow-label 5
```

deny（IPv6）

IPv6 ACL の拒否条件（ACE）を設定するには、IPv6 アクセスリスト コンフィギュレーション モードで **deny** コマンドを使用します。アクセス コントロール エントリを削除するには、コマンドの no 形式を使用します。

構文

deny *protocol* {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} [**ace-priority** *priority]*[**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

deny icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

deny tcp {**any** | {*source-prefix*/*length*} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

deny udp {**any** | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} *[***ace-priority** *priority]*[**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny *protocol* {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny tcp {**any** | {*source-prefix*/*length*} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny udp {**any** | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

パラメータ

- ***protocol***：IP プロトコルの名前または番号。使用可能なプロトコル名は、icmp (58)、tcp (6) および udp (17) です。任意のプロトコルに一致させるには、ipv6 キーワードを使用します。（範囲：0 ～ 255）
- ***source-prefix*/*length***：許可条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。この引数は、RFC 3513 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
- ***destination-prefix / lenght***：許可条件を設定する宛先 IPv6 ネットワークまたはネットワークのクラス。この引数は、RFC 3513 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。

- ***priority***：アクセスコントロールリスト（ACL）内のアクセスコントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- ***dscp number***：DSCP 値を指定します。(範囲：0 ～ 63)
- ***precedence number***：IP プレシデンス値を指定します。
- ***icmp-type***：ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。番号または次の値のいずれかを入力します。destination-unreachable (1)、packet-too-big (2)、time-exceeded (3)、parameter-problem (4)、echo-request (128)、echo-reply (129)、mld-query (130)、mld-report (131)、mldv2-report (143)、mld-done (132)、router-solicitation (133)、router-advertisement (134)、nd-ns (135)、nd-na (136)。（範囲：0 ～ 255）
- ***icmp-code***：ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。（範囲：0 ～ 255）
- ***destination-port***：UDP/TCP宛先ポートを指定します。TCPの場合は、番号または次の値の 1 つを入力します：bgp (179)、chargen (19)、daytime (13)、discard (9)、domain (53)、drip (3949)、echo (7)、finger (79)、ftp (21)、ftp-data (20)、gopher (70)、hostname (42)、irc (194)、klogin (543)、kshell (544)、lpd (515)、nntp (119)、pop2 (109)、pop3 (110)、smtp (25)、sunrpc (1110)、syslog (514)、tacacs-ds (49)、talk (517)、telnet (23)、time (37)、uucp (117)、whois (43)、www (80)。UDP の場合は番号か次の値のいずれかを入力します。biff (512)、bootpc (68)、bootps (67)、discard (9)、dnsix (90)、domain (53)、echo (7)、mobile-ip (434)、nameserver (42)、netbios-dgm (138)、netbios-ns (137)、non500-isakmp (4500)、ntp (123)、rip (520)、snmp (161)、snmptrap (162)、sunrpc (111)、syslog (514)、tacacs (49)、talk (517)、tftp (69)、time (37)、who (513)、xdmcp (177)。（範囲：0 ～ 65535）
- ***source-port***：UDP/TCP 送信元ポートを指定します。定義済みポート名は、destination-port パラメータで定義されます。（範囲：0 ～ 65535）
- ***match-all list-of-flags***：発生する TCP フラグのリスト。フラグのセットが必要な場合は、「+」を先頭に付けます。フラグのセット解除が必要な場合は、「-」を先頭に付けます。使用可能なオプションは +urg、+ack、+psh、+rst、+syn、+fin、-urg、-ack、-psh、-rst、-syn および -fin です。フラグは、1 つの文字列に連結されます。例：+fin-ack。
- ***time-range-name***：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- ***disable-port***：この条件に一致する場合、イーサネット インターフェイスは無効になります。
- ***log-input***：エントリに一致するパケットに関する情報 syslog メッセージを送信することを指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。
- ***flow-label flow-label-value***：IPv6 フローラベル値を指定します。これらの引数の値は、0 ー 1048575 の範囲にする必要があります。

デフォルト設定

IPv6 アクセス リストは定義されていません。

コマンド モード

Ipv6 アクセス リスト コンフィギュレーション モード

使用上のガイドライン

ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priorityは、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

フローラベルとポート範囲を同時に設定することはできません。

フローラベルは出力 ACL には設定できません。

例

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# deny tcp 3001::2/64 any any 80
```

mac access-list

送信元 MAC アドレス フィルタに基づいてレイヤ 2 アクセス リスト（ACL）を定義し、デバイスを MAC アクセス リスト コンフィギュレーション モードにするには、**mac access-list** グローバル コンフィギュレーション モード コマンドを使用します。このコマンドに続くすべてのコマンドは、この ACL を参照します。

アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

構文

mac access-list extended *acl-name*

no mac access-list extended *acl-name*

パラメータ

acl-name：MAC ACL の名前を指します（範囲：1 ～ 32 文字）。

デフォルト設定

定義されている MAC アクセス リストはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

MAC ACL は一意の名前で定義されます。IPv4 ACL、IPv6 ACL、MAC ACL、またはポリシーマップに同じ名前を付けることはできません。ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

例

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

permit（MAC）

MAC ACL の許可条件（ACE）を設定するには、MAC アクセス リスト コンフィギュレーション モードで **permit** コマンドを使用します。アクセス コントロール エントリを削除するには、コマンドの no 形式を使用します。

構文

permit *{***any** | *source source-wildcard} {***any** | *destination destination-wildcard} [***ace-priority** *priority][eth-type 0* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000***] [***vlan** *vlan-id] [***cos** *cos cos-wildcard] [***time-range** *time-range-name]*

*[***log-input]**

no permit *{***any** | *source source-wildcard} {***any** | *destination destination-wildcard} [eth-type 0* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000***] [***vlan** *vlan-id] [***cos** *cos cos-wildcard] [***time-range** *time-range-name]*

*[***log-input]**

パラメータ

- ***source***：パケットの送信元 MAC アドレス。
- ***source-wildcard***：送信元MACアドレスに適用されるワイルドカード ビット。無視するビット位置に使用します。
- ***destination***：パケットの宛先 MAC アドレス。
- ***destination-wildcard***：宛先 MAC アドレスに適用されるワイルドカード ビット。無視するビット位置に使用します。
- ***priority***：アクセスコントロールリスト（ACL）内のアクセス コントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- ***eth-type***：パケットのイーサネット タイプ（16 進表記）。
- ***vlan-id***：パケットの VLAN ID。（範囲：1 ～ 4094）
- ***cos***：パケットのサービス クラス。（範囲：0 ～ 7）
- ***cos-wildcard***：CoS に適用されるワイルドカード ビット。
- ***time-range-name***：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- **log-input**：エントリに一致するパケットに関する情報 syslog メッセージを送信するように指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

使用上のガイドライン

MAC ACL は一意の名前で定義されます。IPv4 ACL、IPv6 ACL、MAC ACL またはポリシーマップを同じ名前にすることはできません。ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

デフォルト設定

定義されている MAC アクセス リストはありません。

コマンド モード

MAC アクセスリスト コンフィギュレーション モード

例

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

deny（MAC）

MAC ACL の拒否条件（ACE）を設定するには、MAC アクセス リスト コンフィギュレーション モードで **deny** コマンドを使用します。アクセス コントロール エントリを削除するには、コマンドの no 形式を使用します。

構文

deny *{***any** | *source source-wildcard} {***any** | *destination destination-wildcard} [***ace-priority** *priority][{eth-type 0}|* **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000***] [***vlan** *vlan-id] [***cos** *cos cos-wildcard] [***time-range** *time-range-name] [***disable-port** |**log-input** *]*

no deny *{***any** | *source source-wildcard} {***any** | *destination destination-wildcard} [{eth-type 0}|* **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000***] [***vlan** *vlan-id] [***cos** *cos cos-wildcard] [***time-range** *time-range-name] [***disable-port** |**log-input** *]*

パラメータ

- ***source***：パケットの送信元 MAC アドレス。
- ***source-wildcard***：送信元MACアドレスに適用されるワイルドカードビット。無視するビット位置に使用します。
- ***destination***：パケットの宛先 MAC アドレス。
- ***destination-wildcard***：宛先 MAC アドレスに適用されるワイルドカード ビット。無視するビット位置に使用します。
- ***priority***：アクセスコントロールリスト（ACL）内のアクセスコントロールエントリ（ACE）の優先順位を指定します。「1」の値が最も高い優先順位を表し、「2147483647」の値が最も低い優先順位を表します（範囲：1 ～ 2147483647）。
- ***eth-type***：パケットのイーサネット タイプ（16 進表記）。
- ***vlan-id***：パケットの VLAN ID。（範囲：1 ～ 4094）
- ***cos***：パケットのサービス クラス。（範囲：0 ～ 7）。
- ***cos-wildcard***：CoS に適用されるワイルドカード ビット。
- ***time-range-name***：この許可ステートメントに適用される時間範囲の名前。（範囲：1 ～ 32）
- ***disable-port***：この条件に一致する場合、イーサネット インターフェイスは無効になります。
- ***log-input***：エントリに一致するパケットに関する情報 syslog メッセージを送信することを指定します。転送またはドロップはハードウェアで、ロギングはソフトウェアで実行されます。したがって、log-input キーワードを含む ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

デフォルト設定

定義されている MAC アクセス リストはありません。

コマンド モード

MAC アクセスリスト コンフィギュレーション モード

使用上のガイドライン

MAC ACL は一意の名前で定義されます。IPv4 ACL、IPv6 ACL、MAC ACL、またはポリシーマップに同じ名前を付けることはできません。

ace-priority を省略した場合、ルールの優先順位は現在の最優先 ACE（現在の ACL 内）+ 20 に設定されます。ace-priority は、ACL ごとに一意である必要があります。ユーザがすでに存在する優先順位を入力した場合、コマンドは拒否されます。

例

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# deny 00:00:00:00:00:01 00:00:00:00:00:ff any
```

service-acl input

アクセスリスト（ACL）をインターフェイスにバインドするには、インターフェイス コンフィギュレーション モードで **service-acl input** コマンドを使用します。

インターフェイスからすべての ACL を削除するには、このコマンドの **no** 形式を使用します。

構文

service-acl input *acl-name1* [*acl-name2*] [**default-action** {**deny-any** | **permit-any**}]

no service-acl input

パラメータ

- ***acl-name***：インターフェイスに適用する ACL を指定します。ユーザ ガイドラインを参照してください。（範囲：1 ～ 32 文字）。
- **deny-any**：この ACL のルールを満たさないすべてのパケット（ポートで入力されたもの）を拒否します。
- **permit-any**：この ACL のルールを満たさないすべてのパケット（ポートで入力されたもの）を転送します。

デフォルト設定

ACL は割り当てられていません。ACL のデフォルトアクションは deny-any です。

コマンド モード

インターフェイス コンフィギュレーション モード（イーサネット、ポートチャネル、VLAN）

使用上のガイドライン

どのような場合に ACL をインターフェイスにバインドできるか、またはインターフェイスからバインド解除できるかは、次のルールに従います。

- IPv4 ACL と IPv6 ACL は、インターフェイスに一緒にバインドできます。
- MAC ACL は、すでに IPv4 ACL または IPv6 ACL がバインドされているインターフェイスにバインドすることはできません。
- 同じタイプの 2 つの ACL をポートにバインドすることはできません。
- まず現在の ACL を削除することなく、ACL にすでにバインドされているポートに ACL をバインドすることはできません。このコマンドでは、両方の ACL を同時に指定する必要があります。
- 一致基準として VLAN を含む MAC ACL は、VLAN にバインドできません。

- いずれかの ACE に時間ベースの設定が使用されている ACL を VLAN にバインドすることはできません。
- シャットダウン アクションが使用されている ACL は VLAN にバインドできません。
- ユーザが ACL をインターフェイスにバインドすると、TCAM リソースが使用されます。MAC または IP ACE ごとに 1 つの TCAM ルール、IPv6 ACE ごとに 2 つの TCAM ルールが使用されます。TCAM の使用量は常に偶数になるため、ルールの数が奇数になった場合は、使用量が 1 増えます。
- ACL は、出力としてバインドされている場合、入力としてバインドできません。

例

```
switchxxxxxx(config)# mac access-list extended server-acl
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# service-acl input server-acl default-action deny-any
```

service-acl output

出力（伝送パス）上のインターフェイスへのアクセスを制御するには、インターフェイス コンフィギュレーション モードで **service-acl output** コマンドを使用します。

アクセス制御を削除するには、このコマンドの **no** 形式を使用します。

構文

service-acl output *acl-name1* [*acl-name2*] [**default-action** {**deny-any** | **permit-any**}]

no service-acl output

パラメータ

- ***acl-name***：インターフェイスに適用する ACL を指定します。ユーザ ガイドラインを参照してください。（範囲：1 ～ 32 文字）。
- **deny-any**：この ACL のルールを満たさない（ポートの出力上の）すべてのパケットを拒否します。
- **permit-any**：この ACL のルールを満たさない（ポートの出力上の）すべてのパケットを転送します。

デフォルト

ACL は割り当てられていません。デフォルトアクションは deny-any です。

コマンド モード

インターフェイス コンフィギュレーション モード（イーサネット、ポートチャネル）

使用上のガイドライン

ルールアクション：log-input はサポートされていません。使用しようとすると、エラーになります。

拒否ルールアクションの disable-port はサポートされていません。使用しようとすると、エラーになります。

IPv4 ACL と IPv6 ACL は、インターフェイス上でバインドできます。

MAC ACL は IPv4 ACL または IPv6 ACL とインターフェイス上でバインドできません。

同じタイプの 2 つの ACL をポートに追加することはできません。

現在の ACL を最初に削除して 2 つの ACL をバインドせずに、すでに ACL にバインドされているポートに ACL を追加することはできません。

入力としてバインドされている ACL は出力としてバインドできません。

例

次に、出力 ACL をポートにバインドする例を示します。

```
switchxxxxxx(config)# mac access-list extended server
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# service-acl output server
```

time-range

さまざまな機能の時間範囲を定義するには、**time-range** グローバル コンフィギュレーション モード コマンドを使用します。また、このコマンドを使用すると時間範囲コンフィギュレーション モードになります。このコマンドの後は、すべてのコマンドが定義されている時間範囲を参照します。

このコマンドは、時間範囲の名前を設定します。実際の時間範囲を設定するには、absolute（115 ページ） コマンドと periodic（116 ページ） コマンドを使用します。

デバイスから時間範囲を削除する場合は、このコマンドの **no** 形式を使用します。

構文

time-range *time-range-name*

no time-range *time-range-name*

パラメータ

time-range-name：時間範囲の名前を指定します。（範囲：1 ～ 32 文字）

デフォルト設定

時間範囲は定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

time-range コマンドに absolute 値と periodic 値の両方が指定されている場合、periodic 項目は absolute start 時刻を経過した後にのみ評価の対象になり、absolute end 時刻を経過した後は再度評価の対象にはなりません。

すべての時間指定は、現地時間と解釈されます。

時間範囲のエントリを希望の時間に有効にするには、ユーザまたは SNTP がソフトウェア クロックを設定する必要があります。ユーザまたはSNTPがソフトウェア クロックを設定しない場合、時間範囲 ACE は有効になりません。

ユーザは、機能にバインドされている時間範囲を削除することはできません。

時間範囲が定義されている場合は、次のコマンドで使用できます。

- dot1x port-control
- power inline
- operation time
- permit (IP)

- deny (IP)
- permit（IPv6）
- deny（IPv6）
- permit（MAC）
- deny（MAC）

例

```
switchxxxxxx(config)# time-range http-allowed
console(config-time-range)#periodic mon 12:00 to wed 12:00
```

absolute

時間範囲が有効になっている場合に絶対時間を指定するには、**absolute** 時間範囲コンフィギュレーション モード コマンドを使用します。時間制限を削除するには、このコマンドの **no** 形式を使用します。

構文

absolute *start* *hh:mm day month year*

no absolute *start*

absolute *end* *hh:mm day month year*

no absolute *end*

パラメータ

- **start**：関連付けられた機能の許可ステートメントまたは拒否ステートメントが有効になる絶対日時。start 日時が指定されていない場合、その機能はただちに有効になります。
- **end**：関連付けられた機能の許可ステートメントまたは拒否ステートメントが有効でなくなる絶対日時。end 日時が指定されていない場合、その機能は無期限に有効になります。
- **hh:mm**：時間（24 時間形式）および分単位の時刻（範囲：0 ～ 23、mm：0 ～ 5）。
- **day**：日付。（範囲：1 ～ 31）
- **month**：月（名前の最初の 3 文字）。（範囲：Jan ～ Dec）
- **year**：年（省略なし）（範囲：2000 ～ 2097）

デフォルト設定

時間範囲が有効になっている場合の絶対時間はありません。

コマンド モード

時間範囲コンフィギュレーション モード

例

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# absolute start 12:00 1 jan 2005
switchxxxxxx(config-time-range)# absolute end 12:00 31 dec 2005
```

periodic

時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定するには、**periodic** 時間範囲コンフィギュレーション モード コマンドを使用します。時間制限を削除するには、このコマンドの **no** 形式を使用します。

構文

periodic *day-of-the-week hh:mm* **to** *day-of-the-week hh:mm*

no periodic *day-of-the-week hh:mm* **to** *day-of-the-week hh:mm*

periodic list *hh:mm* **to** *hh:mm day-of-the-week1 [day-of-the-week2… day-of-the-week7]*

no periodic list *hh:mm* **to** *hh:mm day-of-the-week1 [day-of-the-week2… day-of-the-week7]*

periodic list *hh:mm* **to** *hh:mm all*

no periodic list *hh:mm* **to** *hh:mm all*

パラメータ

- **day-of-the-week**：関連付けられた時間範囲が有効になる開始日。2 つ目は、関連付けられたステートメントが有効な終了日です。2つ目は、翌週にすることができます（ユーザ ガイドラインの説明を参照）。有効な値は、mon、tue、wed、thu、fri、sat、sun です。
- **hh:mm**：この引数の 1 つ目は、関連付けられた時間範囲が有効になる開始時間:分（24 時間形式）です。2 つ目は、関連付けられたステートメントが有効な終了時間:分（24 時間形式）です。2つ目は、翌日にすることができます（ユーザ ガイドラインの説明を参照）。（範囲：0 ～ 23、mm：0 ～ 59）
- **list day-of-the-week**：時間範囲が有効になる曜日のリストを指定します。

デフォルト設定

時間範囲が有効になっている場合の定期的な時間はありません。

コマンド モード

時間範囲コンフィギュレーション モード

使用上のガイドライン

2 つ目の曜日は、翌週にすることができます。たとえば、木曜日から月曜日を指定した場合、時間範囲は木曜日、金曜日、土曜日、日曜日、および月曜日に有効になります。

2 つ目の時刻は、翌日にすることができます（「22:00 ～ 2:00」など）。

例

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00
```

show time-range

時間範囲設定を表示するには、**show time-range** ユーザ EXEC モード コマンドを使用します。

構文

show time-range *time-range-name*

パラメータ

time-range-name：既存の時間範囲の名前を指定します。

コマンド モード

ユーザ EXEC モード

例

```
switchxxxxxx> show time-range
http-allowed
--------------
absolute start 12:00 1 Jan 2005 end  12:00 31 Dec 2005
periodic Monday 12:00 to Wednesday 12:00
```

show access-lists

スイッチで設定されたアクセス コントロール リスト（ACL）を表示するには、**show access-lists** 特権 EXEC モード コマンドを使用します。

構文

show access-lists [*name*]

show access-lists ***time-range-active*** *[name]*

パラメータ

- **name**：ACL の名前を指定します（範囲：1 ～ 160 文字）。
- **time-range-active**：時間範囲が現在アクティブなアクセス コントロール エントリ（ACE）のみを表示します（時間範囲に関連付けられていないものを含む）。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# show access-lists
Standard IP access list 1
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any priority 20 time-range weekdays
permit 234 172.30.23.8 0.0.0.255 any priority 40 time-range weekdays
switchxxxxxx# show access-lists time-range-active
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any priority 20
permit 234 172.30.8.8  0.0.0.0 any priority 40
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any priority 20  time-range weekdays
switchxxxxxx# show access-lists ACL1
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any priority 20
permit 234 172.30.8.8  0.0.0.0 any priority 40
```

clear access-lists counters

アクセス リスト（ACL）のカウンタをクリアするには、**clear access-lists counters** 特権 EXEC モード コマンドを使用します。

構文

clear access-lists counters *[interface-id]*

パラメータ

interface-id：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# clear access-lists counters gi1/0/1
```

show interfaces access-lists trapped packets

アクセス リスト（ACL）のトラップ パケットを表示するには、**show interfaces access-lists trapped packets** 特権 EXEC モード コマンドを使用します。

構文

show interfaces access-lists trapped packets *[interface-id | port-channel-number | VLAN]*

パラメータ

- **interface-id**：インターフェイス ID を指定します。このインターフェイス ID は、イーサネット ポートのポート チャネルです。
- **port-channel**：ポート チャネルを指定します。
- **VLAN**：VLAN を指定します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、インターフェイスでのロギングを有効にして、ACEのヒットからパケットがトラップされているかどうかを表示します。

例 1：

```
switchxxxxxx# show interfaces access-lists trapped packets
Ports/LAGs: gi1/0/1-gi1/0/3, ch1-ch3, ch4
VLANs: VLAN1, VLAN12-VLAN15
Packets were trapped globally due to lack of resources
```

例 2：

```
switchxxxxxx# show interfaces access-lists trapped packets gi1/0/1
Packets were trapped on interface gi1/0/1
```

ip access-list（IP 標準）

IP 標準リストを定義するには、**ip access-list** グローバル コンフィギュレーション モード コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

構文

ip access-list *access-list-name* {**deny**|**permit**} {*src-addr*[*/src-len*] | **any**}

no ip access-list *access-list-name*

パラメータ

- **access-list-name**：標準 IP アクセス リストの名前。名前には、最大で 32 文字まで使用できます。
- **deny/permit**：条件が満たされた場合にアクセスを拒否または許可します。

  src-addr[*/src-len*] | **any**：IP アドレスと長さで定義された IP プレフィックス、または **any**。**any** 値は、すべての IP アドレスに一致します。*src-len* を定義しないと、値は 32 が適用されます。*src-len* の値は、1 ～ 32 である必要があります。

デフォルト設定

定義されているアクセス リストはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

IP アドレス フィルタリングを設定するには、**ip access-list** コマンドを使用します。一致条件に基づいて IP アドレスを許可または拒否するには、アクセス リストを **permit** または **deny** キーワードを指定して設定します。どのアクセスリストのエントリとも一致しないアドレスには、暗黙の **deny** が適用されます。

アクセスリスト エントリは、IP アドレスとビット マスクで構成されています。ビット マスクは、1 ～ 32 の数値です。

アクセス リストによる IP アドレスの評価は、リストの最初のエントリから始まり、一致が検出されるまでリストを下方向に評価します。IP アドレスの一致が見つかると、そのアドレスに permit または deny ステートメントが適用され、リストの残りは評価されません。

アクセス リストを削除するには、**no ip access-list** コマンドを使用します。

IPv4 標準アクセスリストは、送受信された IPv4 ルーティング情報をフィルタ処理するために使用されます。

例

例 1：次の標準アクセス リストの例では、指定した 3 つのネットワークのみを許可します。アクセス リスト ステートメントに一致しない IP アドレスは拒否されます。

```
switchxxxxxx(config)# ip access-list 1 permit 192.168.34.0/24
switchxxxxxx(config)# ip access-list 1 permit 10.88.0.0/16
switchxxxxxx(config)# ip access-list 1 permit 10.0.0.0/8
```

注：その他のアクセスはすべて暗黙で拒否されます。

例 2：次の標準アクセス リストの例では、10.29.2.64 ～ 10.29.2.127 の範囲の IP アドレスのアクセスを許可します。この範囲外のすべての IP アドレスは、拒否されます。

```
switchxxxxxx(config)# ip access-list apo permit 10.29.2.64/26
```

注：その他のアクセスはすべて暗黙で拒否されます。

例 3：多数のアドレスの個別の指定を簡略にするには、マスク長が 32 の場合、指定を省略できます。したがって、次の 2 つの設定コマンドは同様に有効です。

```
switchxxxxxx(config)# ip access-list 2aa permit 10.48.0.3
switchxxxxxx(config)# ip access-list 2aa permit 10.48.0.3/32
```

ipv6 access-list（IP 標準）

ipv6 access-list グローバル コンフィギュレーション モード コマンドによって、IPv6 標準リストを定義します。リストを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 access-list *access-list-name* {**deny**|**permit**} {*src-addr*[*/src-len*] | **any**}

no ipv6 access-list *access-list-name*

パラメータ

- **access-list-name**：標準 IPv6 アクセスリストの名前。名前には、最大で 32 文字まで使用できます。
- **deny**：条件に合致した場合にアクセスを拒否します。
- **permit**：条件が一致した場合にアクセスが許可されます。
- **src-addr[/src-len] | any**：IPv6 アドレスと長さまたは any として定義された IPv6 プレフィックス。**any** 値は、すべての IPv6 アドレスに一致します。*src-len* を定義しない場合、値には 128 が適用されます。*src-len* の値は、1 ～ 128 である必要があります。

デフォルト設定

アクセスリストはありません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

IPv6 アドレスのフィルタ処理を設定するには、**ipv6 access-list** コマンドを使用します。一致条件に基づいて IPv6 アドレスを許可または拒否するには、**permit** キーワードまたは **deny** キーワードでアクセスリストを設定します。どのアクセスリストのエントリとも一致しないアドレスには、暗黙の **deny** が適用されます。

アクセスリスト エントリは、IP アドレスとビット マスクで構成されています。ビットマスクは 1 ～ 128 の数値です。

アクセスリストによる IPv6 アドレスの評価では、リストの最初のエントリから開始して、一致が検出されるまでリストを下方向に評価します。IPv6 アドレスの一致が見つかると、そのアドレスに permit または deny ステートメントが適用され、リストの残りは評価されません。

アクセスリストを削除するには、**no ipv6 access-list** コマンドを使用します。

IPv6 標準アクセスリストは、受信および送信された IPv6 ルーティング情報をフィルタ処理するために使用されます。

例

次に、指定したプレフィックス 1 つのみを許可するアクセスリストの例を示します。アクセスリストのステートメントに一致しない IPv6 アドレスは拒否されます。

```
switchxxxxxx(config)# ipv6 access-list 1 permit 3001::2/64
```

注：その他すべてのアクセスは暗黙的に拒否されます。

アドレス テーブル コマンド

この章は、次の項で構成されています。

- bridge multicast filtering （127 ページ）
- bridge multicast mode （128 ページ）
- bridge multicast address （130 ページ）
- bridge multicast forbidden address （132 ページ）
- bridge multicast ip-address （134 ページ）
- bridge multicast forbidden ip-address （136 ページ）
- bridge multicast source group （137 ページ）
- bridge multicast forbidden source group （139 ページ）
- bridge multicast ipv6 mode （141 ページ）
- bridge multicast ipv6 ip-address （143 ページ）
- bridge multicast ipv6 forbidden ip-address （145 ページ）
- bridge multicast ipv6 source group （147 ページ）
- bridge multicast ipv6 forbidden source group （148 ページ）
- bridge multicast unregistered （150 ページ）
- bridge multicast forward-all （151 ページ）
- bridge multicast forbidden forward-all （152 ページ）
- bridge unicast unknown （153 ページ）
- show bridge unicast unknown （154 ページ）
- mac address-table static （155 ページ）
- clear mac address-table （157 ページ）
- mac address-table aging-time （158 ページ）
- port security （159 ページ）
- port security mode （161 ページ）
- port security max （163 ページ）
- port security routed secure-address （164 ページ）
- show mac address-table （165 ページ）
- show mac address-table count （167 ページ）
- show bridge multicast mode （169 ページ）

- show bridge multicast address-table （170 ページ）
- show bridge multicast address-table static （173 ページ）
- show bridge multicast filtering （175 ページ）
- bridge multicast unregistered （176 ページ）
- show ports security （177 ページ）
- show ports security addresses （179 ページ）
- bridge multicast reserved-address （180 ページ）
- show bridge multicast reserved-addresses （182 ページ）

bridge multicast filtering

マルチキャスト アドレスのフィルタリングを有効にするには、**bridge multicast filtering** グローバル コンフィギュレーション モードを使用します。マルチキャスト アドレスのフィルタリングを無効にするには、このコマンドの **no** 形式を使用します。

構文

bridge multicast filtering

no bridge multicast filtering

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

マルチキャスト アドレス フィルタリングは無効になっています。すべてのマルチキャスト アドレスがすべてのポートにフラッディングされます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

この機能が有効になっている場合、（登録済みのマルチキャスト トラフィックとは対照的に）未登録のマルチキャスト トラフィックは引き続きフラッディングされます。

登録済みのすべてのマルチキャスト アドレスは、マルチキャスト グループに転送されます。マルチキャストグループを管理する方法は 2 つあります。1 つは IGMP スヌーピング機能、もう 1 つは bridge multicast forward-all コマンドです。

例

次の例では、ブリッジ マルチキャスト フィルタリングを有効にしています。

```
switchxxxxxx(config)# bridge multicast filtering
```

bridge multicast mode

マルチキャスト ブリッジ モードを設定するには、**bridge multicast mode** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

構文

bridge multicast mode *{***mac-group** | **ipv4-group** | **ipv4-src-group***}*

no bridge multicast mode

パラメータ

- **mac-group**：マルチキャスト ブリッジングが、パケットの VLAN と MAC アドレスに基づくことを指定します。
- **ipv4-group**：マルチキャスト ブリッジングが、非 IPv4 パケットの場合は VLAN と MAC アドレスに基づき、IPv4 パケットの場合は VLAN と IPv4 宛先アドレスに基づくことを指定します。
- **ipv4-src-group**：マルチキャストブリッジングが、非IPv4パケットの場合はVLANとMACアドレスに基づき、IPv4 パケットの場合は VLAN、IPv4 宛先アドレス、および IPv4 送信元アドレスに基づくことを指定します。

デフォルト設定

デフォルト モードは mac-group です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

マルチキャストMACアドレスに基づくMIBを使用するネットワーク管理システムを使用する場合は、mac-groupオプションを使用します。それ以外の場合は、IPv4マルチキャストアドレスが重複しないため、ipv4 モードを使用することを推奨します。

次の表は、ネットワークで使用されているIGMPバージョンの機能としてForwarding Data Base（FDB）に書き込まれる実際のデータを示しています。

FDB モード	IGMP バージョン 2	IGMP バージョン 3
mac-group	MAC グループ アドレス	MAC グループ アドレス
ipv4-group	IP グループ アドレス	IP グループ アドレス

FDB モード	IGMP バージョン 2	IGMP バージョン 3
ipv4-src-group	（*）	IP ソースおよびグループ アドレス

（*）モードが **ipv4-src-group** の場合、（*,G）は FDB に書き込めません。この場合、新しい FDBエントリは作成されませんが、ポートは要求されたグループに属するスタティック（S,G）エントリに追加されます（存在する場合）。IGMP バージョン2 では、FDB モードを ipv4-group または mac-group に設定することをお勧めします。

デバイスのアプリケーションが (*,G) を要求すると、動作中の FDB モードが ipv4-group に変更されます。

例

次の例では、VLAN 2 のマルチキャスト ブリッジ モードを mac-group に設定しています。

```
switchxxxxxx(config)#  interface vlan 2
switchxxxxxx(config-if)#  bridge multicast mode mac-group
```

bridge multicast address

ブリッジ テーブルに MAC レイヤ マルチキャスト アドレスを登録し、グループのポートを静的に追加または削除するには、**bridge multicast address** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。MAC アドレスを登録解除するには、このコマンドの **no** 形式を使用します。

構文

bridge multicast address {*mac-multicast-address* | *ipv4-multicast-address}* [{**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-list*}]

no bridge multicast address *mac-multicast-address*

パラメータ

- **mac-multicast-address | ipv4-multicast-address**：グループ マルチキャスト アドレスを指定します。
- **add**：（オプション）グループにポートを追加します。
- **remove**：（オプション）グループからポートを削除します。
- **ethernet** *interface-list*：（オプション）イーサーネット ポートのリストを指定します。連続していないイーサネット ポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel** *port-channel-list*：（オプション）ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定する場合はハイフンを使用します。

デフォルト設定

マルチキャスト アドレスは定義されていません。

ethernet *interface-list* または **port-channel** *port-channel-list* が **add** または **remove** を指定せずに指定された場合、デフォルトオプションは **add** になります。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

ポートまたはポート チャネルを追加または削除せずにブリッジ データベースにグループを登録するには、**mac-multicast-address** パラメータのみを指定します。

スタティック マルチキャスト アドレスはスタティック VLAN のみに定義できます。VLAN を作成する前に、このコマンドを実行できます。

例 1：次の例では、MAC アドレスをブリッジ テーブルに登録しています。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast address 01:00:5e:02:02:03
```

例 2：次の例では、MAC アドレスを登録し、ポートを静的に追加しています。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast address 01:00:5e:02:02:03 add gi1/0/1-2
```

bridge multicast forbidden address

特定のポートでの特定のマルチキャスト アドレスの追加または削除を禁止するには、**bridge multicast forbidden address** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

bridge multicast forbidden address {*mac-multicast-address* | *ipv4-multicast-address*} {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-list*}

no bridge multicast forbidden address *mac-multicast-address*

パラメータ

- **mac-multicast-address | ipv4-multicast-address**：グループ マルチキャスト アドレスを指定します。
- **add**：グループへのポートの追加を禁止します。
- **remove**：グループからのポートの削除を禁止します。
- **ethernet** *interface-list*：イーサネット ポートのリストを指定します。連続していないイーサネット ポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel** *port-channel-list*：ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定するには、ハイフンを使用します。

デフォルト設定

禁止アドレスは定義されていません。

デフォルト オプションは **add** です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

禁止されているポートを定義する前に、ブリッジ マルチキャスト アドレスを使用してマルチキャストグループを登録する必要があります。

VLAN を作成する前に、このコマンドを実行できます。

例

次に、VLAN 8 内のポート gi1/0/4 で MAC アドレス 0100.5e02.0203 を禁止する例を示します。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast address 0100.5e02.0203
switchxxxxxx(config-if)#  bridge multicast forbidden address 0100.5e02.0203 add gi1/0/4
```

bridge multicast ip-address

ブリッジテーブルにIP レイヤ マルチキャスト アドレスを登録し、グループのポートを静的に追加または削除するには、**bridge multicast ip-address** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。IP アドレスを登録解除するには、このコマンドの no 形式を使用します。

構文

bridge multicast ip-address *ip-multicast-address* [[**add** | **remove**] {*interface-list* | **port-channel** *port-channel-list*}]

no bridge multicast ip-address *ip-multicast-address*

パラメータ

- **ip-multicast-address**：グループ IP マルチキャスト アドレスを指定します。
- **add**：（オプション）グループにポートを追加します。
- **remove**：（オプション）グループからポートを削除します。
- ***interface-list***：（オプション）イーサーネット ポートのリストを指定します。連続していないイーサネットポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel** *port-channel-list*：（オプション）ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定するには、ハイフンを使用します。

デフォルト設定

マルチキャスト アドレスは定義されていません。

デフォルト オプションは **add** です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

ポートまたはポート チャネルを追加または削除せずにブリッジ データベースにグループを登録するには、**ip-multicast-address** パラメータのみを指定します。

スタティック マルチキャスト アドレスはスタティック VLAN のみに定義できます。

VLAN を作成する前に、このコマンドを実行できます。

例

次の例では、指定された IP アドレスをブリッジ テーブルに登録しています。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast ip-address 239.2.2.2
```

次の例では、IP アドレスを登録し、ポートを静的に追加しています。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast ip-address 239.2.2.2 add gi1/0/4
```

bridge multicast forbidden ip-address

特定のポートでの特定のIPマルチキャストアドレスの追加または削除を禁止するには、**bridge multicast forbidden ip-address** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

bridge multicast forbidden ip-address *{ip-multicast-address}* {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-list*}

no bridge multicast forbidden ip-address *ip-multicast-address*

パラメータ

- **ip-multicast-address**：グループ IP マルチキャスト アドレスを指定します。
- **add**：（オプション）グループへのポートの追加を禁止します。
- **remove**：（オプション）グループからのポートの削除を禁止します。
- **ethernet interface-list**：（オプション）イーサネットポートのリストを指定します。連続していないイーサネットポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel port-channel-list**：（オプション）ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定するには、ハイフンを使用します。

デフォルト設定

禁止アドレスは定義されていません。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

禁止ポートを定義する前に、マルチキャスト グループを登録する必要があります。

VLAN を作成する前に、このコマンドを実行できます。

例

次に、IP アドレス 239.2.2.2 を登録し、VLAN 8 内のポート gi1/0/4 でこの IP アドレスを禁止する例を示します。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast ip-address 239.2.2.2
switchxxxxxx(config-if)#  bridge multicast forbidden ip-address 239.2.2.2 add gi1/0/4
```

bridge multicast source group

ブリッジテーブルに送信元 IP アドレスとマルチキャスト IP アドレスのペアを登録し、送信元グループのポートを静的に追加または削除するには、**bridge multicast source group** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。送信元グループペアを登録解除するには、このコマンドの no 形式を使用します。

構文

bridge multicast source *ip-address* **group** *ip-multicast-address* [[**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-list*}]

no bridge multicast source *ip-address* **group** *ip-multicast-address*

パラメータ

- **ip-address**：送信元 IP アドレスを指定します。
- **ip-multicast-address**：グループ IP マルチキャスト アドレスを指定します。
- **add**：（オプション）特定の送信元 IP アドレスのグループにポートを追加します。
- **remove**：（オプション）特定の送信元 IP アドレスのグループからポートを削除します。
- **ethernet** *interface-list*：（オプション）イーサーネット ポートのリストを指定します。連続していないイーサネットポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel** *port-channel-list*：（オプション）ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定する場合はハイフンを使用します。

デフォルト設定

マルチキャスト アドレスは定義されていません。

デフォルト オプションは **add** です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

VLAN を作成する前に、このコマンドを実行できます。

例

次の例では、送信元 IP アドレスとマルチキャスト IP アドレスのペアをブリッジ テーブルに登録しています。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast source 13.16.1.1 group 239.2.2.2
```

bridge multicast forbidden source group

特定のポートでの特定の IP 送信元アドレスとマルチキャスト アドレスのペアの追加または削除を禁止するには、**bridge multicast forbidden source group** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。デフォルトの設定に戻すには、このコマンドの no 形式を使用します。

構文

bridge multicast forbidden *source* *ip-address* ***group*** *ip-multicast-address* ***{*****add** | **remove*****}*** ***{*****ethernet** *interface-list* | **port-channel** *port-channel-list*}

no bridge multicast forbidden source *ip-address* **group** *ip-multicast-address*

パラメータ

- **ip-address**：送信元 IP アドレスを指定します。
- **ip-multicast-address**：グループ IP マルチキャスト アドレスを指定します。
- **add**：（オプション）特定の送信元 IP アドレスのグループへのポートの追加を禁止します。
- **remove**：（オプション）特定の送信元 IP アドレスのグループからのポートの削除を禁止します。
- **ethernet** *interface-list*：（オプション）イーサネットポートのリストを指定します。連続していないイーサネットポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel***port-channel-list*：（オプション）ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定する場合はハイフンを使用します。

デフォルト設定

禁止アドレスは定義されていません。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

禁止ポートを定義する前に、マルチキャスト グループを登録する必要があります。

VLAN を作成する前に、このコマンドを実行できます。

例

次に、送信元 IP アドレスとマルチキャスト IP アドレスのペアをブリッジ テーブルに登録し、VLAN 8 のポート gi1/0/4 へのペアの追加を禁止する例を示します。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast source 13.16.1.1 group 239.2.2.2
switchxxxxxx(config-if)#  bridge multicast forbidden source 13.16.1.1 group 239.2.2.2
add gi1/0/4
```

bridge multicast ipv6 mode

IPv6 マルチキャスト パケット用にマルチキャスト ブリッジ モードを設定するには、**bridge multicast ipv6 mode** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。デフォルトの設定に戻すには、このコマンドの no 形式を使用します。

構文

bridge multicast ipv6 mode {**mac-group** | **ip-group** | **ip-src-group**}

no bridge multicast ipv6 mode

パラメータ

- **mac-group**：マルチキャスト ブリッジングが、パケットの VLAN と MAC 宛先アドレスに基づくことを指定します。
- **ip-group**：マルチキャスト ブリッジングが、パケットの VLAN と、IPv6 パケットの IPv6 宛先アドレスに基づくことを指定します。
- **ip-src-group**：マルチキャスト ブリッジングが、パケットの VLAN と、IPv6 パケットの IPv6 宛先アドレスと IPv6 送信元アドレスに基づくことを指定します。

デフォルト設定

デフォルト モードは **mac-group** です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

マルチキャストMACアドレスに基づくMIBを使用するネットワーク管理システムを使用する場合は、**mac-group** モードを使用します。

次の表は、ネットワークで使用されているMLDバージョンの機能としてForwarding Data Base（FDB）に書き込まれる実際のデータを示しています。

FDB モード	MLD バージョン 1	MLD バージョン 2
mac-group	MAC グループ アドレス	MAC グループ アドレス
ipv6-group	IPv6 グループ アドレス	IPv6 グループ アドレス
ipv6-src-group	（*）	IPv6 の送信元アドレスおよびグループ アドレス

（*）**ip-src-group** モードでは、4 バイトのマルチキャストアドレスと 4 バイトの送信元アドレスで照合が実行されます。グループアドレスでは、アドレスの最後の4バイトが一致するかどうかが確認されます。送信元アドレスでは、インターフェイス ID の最後の 3 バイトと最後のバイトから 5 番目が確認されます。

（*）モードが **ip-src-group** の場合、（*,G）はFDBに書き込めません。この場合、新しいFDBエントリは作成されませんが、ポートは要求されたグループに属する（S,G）エントリに追加されます（存在する場合）。

デバイスのアプリケーションが（*,G）を要求した場合、動作FDBモードは **ip-group** に変更されます。

VLAN を作成する前に、このコマンドを実行できます。

例

次の例では、VLAN 2 のマルチキャスト ブリッジ モードを **ip-group** に設定しています。

```
switchxxxxxx(config)#  interface vlan 2
switchxxxxxx(config-if)#  bridge multicast ipv6 mode
ip-group
```

bridge multicast ipv6 ip-address

ブリッジ テーブルに IPv6 マルチキャスト アドレスを登録し、グループのポートを静的に追加または削除するには、**bridge multicast ipv6 ip-address** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。IPv6 アドレスを登録解除するには、このコマンドの **no** 形式を使用します。

構文

bridge multicast ipv6 ip-address *ipv6-multicast-address* [[**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-list*}]

no bridge multicast ipv6 ip-address *ip-multicast-address*

パラメータ

- **ipv6-multicast-address**：グループ IPv6 マルチキャスト アドレスを指定します。
- **add**：（オプション）グループにポートを追加します。
- **remove**：（オプション）グループからポートを削除します。
- **ethernet** *interface-list*：（オプション）イーサーネット ポートのリストを指定します。連続していないイーサネット ポートは、カンマ（スペースなし）で区切ります。ポートの範囲はハイフンで指定します。
- **port-channel** *port-channel-list*：（オプション）ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定するには、ハイフンを使用します。

デフォルト設定

マルチキャスト アドレスは定義されていません。

デフォルト オプションは **add** です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

ポートまたはポート チャネルを追加または削除せずにブリッジ データベースにグループを登録するには、**ipv6-multicast-address** パラメータのみを指定します。

スタティック マルチキャスト アドレスはスタティック VLAN のみに定義できます。VLAN を作成する前に、このコマンドを実行できます。

例 1：次の例では、IPv6 アドレスをブリッジ テーブルに登録しています。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1
```

例 2：次の例では、IPv6 アドレスを登録し、ポートを静的に追加しています。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1 add gi1/0/1-2
```

bridge multicast ipv6 forbidden ip-address

特定のポートでの特定の IPv6 マルチキャスト アドレスの追加または削除を禁止するには、**bridge multicast ipv6 forbidden ip-address** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

bridge multicast ipv6 forbidden ip-address {*ipv6-multicast-address*} {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-list*}

no bridge multicast ipv6 forbidden ip-address *ipv6-multicast-address*

パラメータ

- **ipv6-multicast-address**：グループ IPv6 マルチキャスト アドレスを指定します。
- **add**：（オプション）グループへのポートの追加を禁止します。
- **remove**：（オプション）グループからのポートの削除を禁止します。
- **ethernet** *interface-list*：（オプション）イーサーネット ポートのリストを指定します。連続していないイーサネット ポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel** *port-channel-list*：（オプション）ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定するには、ハイフンを使用します。

デフォルト設定

禁止アドレスは定義されていません。

デフォルト オプションは **add** です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

禁止ポートを定義する前に、マルチキャスト グループを登録する必要があります。

VLAN を作成する前に、このコマンドを実行できます。

例

次に、IPv6 マルチキャストアドレスを登録し、VLAN 8 内のポート gi1/0/4 で IPv6 アドレスを禁止する例を示します。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast ipv6 ip-address FF00:0:0:0:4:4:4:1
switchxxxxxx(config-if)#  bridge multicast ipv6 forbidden ip-address FF00:0:0:0:4:4:4:1
 add gi1/0/4
```

bridge multicast ipv6 source group

ブリッジテーブルに送信元 IPv6 アドレスとマルチキャスト IPv6 アドレスのペアを登録し、送信元グループのポートを静的に追加または削除するには、**bridge multicast ipv6 source group** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。送信元グループ ペアを登録解除するには、このコマンドの **no** 形式を使用します。

構文

bridge multicast ipv6 source *ipv6-source-address* **group** *ipv6-multicast-address* [[**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-list}]*

no bridge multicast ipv6 source *ipv6-address* **group** *ipv6-multicast-address*

パラメータ

- **ipv6-source-address**：送信元 IPv6 アドレスを指定します。
- **ipv6-multicast-address**：グループ IPv6 マルチキャスト アドレスを指定します。
- **add**：（オプション）特定の送信元 IPv6 アドレスのグループにポートを追加します。
- **remove**：（オプション）特定の送信元 IPv6 アドレスのグループからポートを削除します。
- **ethernet** *interface-list*：（オプション）イーサーネット ポートのリストを指定します。連続していないイーサネット ポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel** *port-channel-list*：（オプション）ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定するには、ハイフンを使用します。

デフォルト設定

マルチキャスト アドレスは定義されていません。

デフォルト オプションは **add** です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

例

次の例では、送信元 IPv6 アドレスとマルチキャスト IPv6 アドレスのペアをブリッジ テーブルに登録しています。

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast source 2001:0:0:0:4:4:4 group FF00:0:0:0:4:4:4:1
```

bridge multicast ipv6 forbidden source group

特定のポートでの特定の IPv6 送信元アドレスとマルチキャスト アドレスのペアの追加または削除を禁止するには、**bridge multicast ipv6 forbidden source group** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

構文

bridge multicast ipv6 forbidden *source* *ipv6-source-address* **group** *ipv6-multicast-address* {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-list*}

no bridge multicast ipv6 forbidden source *ipv6-address* **group** *ipv6-multicast-address*

パラメータ

- **ipv6-source-address**：送信元 IPv6 アドレスを指定します。
- **ipv6-multicast-address**：グループ IPv6 マルチキャスト アドレスを指定します。
- **add**：特定の送信元 IPv6 アドレスのグループへのポートの追加を禁止します。
- **remove**：特定の送信元 IPv6 アドレスのグループからのポートの削除を禁止します。
- **ethernet** *interface-list*：イーサーネット ポートのリストを指定します。連続していないイーサネット ポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel** *port-channel-list*：ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定する場合はハイフンを使用します。

デフォルト設定

禁止アドレスは定義されていません。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

禁止ポートを定義する前に、マルチキャスト グループを登録する必要があります。

VLAN を作成する前に、このコマンドを実行できます。

例

次に、送信元 IPv6 アドレスとマルチキャスト IPv6 アドレスのペアをブリッジ テーブルに登録し、VLAN 8 での gi1/0/4 へのペアの追加を禁止する例を示します

```
switchxxxxxx(config)#  interface vlan 8
switchxxxxxx(config-if)#  bridge multicast source 2001:0:0:0:4:4:4 group FF00:0:0:0:4:4:4:1
switchxxxxxx(config-if)#  bridge multicast forbidden source 2001:0:0:0:4:4:4:1 group
FF00:0:0:0:4:4:4:1 add gi1/0/4
```

bridge multicast unregistered

未登録のマルチキャスト アドレスの転送を設定するには、**bridge multicast unregistered** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

bridge multicast unregistered {**forwarding** | **filtering**}

no bridge multicast unregistered

パラメータ

- **forwarding**：未登録のマルチキャストパケットを転送します。
- **filtering**：未登録のマルチキャストパケットをフィルタ処理します。

デフォルト設定

未登録のマルチキャスト アドレスが転送されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

224.0.0.x のアドレス範囲はフィルタリングするべきではないため、ルータに接続されているポートでは未登録マルチキャストフィルタリングを有効にしないでください。ルータが必ずしも 224.0.0.x の範囲で IGMP レポートを送信するとは限らないことに注意してください。

VLAN を作成する前に、このコマンドを実行できます。

例

次に、gi1/0/1 で未登録のマルチキャストパケットをフィルタ処理する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  bridge multicast unregistered filtering
```

bridge multicast forward-all

ポートまたはポート チャネルの範囲に対して、すべてのマルチキャスト パケットの転送を有効にするには、**bridge multicast forward-all** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

bridge multicast forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-list*}

no bridge multicast forward-all

パラメータ

- **add**：すべてのマルチキャスト パケットの転送を適用します。
- **remove**：すべてのマルチキャスト パケットの転送を適用しません。
- **ethernet** *interface-list*：イーサネット ポートのリストを指定します。連続していないイーサネット ポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel** *port-channel-list*：ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定するには、ハイフンを使用します。

デフォルト設定

すべてのマルチキャスト パケットの転送は無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

例

次に、ポート gi1/0/4 のすべてのマルチキャストパケットの転送を有効にする例を示します。

```
switchxxxxxx(config)#  interface vlan 2
switchxxxxxx(config-if)#  bridge multicast forward-all add gi1/0/4
```

bridge multicast forbidden forward-all

ポートがマルチキャスト グループに動的に参加することを禁止するには、**bridge multicast forbidden forward-all** インターフェイス（VLAN）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

bridge multicast forbidden forward-all {**add** | **remove**} {**ethernet** *interface-list* | **port-channel** *port-channel-list*}

no bridge multicast forbidden forward-all

パラメータ

- **add**：すべてのマルチキャスト パケットの転送を禁止します。
- **remove**：すべてのマルチキャスト パケットの転送を禁止しません。
- **ethernet** *interface-list*：イーサーネット ポートのリストを指定します。連続していないイーサネット ポートをカンマで、スペースを入れずに区切ります。ポートの範囲を指定するには、ハイフンを使用します。
- **port-channel** *port-channel-list*：ポート チャネルのリストを指定します。連続していないポート チャネルをカンマで、スペースを入れずに区切ります。ポート チャネルの範囲を指定する場合はハイフンを使用します。

デフォルト設定

ポートがマルチキャスト グループに動的に参加することは禁止されていません。

デフォルト オプションは **add** です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

（IGMP などにより）ポートがマルチキャスト グループに動的に参加することを禁止するには、このコマンドを使用します。

この場合も、ポートをマルチキャスト ルータ ポートにすることができます。

例

次に、VLAN 2 内の gi1/0/1 へのマルチキャストパケットの転送を禁止する例を示します。

```
switchxxxxxx(config)#  interface vlan 2
switchxxxxxx(config-if)#  bridge multicast forbidden forward-all add ethernet gi1/0/1
```

bridge unicast unknown

デバイスで宛先MACアドレスが不明なユニキャストパケットの出力フィルタリングを有効にするには、**bridge unicast unknown** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

bridge unicast unknown {**filtering** | **forwarding**}

no bridge unicast unknown

パラメータ

- **filtering**：未登録のユニキャスト パケットをフィルタリングします。
- **forwarding**：未登録のユニキャスト パケットを転送します。

デフォルト設定

Forwarding.

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード。

例

次に、宛先が不明な場合に gi1/0/1 でユニキャスト パケットをドロップする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  bridge unicast unknown filtering
```

show bridge unicast unknown

不明なユニキャストのフィルタリング設定を表示するには、**show bridge unicast unknown** 特権 EXEC モード コマンドを使用します。

構文

show bridge unicast unknown [*interface-id*]

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

特権 EXEC モード

例

Console # **show bridge unicast unknown**	
Port	Unregistered
--------	----------
gi1/0/1	Forward
gi1/0/2	Filter
gi1/0/3	Filter

mac address-table static

MAC アドレス テーブルに MAC レイヤ ステーションの送信元アドレスを追加するには、**mac address-table static** グローバル コンフィギュレーション モード コマンドを使用します。MAC 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。

構文

mac address-table static *mac-address* **vlan** *vlan-id* **interface** *interface-id* [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]|

no mac address-table static [*mac-address]* **vlan** *vlan-id*

パラメータ

- ***mac-address***：MAC アドレス（範囲：有効な MAC アドレス）。
- ***vlan-id***：VLAN を指定します。
- ***interface-id***：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネル（範囲：有効なイーサネット ポート、有効なポート チャネル）のいずれかを指定できます。
- **permanent**：（オプション）固定スタティック MAC アドレス。このキーワードは、デフォルトで適用されます。
- **delete-on-reset**：（オプション）リセット時に削除されるスタティック MAC アドレス。
- **delete-on-timeout**：（オプション）タイムアウト時に削除されるスタティック MAC アドレス。
- **secure**：（オプション）セキュア MAC アドレス。セキュア モードでのみ使用できます。

デフォルト設定

スタティック アドレスは定義されていません。追加されたアドレスのデフォルト モードは permanent です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

任意のモードで指定された存続可能時間のスタティック MAC アドレスを追加したり、セキュア モードでセキュア MAC アドレスを追加するには、このコマンドを使用します。

MAC アドレス テーブルの各 MAC アドレスには、**type** と **time-to-live** の 2 つの属性が割り当てられます。

存続可能時間には次の値がサポートされています。

- **permanent**：MAC アドレスは、手動で削除されるまで保存されます。
- **delete-on-reset**：MAC アドレスは、次に再起動されるまで保存されます。

  delete-on-timeout：エージング タイマーにより削除できる MAC アドレス。

次のタイプがサポートされます。

- **static**：存続可能時間を指定する次のキーワードを持つコマンドにより、手動で追加された MAC アドレス。

  permanent

  delete-on-reset

  delete-on-timeout

  スタティック MAC アドレスは、任意のポート モードで追加できます。

  secure：セキュア モードで、手動で追加された MAC アドレスまたは学習された MAC アドレス。セキュア MAC アドレスを追加するには、**secure** キーワードを持つ **mac address-table static** コマンドを使用します。MAC アドレスを再学習することはできません。

  セキュア MAC アドレスは、セキュア ポート モードでのみ追加できます。

- **dynamic**：非セキュア モードでスイッチにより学習された MAC アドレス。**time-to-live** 属性の値は **delete-on-timeout** です。

例 1：次の例では、2 つの固定スタティック MAC アドレスを追加しています。

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b1 vlan 1 interface gi1/0/1
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/0/1
 permanent
```

例 2：次の例では、リセット時に削除されるスタティック MAC アドレスを追加しています。

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/0/1
 delete-on-reset
```

例 3：次の例では、タイムアウト時に削除されるスタティック MAC アドレスを追加しています。

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/0/1
 delete-on-timeout
```

例 4：次の例では、セキュア MAC アドレスを追加しています。

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface  gi1/0/1
 secure
```

clear mac address-table

転送データベース（FDB）から学習されたエントリまたはセキュアエントリを削除するには、**clear mac address-table** 特権 EXEC モード コマンドを使用します。

構文

clear mac address-table dynamic interface *interface-id*

clear mac address-table secure interface *interface-id*

パラメータ

- **dynamic interface** *interface-id*：指定されたインターフェイス上のすべてのダイナミック（学習された）アドレスを削除します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのタイプを指定できます。インターフェイス ID が指定されていない場合は、すべてのダイナミック アドレスが削除されます。
- **secure interface** *interface-id*：特定のインターフェイスで学習された、すべてのセキュア アドレスを削除します。ポートセキュリティが定義されているポートで学習されたセキュア MAC アドレスです。

デフォルト設定

ダイナミック アドレスでは、interface-id が指定されていない場合は、すべてのダイナミック エントリが削除されます。

コマンド モード

特権 EXEC モード

例 1：FDB からすべてのダイナミック エントリを削除します。

```
switchxxxxxx#  clear mac address-table dynamic
```

例 2：セキュアポート gi1/0/1 で学習された FDB からのすべてのセキュアエントリを削除します。

```
switchxxxxxx#  clear mac address-table secure interface gi1/0/1
```

mac address-table aging-time

アドレス テーブルのエージング タイムを設定するには、**mac address-table aging-time** グローバル コンフィギュレーション コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

構文

mac address-table aging-time *seconds*

no mac address-table aging-time

パラメータ

seconds：時間は秒数です。（範囲：10-400）

デフォルト設定

300

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)#  mac address-table aging-time 600
```

port security

インターフェイスでポート セキュリティ学習モードを有効にするには、**port security** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。インターフェイスでポートセキュリティ学習モードを無効にするには、このコマンドの **no** 形式を使用します。

構文

port security [**forward** | **discard** | **discard-shutdown**] [**trap** *seconds*]

no port security

パラメータ

- **forward**：（オプション）未学習の送信元アドレスを持つパケットを転送しますが、アドレスは学習しません。
- **discard**：（オプション）未学習の送信元アドレスを持つパケットを破棄します。
- **discard-shutdown**：（オプション）未学習の送信元アドレスを持つパケットを破棄し、ポートをシャットダウンします。
- **trap** *seconds*：（オプション）SNMP トラップを送信し、連続するトラップ間の最小時間間隔を秒単位で指定します。（範囲：1 ～ 1000000）

デフォルト設定

この機能はデフォルトで無効に設定されています。

デフォルト モードは **discard** です。

デフォルトの秒数はゼロですが、**trap** を入力した場合は、秒数も入力する必要があります。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドは、インターフェイスが通常モード（MAC 学習が無制限なセキュア以外のモード）の場合のみ使用できます。

インターフェイスで 802.1X 認証がすでにアクティブになっている場合は、そのインターフェイスでポートセキュリティを有効にできません。

port security コマンドによりポートの **lock** モードを有効にすると、そのポートで学習されたすべてのダイナミック アドレスが**永続的なセキュア**アドレスに変更されます。

port security コマンドにより **lock** モードとは異なるモードをポートで有効にすると、そのポートで学習されたすべてのダイナミックアドレスが削除されます。

no port security コマンドによりポートのセキュア モードをキャンセルすると、そのポートで定義されているすべてのセキュア アドレスが**ダイナミック**アドレスに変更されます。

また、モードを設定するには、**port security** コマンドを使用して、送信元 MAC アドレスが学習できないフレームでスイッチが実行するアクションを設定します。

例

次に、不明な送信元からのパケットのアドレスを学習せずにポート gi1/0/1 にすべてのパケットを転送し、不明な送信元アドレスのパケットを受信した場合に100秒ごとにトラップを送信する例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# port security mode lock
switchxxxxxx(config-if)# port security forward trap 100
switchxxxxxx(config-if)# exit
```

port security mode

ポート セキュリティ学習モードを設定するには、**port security mode** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

port security mode {**max-addresses | lock | secure permanent | secure delete-on-reset**}

no port security mode

パラメータ

- **max-addresses**：制限付き学習ダイナミック MAC アドレスを使用する非セキュア モード。
- **lock**：MAC 学習を使用しないセキュア モード。
- **secure permanent**：存続可能時間が **permanent** の、制限付き学習固定セキュア MAC アドレスを使用するセキュア モード。スタティック MAC アドレスおよびセキュア MAC アドレスを手動でポートに追加するには、**mac address-table static** コマンドを使用します。
- **secure delete-on-reset**：存続可能時間が **delete-on-reset** の、制限付き学習セキュア MAC アドレスを使用するセキュア モード。スタティック MAC アドレスおよびセキュア MAC アドレスを手動でポートに追加するには、**mac address-table static** コマンドを使用します。

デフォルト設定

デフォルトのポートセキュリティモードは **lock** です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

デフォルトのポートモードは通常モードと呼ばれます。このモードでは、ポートはダイナミック アドレスの無制限学習を許可します。

このコマンドは、インターフェイスが通常モード（MAC 学習が無制限なセキュア以外のモード）の場合のみ使用できます。

例

次に、gi1/0/4 のポートセキュリティモードを lock に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# port security mode
lock
```

```
switchxxxxxx(config-if)# port security
switchxxxxxx(config-if)# exit
```

port security max

ポートがポート モード、最大アドレス数モード、またはセキュア モードのときにポートで学習できるアドレスの最大数を設定するには、**port security max** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

port security max *max-addr*

no port security max

パラメータ

max-addr：ポートで学習できるアドレスの最大数を指定します。（範囲：0 ～ 256）

デフォルト設定

デフォルトのアドレスの最大数は 1 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドは、インターフェイスが通常モード（MAC 学習が無制限なセキュア以外のモード）の場合のみ使用できます。

例

次の例では、ポートを制限付き学習モードに設定しています。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# port security mode max
switchxxxxxx(config-if)# port security max 20
switchxxxxxx(config-if)# port security
switchxxxxxx(config-if)# exit
```

port security routed secure-address

ルーテッド ポート（IP アドレスが定義されているポート）に MAC レイヤ セキュア アドレスを追加するには、**port security routed secure-address** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。ルーテッド ポートから MAC 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。

構文

port security routed secure-address *mac-address*

no port security routed secure-address *mac-address*

パラメータ

mac-address：MAC アドレスを指定します。

デフォルト設定

アドレスは定義されていません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード。インターフェイスの範囲（範囲コンテキスト）には設定できません。

使用上のガイドライン

このコマンドを使用すると、ポート セキュリティ モードでルーテッド ポートにセキュア MAC アドレスを追加できます。このコマンドは、ポートがルーテッド ポートで、ポート セキュリティ モードの場合に使用できます。ポートのセキュリティ モードが終了した場合や、ルーテッド ポートでなくなった場合、このアドレスは削除されます。

例

次に、MAC レイヤアドレス 00:66:66:66:66:66 を gi1/0/1 に追加する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  port security routed secure-address 00:66:66:66:66:66
```

show mac address-table

MAC アドレス テーブルのエントリを表示するには、**show mac address-table** 特権 EXEC モード コマンドを使用します。

構文

show mac address-table [**dynamic** | **static** | **secure**] [**vlan** *vlan*] [**interface** *interface-id*] [**address** *mac-address]*

パラメータ

- **dynamic**：（オプション）ダイナミック MAC アドレス テーブルのエントリのみを表示します。
- **static**：（オプション）スタティック MAC アドレス テーブルのエントリのみを表示します。
- **secure**：（オプション）セキュア MAC アドレス テーブルのエントリのみを表示します。
- **vlan**：（オプション）特定の VLAN のエントリを表示します。
- **interface** *interface-id*：（オプション）特定のインターフェイス ID のエントリを表示します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。
- **address** *mac-address*：（オプション）特定の MAC アドレスのエントリを表示します。

デフォルト設定

パラメータを入力しなかった場合は、テーブル全体が表示されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

内部使用 VLAN（ルーテッド ポートに自動的に割り当てられた VLAN）は、VLAN ID ではなくポート番号で VLAN 列に表示されます。

例 1 - アドレス テーブル全体を表示します。

```
switchxxxxxx#  show mac address-table
Aging time is 300 sec
```

VLAN	MAC Address	Port	Type
--------	--------------------	----------	----------
1	00:00:26:08:13:23	0	self

1	00:3f:bd:45:5a:b1	gi1/0/1	static
1	00:a1:b0:69:63:f3	gi1/0/2	dynamic
2	00:a1:b0:69:63:f3	gi1/0/3	dynamic
gi1/0/4	00:a1:b0:69:61:12	gi1/0/4	dynamic

例 2：指定された MAC アドレスを含むアドレス テーブルのエントリを表示します。

```
switchxxxxxx#  show mac address-table address 00:3f:bd:45:5a:b1
Aging time is 300 sec
VLAN        MAC Address          Port       Type
-------- -------------------- ---------- ----------
1         00:3f:bd:45:5a:b1      static       gi1/0/4
```

show mac address-table count

転送データベースに存在するアドレスの数を表示するには、**show mac address-table count** 特権 EXEC モード コマンドを使用します。

構文

show mac address-table count [**vlan** *vlan* | **interface** *interface-id*]

パラメータ

- **vlan** *vlan*：（オプション）VLAN を指定します。
- **interface-id** *interface-id*：（オプション）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

転送データベースの容量（エントリの合計数）、空きエントリ（現在も使用可能なエントリの数）、およびエントリのタイプ別の消費済みエントリの内訳を表示するには、**show mac address-table count** コマンドを使用します。次のエントリタイプが表示されます。

- **Used Unicast**：占有中の転送データベースエントリ。これらのエントリはレイヤ 2 MAC ユニキャストアドレスです。
- **Used Multicast**：占有中の転送データベースエントリ。これらのエントリはレイヤ 2 MAC マルチキャストアドレスです。
- **IPv4 hosts**：占有中の転送データベースエントリ。これらのエントリは IPv4 レイヤ 3 ホストエントリです。
- **IPv6 hosts**：占有中の転送ベースエントリ。これらのエントリは IPv6 レイヤ 3 ホストエントリです。
- **Secure**：セキュアなユニキャストエントリの数量。
- **Dynamic Unicast**：ダイナミック ユニキャスト エントリの数量。
- **Static Unicast**：静的（ユーザが設定した）ユニキャストエントリの数量。
- **Internal**：内部エントリの数量。たとえば、デバイス独自の MAC アドレスなどです。

セキュアタイプ、ダイナミックユニキャストタイプ、静的ユニキャストタイプ、および内部エントリタイプは、使用済みユニキャストエントリのさらに詳細な内訳を示します。

消費済みエントリの合計数は、エントリタイプ Used Unicast、Used Multicast、IPv4 hosts、および IPv6 hosts の集約値です。

インターフェイスパラメータが使用されている場合、このコマンドはエントリタイプ Used Unicast、secure、Dynamic Unicast、Static Unicast、および Internal のみを表示します。

例 1：次に、デバイス全体の転送テーブルに存在するエントリの数を表示する例を示します。

```
switchxxxxxx#  show mac address-table count
This may take some time.
Capacity         : 16384
Free               : 16378
Used unicast     : 5
Used multicast   : 1
Used IPv4 hosts  : 1
Used IPv6 hosts  : 1 (each IPv6 host consumes 2 entires in MAC address table)
Secure           : 0
Dynamic unicast  : 2
Static unicast   : 2
Internal         : 1
console#
```

例 2：次に、特定のデバイスインターフェイスの転送テーブルに存在するエントリの数を表示する例を示します。

```
switchxxxxxx#  show mac address-table count interface gi1/0/1
This may take some time.
Capacity         : 16384
Free               : 16378
Used unicast     : 5
Secure           : 0
Dynamic  unicast : 2
Static unicast   : 2
Internal         : 0
console#
```

show bridge multicast mode

すべての VLAN または特定の VLAN のマルチキャスト ブリッジ モードを表示するには、**show bridge multicast mode** 特権 EXEC モード コマンドを使用します。

構文

show bridge multicast mode [*vlan vlan-id*]

パラメータ

vlan *vlan-id*：（オプション）VLAN ID を指定します。

コマンド モード

特権 EXEC モード

例

次の例では、すべての VLAN のマルチキャスト ブリッジ モードを表示しています。

```
switchxxxxxx#  show bridge multicast mode
```

VLAN	IPv4 Multicast Mode		IPv6 Multicast Mode	
	Admin	Oper	Admin	Oper
-----	----------	----------	----------	----------
1	MAC-GROUP	MAC-GROUP	MAC-GROUP	MAC-GROUP
11	IPv4-GROUP	IPv4-GROUP	IPv6-GROUP	IPv6-GROUP
12	IPv4-SRC-GROUP	IPv4-SRC-GROUP	IPv6-SRC-GROUP	IPv6-SRC-GROUP

show bridge multicast address-table

マルチキャスト MAC アドレスまたは IP マルチキャスト アドレス テーブル情報を表示するには、**show bridge multicast address-table** 特権 EXEC モード コマンドを使用します。

構文

show bridge multicast address-table [**vlan** *vlan-id*]

show bridge multicast address-table [**vlan** *vlan-id*] [**address** *mac-multicast-address*] [**format** {**ip** | **mac**}]

show bridge multicast address-table [**vlan** *vlan-id*] [**address** *ipv4-multicast-address]* [**source** *ipv4-source-address*]

show bridge multicast address-table [**vlan** *vlan-id*] [**address** *ipv6-multicast-address*] [**source** *ipv6-source-address*]

パラメータ

- **vlan-id** *vlan-id*：（オプション）指定した VLAN ID のエントリを表示します。
- **address**：（オプション）指定されたマルチキャスト アドレスのエントリを表示します。次の値が可能です。

  mac-multicast-address：（オプション）MAC マルチキャスト アドレスを指定します。

  ipv4-multicast-address：（オプション）IPv4 マルチキャスト アドレスを指定します。

  ipv6-multicast-address：（オプション）IPv6 マルチキャスト アドレスを指定します。
- **format**：（オプション）mac-multicast-address が選択されている場合に適用されます。この場合、MAC 形式または IP 形式で表示できます。指定されたマルチキャスト アドレス形式のエントリを表示します。次の値が可能です。

  ip：マルチキャスト アドレスが IP アドレスであることを指定します。

  mac：マルチキャスト アドレスが MAC アドレスであることを指定します。
- **source**：（オプション）送信元アドレスを指定します。次の値が可能です。

  ipv4-address：（オプション）送信元 IPv4 アドレスを指定します。

  ipv6-address：（オプション）送信元 IPv6 アドレスを指定します。

デフォルト設定

format が指定されていない場合、デフォルトは **mac** になります（mac-multicast-address が入力されている場合のみ）。

VLAN ID が入力されていない場合は、すべての VLAN のエントリが表示されます。

MAC アドレスまたは IP アドレスが指定されていない場合は、すべてのアドレスのエントリが表示されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

MAC アドレスは、0100.5e00.0000 ～ 0100.5e7f.ffff の範囲内に限り、IP 形式で表示できます。

（静的に定義された、または動的に検出された）マルチキャスト ルータ ポートは、すべての MAC グループのメンバーになります。

マルチキャスト モードを変更すると、FDB のハッシュ衝突が原因で、デバイス FDB に書き込まれたスタティック マルチキャスト アドレスがシャドウ設定に移動することがあります。

例

次の例では、ブリッジ マルチキャスト アドレス情報を表示します。

```
switchxxxxxx#  show bridge multicast address-table
Multicast address table for VLANs in MAC-GROUP bridging mode:
Vlan    MAC Address         Type           Ports
---- -----------------    --------------   -----
8    01:00:5e:02:02:03     Static          1-2
Forbidden ports for Multicast addresses:
Vlan    MAC Address         Ports
---- -----------------      -----
8    01:00:5e:02:02:03      gi1/0/4
```

Multicast address table for VLANs in IPv4-GROUP bridging mode:

```
Vlan    MAC Address         Type             Ports
---- -----------------    --------------     -----
1      224.0.0.251         Dynamic          gi1/0/2
Forbidden ports for Multicast addresses:
Vlan    MAC Address         Ports
---- -----------------      -----
1      232.5.6.5
1      233.22.2.6
Multicast address table for VLANs in IPv4-SRC-GROUP bridging mode:
Vlan  Group Address  Source address  Type        Ports
---- --------------- --------------- --------    -----
1     224.2.2.251     11.2.2.3       Dynamic     gi1/0/1
Forbidden ports for Multicast addresses:
Vlan  Group Address  Source Address   Ports
---- --------------- --------------- -------
8    239.2.2.2       *               gi1/0/4
8    239.2.2.2       1.1.1.11        gi1/0/4
Multicast address table for VLANs in IPv6-GROUP bridging mode:
VLAN  IP/MAC Address   Type      Ports
---- ----------------- --------- --------------------
8    ff02::4:4:4       Static    gi1/0/1-2, gi1/0/3, Po1
Forbidden ports for Multicast addresses:
VLAN  IP/MAC Address   Ports
---- ----------------- -----------
8    ff02::4:4:4       gi1/0/4
Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:
Vlan  Group Address  Source address  Type     Ports
---- --------------- --------------- -------- ------------------
8    ff02::4:4:4     *               Static   gi1/0/1-2,gi1/0/3,Po1
8    ff02::4:4:4     fe80::200:7ff:  Static
                     fe00:200
Forbidden ports for Multicast addresses:
```

```
Vlan  Group Address  Source address    Ports
---- --------------- ---------------   ----------
8    ff02::4:4:4     *                  gi1/0/4
8    ff02::4:4:4     fe80::200:7ff:f    gi1/0/4
                     e00:200
```

show bridge multicast address-table static

静的に設定されたマルチキャスト アドレスを表示するには、**show bridge multicast address-table static** 特権 EXEC モード コマンドを使用します。

構文

show bridge multicast address-table static [**vlan** *vlan-id*] [**all**]

show bridge multicast address-table static [**vlan** *vlan-id*] [**address** *mac-multicast-address*] [**mac**| **ip**]

show bridge multicast address-table static [**vlan** *vlan-id*] [**address** *ipv4-multicast-address*] [**source** *ipv4-source-address*]

show bridge multicast address-table static [**vlan** *vlan-id*] [**address** *ipv6-multicast-address*] [**source** *ipv6-source-address*]

パラメータ

- **vlan** *vlan-id*：（オプション）VLAN ID を指定します。
- **address**：（オプション）マルチキャスト アドレスを指定します。次の値が可能です。

  mac-multicast-address：（オプション）MAC マルチキャスト アドレスを指定します。

  ipv4-multicast-address：（オプション）IPv4 マルチキャスト アドレスを指定します。

  ipv6-multicast-address：（オプション）IPv6 マルチキャスト アドレスを指定します。
- **source**：（オプション）送信元アドレスを指定します。次の値が可能です。

  ipv4-address：（オプション）送信元 IPv4 アドレスを指定します。

  ipv6-address：（オプション）送信元 IPv6 アドレスを指定します。

デフォルト設定

all/mac/ip が指定されていない場合は、すべてのエントリ（MACおよびIP）が表示されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

MAC アドレスは、0100.5e00.0000 ～ 0100.5e7f.ffff の範囲内に限り、IP 形式で表示できます。

例

次の例では、静的に設定されたマルチキャスト アドレスを表示しています。

```
switchxxxxxx#  show bridge multicast address-table static
MAC-GROUP table
```

```
Vlan    MAC Address          Ports
----    --------------       --------
1       0100.9923.8787       gi1/0/1, gi1/0/2

Forbidden ports for multicast addresses:

Vlan    MAC Address          Ports
----    --------------       --------

IPv4-GROUP Table

Vlan    IP Address           Ports
----    ----------           --------
1       231.2.2.3            gi1/0/1, gi1/0/2
19      231.2.2.8            gi1/0/2-3

Forbidden ports for multicast addresses:

Vlan    IP Address           Ports
----    ----------           --------
1       231.2.2.3            gi1/0/4
19      231.2.2.8            gi1/0/3

IPv4-SRC-GROUP Table:

Vlan    Group Address        Source address       Ports
----    ---------------      ---------------      ------

Forbidden ports for multicast addresses:

Vlan    Group Address        Source address       Ports
----    ---------------      ---------------      ------

IPv6-GROUP Table

Vlan    IP Address           Ports
----    -----------------    ---------
191     FF12::8              gi1/0/1-4

Forbidden ports for multicast addresses:

Vlan    IP Address           Ports
----    -----------------    ---------
11      FF12::3              gi1/0/4
191     FF12::8              gi1/0/4

IPv6-SRC-GROUP Table:

Vlan    Group Address        Source address          Ports
----    ---------------      ---------------         ------
192     FF12::8              FE80::201:C9A9:FE40:8988 gi1/0/1-4

Forbidden ports for multicast addresses:

Vlan    Group Address        Source address          Ports
----    ---------------      ---------------         ------
192     FF12::3              FE80::201:C9A9:FE40:8988 gi1/0/4
```

show bridge multicast filtering

マルチキャスト フィルタリング設定を表示するには、**show bridge multicast filtering** 特権 EXEC モード コマンドを使用します。

構文

show bridge multicast filtering *vlan-id*

パラメータ

vlan-id：VLAN ID を指定します。（範囲：有効な VLAN）

デフォルト設定

なし

コマンド モード

特権 EXEC モード

例

次の例では、VLAN 1 のマルチキャスト設定を表示しています。

```
switchxxxxxx#  show bridge multicast filtering 1
Filtering: Enabled
VLAN: 1
Forward-All
```

Port	Static	Status
-----	---------	------
gi1/0/1	Forbidden	Filter
gi1/0/2	Forward	Forward(s)
gi1/0/3	-	Forward(d)

bridge multicast unregistered

未登録のマルチキャスト アドレスの転送を設定するには、**bridge multicast unregistered** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

bridge multicast unregistered {**forwarding** | **filtering**}

no bridge multicast unregistered

パラメータ

- **forwarding**：未登録のマルチキャストパケットを転送します。
- **filtering**：未登録のマルチキャストパケットをフィルタ処理します。

デフォルト設定

未登録のマルチキャスト アドレスが転送されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

224.0.0.x のアドレス範囲はフィルタリングするべきではないため、ルータに接続されているポートでは未登録マルチキャスト フィルタリングを有効にしないでください。ルータが必ずしも 224.0.0.x の範囲で IGMP レポートを送信するとは限らないことに注意してください。

VLAN を作成する前に、このコマンドを実行できます。

例

次に、gi1/0/1 で未登録のマルチキャストパケットをフィルタ処理する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  bridge multicast unregistered filtering
```

show ports security

ポート ロック ステータスを表示するには、**show ports security** 特権 EXEC モード コマンドを使用します。

構文

show ports security [*interface-id* | **detailed**]

パラメータ

- ***interface-id***：（オプション）インターフェイス ID を指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのインターフェイスについて表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

例

次の例では、すべてのポートのポート ロック ステータスを表示しています。

```
switchxxxxxx#  show ports security
Port   Status       Learning    Action    Maximum  Trap     Frequency
------- --------    ---------   ------    ---      -------  --------
gi1/0/1
       Enabled      Max-       Discard     3       Enabled  100
                    Addresses
gi1/0/2
      Disabled     Max-         -          28        -        -
                   Addresses
gi1/0/3
     Enabled       Lock      Discard      8       Disabled   -
```

次の表では、上記に示すフィールドについて説明します。

フィールド	説明
ポート	ポート番号

説明
ポート セキュリティのステータス。表示される値は Enabled または Disabled です。
違反時に実施されるアクション。
最大アドレス数モードでこのポートに関連付けることができるアドレスの最大数。
SNMP トラップのステータス。表示される値は Enable または Disable です。
連続するトラップ間の最小時間間隔。

show ports security addresses

ロックされたポートの現在のダイナミック アドレスを表示するには、**show ports security addresses** 特権 EXEC モード コマンドを使用します。

構文

show ports security addresses [*interface-id* | **detailed**]

パラメータ

- ***interface-id***：（オプション）インターフェイス ID を指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのインターフェイスについて表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

例

次の例では、現在ロックされているすべてのポートのダイナミック アドレスを表示しています。

Port	Status	Learning	Current	Maximum
gi1/0/1	Disabled	Lock	0	10
gi1/0/2	Disabled	Lock	0	1
gi1/0/3	Disabled	Lock	0	1
gi1/0/4	Disabled	Lock	0	1
...				

bridge multicast reserved-address

マルチキャスト予約済みアドレスパケットに対するアクションを定義するには、**bridge multicast reserved-address** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

bridge multicast reserved-address *mac-multicast-address* [**ethernet-v2** *ethtype* | **llc** *sap* | **llc-snap** *pid*] {**discard** | **bridge**}

no bridge multicast reserved-address *mac-multicast-address* [**ethernet-v2** *ethtype* | **llc** *sap* | **llc-snap** *pid*]

パラメータ

- **mac-multicast-address**：予約済み MAC アドレス範囲の MAC マルチキャスト アドレス。（範囲：01-80-C2-00-00-00、01-80-C2-00-00-02 ～ 01-80-C2-00-00-2F）
- **ethernet-v2** *ethtype*：（オプション）パケット タイプがイーサネット v2 であることを指定し、イーサネット タイプ フィールド（16 進形式の 16 ビット）を指定します。（範囲：0x0600 ～ 0xFFFF）
- **llc** *sap*：（オプション）パケット タイプがイーサネット LLC であることを指定し、DSAP-SSAP フィールド（16 進形式の 16 ビット）を指定します。（範囲：0xFFFF）
- **llc-snap** *pid*：（オプション）パケット タイプが LLC-SNAP であることを指定し、PID フィールド（16 進形式の 40 ビット）を指定します。（範囲：0x0000000000 ～ 0xFFFFFFFFFF）
- **discard**：パケットの破棄を指定します。
- **bridge**：パケットのブリッジ（転送）を指定します。

デフォルト設定

- ユーザが MAC マルチキャスト アドレスを指定した場合、EtherType およびカプセル化（LLC）は（ピアと呼ばれる）デバイスでサポートされているプロトコルを指定し、デフォルト アクション（破棄またはブリッジ）はこのプロトコルにより決定されます。
- これ以外の場合は、デフォルト アクションは次のようになります。

  01-80-C2-00-00-00、01-80-C2-00-00-02 ～ 01-80-C2-00-00-0F の範囲の MAC アドレスの場合、デフォルトは **discard** です。

  00-80-C2-00-00-10 ～ 01-80-C2-00-00-2F の範囲の MAC アドレスの場合、デフォルトは **bridge** です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

パケットまたはサービス タイプ（EtherType またはカプセル化）が指定されていない場合、設定は MAC アドレスが設定されているすべてのパケットに関係します。

（サービス タイプを含む）具体的な設定は、（MAC アドレスのみを含む）具体的でない設定よりも優先されます。

ブリッジされたパケットは、セキュリティ ACL の対象となります。このコマンドにより定義されたアクションは、デバイスでサポートされているアプリケーションまたはプロトコル（STP や LLDP など）により定義された転送ルールよりも優先されます。

例

```
switchxxxxxx(config)# bridge multicast reserved-address 00:3f:bd:45:5a:b1
```

show bridge multicast reserved-addresses

マルチキャスト予約済みアドレス ルールを表示するには、**show bridge multicast reserved-addresses** 特権 EXEC モード コマンドを使用します。

構文

show bridge multicast reserved-addresses

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx # show bridge multicast reserved-addresses
MAC Address           Frame Type    Protocol          Action
----------------- -  ----------  - --------------  - -----------
01-80-C2-00-00-00 LLC-SNAP 00-00-0C-01-29 Bridge
```

AAA コマンド

この章は、次の項で構成されています。

- aaa authentication login （184 ページ）
- aaa authentication enable （186 ページ）
- login authentication （188 ページ）
- enable authentication （189 ページ）
- ip http authentication （190 ページ）
- show authentication methods （192 ページ）
- login block-for （193 ページ）
- login delay （195 ページ）
- login quiet-mode access-class （196 ページ）
- show login （198 ページ）
- show login failures （200 ページ）
- clear login failures （202 ページ）
- clear login quiet-mode （203 ページ）
- password （204 ページ）
- enable password （206 ページ）
- service password-recovery （209 ページ）
- username （210 ページ）
- show users accounts （213 ページ）
- aaa accounting login start-stop （214 ページ）
- aaa accounting dot1x （216 ページ）
- show accounting （218 ページ）
- passwords complexity （219 ページ）
- passwords aging （220 ページ）
- password complexity history （221 ページ）
- aaa login-history file （222 ページ）
- show passwords configuration （223 ページ）
- show users login-history （224 ページ）

aaa authentication login

ログイン時に適用される 1 つ以上の認証方式を設定するには、**aaa authentication login** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトの認証方式に戻すには、このコマンドの **no** 形式を使用します。

構文

aaa authentication login [**authorization**] {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication login {**default** | *list-name*}

パラメータ

- **authorization**：特定のリストに認証と許可の適用を指定します。キーワードを設定しない場合は、特定のリストにのみ認証が適用されます。
- **default**：この引数の後に続く認証方式を、ユーザがログインするときのデフォルト方式リストとして使用します（このリストに名前はありません）。
- ***list-name***：ユーザがログインするときに有効にされる、認証方式のリストの名前を指定します（長さ：1 ～ 12 文字）。
- ***method1*** [*method2...*]：認証アルゴリズムが（指定された順序で）試行する方式のリストを指定します。他の認証方式が使用されるのは、前の方式が失敗した場合ではなく、エラーが返された場合に限られます。すべての方式でエラーが返された場合でも認証を成功させるには、コマンド ラインに最後の方式として **none** を指定します。次のリストから 1 つ以上の方式を選択します。

キーワード	説明
enable	認証に有効化パスワードを使用します。
line	認証にライン パスワードを使用します。
local	ローカルに定義されたユーザ名を認証に使用します。
none	認証を使用しません。
radius	認証にすべてのRADIUSサーバのリストを使用します。
tacacs	認証にすべての TACACS+ サーバのリストを使用します。

デフォルト設定

方式を指定しない場合、デフォルトではローカルで定義されたユーザとパスワードが使用されます。これは、**aaa authentication login local** コマンドを入力した場合と同じです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

list-name パラメータとともにこのコマンドを入力して、認証方式のリストを作成します。*list-name* は、任意の文字列です。method 引数は、認証アルゴリズムが指定された順番で試行する方式のリストを指定します。

注。ログインに対して認証が有効になっており、スイッチが TACACS+ サーバからユーザレベル 15 を受信する場合は enable コマンドは必要なく、レベル 1 を受信する場合は enable コマンドが必要です。

no aaa authentication login *list-name* コマンドは、別のコマンドで参照されていない場合にのみ、リスト名を削除します。

例

次の例では、コンソールの認証ログイン方式を設定しています。

```
switchxxxxxx(config)# aaa authentication login authen-list radius local none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication authen-list
```

aaa authentication enable

aaa authentication enable グローバル コンフィギュレーション モード コマンドは、より高い特権レベルにアクセスするための 1 つ以上の認証方式を設定します。デフォルトの認証方法に戻すには、このコマンドの **no** 形式を使用します。

構文

aaa authentication enable [**authorization**] {**default** | *list-name*} *method* [*method2...*]}

no aaa authentication enable {**default** | *list-name*}

パラメータ

- **authorization**：特定のリストに認証と許可の適用を指定します。キーワードを設定しない場合は、特定のリストにのみ認証が適用されます。
- **default**：この引数の後にリストされた認証方式を、より高い特権レベルにアクセスするときのデフォルト方式リストとして使用します。
- ***list-name***：ユーザがより高い権限レベルにアクセスするときに有効にする認証方式のリストの名前を指定します。（長さ：1 ～ 12 文字）
- ***method*** [*method2...*]：特定の順序で認証アルゴリズムが試行する方式のリストを指定します。追加の認証方式が使用されるのは、前の方式が失敗した場合ではなく、エラーが戻った場合に限られます。すべての方式でエラーが返された場合でも認証を成功させるには、コマンド ラインに最後の方式として **none** を指定します。次のリストから 1 つ以上の方式を選択します。

キーワード	説明
enable	認証に有効化パスワードを使用します。
line	認証にライン パスワードを使用します。
none	認証を使用しません。
radius	認証にすべての RADIUS サーバのリストを使用します。
tacacs	認証にすべての TACACS+ サーバのリストを使用します。

デフォルト設定

デフォルトでは、認証リストはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

aaa authentication enable *list-name method1 [method2...]* コマンドを入力してリストを作成します。ここで、*list-name* はこのリストに名前を付けるのに使用する文字列です。method 引数は、認証アルゴリズムが指定された順番で試行する方式のリストを指定します。

デバイスから RADIUS サーバに送信されたすべての **aaa authentication enable** 要求には、ユーザ名 **$enabx$** が含まれています。ここで、**x** は要求された特権レベルです。

デバイスから TACACS+ サーバに送信されたすべての **aaa authentication enable** 要求には、ログイン認証用に入力されたユーザ名が含まれています。

追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返された場合でも認証を成功させるために、コマンド ラインに最後の方式として **none** を指定します。

no aaa authentication enable *list-name* は、参照されていない場合にのみ、リスト名を削除します。

例

次の例では、より高い特権レベルにアクセスするための認証用の有効化パスワードを設定しています。

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

login authentication

login authentication ライン コンフィギュレーション モード コマンドは、リモート Telnet またはコンソールセッションのログイン認証方式リストを指定します。デフォルトの認証方式に戻すには、このコマンドの **no** 形式を使用します。

構文

login authentication {**default** | *list-name*}

no login authentication

パラメータ

- **default**：**aaa authentication login** コマンドで作成された、デフォルト リストを使用します。
- ***list-name***：**aaa authentication login** コマンドで作成された、指定されたリストを使用します。

デフォルト設定

default

コマンド モード

ライン コンフィギュレーション モード

例 1：次の例では、ログイン認証方式をコンソール セッションのデフォルト方式として指定しています。

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication default
```

例 2：次の例では、コンソールの認証ログイン方式を方式のリストとして設定しています。

```
switchxxxxxx(config)# aaa authentication login authen-list radius local none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication authen-list
```

enable authentication

enable authentication ライン コンフィギュレーション モード コマンドは、リモート Telnet またはコンソールから、より高い特権レベルにアクセスするための認証方式を指定します。デフォルトの認証方式に戻すには、このコマンドの **no** 形式を使用します。

構文

enable authentication {**default** | *list-name}*

no enable authentication

パラメータ

- **default**：**aaa authentication enable** コマンドで作成された、デフォルト リストを使用します。
- ***list-name***：**aaa authentication enable** コマンドで作成された、指定されたリストを使用します。

デフォルト設定

default です。

コマンド モード

ライン コンフィギュレーション モード

例 1：次の例では、コンソールからより高い特権レベルにアクセスするときの認証方式を、デフォルト方式として指定しています。

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication default
```

例 2：次の例では、より高い特権レベルにアクセスするための認証方式のリストを設定しています。

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

ip http authentication

ip http authentication グローバル コンフィギュレーション モード コマンドは、HTTP サーバ アクセス用の認証方式を指定します。デフォルトの認証方式に戻すには、このコマンドの **no** 形式を使用します。

構文

ip http authentication aaa login-authentication [**login-**authorization] *method1* [*method2...*]

no ip http authentication aaa login-authentication

パラメータ

- **login-**authorization：認証と許可の適用を指定します。キーワードを設定しない場合は、認証のみが適用されます。
- ***method*** [*method2...*]：特定の順序で認証アルゴリズムが試行する方式のリストを指定します。追加の認証方式が使用されるのは、前の方式が失敗した場合ではなく、エラーが戻った場合に限られます。すべての方式でエラーが返された場合でも認証を成功させるには、コマンド ラインに最後の方式として **none** を指定します。次のリストから 1 つ以上の方式を選択します。

キーワード	説明
local	認証にローカルなユーザ名データベースを使用します。
none	認証を使用しません。
radius	認証にすべての RADIUS サーバのリストを使用します。
tacacs	認証にすべての TACACS+ サーバのリストを使用します。

デフォルト設定

ローカル ユーザ データベースがデフォルトの認証ログイン方式です。これは、**ip http authentication local** コマンドを入力した場合と同じです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、HTTP および HTTPS サーバ ユーザに関係します。

例

次の例では、HTTP アクセス認証方式を指定しています。

```
switchxxxxxx(config)# ip http authentication aaa login-authentication radius local none
```

show authentication methods

show authentication methods 特権 EXEC モード コマンドは、認証方式に関する情報を表示します。

構文

show authentication methods

コマンド モード

特権 EXEC モード

例

次の例では、認証の設定を表示しています。

switchxxxxxx# **show**

```
authentication methods
Login Authentication Method Lists
---------------------------------
Default: Radius, Local, Line
Consl_Login(with authorization): Line, None
Enable Authentication Method Lists
---------------------------------
Default: Radius, Enable
Consl_Enable(with authorization): Enable, None
```

.

Line	Login Method List	Enable Method List
Console	Consl_Login	Consl_Enable
Telnet	Default	Default
SSH	Default	Default

```
HTTP, HHTPS: Radius, local
Dot1x: Radius
```

login block-for

Login Block-for

次のグローバル コンフィギュレーション モード コマンドを使用して、指定された回数のログイン試行失敗後の静音モード期間を設定します。デフォルト設定に戻すには、コマンドの no 形式を使用します。

構文

login block-for seconds **attempts** tries **within** seconds

no login block-for

パラメータ

- **Block for seconds**：静音モード期間（ログイン試行が拒否される時間）の長さ（秒単位）（範囲は 1 ～ 65535（18 時間）秒）。
- **attempts** tries：静音モード期間をトリガーするログイン試行の失敗回数（範囲は 1 ～ 100）。
- **within** seconds：静音モード期間のトリガーに必要な、その回数のログイン試行失敗が生じる時間の長さ（秒単位）（範囲 1 ～ 3600（1 時間）秒）。

デフォルト設定

デバイスで静音モードが設定されていません。

コマンド モード

グローバル コンフィギュレーション モード。

使用上のガイドライン

指定の時間（**within** seconds）内に、指定された回数の接続試行が失敗した（**attempt** tries）場合、デバイスは指定の期間（**block-for** seconds）の間、追加のログイン試行を受け入れません。

静音モード期間中、デバイスへの管理接続は、指定された接続のみを許可する静音モードアクセスクラスによって制限されます（コマンド **login quiet-mode access-class**）。コンソール接続をサポートするデバイスの場合、「console_only」管理アクセスリストがデフォルトの静音モードアクセスクラスとして使用されます。この場合、静音モード期間中は、ネットワーク（Telnet、SSH、SNMP、HTTP、または HTTPS）を介したすべてのログイン試行が拒否されます。

このコマンドは、静音モードアクセスクラス（デフォルトまたはユーザー定義）が設定されている場合にのみ設定できます。「login quiet-mode access-class」を参照してください。

login block-for コマンドがデバイスですでに設定されており、そのコマンドが「監視期間」中に新しいパラメータで再設定された場合、現在のカウントは終了し、新しいパラメータを使用

して新しいカウントが開始されます。ログイン攻撃の静音モード期間中に設定された場合、そのコマンドは拒否されます。

コマンドの **no** 形式を使用すると、この機能が無効になり、静音モード期間が終了します（アクティブな場合）。

例

例 1：次の例では、180 秒以内に 18 回を超えてログイン試行に失敗した場合に、すべてのログイン要求を 180 秒間ブロックする方法を示します。

```
switchxxxxxx(config)# login block-for 180 attempts 18 within 180
```

例 2：次の例では、デバイスの静音モード期間中にコマンドを設定しようとしています。

```
switchxxxxxx(config)# login block-for 18 attempts 8 within 50
```

デバイスが静音モードの間は、login block-for の設定はできません。

例 3：次の例では、コマンドの設定に失敗しています。失敗の理由：静音モードアクセスクラス（デフォルトまたはユーザー定義）が設定されていません。

```
switchxxxxxx(config)# login block-for 770 attempts 7 within 613
```

静音モードアクセスクラスが設定されていないため、login block-for を設定できません。

login delay

失敗したログイン試行に対するデバイス応答の遅延を設定するには、 **login delay** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

login delay seconds

no login delay

パラメータ

- seconds：失敗したログイン試行間に課される遅延（秒単位）（範囲 1 ～ 10 秒）。

デフォルト設定

デフォルトでは、ログイン遅延は無効になっています。

コマンド モード

デフォルトでは、ログイン遅延は無効になっています。

使用上のガイドライン

login delay コマンドを使用すると、ログイン試行に失敗した後のデバイスの応答に遅延が生じます（HTTP、HTTPS、Telnet、SSH、およびSNMP）。遅延により、見込まれる辞書攻撃からの保護が強化されます。

例

例 1：次の例では、ログイン試行が失敗した後に 5 秒の遅延を設定しています。

```
switchxxxxxx(config)# login delay 5
```

login quiet-mode access-class

デバイスがログイン静音モードに移行するときに適用される管理アクセス制御リスト（MACL）を指定するには、login quiet-mode access-class グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

login quiet-mode access-class name

no login quiet-mode access-class

パラメータ

- ***name***：ログイン静音モードでデバイスに適用する管理 ACL の名前。

デフォルト設定

デフォルトでは、「console-only」管理アクセスリストがデフォルトの静音モードアクセスクラスとして適用されます。コンソールをサポートしていないデバイスの場合、静音モードアクセスクラスにデフォルトはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

login quiet-mode access-class コマンドを使用して、ログイン待機期間中に選択したホストがデバイス管理にアクセスできるようにします。指定した管理 ACL に基づいてアクセスが許可されます。management access-list コマンドを使用してこのコマンドを設定する前に、管理アクセスリストを作成する必要があります。

この設定により、静音モード期間中であっても、クライアントまたはクライアントのリストへのアクセスを許可できるようになります。コンソール接続をサポートするデバイスでは、静音モード期間中はデフォルトで「console-only」管理アクセスリストが適用されます。つまり、すべてのネットワークログイン接続（telnet、SSH、SNMP、HTTP、HTTPS）が拒否されますが、コンソールからの接続は許可されます。コンソールをサポートしていないデバイスでは、デフォルトのアクセスクラスはなく、ユーザーが最初に静音モードアクセスクラスを定義していない場合は、login block-for コマンドを設定できません。

静音モード期間中に設定した場合、そのコマンドは拒否されます。

このコマンドの no 形式を使用すると、静音モードアクセスクラスがデフォルト設定に戻ります。コンソールのないデバイスでは、login block-for コマンドが設定されている場合、no コマンドを適用できません。

例

例 1 ：次の例は、quiet-acl 管理アクセスリストに基づいて、静音モード期間中に接続を受け入れるようにデバイスを設定する方法を示しています。

```
switchxxxxxx(config)# login quiet-mode access-class quiet-acl
```

show login

ログイン設定とステータスを表示するには、次の特権 EXEC モードコマンドを使用します。

構文

show login

パラメータ

該当なし

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、コマンド **login delay**、**Login block-for and login quiet-mode access-class** に関連する設定とステータスを表示します。

例

例 1：次の例は、ログイン設定が適用または変更されていない場合の出力を示しています。

```
switchxxxxxx# show login
Login delay: disabled
Login Attacks watch: disabled
Quiet-Mode access list: console-only (the default)
```

例 2：次の例は、ユーザーがログイン遅延を 5 秒に設定し、ログインブロック期間を設定し、デバイスが静音モードではない場合の show login コマンドの出力を示しています。

```
switchxxxxxx# show login
Login delay: 5 second
Login Attacks watch: enabled
If more than 4 login failures occur in 60 seconds or less, logins will be disabled for
60 seconds.
Quiet-Mode access list: console-only (the default)
Quiet-Mode: inactive
Watch Window remaining time: 44 seconds.
Present login failure count: 3.
```

（注） ログイン失敗数は、（監視ウィンドウ内で）まだ有効である最も早い失敗ログインからカウントされます。

例 3：次の例は、ユーザーがログイン遅延を 5 秒に設定し、ログインブロック期間を設定し、デバイスが静音モードになっている場合の出力を示しています。

```
switchxxxxxx# show login
Login delay: 5 second
Login Attacks watch: enabled
If more than 4 login failures occur in 60 seconds or less, logins will be disabled for
60 seconds.
Quiet-Mode access list: console-only (the default)
Quiet-Mode: active (time remaining: 20 seconds)
```

show login failures

失敗したログイン試行に関する情報を表示するには次の特権EXECモードコマンドを使用します。

構文

Show login failures

パラメータ

該当なし

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、最近 50 回の失敗したログイン試行に関する情報を表示します。情報には、失敗した試行で入力されたユーザー名（試行の一部として入力された場合）、失敗した試行で使用された送信元IP、失敗した試行で要求されたサービス、この接続の失敗試行回数、およびこの接続の最後の失敗試行のタイムスタンプが含まれます。エントリは、最新のタイムスタンプから最も古いものへとソートされます。

例

```
switchxxxxxx#  show login failures
```

このデバイスでの最近 50 回のログイン失敗に関する情報。

ユーザ名	Source IP	サービス	Count	Timestamp
————	————	————	————	————
ffff	10.5.44.25	Telnet	3	2021 年 7 月 7 日（水）00:01:23 edt
fff	10.5.44.25	Telnet	4	2021 年 7 月 8 日（木）08:37:08 edt
bb	10.5.44.25	ssh	2	2021 年 7 月 7 日（水）00:17:59 edt
fff	10.5.44.25	ssh	2	2021 年 7 月 7 日（水）00:20:37 edt

ユーザ名	Source IP	サービス	Count	Timestamp
ffff	10.5.44.25	ssh	2	2021 年 7 月 7 日（水）00:21:12 edt
aaaa	fe80::1111	ssh	2	2021 年 7 月 7 日（水）00:21:26 edt
	10.5.44.25	Telnet	3	2021 年 7 月 7 日（水）00:38:14 edt
aaa	10.5.44.22	Telnet	1	2021 年 7 月 8 日（木）08:37:16 edt
555	10.5.44.23	Telnet	1	2021 年 7 月 8 日（木）08:37:26 edt

clear login failures

ログイン失敗データベースをクリアするには、次の特権EXECモードコマンドを使用します。

構文

clear login failures

パラメータ

該当なし

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

ログイン失敗データベース内のすべてのエントリをクリアするには、このコマンドを使用します（コマンド **show login failures**）。

例

```
switchxxxxxx#  clear login failures
```

clear login quiet-mode

アクティブな静音モード期間をただちに終了するには、次の特権EXECモードコマンドを使用します。

構文

clear login quiet-mode

パラメータ

該当なし

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

機能を無効にせずにアクティブな静音期間を終了するには、このコマンドを使用します（コマンド **login block-for**）。静音モード期間タイマーがタイムアップにならなくても、静音モード期間が終了します。

例

```
switchxxxxxx#  clear login quiet-mode
11-Aug-2021 10:33:12 :%ABC-I-XXX: Quiet-Mode is OFF, terminated by user
```

password

ライン（アクセス方式とも呼ばれ、コンソールやTelnetなどがあります）のパスワードを指定するには、**password** ライン コンフィギュレーション モード コマンドを使用します。デフォルトのパスワードに戻すには、このコマンドの **no** 形式を使用します。

構文

password {*unencrypted-password* [**method** *hash-method***]** | *encrypted-password* **encrypted**}

password generate-password [**method** hash-method]

no password

パラメータ

- ***unencrypted-password***：ユーザの認証パスワード。（範囲：1 ～ 64）
- [**method** *hash-method***]** ：（オプション）クリアテキストパスワードの暗号化に使用する方式を指定します。サポートされる値：
  - **sha512**：基盤のハッシュアルゴリズムとしてSHA512を使用したHMACによるPBKDF2暗号化。**method** パラメータを指定しない場合は、これがデフォルトの方式になります。
- **encrypted** encrypted-password：パスワードが暗号化され、ソルトを使用してハッシュされることを指定します。すでに暗号化されているパスワード（たとえば、別のデバイスのコンフィギュレーション ファイルからコピーしたパスワード）を入力するには、このキーワードを使用します。*encrypted-password* は *$<type>$<salt>$<encrypted-password* > 形式で指定します。ここで、
  - **<*type*>**：ハッシュの生成に使用するハッシュアルゴリズムのタイプを示す整数値です。
  - **<salt>**：ソルトに使用する 96 ビットの Base64 エンコーディング（長さ：16 バイト）
  - **<*encrypted-password*>**：暗号化されたハッシュ出力のBase64エンコーディング（長さ：86 バイト）

デフォルト設定

パスワードは定義されていません。

コマンド モード

ライン コンフィギュレーション モード

使用上のガイドライン

unencrypted-password は、パスワードの複雑さの要件を順守する必要があります。

generate-password オプションが選択されている場合、ユーザーがパスワードを入力する必要はありません。代わりに、デバイスがランダムベースのパスワード提案を自動的に生成します。この提案はユーザーに示され、提案されたパスワードを受け入れるか拒否するかを選択するオプションが表示されます。ユーザーが提示されたパスワードを受け入れることを選択した場合、指定したユーザー名とこのパスワード（暗号化形式）がデバイス設定ファイルに追加されます。提示されたパスワードをユーザが拒否した場合は、ユーザーが新しいコマンドを入力する必要があります。

例

例 1：次の例では、コンソール行にパスワード「secreT123!」を指定しています。

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password secreT123!
```

例 2：この例のコマンドには、generate-password キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを受け入れることを選択しています。

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
“Configuration and password are added to device configuration. Please Note
password for future use.”
```

例 3：この例のコマンドには、generate-password キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを拒否することを選択しています。

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
“Auto generated password rejected by user. Password configuration is not added to
device configuration”
```

enable password

通常レベルおよび特権レベルへのアクセスを制御するためのローカルパスワードを設定するには、**enable password** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトのパスワードに戻すには、このコマンドの **no** 形式を使用します。

構文

enable password [**level** *privilege-level*] {[**method** *hash-method***]** *unencrypted-password* | **encrypted** encrypted-password}

no enable password [**level** *privilege-level*]

パラメータ

- **level** privilege-level：パスワードが適用されるレベル。指定しない場合、レベルは 15 になります。（範囲：1 ～ 15）
- [**method** *hash-method***]** ：（オプション）クリアテキストパスワードの暗号化に使用する方式を指定します。サポートされる値：
  - **sha512**：基盤のハッシュアルゴリズムとしてSHA512を使用したHMACによるPBKDF2暗号化。**method** パラメータを指定しない場合は、これがデフォルトの方式になります。
- *unencrypted-password*：このレベルのパスワード。（範囲：0 ～ 159 文字）
- **encrypted** encrypted-password：パスワードが暗号化され、ソルトを使用してハッシュされることを指定します。すでに暗号化されているパスワード（たとえば、別のデバイスのコンフィギュレーション ファイルからコピーしたパスワード）を入力するには、このキーワードを使用します。*encrypted-password* は *$<type>$<salt>$<encrypted-password* > 形式で指定します。ここで、
  - ***<type>***：ハッシュの生成に使用するハッシュアルゴリズムのタイプを示す整数値です。
  - **<salt>**：ソルトに使用する 96 ビットの base64 エンコーディング（長さ：16 バイト）
  - ***<encrypted-password>***：暗号化されたハッシュ出力のBase64エンコーディング（長さ：86 バイト）

デフォルト設定

level のデフォルは 15 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

unencrypted-password は、パスワードの複雑さの要件を順守する必要があります。

管理者が新しい **enable** パスワードを設定すると、そのパスワードは自動的に暗号化され、コンフィギュレーションファイルに保存されます。どのようにパスワードを入力した場合でも、コンフィギュレーション ファイルにはキーワード **encrypted** と暗号化された値で表示されます。暗号化されたキーワードを実際に入力する場合にのみ、管理者は **encrypted** キーワードを使用する必要があります。

あるスイッチ（たとえば、スイッチB）で設定されたパスワードを別のスイッチ（たとえば、スイッチ A）に手動でコピーする場合、管理者はスイッチ A で **enable** コマンドを入力するときに、この暗号化されたパスワードの前に **encrypted** を追加する必要があります。この方法では、2 つのスイッチのパスワードが同じになります。

暗号化されたキーワードを実際に入力する場合にのみ、管理者は **encrypted** キーワードを使用する必要があります。

generate-password オプションを使用すると、パスワードを入力する代わりに、ランダムに生成されたパスワードの提案がユーザーに示されます。この提案は、現在のすべてのパスワード強度設定に準拠します

ユーザーは、提示されたパスワードを受け入れるか拒否するかを選択できます。ユーザーがパスワードを受け入れることを選択した場合、このパスワードは、構成ファイルで設定したイネーブルレベルに対して（暗号化された形式で）追加されます。

ユーザーがパスワードの提案を拒否した場合は、このイネーブルレベルを設定するためにコマンドを再度入力する必要があります。

例

例 1：このコマンドは、すでに暗号化されているパスワードを設定します。パスワードは、入力されたとおりにコンフィギュレーションファイルにコピーされます。このパスワードを使用してデバイスにログインするには、ユーザは暗号化されていない形式を知っている必要があります。

```
switchxxxxxx(config)# enable password encrypted
$15$TqKC13RgV/QJb2Ma$4JmeD7wgRGH2iwGKMM+g4M53uQxpOMlhkUN56UMAEUuMqhw0bsRH27zakc7
2hLxt/YhEknPA6LX7fTgqwZn6Vw==
```

例 2：次に、レベル 1 の暗号化されていないパスワードを設定する例を示します（コンフィギュレーション ファイルで暗号化されます）。

```
switchxxxxxx(config)# enable password level 1 let-me-In
```

例 3：この例のコマンドには、**generate-password** キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを**受け入れる**ことを選択しています。

```
switchxxxxxx(config)# enable password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
“Configuration and password are added to device configuration. Please Note
password for future use”
```

例 4：この例のコマンドには、generate-password キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを拒否することを選択しています。

```
switchxxxxxx(config)# enable password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
"Auto generated password rejected by user. Password configuration is not added to
device configuration"
```

service password-recovery

パスワード回復メカニズムを有効にするには、**service password-recovery** グローバル コンフィギュレーション モード コマンドを使用します。このメカニズムにより、デバイスのコンソール ポートに物理的にアクセスしているエンドユーザは、ブート メニューを表示して、パスワードの回復プロセスを起動することができます。パスワード回復メカニズムを無効にするには、**no service password-recovery** コマンドを使用します。パスワード回復メカニズムが無効になっている場合でも、ブート メニューへのアクセスは許可され、ユーザはパスワード回復プロセスを起動できます。この場合の異なる点は、すべてのコンフィギュレーション ファイルとすべてのユーザ ファイルが削除されることです。「All the configuration and user files were removed」というログ メッセージが端末に生成されます。

構文

service password-recovery

no service password-recovery

デフォルト設定

サービス パスワードの回復はデフォルトで有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

- パスワードの回復が有効になっている場合、ユーザはブート メニューにアクセスし、ブート メニューでパスワードの回復を起動することができます。すべてのコンフィギュレーション ファイルとユーザ ファイルが保持されます。
- パスワードの回復が無効になっている場合、ユーザはブート メニューにアクセスし、ブート メニューでパスワードの回復を起動することができます。コンフィギュレーション ファイルとユーザ ファイルが削除されます。
- デバイスでセンシティブ データをユーザ定義パスフレーズで保護するように設定している場合（Secure Sensitive Data の場合）、パスワードの回復が有効になっていても、[Boot] メニューからパスワードの回復をトリガーできません。

例

次のコマンドはパスワードの回復を無効にします。

```
switchxxxxxx(config)# no service password recovery
Note that choosing to use Password recovery option in the Boot Menu during the boot
process will remove the configuration files and the user files. Would you like to continue
 ? Y/N.
```

username

ユーザ名ベースのユーザ認証アカウントを作成または編集するには、**username** グローバル コンフィギュレーション モード コマンドを使用します。ユーザアカウントを削除するには **no** 形式を使用します。

構文

username name {[**method** *hash-method*] **password** {*unencrypted-password* | {**encrypted** encrypted-password}} | {**privilege** privilege-level {[**method** *hash-method*] *unencrypted-password* | {**encrypted** encrypted-password}}}}

username name {[**method** hash-method] **generate-password** | {**privilege** privilege-level{[**method** hash-method] **generate-password**}

no username name

パラメータ

- ***name***：ユーザの名前。（範囲：1 ～ 20 文字）
- [**method** *hash-method*]：（オプション）クリアテキストパスワードの暗号化に使用する方式を指定します。サポートされる値：
  - **sha512**：基盤のハッシュアルゴリズムとして SHA512 を使用した HMAC による PBKDF2 暗号化。**method** パラメータを指定しない場合は、これがデフォルトの方式になります。
- **password**：このユーザ名のパスワードを指定します。
- unencrypted-password：ユーザの認証パスワード。（範囲：1 ～ 64）
- **encrypted** encrypted-password：パスワードが暗号化され、ソルトを使用してハッシュされることを指定します。すでに暗号化されているパスワード（たとえば、別のデバイスのコンフィギュレーション ファイルからコピーしたパスワード）を入力するには、このキーワードを使用します。*encrypted-password* は *$<type>$<salt>$<encrypted-password* > 形式で指定します。ここで、
  - ***<type>***：ハッシュの生成に使用するハッシュアルゴリズムのタイプを示す整数値です。
  - ***<salt>***：ソルトに使用する 96 ビットの Base64 エンコーディング（長さ：16 バイト）
  - ***<encrypted-password>***：暗号化されたハッシュ出力の Base64 エンコーディング（長さ：86 バイト）
- **generate-password** ：デバイスは、ランダムベースのパスワード提案を自動的に生成します。ユーザーは、提示されたパスワードを受け入れるか拒否するかを選択できます。

- **privilege** privilege-level：ユーザアカウントの権限レベル。指定しない場合、レベルは 1 になります。（範囲：1 ～ 15）。

デフォルト設定

ユーザは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

unencrypted-password は、パスワードの複雑さの要件を順守する必要があります。

generate-password オプションを使用すると、パスワードを入力する代わりに、ランダムに生成されたパスワードの提案がユーザーに示されます。この提案は、現在のすべてのパスワード強度設定に準拠します。ユーザーは、提示されたパスワードを受け入れるか拒否するかを選択できます。ユーザーがパスワードを受け入れることを選択した場合、このパスワードは、構成ファイルで設定したユーザー名に対して（暗号化された形式で）追加されます。

ユーザーがパスワードの提案を拒否した場合は、このユーザーを設定するためにコマンドを再度入力する必要があります。

ユーザーは、（現在のユーザー名を維持しつつ）現在のセッションへのログインに使用するアカウントのパスワードの変更を要求する場合、現在のパスワードを知っている必要があります。ユーザーは、現在のパスワードをクリアテキスト形式で入力するように求められます。パスワードの変更は、ユーザーが現在のパスワードを正しく入力した場合にのみ成功します。

最後のレベル 15 のユーザーは削除できず、リモートユーザーになることもできません。

例

例 1：ユーザー tom（レベル 15）の暗号化されていないパスワードを設定します。パスワードは、コンフィギュレーション ファイルで暗号化されます。

```
switchxxxxxx(config)# username tom password 1234Ab$5678
```

例 2：すでに暗号化されているユーザ jerry（レベル 15）用のパスワードを設定します。パスワードは、入力されたとおりにコンフィギュレーションファイルにコピーされます。使用するには、ユーザが暗号化前の形式を知っている必要があります。

```
switchxxxxxx(config)# username jerry privilege 15 encrypted
$15$TqKC13RgV/QJb2Ma$4JmeD7wgRGH2iwGKMM+g4M53uQxpOM1hkUN56UMAEUuMqhw0bsRH27zakc72hLxt/YhEknPA6LX7fTgqwZn6Vw==
```

例 3：この例のコマンドには、generate-password キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを受け入れることを選択しています。

```
switchxxxxxx(config)# username tom generate-password privilege 15
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
"Configuration and password are added to device configuration. Please Note
password for future use."
```

例 4：この例のコマンドには、generate-password キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを拒否することを選択しています。

```
switchxxxxxx(config)# username tom generate-password privilege 15
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
“Auto generated password rejected by user. Password configuration is not added to
device configuration.”
```

show users accounts

show users accounts 特権 EXEC モード コマンドは、ユーザのローカル データベースに関する情報を表示します。

構文

show users accounts

コマンド モード

特権 EXEC モード

例

次の例では、ユーザ ローカル データベースに関する情報を表示します。

```
switchxxxxxx# show users accounts

Username        Privilege       Password
--------        ---------       Expiry date
Bob             15              ----------
Robert          15              Jan 18 2005
Smith           15              Jan 19 2005
```

次の表に、この出力で表示される重要なフィールドについて説明します。

フィールド	説明
Username	ユーザ名。
Privilege	ユーザの特権レベル。
Password Expiry date	ユーザのパスワードの有効期限。

aaa accounting login start-stop

デバイス管理セッションのアカウンティングを有効にするには、グローバル コンフィギュレーション モードで **aaa accounting login start-stop** コマンドを使用します。アカウンティングを無効にするには、このコマンドの **no** 形式を使用します。

構文

aaa accounting login start-stop group {**radius** | **tacacs+**}

no aaa accounting login start-stop

パラメータ

- **group radius**：アカウンティングに RADIUS サーバを使用します。
- **group tacacs+**：アカウンティングに TACACS+ サーバを使用します。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、デバイス管理セッション（SNMP ではなく、Telnet、シリアル、および WEB）の記録を有効にします。

ユーザ名で識別されたユーザのみが記録されます（たとえば、ラインパスワードでログインしたユーザは記録されません）。

アカウンティングが有効になっている場合、ユーザがログインまたはログアウトするたびに、デバイスが RADIUS サーバに「開始」メッセージまたは「停止」メッセージを送信します。

デバイスは、利用可能な RADIUS または TACACS+ サーバの設定された優先順位を使用して、RADIUS または TACACS+ サーバを選択します。

次の表では、サポートされている RADIUS アカウンティング属性値と、その属性値がスイッチによりどのメッセージで送信されるかについて説明します。

名前	Start メッセージ	Stop メッセージ	説明
User-Name (1)	対応	対応	ユーザの ID。
NAS-IP-Address (4)	対応	対応	RADIUS サーバとのセッションで使用されるスイッチの IP アドレス。

名前	Start メッセージ	Stop メッセージ	説明
Class (25)	対応	対応	指定したセッションのすべてのアカウンティング パケットに任意の値が含まれています。
Called-Station-ID (30)	対応	対応	管理セッションで使用されるスイッチの IP アドレス。
Calling-Station-ID (31)	対応	対応	ユーザの IP アドレス。
Acct-Session-ID (44)	対応	対応	一意のアカウンティング ID。
Acct-Authentic (45)	対応	対応	サプリカントの認証方法を示します。
Acct-Session-Time（46）	非対応	対応	ユーザがログインしていた期間を示します。
Acct-Terminate-Cause（49）	非対応	対応	セッションが終了した理由。

次の表では、サポートされている TACACS+ アカウンティング引数と、その引数がスイッチによりどのメッセージで送信されるかについて説明します。

名前	説明	Start メッセージ	Stop メッセージ
task_id	一意のアカウンティング セッション ID。	対応	対応
user	ログイン認証用に入力されたユーザ名。	対応	対応
rem addr	ユーザの IP アドレス	対応	対応
elapsed-time	ユーザがログインしていた期間を示します。	非対応	対応
reason	セッションが終了した理由。	非対応	対応

例

```
switchxxxxxx(config)# aaa accounting login start-stop group radius
```

aaa accounting dot1x

802.1x セッションのアカウンティングを有効にするには、**aaa accounting dot1x** グローバル コンフィギュレーション モード コマンドを使用します。アカウンティングを無効にするには、このコマンドの **no** 形式を使用します。

構文

aaa accounting dot1x start-stop group radius

no aaa accounting dot1x start-stop group radius

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、802.1x セッションの記録を有効にします。

アカウンティングが有効になっている場合、ネットワークに対してユーザがログインまたはログアウトするたびに、デバイスがRADIUSサーバに開始メッセージまたは停止メッセージを送信します。デバイスは、利用可能なRADIUSサーバの設定された優先順位を使用して、RADIUSサーバを選択します。

新しいサプリカントにより古いサプリカントが置き換えられた場合（ポートステートが許可のままでも）、ソフトウェアは古いサプリカントの停止メッセージと、新しいサプリカントの開始メッセージを送信します。

マルチセッション モード（dot1x 複数ホスト認証）では、ソフトウェアは認証されたサプリカントごとに開始メッセージまたは停止メッセージを送信します。

複数ホスト モード（dot1x 複数ホスト）では、ソフトウェアは認証されたサプリカントにのみ開始メッセージまたは停止メッセージを送信します。ポートがforce-authorizedの場合、ソフトウェアは開始メッセージまたは停止メッセージを送信しません。

ソフトウェアは、ゲスト VLAN または認証されていない VLAN 上でトラフィックを送信しているホストの開始メッセージまたは停止メッセージを送信しません。

次の表では、サポートされているRADIUSアカウンティング属性値と、その属性値がスイッチによりいつ送信されるかについて説明します。

名前	Start	停止	説明
User-Name (1)	対応	対応	サプリカントの ID。

名前	Start	停止	説明
NAS-IP-Address (4)	対応	対応	RADIUS サーバとのセッションで使用されるスイッチの IP アドレス。
NAS-Port (5)	対応	対応	サプリカントがログインしているスイッチ ポート。
Class (25)	対応	対応	特定のセッションのすべてのアカウンティング パケットに含まれる任意の値。
Called-Station-ID (30)	対応	対応	スイッチの MAC アドレス。
Calling-Station-ID (31)	対応	対応	サプリカントの MAC アドレス。
Acct-Session-ID (44)	対応	対応	一意のアカウンティング ID。
Acct-Authentic (45)	対応	対応	サプリカントの認証方法を示します。
Acct-Session-Time（46）	非対応	対応	サプリカントがログインしていた時間を示します。
Acct-Terminate-Cause（49）	非対応	対応	セッションが終了した理由。
Nas-Port-Type (61)	対応	対応	サプリカントの物理ポートタイプを示します。

例

```
switchxxxxxx(config)# aaa accounting dot1x start-stop group radius
```

show accounting

show accounting EXEC モード コマンドは、スイッチでどのタイプのアカウンティングが有効になっているかに関する情報を表示します。

構文

show accounting

コマンド モード

ユーザ EXEC モード

例

次の例では、アカウンティング ステータスに関する情報を表示しています。

```
switchxxxxxx# show accounting
Login: Radius
802.1x: Disabled
```

passwords complexity

パスワードの複雑さが有効になっている場合のパスワードの最小要件を制御するには、**passwords complexity** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

passwords complexity {**min-length** number} | {**min-classes** number} | {**no-repeat** number} | **not-current** | **not-username** | **not-manufacturer-name**

no passwords complexity min-length | **min-classes** | **no-repeat** | **not-current** | **not-username** | **not-manufacturer-name**

パラメータ

- **min-length** number：パスワードの最小長を設定します。（範囲：8 ー 64）
- **min-classes** number：最小限の文字クラス（標準のキーボードで利用可能な大文字、小文字、数字、および特殊文字など）を設定します。（範囲：1 ～ 4）
- **no-repeat** number：新しいパスワードで連続して繰り返すことができる最大文字数を指定します。（範囲：1 ー 16）
- **not-current**：新しいパスワードを現在のパスワードと同じにできないことを指定します。
- **not-username**：パスワードでユーザ名またはユーザ名の大文字と小文字を変更した類似の名前を繰り返したり、逆にして使用することができないことを指定します。
- **not-manufacturer-name**：パスワードで製造者名または製造者名の大文字と小文字を変更した類似の名前を繰り返したり、逆にして使用することができないことを指定します。

デフォルト設定

最小長は 8 です。

クラスの数は 3 です。

no-repeat のデフォルトは 3 です。

その他のすべての制御はデフォルトで有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、最小限必要なパスワードの長さを 10 文字に設定しています。

```
switchxxxxxx(config)# passwords complexity min-length 10
```

passwords aging

パスワード エージングを適用するには、**passwords aging** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

passwords aging *days*

no passwords aging

パラメータ

- ***days***：パスワード変更が強制されるまでの日数を指定します。0 を使用すると、エージングを無効にできます。（範囲：0 ～ 365）。

デフォルト設定

パスワードエージングは、デフォルトで無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

パスワードエージング設定は、ローカルデータベースのユーザー、イネーブルパスワード、および回線パスワードに関連します。

パスワードエージングが有効になっている場合、パスワードの有効期限日まで 10 日以内の期間にユーザーがデバイスにログインすると、パスワードがまもなく期限切れになることを通知する警告が表示されます。ユーザーは、パスワードを変更しなくてもデバイスへのアクセスが許可されます。この段階で、期限日までにパスワードを変更するのはユーザーの責任です。

パスワードの有効期限が切れた後にユーザーがデバイスにログインすると、新しいパスワードを入力するように求められ、新しいパスワードが設定されるまでデバイス管理へのアクセスが許可されません。

パスワード エージングを無効にするには、**passwords aging 0** を使用します。

例

次の例では、エージング タイムを 24 日に設定しています。

```
witchxxxxxx(config)# passwords aging 24
```

password complexity history

passwords complex history グローバル コンフィギュレーション モード コマンドは、パスワードを再利用できるようになるまでに必要なパスワード変更の回数を設定します。デフォルト設定に戻すには、このコマンドの no 形式を使用します

構文

passwords complexity history *number*

no passwords complexity history

パラメータ

number：パスワードの再利用が可能になるまでに必要なパスワード変更の回数を指定します。（範囲：3 ～ 12）。

デフォルト設定

デフォルトでは、パスワードの再利用までに必要なパスワード変更の回数は 12 回です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

この設定は、ローカルユーザーのパスワード、回線パスワード、およびイネーブルパスワードに関連します。

ローカルユーザーの履歴は、デバイスでサポートされているローカルユーザー数までのユーザーについて保持されます。

設定のダウンロード中は、パスワード履歴はチェックされません。

パスワード履歴チェックが無効になっている場合でも、パスワード履歴は保持されます。

例

次の例では、パスワードの再利用が可能になるまでに必要なパスワード変更の回数を 10 に設定しています。

```
switchxxxxxx(config)# passwords complexity history 10
```

aaa login-history file

aaa login-history file グローバル コンフィギュレーション モード コマンドは、ログイン履歴ファイルへの書き込みを有効にします。ログイン履歴ファイルへの書き込みを無効にするには、このコマンドの no 形式を使用します。

構文

aaa login-history file

no aaa login-history file

デフォルト設定

ログイン履歴ファイルへの書き込みが有効になっています。

コマンド モード

グローバル コンフィギュレーション モード。

使用上のガイドライン

ログイン履歴は、デバイスの内部バッファに保存されます。

例

次の例では、ログイン履歴ファイルへの書き込みを有効にしています。

```
switchxxxxxx(config)# aaa login-history file
```

show passwords configuration

show passwords configuration 特権 EXEC モード コマンドは、パスワードの管理設定に関する情報を表示します。

構文

show passwords configuration

パラメータ

該当なし

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords history is enabled, the number of previous passwords to check is 12
Passwords complexity is enabled with the following attributes:
 Minimal length: 8 characters
 Minimal classes: 3
 Maximum consecutive same characters: 3
 Password cannot include more than 2 sequential numbers or characters
Password cannot contain the username, manufacturer name or product name
Password must be different from current password
Password cannot contain commonly used passwords or known breached passwords
```

show users login-history

show users **login-history** 特権 EXEC モードコマンドは、ユーザーのログイン履歴に関する情報を表示します。

構文

show users login-history [**username** name]

パラメータ

- name：ユーザーの名前。（範囲：1 ～ 20 文字）。

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード。

使用上のガイドライン

このコマンドは、Radius や TACACS などのリモート AAA サーバーを使用して認証されたユーザーではなく、ローカル AAA データベースを使用して認証されたユーザーに関する情報を表示します。

例

次に、ユーザーのログイン履歴に関する情報を表示する例を示します。

例 1：次の例では、180 秒以内に 18 回を超えてログイン試行に失敗した場合に、すべてのログイン要求を 180 秒間ブロックする方法を示します。

```
switchxxxxxx# show users login-history
File save: Enabled.
Login Time              Username  Protocol    Location
--------------------
Jan 18 2004 23:58:17    Robert    HTTP        172.16.1.8
Jan 19 2004 07:59:23    Robert    HTTP        172.16.1.8
Jan 19 2004 08:23:48    Bob       Serieal
Jan 19 2004 08:29:29    Robert    HTTP        172.16.1.8
Jan 19 2004 08:42:31    John      SSH         172.16.0.1
Jan 19 2004 08:49:52    Betty     Telnet      172.16.1.7
```

自動更新と自動設定

この章は、次の項で構成されています。

- boot host auto-config （226 ページ）
- boot host auto-update （228 ページ）
- show boot （229 ページ）
- ip dhcp tftp-server ip address （231 ページ）
- ip dhcp tftp-server file （232 ページ）
- ip dhcp tftp-server image file （233 ページ）
- show ip dhcp tftp-server （234 ページ）

boot host auto-config

DHCP を介した自動設定を有効にするには、**boot host auto-config** グローバル コンフィギュレーション モード コマンドを使用します。DHCP 自動設定を無効にするには、このコマンドの **no** 形式を使用します。

構文

boot host auto-config [**tftp** | **scp** | **auto** [*extension*]]

no boot host auto-config

パラメータ

- **tftp**：自動設定で TFTP プロトコルのみが使用されます。
- **scp**：自動設定で SCP プロトコルのみが使用されます。
- **auto**：（デフォルト）自動設定で、コンフィギュレーション ファイルの拡張子に応じて TFTP プロトコルまたは SCP プロトコルが使用されます。このオプションを選択した場合は、extension パラメータを指定できます。指定しない場合は、デフォルトの拡張子が使用されます。
- ***extension***：SCP ファイルの拡張子。値が指定されていない場合は、「scp」が使用されます。（範囲：1 ～ 16 文字）

デフォルト設定

デフォルトでは、**auto** オプションを使用して有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

コンフィギュレーション ファイルをダウンロードまたはアップロードするために、TFTP プロトコルまたは SCP プロトコルが使用されます。

例 1。次の例では、auto モードを指定し、SCP 拡張子として「scon」を指定しています。

```
switchxxxxxx(config)# boot host auto-config auto scon
```

例 2。次の例では、auto モードを指定し、SCP 拡張子を指定していません。

この場合は、「scp」が使用されます。

```
switchxxxxxx(config)# boot host auto-config auto
```

例 3。次の例では、SCP プロトコルのみが使用されるように指定しています。

```
switchxxxxxx(config)# boot host auto-config scp
```

boot host auto-update

DHCP を介した自動更新のサポートを有効にするには、**boot host auto-update** グローバル コンフィギュレーション モード コマンドを使用します。DHCP 自動設定を無効にするには、このコマンドの **no** 形式を使用します。

構文

boot host auto-update [**tftp** | **scp** | **auto** [*extension*]]

no boot host auto-update

パラメータ

- **tftp**：自動更新で TFTP プロトコルのみが使用されます。
- **scp**：自動更新で SCP プロトコルのみが使用されます。
- **auto**（デフォルト）：自動更新は間接イメージファイルの拡張子に応じて TFTP プロトコルまたは SCP プロトコルを使用します。このオプションを選択した場合は、extension パラメータを指定できます。指定しない場合は、デフォルトの拡張子が使用されます。
- ***extension***：SCP ファイルの拡張子。値が指定されていない場合は、「scp」が使用されます。（範囲：1 ～ 16 文字）

デフォルト設定

デフォルトでは、**auto** オプションを使用して有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

イメージ ファイルをダウンロードまたはアップロードするために、TFTP プロトコルまたは SCP プロトコルが使用されます。

例 1：次の例では、auto モードを指定し、SCP 拡張子として「scon」を指定しています。

```
switchxxxxxx(config)# boot host auto-update auto scon
```

例 2：次の例では、auto モードを指定し、SCP 拡張子を指定していません。この場合は、「scp」が使用されます。

```
switchxxxxxx(config)# boot host auto-update auto
```

例 3：次の例では、SCP プロトコルのみが使用されるように指定しています。

```
switchxxxxxx(config)# boot host auto-update scp
```

show boot

IP DHCP 自動設定プロセスのステータスを表示するには、**show boot** 特権 EXEC モード コマンドを使用します。

構文

show boot

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
Download Protocol: auto
SCP protocol will be used for files with extension: scp
Configuration file auto-save: enabled
Auto Config State: Finished successfully
Server IP address: 1.2.20.2
Configuration filename: /config/configfile1.cfg
      Auto Update
      -----------
Image Download via DHCP: enabled
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
Download Protocol: scp
Configuration file auto-save: enabled
Auto Config State: Opening <hostname>-config file
      Auto Update
      -----------
Image Download via DHCP: enabled
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
"Download Protocol: scp
Configuration file auto-save: enabled
Auto Config State: Downloading configuration file
      Auto Update
      -----------
Image Download via DHCP: enabled
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
Download Protocol: tftp
Configuration file auto-save: enabled
Auto Config State: Searching device hostname in indirect file
      Auto Update
      -----------
Image Download via DHCP: enabled
```

```
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
Download Protocol: tftp
Configuration file auto-save: enabled
      Auto Update
      -----------
Image Download via DHCP: enabled
Auto Update State: Downloaded indirect image file
Indirect Image filename: /image/indirectimage.txt
```

ip dhcp tftp-server ip address

バックアップ サーバの IP アドレスを設定するには、**ip dhcp tftp-server ip address** グローバル コンフィギュレーション モード コマンドを使用します。このアドレスは、DHCP サーバからアドレスが受信されなかった場合にスイッチにより使用されるデフォルト アドレスとなります。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

ip dhcp tftp-server ip address *ip-addr*

no ip dhcp tftp-server ip address

パラメータ

- ***ip-addr***：TFTP サーバまたは SCP サーバの、IPv4 アドレス、IPv6 アドレス、または DNS 名。

デフォルト設定

IP アドレスはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

バックアップ サーバには、TFTP サーバまたは SCP サーバを使用できます。

例

例 1。次の例では、TFTP サーバの IPv4 アドレスを指定しています。

```
switchxxxxxx(config)# ip dhcp tftp-server ip address 10.5.234.232
```

例 2。この例では、TFTP サーバの IPv6 アドレスを指定します。

```
switchxxxxxx(config)# ip dhcp tftp-server ip address 3000:1::12
```

例 3。この例では、TFTP サーバの IPv6 アドレスを指定します。

```
switchxxxxxx(config)# ip dhcp tftp-server ip address tftp-server.company.com
```

ip dhcp tftp-server file

コンフィギュレーション ファイルが DHCP サーバから受信されなかった場合にバックアップ サーバからダウンロードするコンフィギュレーション ファイルの完全なファイル名を設定するには、**ip dhcp tftp-server file** グローバル コンフィギュレーション モード コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。

構文

ip dhcp tftp-server file *file-path*

no ip dhcp tftp-server file

パラメータ

- ***file-path***：サーバ上のコンフィギュレーション ファイルの完全なファイル パスおよび名前。

デフォルト設定

ファイル名はありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

バックアップ サーバには、TFTP サーバまたは SCP サーバを使用できます。

例

```
switchxxxxxx(config)# ip dhcp tftp-server file conf/conf-file
```

ip dhcp tftp-server image file

イメージファイルがDHCPサーバから受信されなかった場合にバックアップサーバからダウンロードするイメージファイルの間接ファイル名を設定するには、**ip dhcp tftp-server image file** グローバル コンフィギュレーション モード コマンドを使用します。ファイル名前を削除するには、このコマンドの **no** 形式を使用します。

構文

ip dhcp tftp-server image file *file-path*

no ip dhcp tftp-server image file

パラメータ

- ***file-path***：サーバ上のコンフィギュレーション ファイルの完全な間接ファイル パスおよび名前。

デフォルト設定

ファイル名はありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

バックアップ サーバには、TFTP サーバまたは SCP サーバを使用できます。

例

```
switchxxxxxx(config)# ip dhcp tftp-server image file imag/imag-file
```

show ip dhcp tftp-server

バックアップ サーバに関する情報を表示するには、**show ip dhcp tftp-server** EXEC モード コマンドを使用します。

構文

show ip dhcp tftp-server

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

バックアップ サーバには、TFTP サーバまたは SCP サーバを使用できます。

例

```
show ip dhcp tftp-server
server address
active 1.1.1.1 from sname
manual 2.2.2.2
file path on server
active conf/conf-file from option 67
manual conf/conf-file1
```

Bluetooth コマンド

この章は、次の項で構成されています。

- bluetooth device-name （236 ページ）
- bluetooth pin （237 ページ）
- shutdown （238 ページ）
- show bluetooth status （239 ページ）

bluetooth device-name

ペアリングプロセスおよびその後の Bluetooth 操作で使用する Bluetooth デバイス名を設定するには、Bluetooth インターフェイスモードで bluetooth device-name コマンドを使用します。デフォルト設定に戻すには、コマンドの no 形式を使用します。

構文

bluetooth device-name *device-name*

no bluetooth device-name

パラメータ

デバイス名：Bluetooth インターフェイスに関連付けられた名前を指定します。（長さ：1 ～ 20 文字）。

デフォルト設定

デフォルトの device-name はデバイスのホスト名です。

コマンド モード

Bluetooth インターフェイス コンフィギュレーション モード。

使用上のガイドライン

Bluetooth インターフェイスに関連付けられたデバイス名を設定するには、bluetooth device-name コマンドを使用します。Bluetooth デバイス名は、Bluetooth ペアリングプロセスで Bluetooth インターフェイスを識別するために使用されます。Bluetooth デバイス名が設定されていない場合、デバイスのホスト名がデバイス名として使用されます。

例

次の例では、Bluetooth 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、Bluetooth インターフェイスのデバイス名として「Switch BT」を設定する方法を示します。

```
switchxxxxxx(config)# interface bluetooth 0
switchxxxxxx(config-if)# bluetooth device-name "Switch BT"
```

bluetooth pin

ペアリングプロセスで使用する 6 桁のピンを設定するには、Bluetooth インターフェイスモードで bluetooth pin コマンドを使用します。デフォルト設定に戻すには、コマンドの no 形式を使用します。

構文

bluetooth pin *pin*

no bluetooth pin.

パラメータ

PIN：4 桁の個人識別番号

デフォルト設定

デフォルトの PIN は 9999 です。

コマンド モード

Bluetooth インターフェイス コンフィギュレーション モード。

使用上のガイドライン

bluetooth pin コマンドを使用して、デバイスの Bluetooth インターフェイスと Bluetooth パートナー間の Bluetooth ペアリングプロセスで使用する 4 桁の PIN を設定します。

例

次に、Bluetooth インターフェイスで PIN を 1234 に設定する例を示します。

```
switchxxxxxx(config)# interface bluetooth 0
 switchxxxxxx(config-if)# shutdown
```

shutdown

Bluetoothインターフェイスの動作を無効にするには、インターフェイス（Bluetooth）コンフィギュレーション モードで shutdown コマンドを使用します。デフォルト設定に戻すには、コマンドの no 形式を使用します。

構文

shutdown

no shutdown

デフォルト設定

デフォルトでは Bluetooth インターフェイスがアクティブになっています

コマンド モード

インターフェイス（Bluetooth）コンフィギュレーション モード。

例

例 1

次の例では、Bluetooth の動作をシャットダウンします。

```
switchxxxxxx(config)# interface bluetooth 0
 switchxxxxxx(config-if)# shutdown
```

show bluetooth status

Bluetoothインターフェイスの設定とステータスに関する情報を表示するには、特権EXECモードで show bluetooth status コマンドを使用します。

構文

show bluetooth status

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード。

使用上のガイドライン

デバイスの Bluetooth インターフェイスに関する情報を表示するには、show bluetooth status コマンドを使用します。

例

例 1

次の例では、ドングルが USB ポートに挿入されていない場合のデフォルト状態での BT インターフェイス情報が表示されます。

```
switchxxxxxx# show bluetooth status
Dongle MAC: Not Available
BT Dongle Present: no
State: not ready
BT Local Name: switch112233 (the default)
PIN: 999999 (the default)
BT Partner Name: Not Available
```

例 2

次の例では、ドングルが USB ポートに挿入されており、ユーザーが Bluetooth インターフェイスでデバイス名と PIN を設定した場合の Bluetooth インターフェイス情報が表示されます。Bluetooth インターフェイスは検出可能ですが、リモートの Bluetooth パートナーにはまだ接続されていません。

```
switchxxxxxx# show bluetooth status
Dongle MAC: 00:1a:7d:da:71:13
Bus: USB
BT Dongle Present: Yes
State: Discoverable
BT Local Name: My_BT
PIN (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
BT Partner Name: Not Available
```

例 3

次の例では、Bluetooth インターフェイスがペアリングされ、リモートの Bluetooth パートナーに接続されている場合の Bluetooth インターフェイス情報が表示されます。

```
switchxxxxxx# show bluetooth status
Dongle MAC: 00:1a:7d:da:71:13
Bus: USB
BT Dongle Present: Yes
State: Connected
BT Local Name: My_BT
PIN (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
BT Partner Name: Tablet123
```

例 4

次の例では、Bluetooth インターフェイスがペアリングされ、リモートの Bluetooth パートナーに接続されている場合の Bluetooth インターフェイス情報が表示されます。switchxxxxxx# show bluetooth status

```
switchxxxxxx# show bluetooth status
Dongle MAC: 00:1a:7d:da:71:13
Bus: USB
BT Dongle Present: Yes
State: Admin Down
BT Local Name: My_BT
PIN (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
BT Partner Name: Not available
```

Bonjour コマンド

この章は、次の項で構成されています。

- bonjour enable （242 ページ）
- bonjour interface range （243 ページ）
- show bonjour （244 ページ）

bonjour enable

Bonjourをグローバルに有効にするには、グローバル コンフィギュレーション モードで**bonjour enable** コマンドを使用します。Bonjourをグローバルに無効にするには、このコマンドの**no**形式を使用します。

構文

bonjour enable

no bonjour enable.

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# bonjour enable
```

bonjour interface range

L2 インターフェイスを Bonjour L2 インターフェイス リストに追加するには、グローバル コンフィギュレーション モードで **bonjour interface range** コマンドを使用します。このリストから L2 インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

構文

bonjour interface range *interface-list*

no bonjour interface range [*interface-list*]

パラメータ

- ***interface-list*** : インターフェイスのリストを指定します。L2 マルチキャスト転送をサポートするインターフェイスのみを指定できます。LAN とポイントについて、サポートされるのは次のタイプです。OOB、イーサネット ポート、ポート チャネル、および VLAN。

デフォルト設定

リストには、デフォルトの VLAN と OOB が含まれています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

Bonjour L2 インターフェイス リストで Bonjour が有効なインターフェイス セットを指定します。

指定したインターフェイスを Bonjour L2 インターフェイス リストに追加するには、**bonjour interface range** *interface-list* コマンドを使用します。

Bonjour L2 インターフェイス リストから指定したインターフェイスを削除するには、**no bonjour interface range** *interface-list* コマンドを使用します。

Bonjour L2 インターフェイス リストをクリアするには、**no bonjour interface range** コマンドを使用します。

例

```
switchxxxxxx(config)# bonjour interface range VLAN 100-103
```

show bonjour

Bonjour 情報を表示するには、特権 EXEC モードで **show bonjour** コマンドを使用します。

構文

show bonjour [*interface-id*]

パラメータ

- ***interface-id***：インターフェイスを指定します。

コマンド モード

特権 EXEC モード

例

この例では、Bonjour ステータスを表示しています。

```
switchxxxxxx# show bonjour
Bonjour global status: enabled
Bonjour L2 interfaces list: vlans 1
Service     Admin Status     Oper Status
-------     ------------     --------------
csco-sb     enabled              enabled
http        enabled              enabled
https       enabled              disabled
ssh         enabled              disabled
telnet      enabled              disabled
```

CA 証明書コマンド

この章は、次の項で構成されています。

- ca-certificate install （246 ページ）
- ca-certificate revoke （248 ページ）
- show ca-certificate （249 ページ）
- show ca-certificate revocation （251 ページ）

ca-certificate install

CA 証明書を手動でインストールするには、グローバル コンフィギュレーション モードで **ca-certificate install** コマンドを使用します。静的 CA 証明書を削除するには、このコマンドの **no** 形式を使用します。

構文

ca-certificate install name *name* [**owner** owner]

no ca-certificate install {**name** *name* | **owner** *owner*}

パラメータ

- ***name***：証明書名を指定します。範囲は 1 ～ 160 文字です。
- ***owner***：証明書の所有者を指定します。これは、0 ー 32 文字の文字列です。所有者を指定しない場合、デフォルトで所有者は「Static」になります。

証明書を追加する場合は、証明書自体をコマンドラインのコマンドの後に続ける必要があります。

デフォルト設定

証明書がインストールされていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

CA 証明書をインストールするには、**ca-certificate install** *name* コマンドを使用します。

コマンドを実行すると、コマンドラインに証明書を入力するように求められます。

ユーザは証明書を入力するか貼り付ける必要があります。別の行にピリオドを入力すると、証明書の入力が完了したことを示します。

入力する証明書には pem 形式を使用する必要があります。

ユーザがシステムクロックを設定していないか、またはSNTPと同期していない場合、あるいはハードウェアベースのリアルタイムクロック（RTC）に基づいている場合、証明書は有効になりません。

最大 256 の証明書をインストールできます。

このコマンドの **no** 形式を使用して証明書を削除する場合は、特定の証明書を**名前**で削除できます。または、**owner**キーワードを使用して、特定の所有者に属するすべての静的証明書を削除できます。

例 1。次に、コマンドラインから CA 証明書をインストールする例を示します。

```
switchxxxxxx(config)# ca-certificate install root1
Please paste the input now, add a period (.) on a separate line after the
input,and press Enter.
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
OOg9XM1AxfOiqLlQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5sO4lv0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
-----END CERTIFICATE-----
switchxxxxxx(config)#
```

ca-certificate revoke

失効リストに証明書を追加するには、グローバル コンフィギュレーション モードで **ca-certificate revoke** コマンドを使用します。失効リストから証明書を削除するには、このコマンドの **no** 形式を使用します。

構文

ca-certificate revoke issuer *issuer* **serial-number** *serial-number*

no ca-certificate revoke issuer *issuer* **serial-number** *serial-number*

パラメータ

- ***issuer***：失効した証明書に表示する、すべてのパラメータを含む発行者の文字列（範囲：1 ～ 160 文字）。
- ***serial-number***：失効した証明書のシリアル番号。これは 16 進形式の文字列です（範囲：1 ～ 16 組の文字）。

デフォルト設定

失効した証明書はありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

失効リストに証明書を追加するには、**ca-certificate revoke** コマンドを使用します。

発行者情報を入力する場合は、証明書に表示される発行者の文字列を完全に入力する必要があります。文字列にスペースが含まれている場合は、全体を引用符で囲む必要があります。

このリストに証明書を追加すると、この証明書のステータスが「revoked」に変更されます（インストールされている場合）。証明書をインストールしていない場合に後日インストールすると、失効ステータスが返されます。

最大 512 の証明書を失効リストに追加できます。

例 1。次に、失効リストに CA 証明書を追加する例を示します。

```
switchxxxxxx(config)# ca-certificate revoke issuer "C=US, O=GlobalSign nv-sa, CN=GlobalSign
 Organization Validation" serial-number 10ad0044a8418ad5005e45b6
switchxxxxxx(config)#
```

show ca-certificate

デバイスにインストールされている CA 証明書とそのステータスを表示するには、特権 EXEC モードで **show ca-certificate** コマンドを使用します。

構文

show ca-certificate [name *name*][type *type*][owner *owner-name*][detailed]

パラメータ

- **name** *name*：証明書名を指定します。（範囲：1 ー 160 文字）。
- **type** *type*：証明書タイプを指定します。使用可能な値は、static、dynamic、または signer です。
- **owner** *owner-name*：証明書所有者の名前を指定します。これは、ダイナミック証明書をインストールしたアプリケーションです。（範囲：1 ～ 32 文字）。
- **detailed**：このオプションパラメータは、表示される証明書の詳細情報を表示します。このパラメータを使用しない場合は、証明書ごとに限られた情報のみが表示されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

インストール済みのすべての CA 証明書を表示するには、**show ca-certificate** コマンドを使用します。

証明書のサブセットの情報を表示するには、オプションの **name**、**type**、および **owner** パラメータを使用します。

例 1：次に、すべての静的 CA 証明書の情報を簡潔に表示する例を示します。

```
switchxxxxxx# show ca-certificate type static
Name           Type    Owner     Valid From   Valid To     Status
-------------  ------  --------  -----------  -----------  ----------
local.cert     static  rnd       03-Aug-2019  03-Aug-2020  Valid
app1.cert1     static  app1      16-Jan-2021  16-Jul-2023  Premature
app1.cert2     static  app1      15-Mar-2017  14-Mar-2018  Expired
trusted-cert1  static  app2      27-Jun-2019  26-Jun-2024  Valid
certif3        static  app3      08-Feb-2018  08-Feb-2020  Revoked
```

例 2：次に、すべての CA 情報の詳細情報を表示する例を示します。

```
switchxxxxxx# show ca-certificate detailed
>C-CountryName, ST-StateOrProvinceName, L-Locality, O-Organization,
>OU-OrganizationalUnit, CN-CommonName
cert1
  Type: Signer
  Owner: N/A
```

```
 Version: 3 (0x2)
 Serial Number: 10:ad:00:44:a8:41:8a:d5:00:5e:45:b6
 Issuer: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
 Status: Valid
 Validity
   Not Before: Nov 21 08:00:00 2015 GMT
   Not After : Nov 22 07:59:59 2020 GMT
 Subject: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
 Public Key Type: ECDSA_P256
 Public Key Length: 2048 bits
   Signature Algorithm: sha256RSA
certA
 Type: Static
 Owner: Static
 Parent: cert1
 Version: 3 (0x2)
 Serial Number: 10:e6:fc:62:b7:41:8a:d5:00:5e:45:b6
 Issuer: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
 Status: Not Valid (expired)
 Validity
   Not Before: Nov 21 08:00:00 2016 GMT
   Not After : Nov 22 07:59:59 2017 GMT
 Subject: C=US, ST=California, L=San Francisco, O=AKB Foundation, Inc.,
          CN=*.wikipedia.org
 Finger print: DC72343 DC88A988 127897BC BB789788
 Public Key Type: ECDSA_P256
 Public Key Length: 2048 bits
   Signature Algorithm: sha256RSA
 certB
 Type: Dynamic
 Owner: PnP
 Parent: cert1
 Version: 3 (0x2)
 Serial Number: 88:cc:55:ae:a8:41:8a:d5:00:5e:45:b6
 Issuer: C=US, O=Google Trust Services, CN=GTS CA 101
 Status: Not Valid (revoked)
 Validity
   Not Before: Sep 21 08:00:00 2019 GMT
   Not After : Sep 22 07:59:59 2020 GMT
 Subject: C=US, S=California, L=Mountain View O=Google LLC, CN=*.google.com
 Finger print: DC789788 DC88A988 127897BC BB789788
 Public Key Type: ECDSA_P256
 Public Key Length: 2048 bits
 Signature Algorithm: sha256RSA
```

show ca-certificate revocation

CA 証明書の失効リストを表示するには、特権 EXEC モードで **show ca-certificate revocation** コマンドを使用します。

構文

show ca-certificate revocation

コマンド モード

特権 EXEC モード

使用上のガイドライン

CA 証明書の失効リストを表示するには、**show ca-certificate revocation** コマンドを使用します。

例次のように失効リストが表示されます。

```
switchxxxxxx# show ca-certificate revocation
>C-CountryName, ST-StateOrProvinceName, L-Locality, O-Organization,
>OU-OrganizationalUnit, CN-CommonName
  Issuer: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
  Serial Number: 10:ad:00:44:a8:41:8a:d5:00:5e:45:b6
------------------------------------------------------------------------
  Issuer: C=US, O=Google Trust Services, CN=GTS CA 101
  Serial Number: 00:9e:44:1b:49:08:8d:75:bb:02:00:00:00:00:40:a5:b4
```

CBD Probe コマンド

この章は、次の項で構成されています。

- cbd probe enable （254 ページ）
- cbd address （255 ページ）
- cbd organization name （257 ページ）
- cbd network name （258 ページ）
- cbd key （259 ページ）
- cbd connection enable （260 ページ）
- cbd reset （261 ページ）
- clear cbd probe database （262 ページ）
- show cbd （263 ページ）

cbd probe enable

デバイスで Cisco Business Dashboard Probe 操作を有効にするには、グローバル コンフィギュレーション モードで **cbd probe enable** コマンドを使用します。Cisco Business Dashboard Probe 操作を無効にするには、このコマンドの **no** 形式を使用します。

構文

cbd probe enable

no cbd probe enable

デフォルト設定

Cisco Business Dashboard プローブが無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

コマンドを使用して、デバイスで Cisco Business Dashboard Probe を有効にします。

例

次に、デバイスで Cisco Business Dashboard Probe を有効にする例を示します。

```
switchxxxxxx(config)# cbd probe enable
This operation may take a few seconds....
```

cbd address

Cisco Business Dashboard の詳細を設定するには、グローバル コンフィギュレーション モードで **cbd address** コマンドを使用します。Cisco Business Dashboard の詳細を削除するには、このコマンドの **no** 形式を使用します。

構文

cbd address {*ip-address* | *hostname*} [**port** *port*]

no cbd address

パラメータ

- **address** *ip-address*：Cisco Business Dashboard の IP アドレスを指定します。IPv4 アドレスを指定できます。
- **address** *hostname*：Cisco Business Dashboard をホスト名として指定します（範囲：1 ～ 158 文字。ホスト名の各ポートの最大ラベルサイズ：63）。
- **port**：Cisco Business Dashboard への接続に使用する TCP ポートを指定します。（範囲：1 ～ 65535）

デフォルト設定

アドレスが設定されていません。CBD **port** のデフォルトは 443 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

Cisco Business Dashboard の IP アドレスと Cisco Business Dashboard への接続に使用する TCP ポートを設定するには、**cbd address** コマンドを使用します。このパラメータを変更する前に、**cbd connection enable** 設定を削除する必要があります。

例

次に、Cisco Business Dashboard の IPv4 アドレスを 1.1.1.1 に設定し、TCP ポートを 8443 に設定する例を示します。

```
switchxxxxxx(config)# cbd address 1.1.1.1 port 8443
```

次に、ダッシュボードへの接続が有効になっているため、Cisco Business Dashboard の IPv4 アドレスの設定が失敗する例を示します。

```
switchxxxxxx(config)# cbd address 1.1.1.1
Command failed!
Please disable connection to Cisco Business Dashboard before configuring this command,
using command "no cbd connection enable". Only after configuring all Dashboard settings
```

```
(Dashboard address, Key parameters, Organization and Network name) re-enable connection
(command "cbd connection enable") to allow Probe connection to Cisco Business Dashboard
```

cbd organization name

Cisco Business Dashboard の組織名を設定するには、グローバル コンフィギュレーション モードで **cbd organization name** コマンドを使用します。Cisco Business Dashboard の組織名の設定を削除するには、このコマンドの **no** 形式を使用します。

構文

cbd organization name *organization-name*

no cbd organization name

パラメータ

organization name *organization-name*：デバイスで実行されている Cisco Business Dashboard Probe の組織名を指定します。パラメータは、記号と空白を**含む**英数字文字列として指定できます（範囲：1 ー 64）。

デフォルト設定

CBD 組織名が定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

Cisco Business Dashboard の組織名を設定するには、**cbd organization name** コマンドを使用します。このパラメータを変更する前に、**cbd connection enable** 設定を削除する必要があります。

例

次に、Cisco Business Dashboard の組織名を設定する例を示します。

```
switchxxxxxx(config)# cbd organization name "my organization"
```

cbd network name

Cisco Business Dashboard のネットワーク名を設定するには、グローバル コンフィギュレーション モードで **cbd network name** コマンドを使用します。Cisco Business Dashboard ネットワーク名の設定を削除するには、このコマンドの **no** 形式を使用します。

構文

cbd network name *network-name*

no cbd network name

パラメータ

network name *network-name*：デバイスで実行している Cisco Business Dashboard Probe のサイト名を指定します。ネットワーク名は、記号と空白を**含む**英数字文字列として指定できます（範囲：1 ー 64）。

デフォルト設定

CBD ネットワーク名が定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

Cisco Business Dashboard ネットワーク名を設定するには、**cbd network name** コマンドを使用します。このパラメータを変更する前に、**cbd connection enable** 設定を削除する必要があります。

例

次に、Cisco Business Dashboard のネットワーク名を設定する例を示します。

```
switchxxxxxx(config)# cbd network name "my network"
```

cbd key

Cisco Business Dashboard のキー ID と秘密を設定するには、グローバル コンフィギュレーション モードで **cbd key** コマンドを使用します。Cisco Business Dashboard のキー ID と秘密の設定を削除するには、このコマンドの **no** 形式を使用します。

構文

cbd key id *id-string* **secret** *secret-string*

encrypted cbd key id *id-string* **secret** *encrypted-secret-string*

no cbd key

パラメータ

- **id** *id-string*：デバイス上で実行している Cisco Business Dashboard Probe と Cisco Business Dashboard 間の最初の認証で使用するキー ID（24 桁の 16 進数の文字列）を指定します。
- **secret** *secret-string*：認証に使用する秘密を指定します。空白を**含まない**英数字文字列として指定できます。キーには最大 160 文字を使用できます。
- **secret** *encrypted-secret-string*：*secret-string* パラメータと同じですが、秘密は暗号化形式です。

デフォルト設定

CBD キー ID と秘密が定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

Cisco Business Dashboard のキー ID と秘密を設定するには、**cbd key** コマンドを使用します。このパラメータを変更する前に、**cbd connection enable** 設定を削除する必要があります。

例

次に、初期認証に使用する Cisco Business Dashboard のキー ID と秘密を設定する例を示します。

```
switchxxxxxx(config)# cbd key id 5cecde9f21bb450005fb790b secret secretExample123
```

cbd connection enable

Cisco Business Dashboard に接続するようにプローブを設定するには、グローバル コンフィギュレーション モードで **cbd connection enable** コマンドを使用します。Cisco Business Dashboard へのプローブ接続を無効にするには、このコマンドの **no** 形式を使用します。

構文

cbd connection enable

no cbd connection enable

デフォルト設定

プローブが Cisco Business Dashboard への接続に対して有効になっていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

プローブが Cisco Business Dashboard に接続できるようにするには、**cbd connection enable** コマンドを使用します。Cisco Business Dashboard Probe が有効になっている場合、このコマンドの設定により、CBD Probe が Cisco Business Dashboard に接続されます。

cbd connection enable コマンドを正常に実行するには、**cbd organization name**、**cbd network name**、**cbd address**、および **cbd key** の設定が必要です。プローブを Cisco Business Dashboard から切断し、ユーザが上記の Cisco Business Dashboard の設定を変更できるようにするには、**no cbd connection enable** コマンドを使用します。

例

次に、プローブを Cisco Business Dashboard に接続できるようにする例を示します。

```
switchxxxxxx(config)# cbd connection enable
```

次に、接続に必要な Dashboard の設定が行われていなかったため、コマンドが失敗する例を示します。

```
switchxxxxxx(config)# cbd connection enable
Command failed. Please make sure all of the following dashboard parameters are configured:
 dashboard address, organization name, network name and key;
```

cbd reset

Cisco Business Dashboard への Cisco Business Dashboard Probe の接続をリセットするには、特権 EXEC モードで **cbd reset** コマンドを使用します。

構文

cbd reset

コマンド モード

特権 EXEC モード

使用上のガイドライン

Cisco Business Dashboard への接続をリセットするには、**cbd reset** コマンドを使用します。このコマンドを適用すると、ダッシュボードとの現在の接続が切断され、CBD Probe のキャッシュデータがフラッシュされて Cisco Business Dashboard への再接続が試行されます。

このコマンドは、プローブエージェントが有効になっており（コマンド cbd probe enable （254 ページ））、Cisco Business Dashboard への接続も有効になっている（コマンド cbd connection enable （260 ページ））場合にのみ実行されます。

例

次に、設定したキー ID と秘密を使用して再接続を試行する例を示します。

```
switchxxxxxx# cbd reset
```

次に、ネットワークの Cisco Business Dashboard へのプローブ接続が有効になっていないため、reset コマンドが失敗する例を示します。

```
switchxxxxxx# cbd reset
Operation failed because Probe connection to Cisco Business Dashboard is not enabled.
Please enable conntection to Cisco Business Dashboard using command "cbd connection
enable".
```

次に、デバイスでプローブエージェントが有効になっていないため、reset コマンドが失敗する例を示します。

```
switchxxxxxx# cbd reset
Operation failed because Probe is not enabled
Please enable Probe using command "cbd probe enable".
```

clear cbd probe database

Cisco Business Dashboard Probe データベースをクリアするには、特権 EXEC モードで **clear cbd probe database** コマンドを使用します。

構文

clear cbd probe database

コマンド モード

特権 EXEC モード

使用上のガイドライン

Cisco Business Dashboard Probe データベースをクリアするには、**clear cbd probe** データベースを使用します。

このコマンドは、Cisco Business Dashboard Probe エージェントが無効になっている場合にのみ実行されます。

例

次に、Cisco Business Dashboard Probe データベースをクリアする例を示します。

```
switchxxxxxx# clear cbd probe database
```

次に、Cisco Business Dashboard Probe がスイッチで有効になっているため、clear コマンドが失敗する例を示します。

```
switchxxxxxx# clear cbd probe database
Operation failed because Cisco Business Dashboard Probe is enabled on the switch.
Please disable Probe on switch using command "no cbd probe enable".
```

show cbd

Cisco Business Dashboard Probe コンフィギュレーションとステータスを表示するには、特権 EXEC モードで **show cbd** コマンドを使用します。

構文

show cbd

コマンド モード

特権 EXEC モード

使用上のガイドライン

デバイスで実行されている Cisco Business Dashboard Probe に関する情報を表示するには、**show cbd** コマンドを使用します。

例

次に、**show cbd** コマンドの出力例を示します。

```
switchxxxxxx# show cbd
Network Probe is enabled
Operational status: Active
Probe version: 1.1.2.20181019
Dashboard address: 1.1.1.1
Dashboard port: 443
Key ID: MyKey
Key Secret (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
Organization name: ABC Company
Network name: my network
Dashboard status: connected
```

次の表で、さまざまな Cisco Business Dashboard Probe の設定と動作、および関連する管理状態と動作状態の表示について説明します。

Cisco Business Dashboard Probe の設定とステータス	管理状態の表示	動作状態の表示
Cisco Business Dashboard Probe は無効になっています	Disabled	Inactive
Cisco Business Dashboard Probe は有効になっておりアクティブです	Enabled	Active
Cisco Business Dashboard Probe は有効ですがアクティブではありません（障害を示す）	Enabled	Fault

CDP コマンド

この章は、次の項で構成されています。

- cdp advertise-v2 （266 ページ）
- cdp appliance-tlv enable （267 ページ）
- cdp device-id format （268 ページ）
- cdp enable （269 ページ）
- cdp holdtime （270 ページ）
- cdp log mismatch duplex （271 ページ）
- cdp log mismatch native （272 ページ）
- cdp log mismatch voip （273 ページ）
- cdp mandatory-tlvs validation （274 ページ）
- cdp pdu （275 ページ）
- cdp run （276 ページ）
- cdp source-interface （277 ページ）
- cdp timer （278 ページ）
- clear cdp counters （279 ページ）
- clear cdp table （280 ページ）
- show cdp （281 ページ）
- show cdp entry （282 ページ）
- show cdp interface （284 ページ）
- show cdp neighbors （285 ページ）
- show cdp tlv （289 ページ）
- show cdp traffic （292 ページ）

cdp advertise-v2

送信される CDP パケットのバージョン 2 を指定するには、グローバル コンフィギュレーション モードで **cdp advertise-v2** コマンドを使用します。バージョン 1 を指定するには、このコマンドの **no** 形式を使用します。

構文

cdp advertise-v2

no cdp advertise-v2

デフォルト設定

バージョン 2

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# cdp run
switchxxxxxx(config)# cdp advertise-v2
```

cdp appliance-tlv enable

アプライアンス TLV の送信を有効にするには、グローバル コンフィギュレーション モードで **cdp appliance-tlv enable** コマンドを使用します。アプライアンス TLV の送信を無効にするには、このコマンドの **no** 形式を使用します。

構文

cdp appliance-tlv enable

no cdp appliance-tlv enable

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

この MIB は、このポートが属する音声 VLAN ID（VVID）を指定します。

- **0**：このポートから送信する CDP パケットには、値が 0 のアプライアンス VLAN-ID TLV が含まれます。VoIP および関連するパケットは、VLAN-ID=0 および 802.1p プライオリティで送受信されることになります。
- **1 ～ 4094**：このポートを介して送信される CDP パケットには、N のアプライアンス VLAN ID TLV が含まれています。VoIP および関連するパケットは、VLAN-ID=N および 802.1p プライオリティで送受信されることになります。
- **4095**：このポートから送信する CDP パケットには、値が 4095 のアプライアンス VLAN-ID TLV が含まれます。VoIP と関連パケットは、タグなしで 802.1p の優先順位を使用せずに送受信されることが想定されます。
- **4096**：このポートを介して送信される CDP パケットには、アプライアンス VLAN-ID TLV が含まれていません。または、ポートで VVID がサポートされていない場合には、この MIB オブジェクトは設定できず、4096 が返されます。

例

```
switchxxxxxx(config)# cdp appliance-tlv enable
```

cdp device-id format

Device-ID TLV の形式を指定するには、グローバル コンフィギュレーション モードで **cdp device-id format** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

cdp device-id format {mac | serial-number | hostname}

no cdp device-id format

パラメータ

- **mac**：デバイス ID TLV にデバイスの MAC アドレスが含まれることを指定します。
- **serial-number**：デバイス ID TLV にデバイスのハードウェア シリアル番号が含まれることを指定します。
- **hostname**：デバイス ID TLV にデバイスのホスト名が含まれることを指定します。

デフォルト設定

デフォルトでは MAC アドレスが選択されています。

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# cdp device-id format serial-number
```

cdp enable

インターフェイスでCDPを有効にするには、インターフェイス（イーサネット）コンフィギュレーション モードで **cdp enable** コマンドを使用します。インターフェイスで CDP を無効にするには、この CLI コマンドの **no** 形式を使用します。

構文

cdp enable

デフォルト設定

有効

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

インターフェイスで CDP を有効にするには、まず cdp advertise-v2 （266 ページ） を使用して CDP をグローバルに有効にする必要があります。

例

```
switchxxxxxx(config)# cdp run
switchxxxxxx(config-if)# interface gi1/0/1
switchxxxxxx(config-if)# cdp enable
```

cdp holdtime

Time-to-Live フィールドの値を送信される CDP メッセージに指定するには、グローバル コンフィギュレーション モードで **cdp holdtime** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

cdp holdtime *seconds*

no cdp holdtime

パラメータ

seconds：秒単位の Time-to-Live フィールドの値。送信タイマーの値より大きい値を指定する必要があります。

パラメータの範囲

seconds：10 ～ 255。

デフォルト設定

180 秒。

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# cdp holdtime 100
```

cdp log mismatch duplex

CDPパケットで受信したポートのデュプレックスステータスがポートの実際の設定と一致していることを検証し、一致しない場合はSYSLOGデュプレックス不一致メッセージの生成を有効にするには、グローバル コンフィギュレーション モードとインターフェイス（イーサネット）コンフィギュレーションモードで**cdp log mismatch duplex**コマンドを使用します。SYSLOGメッセージの生成を無効にするには、このCLIコマンドの**no**形式を使用します。

構文

cdp log mismatch duplex

no cdp log mismatch duplex

デフォルト設定

スイッチがすべてのポートのデュプレックスの不一致を報告します。

コマンド モード

グローバル コンフィギュレーション モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# cdp log mismatch duplex
```

cdp log mismatch native

CDP パケットで受信したネイティブ VLAN が、ポートの実際のネイティブ VLAN と一致することの検証、および不一致がある場合は、SYSLOG VLAN ネイティブ ミスマッチ メッセージの生成を有効にするには、グローバル コンフィギュレーション モードおよびインターフェイス（イーサネット）コンフィギュレーション モードで **cdp log mismatch native** グローバルおよびインターフェイス コンフィギュレーション モード コマンドを使用します。SYSLOG メッセージの生成を無効にするには、この CLI コマンドの **no** 形式を使用します。

構文

cdp log mismatch native

no cdp log mismatch native

デフォルト設定

スイッチがすべてのポートのネイティブ VLAN の不一致を報告します。

コマンド モード

グローバル コンフィギュレーション モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# cdp log mismatch native
```

cdp log mismatch voip

CDP パケットで受信したポートの VoIP ステータスが、ポートの実際の設定と一致することの検証、および不一致がある場合は、SYSLOG VoIP ミスマッチ メッセージの生成を有効にするには、グローバル コンフィギュレーション モードおよびインターフェイス（イーサネット）コンフィギュレーション モードで **cdp log mismatch voip** グローバルおよびインターフェイス コンフィギュレーション モード コマンドを使用します。SYSLOG メッセージの生成を無効にするには、この CLI コマンドの **no** 形式を使用します。

構文

cdp log mismatch voip

no cdp log mismatch voip

デフォルト設定

スイッチがすべてのポートの VoIP の不一致を報告します。

コマンド モード

グローバル コンフィギュレーション モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# cdp log mismatch voip
```

cdp mandatory-tlvs validation

すべての必須（CDP プロトコルによる）TLV が受信 CDP フレームに存在することを検証するには、グローバル コンフィギュレーション モードで **cdp mandatory-tlvs validation** コマンドを使用します。検証を無効にするには、このコマンドの **no** 形式を使用します。

構文

cdp mandatory-tlvs validation

no cdp mandatory-tlvs validation

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

すべての必須 TLV を含んでいない CDP パケットを削除するには、このコマンドを使用します。

例

この例では、必須 TLV の検証をオフにしています。

```
switchxxxxxx(config)# no cdp mandatory-tlvs validation
```

cdp pdu

CDP がグローバルに無効な場合の CDP パケット処理を指定するには、グローバル コンフィギュレーション モードで **cdp pdu** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

cdp pdu [filtering | bridging | flooding]

no cdp pdu

パラメータ

- **filtering**：CDP がグローバルに無効になっている場合に、CDP パケットがフィルタリング（削除）されるように指定します。
- **bridging**：CDP がグローバルに無効になっている場合に、CDP パケットが通常のデータ パケットとしてブリッジされる（VLAN に基づいて転送される）ように指定します。
- **flooding**：CDP がグローバルに無効になっている場合に、STP フォワーディング ステートの製品内のすべてのポートに CDP パケットがフラッディングされ、VLAN フィルタリング ルールは無視されるように指定します。

デフォルト設定

bridging

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

CDP がグローバルに有効になっている場合は、CDP が無効になっているポートでは CDP パケットがフィルタリング（破棄）されます。

フラッディング モードでは、VLAN フィルタリング ルールは適用されず、STP ルールが適用されます。MSTP の場合、CDP パケットはインスタンス 0 に分類されます。

例

```
switchxxxxxx(config)# cdp run
switchxxxxxx(config)# cdp pdu flooding
```

cdp run

CDP をグローバルに有効にするには、グローバル コンフィギュレーション モードで **cdp run** コマンドを使用します。CDP をグローバルに無効にするには、このコマンドの **no** 形式を使用します。

構文

cdp run

no cdp run

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

CDP は、直接接続された CDP/LLDP 対応デバイス用のリンク層プロトコルで、自身とその機能をアドバタイズします。CDP/LLDP 対応デバイスが直接接続されておらず、CDP/LLDP 非対応デバイスで分離されている展開では、CDP/LLDP 非対応デバイスが受信した CDP/LLDP パケットをフラッディングした場合にのみ、CDP/LLDP 対応デバイスが他のデバイスからのアドバタイズメントを受信できます。CDP/LLDP 非対応デバイスが VLAN 認識型のフラッディングを実行する場合、CDP/LLDP 対応デバイスは、同じ VLAN 内にある場合にのみ、相互に通信できます。CDP/LLDP 非対応デバイスが CDP/LLDP パケットをフラッディングする場合は、CDP/LLDP 対応デバイスが複数の装置からのアドバタイズメントを受信する可能性があることに注目してください。

CDP 情報を学習してアドバタイズするには、グローバルに有効にして（デフォルト）、インターフェイスでも有効にする（同様にデフォルト）必要があります。

例

```
switchxxxxxx(config)# cdp run
```

cdp source-interface

送信元 IP アドレス選択に使用する CDP 送信元ポートを指定するには、グローバル コンフィギュレーション モードで **cdp source-interface** コマンドを使用します。送信元インターフェイスを削除にするには、このコマンドの **no** 形式を使用します。

構文

cdp source-interface *interface-id*

no cdp source-interface

パラメータ

interface-id：送信元 IP アドレスの選択に使用される送信元ポート。

デフォルト設定

CDP 送信元インターフェイスは指定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

発信インターフェイスの最小 IP アドレスではなく、最小 IP アドレスが TVL にアドバタイズされるインターフェイスを指定するには、**cdp source-interface** コマンドを使用します。

例

```
switchxxxxxx(config)# cdp source-interface gi1/0/1
```

cdp timer

CDP パケットの送信頻度を指定するには、グローバル コンフィギュレーション モードで **cdp timer** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

cdp timer *seconds*

no cdp timer

パラメータ

seconds：秒単位の送信タイマーの値。範囲：5 ～ 254 秒。

デフォルト設定

60 秒

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# cdp timer 100
```

clear cdp counters

CDP トラフィック カウンタを 0 にリセットするには、特権 EXEC モードで **clear cdp counters** コマンドを使用します。

構文

clear cdp counters [**global** | *interface-id*]

パラメータ

- **global**：グローバル カウンタのみをクリアします。
- ***interface-id***：クリアするカウンタのインターフェイス ID を指定します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

すべてのカウンタをクリアするには、パラメータを使用せずに **clear cdp counters** コマンドを使用します。

グローバル カウンタのみをクリアするには、**clear cdp counters global** コマンドを使用します。

指定したインターフェイスのカウンタをクリアするには、**clear cdp counters** *interface-id* コマンドを使用します。

例

例 1。この例では、すべての CDP カウンタをクリアしています。

```
switchxxxxxx# clear cdp couters
```

例 2。この例では、CDP グローバル カウンタをクリアしています。

```
switchxxxxxx# clear cdp couters global
```

例 3。次に、イーサネットポート gi1/0/1 の CDP カウンタをクリアする例を示します。

```
switchxxxxxx# clear cdp couters interface gi1/0/1
```

clear cdp table

CDP キャッシュ テーブルを削除するには、特権 EXEC モードで **clear cdp table** コマンドを使用します。

構文

clear cdp table

コマンド モード

特権 EXEC モード

例この例では、**CDP** キャッシュ テーブルからすべてのエントリを削除しています。

```
switchxxxxxx# clear cdp table
```

show cdp

アドバタイズメント間隔、アドバタイズメントが有効な期間（秒単位）およびアドバタイズメントのバージョンを表示するには、特権 EXEC モードで **show cdp** 特権 EXEC モード コマンドを使用します。

構文

show cdp

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# show cdp
Global CDP information:
   cdp is globally enabled
   cdp log duplex mismatch is globally enabled
   cdp log voice VLAN mismatch is globally enabled
   cdp log native VLAN mismatch is globally disabled
   Mandatory TLVs are
     Device-ID TLV (0x0001
     Address TLV (0x0002)
     Port-ID TLV (0x0003)
     Capabilities TLV (0x0004)
     Version TLV (0x0005)
     Platform TLV (0x0006)
   Sending CDPv2 advertisements is enabled
   Sending Appliance TLV is enabled
   Device ID format is Serial Number
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
```

show cdp entry

指定したネイバーに関する情報を表示するには、特権 EXEC モードで **show cdp entry** コマンドを使用します。

構文

show cdp entry {***** | *device-name}* [**protocol** | **version**]

パラメータ

- *****：すべての ネイバーを指定します。
- **device-name**：ネイバーの名前を指定します。
- **protocol**：ネイバーで有効になっているプロトコルに関する情報に表示を制限します。
- **version**：ネイバーで実行されているソフトウェアのバージョンに関する情報に表示を制限します。

デフォルト設定

protocol と version のキーワードが指定されていない場合は、すべてのエントリ情報が表示されます。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# show cdp entry
Device-ID: Site1-C1300-Stack-10
Advertisement version: 2
Platform: Cisco C1300-24P-4X (PID:C1300-24P-4X)-VSD
Capabilities: Router Switch IGMP
Interface: gi10, Port ID (outgoing port): gi2/0/20
Holdtime: 129
Version: 4.1.0.68
Duplex: full
Native VLAN: 1
Application: VoIP using VLAN 114
SysName: Site1-C1300-Stack-10
Addresses:
          IP 172.16.1.31
          IPv6 fe80::e64e:2dff:fe4a:32eb (link-local)
Site1-C1200-8T-16#

Site1-C1200-8T-16#sh cdp entry Site1-C1300-Stack-10 protocol
-------------------------------------------
Device-ID: Site1-C1300-Stack-10
Addresses:
          IP 172.16.1.31
          IPv6 fe80::e64e:2dff:fe4a:32eb (link-local)
```

```
Site1-C1200-8T-16#
Site1-C1200-8T-16#
Site1-C1200-8T-16#sh cdp entry Site1-C1300-Stack-10 version
-------------------------------------------
Device-ID: Site1-C1300-Stack-10
Version: 4.0.0.81
Site1-C1200-8T-16#
```

```
switchxxxxxx# show cdp entry device.cisco.com version
Device-ID: Site1-C1300-Stack-10
Advertisement version: 2
Platform: Cisco C1300-24P-4X (PID:C1300-24P-4X)-VSD
Capabilities: Router Switch IGMP
Interface: gi10, Port ID (outgoing port): gi2/0/20
Holdtime: 129
Version: 4.1.0.68
Duplex: full
Native VLAN: 1
Application: VoIP using VLAN 114
SysName: Site1-C1300-Stack-10
Addresses:
          IP 172.16.1.31
          IPv6 fe80::e64e:2dff:fe4a:32eb (link-local)
Site1-C1200-8T-16#
Site1-C1200-8T-16#sh cdp entry Site1-C1300-Stack-10 protocol
-------------------------------------------
Device-ID: Site1-C1300-Stack-10
Addresses:
          IP 172.16.1.31
          IPv6 fe80::e64e:2dff:fe4a:32eb (link-local)
Site1-C1200-8T-16#
Site1-C1200-8T-16#
Site1-C1200-8T-16#sh cdp entry Site1-C1300-Stack-10 version
-------------------------------------------
Device-ID: Site1-C1300-Stack-10
Version: 4.0.0.81
Site1-C1200-8T-16#
```

```
switchxxxxxx# show cdp entry device.cisco.com protocol
Device-ID: Site1-C1300-Stack-10
Addresses:
          IP 172.16.1.31
          IPv6 fe80::e64e:2dff:fe4a:32eb (link-local)
Site1-C1200-8T-16#
Site1-C1200-8T-16#
Site1-C1200-8T-16#sh cdp entry Site1-C1300-Stack-10 version
```

```
switchxxxxxx# show cdp entry device.cisco.com version
Device-ID: Site1-C1300-Stack-10
Version: 4.0.0.81
Site1-C1200-8T-16#
```

show cdp interface

CDP が有効なポートに関する情報を表示するには、特権 EXEC モードで **show cdp interface** コマンドを使用します。

構文

show cdp interface ***interface-id***

パラメータ

interface-id：ポート ID。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# show cdp interface gi1/0/1
CDP is globally enabled
CDP log duplex mismatch
  Globally is enabled
  Per interface is enabled
CDP log voice VLAN mismatch
  Globally is enabled
  Per interface is enabled
CDP log native VLAN mismatch
  Globally is disabled
  Per interface is enabled
gi1/0/1 is Down, CDP is enabled
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
```

show cdp neighbors

メインまたはセカンダリ キャッシュに保持されているネイバーに関する情報を表示するには、特権 EXEC モードで **show cdp neighbors** コマンドを使用します。

構文

show cdp neighbors [***interface-id***] [**detail** | **secondary**]

パラメータ

- **interface-id**：このポートに接続されているネイバーを表示します。
- **detail**：メイン キャッシュからのネイバーの詳細を表示します（ネットワーク アドレス、有効なポート、ホールド時間、ソフトウェア バージョンなど）。
- **secondary**：2 次キャッシュからのネイバーの詳細を表示します。

デフォルト設定

インターフェイス ID が指定されていない場合、このコマンドはすべてのポートのネイバーに関する情報を表示します。

detail または secondary が指定されていない場合は、すべてのネイバーのサマリーテーブルが表示されます。

コマンド モード

特権 EXEC モード

例

switchxxxxxx# **show cdp neighbors**

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,P - VoIP Phone,
M - Remotely-Managed Device, C - CAST Phone Port, W - Two-Port MAC Relay
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - VoIP Phone
                  M - Remotely-Managed Device, C - CAST Phone Port,
                  W - Two-Port MAC Relay
    Device ID       Local      Adv  Time To Capability   Platform     Port ID
                    Interface  Ver. Live
------------------ ----------- ---- ------- ---------- ------------ -----------
PTK-SW-A-86.company   gi48      2     147      S I     Company        gi3/39
l.com                                                  XX-10R-E
    ESW-520-8P        gi48      2     153     S I M    ESW-520-8P     g1
    ESW-540-8P        gi48      2     146     S I M    ESW-540-8P     g9
   003106131611       gi48      2     143      S I     Company        fa2/1
                                                       XX-23R-E
   001828100211       gi48      2     173      S I     Company        fa2/2
                                                       XX-23R-E
    c47d4fed9302       gi48      2     137      S I    Company        fa2/5
                                                       XX-23R-E
```

```
switchxxxxxx# show cdp neighbors detail
-------------------------
Device ID: lab-7206
Advertisement version: 2
Entry address(es):
IP address: 172.19.169.83
Platform: company x5660, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): gi1/0/0
Time To Live : 123 sec
Version :
Company Network Operating System Software
NOS (tm) x5660 Software (D5660-I-N), Version 18.1(10.4), MAINTENANCE INTERIM
SOFTWARE
Copyright (c) 1986-1997 by company Systems, Inc.
Compiled Mon 07-Apr-97 19:51 by xxdeeert
Duplex: half
-------------------------
Device ID: lab-as5300-1
Entry address(es):
IP address: 172.19.169.87
Platform: company TD6780, Capabilities: Router
Device ID: SEP000427D400ED
Advertisement version: 2
Entry address(es):
IP address: 1.6.1.81
Platform: Company IP Phone x8810, Capabilities: Host
Interface: gi1/0/1, Port ID (outgoing port): Port 1
Time To Live: 150 sec
Version :
P00303020204
Duplex: full
sysName: a-switch
Power drawn: 6.300 Watts

switchxxxxxx# show cdp neighbors secondary
Interface gi1/0/1, Port ID (outgoing port): gi2/0/20
MAC Address: 00:00:01:23:86:9c
Holdtime: 157
Capabilities: Router Switch
VLAN-ID: 10
Platform: 206VXRYC
Device-ID: 00000123869c
Addresses: IP 60.0.0.5, IPv6 2020::2020
nterface gi1/0/2, Port ID (outgoing port): gi2/0/21
MAC Address: 00:00:01:53:86:9c
Holdtime: 163
Capabilities: Router Switch
VLAN-ID: 10
Platform: ABCD-VSD
Device-ID: 00000153869c
Addresses: IP 61.0.0.4
Power Available: 30000
Request-ID: 1
Power management-ID: 234
Management-Power-Level is 0xFFFFFFFF
Interface gi1/0/3, Port ID (outgoing port): gi2/0/25
MAC Address: 00:00:22:23:86:9c
Holdtime: 144
Capabilities: Router Switch
VLAN-ID: 1210
Platform: bbbb
Device-ID: 00002223869c
Addresses: IP 70.0.0.4
4-wire Power-via-MDI (UPOE) TLV:
4-pair PoE Supported: Yes
```

```
Spare pair Detection/Classification required: Yes
PD Spare Pair Desired State: Disabled
PSE Spare Pair Operational State: Disabled
Power Available: 154000
Request-ID: 5
Power management-ID: 969
Management-Power-Level is 0xFFFFFFFF
Interface gi1/0/3, Port ID (outgoing port): gi1/0/11
MAC Address: 00:00:01:2c:86:9c
Holdtime: 120
Capabilities: Switch
VLAN-ID: 1005
Platform: CAT-3000
Device-ID: 0000012c869c
Addresses: IP 70.0.0.5
```

フィールドの定義：

- **Advertisement version**：CDP のアドバタイズメントに使用されている CDP のバージョン。
- **Capabilities**：ネイバーのデバイス タイプ。このデバイスは、ルータ、ブリッジ、トランスペアレント ブリッジ、ソース ルーティング ブリッジ、スイッチ、ホスト、IGMP デバイス、またはリピータです。
- **COS for Untrusted Ports**：信頼できないポートで受信されたすべてのパケットが、個々のパケットを分類できない単純なスイッチング デバイスによりマークされるときに使用される COS 値。
- **Device ID**：ネイバー デバイスの名前、およびそのデバイスの MAC アドレスまたはシリアル番号。
- **Duplex**：現在のデバイスとネイバー デバイス間の接続のデュプレックス ステート。
- **Entry address(es)**：ネイバー デバイスのネットワーク アドレスのリスト。
- **Extended Trust**：拡張された信頼。
- **External Port-ID**：CDP パケットが送信される物理コネクタ ポートを識別します。複数のハードウェア インターフェイスからの信号が単一の物理ポートを介して多重化される、光ポートを備えたデバイスなどで使用されます。多重化された信号が送信される、外部物理ポートの名前が含まれます。
- **Interface**：現在のデバイス上のポートのプロトコルおよびポート番号です。
- **IP Network Prefix**：オンデマンドルーティング（ODR）で使用されます。ハブ ルータにより送信される場合は、デフォルト ルート（IP アドレス）です。スタブ ルータにより送信される場合は、送信スタブ ルータが IP パケットを転送できるスタブ ネットワークのネットワーク プレフィックスのリストです。
- **Management Address**：存在する場合は、デバイスが SNMP メッセージを受け入れるすべてのアドレスのリストが含まれます。これには、CDP パケットの送信元のインターフェイス以外のインターフェイスで受信された場合にのみ受け入れるアドレスも含まれます。
- **MTU**：CDP パケットの送信元のインターフェイスの MTU。
- **Native VLAN**：ネイバー デバイス上の VLAN の ID 番号。

- **Physical Location**：この TLV を含む CDP パケットの送信元のインターフェイス上のコネクタ（つまり、インターフェイスに物理的に接続されているコネクタ）の、物理的な場所を示す文字列。
- **Platform**：ネイバー デバイスの製品名および製品番号。2 次キャッシュの場合は、値の最後の 8 文字のみが出力されます。
- **Power Available**：すべてのスイッチ インターフェイスが、Power Available TLV で情報を送信します。これにより、電力を必要とするデバイスがネゴシエートし、適切な電力設定を選択できるようになります。Power Available TLV には、4 つのフィールドが含まれています。
- **Power Consumption**：CDP パケットの送信元のインターフェイスから取得されて消費されると予想される最大電力量（ミリワット）。
- **Power Drawn**：要求される最大電力。

  注：IP フォンの場合、表示される値は要求される最大電力（6.3 ワット）です。この値は、ルーティング デバイスにより供給される実際の電力（通常は 5 ワット。show power コマンドを使用して表示します）とは異なる場合があります。
- **Protocol-Hello**：特定のプロトコルでは、CDP によって「hello」メッセージが送信 CDP パケット内にピギーバックされるよう指定します。
- **Remote Port_ID**：CDP パケットが送信されるポートを識別します。
- **sysName**：送信側デバイスの sysName MIB オブジェクトと同じ値を含む ASCII 文字列。
- **sysObjectID**：送信側デバイスの sysObjectID MIB オブジェクトの OBJECT-IDENTIFIER 値。
- **Time To Live**：現在のデバイスが、送信ルータからの CDP アドバタイズメントを破棄するまでの残り時間（秒）。
- **Version**：ネイバー デバイスで実行されているソフトウェア バージョン。
- **Voice VLAN-ID**：音声 VLAN ID。
- **VTP Management Domain**：ネイバー デバイスに関連付けられている VLAN の集合グループの名前である文字列。

show cdp tlv

すべてのポートまたは指定したポートで CDP が送信する TLV に関する情報を表示するには、特権 EXEC モードで **show cdp tlv** コマンドを使用します。

構文

show cdp tlv [***interface-id***]

パラメータ

interface-id：ポート ID。

デフォルト設定

すべてのポートの TLV。

コマンド モード

特権 EXEC モード

使用上のガイドライン

show cdp tlv コマンドを使用して、CDP パケットで送信するように設定されている TLV を確認できます。**show cdp tlv** コマンドは、ポートが指定されている場合は単一のポートの情報を表示し、指定されていない場合はすべてのポートの情報を表示します。CDP がポートで実際に実行されている場合（つまり、CDP がグローバルに、およびポートで有効になっていて、ポートがアップしている場合）にのみ、ポートの情報が表示されます。

例 1：この例では、CDP が無効になっているため、情報は表示されません。

```
switchxxxxxx# show cdp tlv
cdp globally is disabled
```

例 2：この例では、CDP がグローバルに有効になっていますが、ポートで無効になっているため、情報は表示されません。

```
switchxxxxxx# show cdp tlv gi1/0/2
cdp globally is enabled
Capability Codes: R - Router,T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone,M - Remotely-Managed Device,
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/0/2
CDP is disabled on gi1/0/2
```

例 3：この例では、CDP はグルーバルに有効で、このポートでも有効ですが、ポートがダウンしているため、情報は表示されません。

```
switchxxxxxx# show cdp tlv interface gi1/0/2
cdp globally is enabled
Capability Codes: R - Router,T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone,M - Remotely-Managed Device,
```

```
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/0/3
CDP is enabled on gi1/0/3
Ethernet gi1/0/3 is down
```

例 4：この例では、CDP はグローバルに有効で、ポートは指定されていません。そのため、CDP が有効でアップ状態のすべてのポートに関する情報が表示されます。

```
switchxxxxxx# show cdp tlv interface
cdp globally is enabled
Capability Codes: R - Router,T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone,M - Remotely-Managed Device,
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/0/1
CDP is enabled
Ethernet gi1/0/1 is up,
Device ID TLV: type is MAC address; Value is 00:11:22:22:33:33:44:44
Address TLV: IPv4:  1.2.2.2 IPv6:
Port_ID TLV: gi1/0/1
Capabilities: S, I
Version TLV: 1 and 2
Platform TLV: VSD Ardd
Native VLAN TLV: 1
Full/Half Duplex TLV: full-duplex
Appliance VLAN_ID TLV: Appliance-ID is 1; VLAN-ID is 100
COS for Untrusted Ports TLV: 1
sysName: a-switch
4-wire Power-via-MDI (UPOE) TLV:
                     4-pair PoE Supported: No
Power Available TLV: Request-ID is 1 Power management-ID is 1;
                                     Available-Power is 15.4;
                                     Management-Power-Level is 0xFFFFFFFF
Interface TLV: gi1/0/2
CDP is disabled on gi1/0/2
Interface TLV: gi1/0/3
CDP is enabled on gi1/0/3
Ethernet gi1/0/3 is down
```

例 5：次に、CDP がグローバルに有効になっていて、また、PSE PoE ポートで有効になっており、ポートがアップしているため、情報が表示される例を示します。

```
switchxxxxxx# show cdp tlv interface gi1/0/1
cdp globally is enabled
Capability Codes: R - Router,T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone,M - Remotely-Managed Device,
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/0/1
CDP is enabled
Ethernet gi1/0/1 is up,
Device ID TLV: type is MAC address; Value is 00:11:22:22:33:33:44:44
Address TLV: IPv4:  1.2.2.2 IPv6:
Port_ID TLV: gi1/0/1
Capabilities: S, I
Version TLV: 1 and 2
Platform TLV: VSD Ardd
Native VLAN TLV: 1
Full/Half Duplex TLV: full-duplex
Appliance VLAN_ID TLV: Appliance-ID is 1; VLAN-ID is 100
COS for Untrusted Ports TLV: 1
sysName: a-switch
Power Available TLV: Request-ID is 1 Power management-ID is 1;
                                     Available-Power is 15.4;
```

```
                                        Management-Power-Level is 0xFFFFFFFF
4-wire Power-via-MDI (UPOE) TLV:
                      4-pair PoE Supported: Yes
                      Spare pair Detection/Classification required: Yes
                      PD Spare Pair Desired State: Disabled
                      PSE Spare Pair Operational State: Disabled
Request-ID is 1 Power management-ID is 1;
                                        Available-Power is 15.4;
                                        Management-Power-Level is 0xFFFFFFFF
```

show cdp traffic

送受信パケット数、チェックサム エラー数など、CDP カウンタを表示するには、特権 EXEC モードで **show cdp traffic** コマンドを使用します。

構文

show cdp traffic [**global** | *interface-id*]

パラメータ

- **global**：グローバル カウンタのみを表示します。
- ***interaface-id***：カウンタを表示するポート。

コマンド モード

特権 EXEC モード

使用上のガイドライン

すべてのカウンタを表示するには、パラメータを指定せずに **show cdp traffic** コマンドを使用します。

グローバルカウンタのみを表示するには、**show cdp traffic global** コマンドを使用します。

特定のポートのカウンタを表示するには、**show cdp traffic** *interface-id* コマンドを使用します。

例

```
switchxxxxxx# show cdp traffic
CDP Global counters:
     Total packets output: 81684,  Input: 81790
     Hdr syntax:  0, Chksum error: 0, Invalid packet: 0
     No memory in main cache: 0, in secondary cache: 0
     CDP version 1 advertisements output:  100,    Input  0
     CDP version 2 advertisements output:  81784,  Input  0
gi1/0/1
     Total packets output: 81684,  Input: 81790
     Hdr syntax:  0, Chksum error: 0, Invalid packet: 0
     No memory in main cache: 0, in secondary cache: 0
     CDP version 1 advertisements output:  100,    Input  0
     CDP version 2 advertisements output:  81784,  Input  0
gi1/0/2
     Total packets output: 81684,  Input: 81790
     Hdr syntax:  0, Chksum error: 0, Invalid packet: 0
     No memory in main cache: 0, in secondary cache: 0
     CDP version 1 advertisements output:  100,    Input  0
     CDP version 2 advertisements output:  81784,  Input  0
```

フィールド定義：

- **Total packets output**：ローカル デバイスが送信した CDP アドバタイズメントの数。この値は、CDP Version 1 advertisements output フィールドと CDP Version 2 advertisements output フィールドの合計です。
- **Input**：ローカル デバイスが受信した CDP アドバタイズメントの数。この値は、CDP Version 1 advertisements input フィールドと CDP Version 2 advertisements input フィールドの合計です。
- **Hdr syntax**：ローカル デバイスが受信した、適切でないヘッダーを持つ CDP アドバタイズメントの数。
- **Chksum error**：着信 CDP アドバタイズメントに対するチェックサム（検証）操作が失敗した回数。
- **No memory**：ローカル デバイスが送信のためにアドバタイズメント パケットを組み立てようとしたとき、または受信時にアドバタイズメント パケットを解析しようとしたときに、メモリが不足していてアドバタイズメント キャッシュ テーブルに CDP アドバタイズメントを格納できなかった回数。
- **Invalid**：受信した無効な CDP アドバタイズメントの数。
- **CDP version 1 advertisements output**：ローカルデバイスが送信した CDP バージョン 1 のアドバタイズメントの数。
- **CDP version 1 advertisements Input**：ローカル デバイスによって受信された CDP バージョン 1 アドバタイズメントの数。
- **CDP version 2 advertisements output**：ローカル デバイスが送信した CDP バージョン 2 のアドバタイズメントの数。
- **CDP version 2 advertisements Input**：ローカル デバイスによって受信された CDP バージョン 2 アドバタイズメントの数。

クロック コマンド

この章は、次の項で構成されています。

- absolute （296 ページ）
- clock dhcp timezone （297 ページ）
- clock set （298 ページ）
- clock source （299 ページ）
- clock summer-time （300 ページ）
- clock timezone （302 ページ）
- periodic （303 ページ）
- sntp anycast client enable （304 ページ）
- sntp authenticate （305 ページ）
- sntp authentication-key （306 ページ）
- sntp broadcast client enable （307 ページ）
- sntp client enable （308 ページ）
- sntp client enable（インターフェイス） （309 ページ）
- sntp server （310 ページ）
- sntp source-interface （312 ページ）
- sntp source-interface-ipv6 （313 ページ）
- sntp trusted-key （314 ページ）
- sntp unicast client enable （315 ページ）
- sntp unicast client poll （316 ページ）
- show clock （317 ページ）
- show sntp configuration （319 ページ）
- show sntp status （320 ページ）
- show time-range （322 ページ）
- time-range （323 ページ）

absolute

時間範囲が有効である場合に絶対時間を指定するには、時間範囲コンフィギュレーションモードで **absolute** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

absolute start *hh:mm day month year*

no absolute start

absolute end *hh:mm day month year*

no absolute end

パラメータ

- **start**：関連付けられた機能の許可ステートメントまたは拒否ステートメントが有効になる絶対日時。start 日時が指定されていない場合、その機能はただちに有効になります。
- **end**：関連付けられた機能の許可ステートメントまたは拒否ステートメントが有効でなくなる絶対日時。end 日時が指定されていない場合、その機能は無期限に有効になります。
- ***hh:mm***：時間（24 時間形式）および分単位の時刻（範囲：0 ～ 23、mm：0 ～ 5）。
- ***day***：日付。（範囲：1 ～ 31）
- ***month***：月（名前の最初の 3 文字）。（範囲：Jan ～ Dec）
- ***year***：年（省略なし）（範囲：2000 ～ 2037）

デフォルト設定

時間範囲が有効になっている場合の絶対時間はありません。

コマンド モード

時間範囲コンフィギュレーション モード

例

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# absolute start 12:00 1 jan 2005
switchxxxxxx(config-time-range)# absolute end 12:00 31 dec 2005
```

clock dhcp timezone

システムのタイムゾーンと夏時間を DHCP タイムゾーン オプションから取得できるように指定するには、グローバル コンフィギュレーション モードで **clock dhcp timezone** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

clock dhcp timezone

no clock dhcp timezone

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

DHCPサーバから取得されたタイムゾーンは、スタティックなタイムゾーンよりも優先されます。

DHCP サーバから取得された夏時間は、スタティックな夏時間よりも優先されます。

タイムゾーンと夏時間は、IP アドレスのリース時間が終了した後も有効なままです。

DHCP サーバから取得されたタイムゾーンと夏時間は、再起動後にクリアされます。

このコマンドの **no** 形式を使用すると、DHCP サーバからのダイナミックなタイム ゾーンと夏時間がクリアされます。

DHCP対応の複数のインターフェイスの場合、次の優先順位が適用されます。DHCP-TimeZoneオプションを取得しれたDHCPクライアントを無効にすると、ダイナミックタイムゾーンと夏時間の設定がクリアされます。

- DHCPv6 から受信した情報は DHCPv4 から受信した情報よりも優先されます。
- 下位のインターフェイスで実行されているDHCPクライアントから受信した情報は上位のインターフェイスで実行されているDHCPクライアントから受信した情報よりも優先されます。

例

```
switchxxxxxx(config)# clock dhcp timezone
```

clock set

システム クロックを手動で設定するには、特権 EXEC モードで **clock set** コマンドを使用します。

構文

clock set *hh*:*mm*:*ss* {[*day month*] | [*month day*]} *year*

パラメータ

- ***hh:mm:ss***：現在の時間（24 時間形式）、分、秒を指定します。（範囲：hh：0 ～ 23、mm：0 ～ 59、ss：0 ～ 59）
- ***day***：現在の日を指定します。（範囲：1 ～ 31）
- ***month***：月の名前の最初の 3 文字を使用して、現在の月を指定します。（範囲：Jan ～ Dec）
- ***year***：現在の年を指定します。（範囲：2020 ～ 2037）

デフォルト設定

イメージ作成の時間。

コマンド モード

特権 EXEC モード

使用上のガイドライン

起動後、システム クロックはイメージ作成の時間に設定されます。

例

次の例では、システム時刻を 2005 年 3 月 7 日の 13:32:00 に設定しています。

```
switchxxxxxx# clock set 13:32:00 7 Mar 2005
```

clock source

システム クロックの外部時刻源を設定するには、グローバル コンフィギュレーション モードで **clock source** コマンドを使用します。外部時刻源を無効にするには、このコマンドの **no** 形式を使用します。

構文

clock source {**sntp | browser**}

no clock source {**sntp | browser**}

パラメータ

- **sntp**：（オプション）SNTP サーバが外部クロック ソースであることを指定します。
- **browser**：（オプション）システム クロックが（手動または SNTP により）まだ設定されておらず、ユーザが Web ブラウザを使用して（HTTP または HTTPS 経由で）デバイスにログインした場合、ブラウザの時刻情報に基づいてシステムクロックが設定されるように指定します。

デフォルト設定

SNTP

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

起動後、システム クロックはイメージ作成の時間に設定されます。

パラメータを指定していない場合は、SNTP が時刻源として設定されます。

このコマンドが2回実行され、それぞれ異なるクロック ソースが使用された場合には、両方のソースが運用され、ブラウザからの時刻よりも SNTP の優先順位が高くなります。

例

次の例では、SNTP サーバをシステム クロックの外部時刻源として設定しています。

```
switchxxxxxx(config)# clock source sntp
switchxxxxxx(config)# clock source browser
switchxxxxxx(config)# exit
switchxxxxxx# show clock
*10:46:48 UTC May 28 2013
Time source is sntp
Time from Browser is enabled
```

clock summer-time

夏時間に自動的に切り替わるようにシステムを設定するには、グローバル コンフィギュレーション モードで **clock summer-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

clock summer-time *zone* recurring {**usa** | eu | {*week day month hh:mm week day month hh:mm*}} [*offset*]

clock summer-time *zone* date *day month year hh:mm date month year hh:mm* [*offset*]

clock summer-time *zone* date *month day year hh:mm month day year hh:mm* [*offset*]

no clock summer-time

パラメータ

- ***zone***：タイム ゾーンの略語。（範囲：1 ー 4 文字）。頭字語には文字のみを含めることができます。
- **recurring**：毎年対応する指定日に夏時間が開始され、終了することを示します。
- **date**：夏時間が、コマンドで指定された最初の日付から始まり、2 番目の日付で終わることを示します。
- **usa**：夏時間ルールが米国ルールになります。
- **eu**：夏時間ルールが EU ルールになります。
- ***week***：週。1 ～ 5（最初の週から最後の週）を指定できます。
- ***day***：曜日（Sun などの、名前の最初の 3 文字）。
- ***date***：月の日。（範囲：1 ～ 31）
- ***month***：月（Feb などの、名前の最初の 3 文字）。
- ***year***：年（省略なし）。（範囲：2020 ～ 2037）
- ***hh:mm***：時間と分単位の時刻（24 時間形式）。（範囲：hh：0 ～ 23、mm：0 ～ 59）
- ***offset***：（オプション）夏時間中に追加する分数（デフォルトは 60）。（範囲：1440）

デフォルト設定

夏時間は無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

date コマンド形式でも **recurring** コマンド形式でも、コマンドの最初の部分は夏時間がいつ始まるかを指定し、2 番目の部分はいつ終わるかを指定します。すべての時刻は、現地のタイムゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月よりも時間的に後の場合は、南半球にいるものと想定されます。

夏時間の米国ルール：

- **2007 年から**：

  開始：3 月の第 2 日曜日

  終了：11 月の第 1 日曜日

  時刻：午前 2 時（ローカル タイム）

- **2007 より前**：

  開始：4 月の第 1 日曜日

  終了：10 月の最終日曜日

  時刻：午前 2 時（ローカル タイム）

EU の夏時間のルール：

- **開始**：3 月の最終日曜日
- **終了**：10 月の最終日曜日

  時間：グリニッジ標準時（GMT）午前 1.00（01:00）

例

```
switchxxxxxx(config)# clock summer-time abc date apr 1 2010 09:00 aug 2 2010 09:00
```

clock timezone

表示用のタイム ゾーンを設定するには、グローバル コンフィギュレーション モードで **clock timezone** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

clock timezone *zone hours-offset* [*minutes-offset*]

no clock timezone

パラメータ

- ***zone***：タイム ゾーンの略語。（範囲：1 ー 4 文字）。頭字語には文字のみを含めることができます。
- ***hours-offset***：UTC との時間の差。（範囲：-12 ～ +13）
- ***minutes-offset***：（オプション）UTC との分の差。（範囲：0 ～ 59）

デフォルト設定

協定世界時（UTC）またはグリニッジ標準時（GMT）。これは、次の場合と同じです。

- オフセットが *0* の場合。
- 略語が空の場合。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

システムは内部的に UTC で時刻を管理しているため、このコマンドは表示専用で、時刻を手動で設定するときにだけ使用します。

例

```
switchxxxxxx(config)# clock timezone abc +2 minutes 32
```

periodic

時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定するには、時間範囲コンフィギュレーション モードで**periodic** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

periodic *day-of-the-week hh:mm* **to** *day-of-the-week hh:mm*

no periodic *day-of-the-week hh:mm* **to** *day-of-the-week hh:mm*

periodic list *hh:mm* **to** *hh:mm day-of-the-week1* [*day-of-the-week2… day-of-the-week7*]

no periodic list *hh:mm* **to** *hh:mm day-of-the-week1* [*day-of-the-week2… day-of-the-week7*]

periodic list *hh:mm* **to** *hh:mm all*

no periodic list *hh:mm* **to** *hh:mm all*

パラメータ

- ***day-of-the-week***：関連付けられた時間範囲が有効になる開始日。2 つ目は、関連付けられたステートメントが有効な終了日です。2つ目は、翌週にすることができます（ユーザ ガイドラインの説明を参照）。有効な値は、mon、tue、wed、thu、fri、sat、sun です。
- ***hh:mm***：この引数の 1 つ目は、関連付けられた時間範囲が有効になる開始時間:分（24 時間形式）です。2 つ目は、関連付けられたステートメントが有効な終了時間:分（24 時間形式）です。2つ目は、翌日にすることができます（ユーザガイドラインの説明を参照）。（範囲：0 ～ 23、mm：0 ～ 59）
- **list** *day-of-the-week1*：時間範囲が有効になる曜日のリストを指定します。

デフォルト設定

時間範囲が有効になっている場合の定期的な時間はありません。

コマンド モード

時間範囲コンフィギュレーション モード

使用上のガイドライン

2 つ目の曜日は、翌週にすることができます。たとえば、木曜日から月曜日を指定した場合、時間範囲は木曜日、金曜日、土曜日、日曜日、および月曜日に有効になります。

2 つ目の時刻は、翌日にすることができます（「22:00 ～ 2:00」など）。

例

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00
```

sntp anycast client enable

SNTP エニーキャスト クライアントを有効にするには、グローバル コンフィギュレーション モードで **sntp anycast client enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sntp anycast client enable *[***both** | **ipv4** | **ipv6***]*

パラメータ

- **both**：（オプション）IPv4 および IPv6 SNTP エニーキャスト クライアントを有効にすることを指定します。パラメータが定義されない場合のデフォルト値です。
- **ipv4**：（オプション）IPv4 SNTP エニーキャスト クライアントを有効にすることを指定します。
- **ipv6**：（オプション）IPv6 SNTP エニーキャスト クライアントを有効にすることを指定します。

デフォルト設定

SNTP エニーキャスト クライアントは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、SNTP エニーキャスト クライアントを有効にする場合に使用します。

例

次の例では、SNTP エニーキャスト クライアントを有効にしています。

```
switchxxxxxx(config)# sntp anycast client enable
```

sntp authenticate

サーバからの受信SNTPトラフィックの認証を有効にするには、グローバルコンフィギュレーション モードで **sntp authenticate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sntp authenticate

no sntp authenticate

デフォルト設定

認証は無効です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、受信SNTPトラフィックの認証を有効にし、キーと暗号キーを設定しています。

```
switchxxxxxx(config)# sntp authenticate
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
```

sntp authentication-key

Simple Network Time Protocol（SNTP）の認証キーを定義するには、グローバル コンフィギュレーション モードで **sntp authentication-key** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sntp authentication-key *key-number* **md5** *key-value*

encrypted sntp authentication-key *key-number* **md5** encrypted-*key-value*

no sntp authentication-key *key-number*

パラメータ

- ***key-number***：キー番号を指定します。（範囲：1 ～ 4294967295）
- ***key-value***：キー値を指定します。（長さ：1 ～ 8 文字）
- ***encrypted-key-value***：暗号化形式のキー値を指定します。

デフォルト設定

認証キーは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、SNTP の認証キーを定義しています。

```
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authenticate
```

sntp broadcast client enable

SNTPブロードキャストクライアントを有効にするには、グローバルコンフィギュレーションモードで **sntp broadcast client enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sntp broadcast client enable *[***both** | **ipv4** | **ipv6***]*

no sntp broadcast client enable

パラメータ

- **both**：（オプション）IPv4 および IPv6 SNTP ブロードキャスト クライアントを有効にすることを指定します。パラメータが定義されない場合のデフォルト値です。
- **ipv4**：（オプション）IPv4 SNTP ブロードキャスト クライアントを有効にすることを指定します。
- **ipv6**：（オプション）IPv6 SNTP ブロードキャスト クライアントを有効にすることを指定します。

デフォルト設定

SNTP ブロードキャスト クライアントは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

特定のインターフェイスで SNTP ブロードキャスト クライアントを有効にするには、**sntp broadcast client enable** インターフェイス コンフィギュレーション モード コマンドを使用します。

例

次の例では、SNTP ブロードキャスト クライアントを有効にしています。

```
switchxxxxxx(config)# sntp broadcast client enable
```

sntp client enable

SNTPブロードキャストおよびエニーキャストクライアントを有効にするには、グローバルコンフィギュレーション モードで **sntp client enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sntp client enable *interface-id*

no sntp client enable *interface-id*

パラメータ

- ***interface-id***：インターフェイス ID を指定します。イーサネット ポート、ポートチャネルまたは VLAN のいずれかのタイプを指定できます。

デフォルト設定

SNTP クライアントは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

SNTP ブロードキャストおよびエニーキャスト クライアントを有効にするには、**sntp client enable** コマンドを使用します。

例

次の例では、VLAN 100 で SNTP ブロードキャストおよびエニーキャスト クライアントを有効にしています。

```
switchxxxxxx(config)# sntp client enable vlan 100
```

sntp client enable（インターフェイス）

インターフェイスでSNTPブロードキャストおよびエニーキャストクライアントを有効にするには、インターフェイス コンフィギュレーション モードで **sntp client enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sntp client enable

no sntp client enable

デフォルト設定

インターフェイスの SNTP クライアントは、無効になっています。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

このコマンドは、インターフェイスでSNTPブロードキャストおよびエニーキャストクライアントを有効にします。SNTPクライアントを無効にするには、このコマンドの**no**形式を使用します。

例

次の例では、インターフェイスでSNTPブロードキャストおよびエニーキャストクライアントを有効にしています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# sntp client enable
switchxxxxxx(config-if)# exit
```

sntp server

SNTP を使用して、指定したサーバからの Network Time Protocol（NTP）トラフィックを要求して受信するようにデバイスを設定するには（SNTP サーバからシステム時刻を受信することを意味します）、グローバル コンフィギュレーション モードで **sntp server** コマンドを使用します。SNTP サーバのリストから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。

構文

sntp server {**default** | {{*ip-address* | *hostname*} [**poll**] [**key** *keyid*]}}

no sntp server [*ip-address* | *hostname*]

パラメータ

- **default**：デフォルトの定義済み SNTP サーバ。
- ***ip-address***：サーバ IP アドレスを指定します。これは、IPv4、IPv6 または IPv6z アドレスにできます。
- ***hostname***：サーバのホスト名を指定します。IPv4 アドレスへの変換のみがサポートされています。（長さ：1 ～ 158 文字、ホスト名の各部分のラベルの最大長：63 文字）
- **poll**：（オプション）ポーリングを有効にします。
- **key** *keyid*：（オプション）このピアにパケットを送信するときに使用する認証キーを指定します。（範囲：1 ～ 4294967295）

デフォルト設定

次のサーバが、ポーリング使用、認証なしに定義されます。

- ***time-a.timefreq.bldrdoc.gov***
- ***time-b.timefreq.bldrdoc.gov***
- ***time-c.timefreq.bldrdoc.gov***
- ***pool.ntp.org***
- ***time-pnp.cisco.com***

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

SNTP サーバを定義するには、**sntp server** {***ip-address*** | ***hostname***} [**poll**] [**key** ***keyid***] コマンドを使用します。スイッチでは、最大 8 つの SNTP サーバがサポートされます。

デフォルト設定に戻すには、**sntp server default** コマンドを使用します。

特定の SNTP サーバを削除するには、**no sntp server** *ip-address* | *hostname* コマンドを使用します。

すべての SNTP サーバを削除するには、**no sntp server** を使用します。

例

次の例では、ポーリングを使用して 192.1.1.1 上のサーバから SNTP トラフィックを受信するようにデバイスを設定しています。

```
switchxxxxxx(config)# sntp server 192.1.1.1 poll
```

sntp source-interface

IPv4 SNTP サーバとの通信用に、送信元 IPv4 アドレスとして IPv4 アドレスが使用される送信元インターフェイスを指定するには、グローバル コンフィギュレーション モードで **sntp source-interface** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sntp source-interface *interface-id*

no sntp source-interface

パラメータ

- ***interface-id***：送信元インターフェイスを指定します。

デフォルト設定

送信元 IPv4 アドレスは、発信インターフェイスで定義され、ネクスト ホップ IPv4 サブネットに属する IPv4 アドレスです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスの場合は、ネクスト ホップ IPv4 サブネットに属するインターフェイス IP アドレスが適用されます。

送信元インターフェイスが発信インターフェイスでない場合は、インターフェイスで定義されている最小 IPv4 アドレスが適用されます。

使用可能な IPv4 送信元アドレスがない場合は、IPv4 SNTP サーバとの通信時に SYSLOG メッセージが送信されます。

送信元インターフェイスとして OOB は定義できません。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# sntp source-interface vlan 10
```

sntp source-interface-ipv6

IPv6 SNTP サーバとの通信用に、送信元 IPv6 アドレスとして IPv6 アドレスが使用される送信元インターフェイスを指定するには、グローバル コンフィギュレーション モードで **sntp source-interface-ipv6** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sntp source-interface-ipv6 *interface-id*

no sntp source-interface-ipv6

パラメータ

- ***interface-id***：送信元インターフェイスを指定します。

デフォルト設定

IPv6送信元アドレスは、発信インターフェイスに定義され、RFC6724に従って選択されるIPv6アドレスです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

発信インターフェイスは、SNTP サーバの IP アドレスに基づいて選択されます。送信元インターフェイスが発信インターフェイスの場合は、このインターフェイスに定義された IPv6 アドレスになり、RFC 6724 に従って選択されます。

送信元インターフェイスが発信インターフェイスでない場合は、インターフェイス上で宛先 IPv6 アドレスの範囲で定義された最小 IPv4 アドレスが適用されます。

使用可能な IPv6 送信元アドレスがない場合は、IPv6 SNTP サーバとの通信時に SYSLOG メッセージが送信されます。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# sntp source-interface-ipv6 vlan 10
```

sntp trusted-key

信頼できるキーを定義するには、グローバル コンフィギュレーション モードで **sntp trusted-key** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sntp trusted-key *key-number*

no sntp trusted-key *key-number*

パラメータ

- ***key-number***：信頼する認証キーのキー番号を指定します。（範囲：1 ～ 4294967295）。

デフォルト設定

信頼できるキーは指定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

信頼できるキーは、パーソナルキーが割り当てられていないすべてのサーバの認証に使用されます。

例

次の例では、キー 8 を認証しています。

```
switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authenticate
```

sntp unicast client enable

デバイスで Simple Network Time Protocol（SNTP）ユニキャスト クライアントを使用できるようにするには、グローバル コンフィギュレーション モードで **sntp unicast client enable** コマンドを使用します。SNTP ユニキャスト クライアントを無効にするには、このコマンドの **no** 形式を使用します。

構文

sntp unicast client enable

no sntp unicast client enable

デフォルト設定

SNTP ユニキャストクライアントが有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

SNTP サーバを定義するには、**sntp server** グローバル コンフィギュレーション モード コマンドを使用します。

例

次の例では、デバイスが SNTP ユニキャスト クライアントを使用できるようにしています。

```
switchxxxxxx(config)# sntp unicast client enable
```

sntp unicast client poll

SNTP ユニキャスト クライアントのポーリングを有効にするには、グローバル コンフィギュレーション モードで **sntp unicast client poll** コマンドを使用します。ポーリングを無効にするには、このコマンドの **no** 形式を使用します。

構文

sntp unicast client poll

no sntp unicast client poll

デフォルト設定

ポーリングは有効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ポーリング間隔は 1024 秒です。

例

次の例では、SNTP ユニキャスト クライアントのポーリングを有効にしています。

```
switchxxxxxx(config)# sntp unicast client poll
```

show clock

システム クロックからの日時を表示するには、ユーザ EXEC モードで **show clock** コマンドを使用します。

構文

show clock [**detail**]

パラメータ

- **detail**：（オプション）タイム ゾーンと夏時間の設定を表示します。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

コマンドのデフォルト出力には、現在のシステムの日付と時刻、システム時刻の運用元の情報、および一般的なクロック関連の設定が表示されます。

コマンドの詳細な出力には、タイムゾーンと夏時間の設定に関する追加情報が表示されます。

運用システムの時刻源に使用可能な値は次のとおりです。

- RTC：システム時刻がリアル タイム クロック コンポーネントから設定されたことを示します。これは、システムクロックが SNTP、ユーザ、またはブラウザによって設定されていない場合に発生します。
- User：システムクロックがユーザによって最後に手動で設定されたことを示します。
- SNTP：システムクロックが SNTP によって最後に設定されたことを示します。この場合、SNTP サーバとの最後の同期以降の時間も表示されます。
- None：最後のリブート以降にクロックがいかなる方法によっても設定されておらず、システムに RTC コンポーネントがないことを示します。

例 1：次に、一般的なシステム時刻と日付の情報を表示する例を示します。

```
switchxxxxxx# show clock
 15:29:03 PDT(UTC-7) Jun 17 2019
Operational Time Source: SNTP (last synchronized 2 days, 18 hours, 29 minutes and 3
seconds ago)
Time from SNTP is enabled
Time from Browser is disabled
```

例 2：次に、システム時刻と日付に加えて、タイムゾーンと夏時間の設定を表示する例を示します。

```
switchxxxxxx# show clock detail
 15:22:55 SUN Apr 23 2019
```

```
Operational Time Source: User
Time from SNTP is disabled
Time from Browser is enabled
Time zone (DHCPv4 on VLAN1):
Acronym is RAIN
Offset is UTC+2
Time zone (Static):
Offset is UTC+0
Summertime (DHCPv4 on VLAN1):
Acronym is SUN
Recurring every year.
Begins at first Sunday of Apr at 02:00.
Ends at first Tuesday of Sep at 02:00.
Offset is 60 minutes.
Summertime (Static):
Acronym is GMT
Recurring every year.
Begins at first Sunday of Mar at 10:00.
Ends at first Sunday of Sep at 10:00.
Offset is 60 minutes.
DHCP timezone: Enabled
```

show sntp configuration

デバイスの SNTP 設定を表示するには、特権 EXEC モードで **show sntp configuration** コマンドを使用します。

構文

show sntp configuration

コマンド モード

特権 EXEC モード

例

次の例では、デバイスの現在の SNTP 設定を表示しています。

```
switchxxxxxx# show sntp configuration
SNTP port : 123
Polling interval: 1024 seconds
MD5 Authentication Keys
-----------------------------------
2   John123
3   Alice456
-----------------------------------
Authentication is not required for synchronization.
No trusted keys
Unicast Clients: enabled
Unicast Clients Polling: enabled
Server: 1.1.1.121
  Polling: disabled
  Encryption Key: disabled
Server: 3001:1:1::1
  Polling: enabled
  Encryption Key: disabled
Server: dns_server1.comapany.com
  Polling: enabled
  Encryption Key: disabled
Server: dns_server2.comapany.com
  Polling: enabled
  Encryption Key: disabled
Broadcast Clients: enabled for IPv4 and IPv6
Anycast Clients: disabled
No Broadcast Interfaces
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
```

show sntp status

SNTP サーバのステータスを表示するには、特権 EXEC モードで **show sntp status** コマンドを使用します。

構文

show sntp status

コマンド モード

特権 EXEC モード

例

次の例では、SNTP サーバのステータスを表示しています。

```
switchxxxxxx# show sntp status
Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is afe2525e.70597b34 (00:10:22.438 PDT Jul 5 1993)
Unicast servers:
Server: 176.1.1.8
  Source: DHCPv4 on VLAN 1
  Status: Up
  Last response: 19:58:22.289 PDT Feb 19 2015
  Last request: 19:58:21.555 PDT Feb 19 2015
  Stratum Level: 1
  Offset: 7.33mSec
  Delay: 117.79mSec
Server: dns_server.comapany.com
  Source:  static
  Status: Unknown
  Last response: 12:17.17.987 PDT Feb 19 2015
  Last request: 12:58:21.555 PDT Feb 19 2015
  Stratum Level: 1
  Offset: 8.98mSec
  Delay: 189.19mSec
Server: 3001:1:1::1
  Source: DHCPv6 on VLAN 2
  Status: Unknown
  Last response:
  Last request:
  Offset: mSec
  Delay: mSec
Server: dns1.company.com
  Source: DHCPv6 on VLAN 20
  Status: Unknown
  Last response:
  Last request:
  Offset: mSec
  Delay: mSec
Anycast servers:
Server: 176.1.11.8
  Interface:  VLAN 112
  Status: Up
  Last response: 9:53:21.789 PDT Feb 19 2005
  Last request: 9:53:21.689 PDT Feb 19 2005
  Stratum Level: 10
```

```
  Offset: 9.98mSec
  Delay: 289.19mSec
Broadcast servers:
Server: 3001:1::12
  Interface:  VLAN 101
  Last response: 9:53:21.789 PDT Feb 19 2005
  Last reqeust: 9:53:21.689 PDT Feb 19 2005
  Stratum Level: 255
```

show time-range

時間範囲の設定を表示するには、ユーザ EXEC モードで **show time-range** コマンドを使用します。

構文

show time-range *time-range-name*

パラメータ

- ***time-range-name***：既存の時間範囲の名前を指定します。

コマンド モード

ユーザ EXEC モード

例

```
switchxxxxxx# show time-range
http-allowed
--------------
absolute start 12:00 1 Jan 2005 end  12:00 31 Dec 2005
periodic Monday 12:00 to Wednesday 12:00
```

time-range

時間範囲を定義して、時間範囲コンフィギュレーション モードにするには、グローバル コンフィギュレーション モードで**time-range**コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

time-range *time-range-name*

no time-range *time-range-name*

パラメータ

- ***time-range-name***：時間範囲の名前を指定します。（範囲：1 ～ 32 文字）。

デフォルト設定

時間範囲は定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドで時間範囲コンフィギュレーション モードにした後に、**absolute** コマンドと **periodic** コマンドを使用して実際に時間範囲を設定します。時間範囲では、複数の **periodic** コマンドを使用できます。**absolute** コマンドは 1 つのみが使用できます。

time-range コマンドに absolute 値と periodic 値の両方が指定されている場合、periodic 項目は absolute start 時刻を経過した後にのみ評価の対象になり、absolute end 時刻を経過した後は再度評価の対象にはなりません。

すべての時間指定は、現地時間と解釈されます。

時間範囲のエントリを希望の時間に有効にするには、ユーザまたは SNTP がソフトウェア クロックを設定する必要があります。ユーザまたはSNTPがソフトウェア クロックを設定しない場合、時間範囲は有効になりません。

例

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00
```

DoS コマンド

この章は、次の項で構成されています。

- security-suite deny fragmented （326 ページ）
- security-suite deny icmp （327 ページ）
- security-suite deny martian-addresses （329 ページ）
- security-suite deny syn （331 ページ）
- security-suite deny syn-fin （333 ページ）
- security-suite dos protect （334 ページ）
- security-suite dos syn-attack （335 ページ）
- security-suite enable （337 ページ）
- security-suite syn protection mode （339 ページ）
- security-suite syn protection recovery （340 ページ）
- security-suite syn protection threshold （341 ページ）
- show security-suite configuration （342 ページ）
- show security-suite syn protection （343 ページ）

security-suite deny fragmented

特定のインターフェイスから断片化された IP パケットを破棄するには、**security-suite deny fragmented** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。

断片化された IP パケットを許可するには、このコマンドの **no** 形式を使用します。

構文

security-suite deny fragmented *{[***add** *{ip-address* | **any***} {mask* | */prefix-length}]* | *[***remove** *{ip-address* | **any***} {mask* | */prefix-length}]}*

no security-suite deny fragmented

パラメータ

- **add** *ip-address* | *any*：宛先 IP アドレスを指定します。**any** を使用して、すべての IP アドレスを指定します。
- **mask**：IP アドレスのネットワーク マスクを指定します。
- **prefix-length**：IP アドレス プレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。

デフォルト設定

断片化されたパケットはすべてのインターフェイスから許可されます。

mask が指定されていない場合、デフォルトは 255.255.255.255 です。

prefix-length が指定されていない場合、デフォルトは 32 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （342 ページ） がグローバルとインターフェイスの両方で有効である必要があります。

例

次の例では、インターフェイスからの断片化された IP パケットの破棄を試みています。

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite deny fragmented add any /32
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny icmp

（デバイスがネットワーク上にあることを攻撃者に知られることを防ぐために）特定のインターフェイスからの ICMP エコー要求を破棄するには、**security-suite deny icmp** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。

エコー要求を許可するには、このコマンドの **no** 形式を使用します。

構文

security-suite deny icmp *{[***add** *{ip-address* | **any***} {mask* | */prefix-length}]* | *[***remove** *{ip-address* | **any***} {mask* | */prefix-length}]}*

no security-suite deny icmp

パラメータ

- **ip-address** | **any**：宛先 IP アドレスを指定します。**any** を使用して、すべての IP アドレスを指定します。
- **mask**：IP アドレスのネットワーク マスクを指定します。
- **prefix-length**：IP アドレス プレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。

デフォルト設定

エコー要求はすべてのインターフェイスから許可されます。

mask が指定されていない場合、デフォルトは 255.255.255.255 です。

prefix-length が指定されていない場合、デフォルトは 32 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （342 ページ） がグローバルとインターフェイスの両方で有効である必要があります。

このコマンドは、指定されたインターフェイスに入る、ICMP タイプがエコー要求の ICMP パケットを破棄します。

例

次の例では、インターフェイスからのエコー要求の破棄を試みています。

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite deny icmp add any /32
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny martian-addresses

システム予約済み IP アドレスまたはユーザ定義 IP アドレスを含むパケットを拒否するには、**security-suite deny martian-addresses** グローバル コンフィギュレーション モード コマンドを使用します。

デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

構文

security-suite deny martian-addresses *{***add** *{ip-address {mask | /prefix-length}} |* ***remove*** *{ip-address {mask | /prefix-length}}*（ユーザ指定 IP アドレスの追加または削除）

security-suite deny martian-addresses ***reserved*** *{***add** | **remove***}* *(*Add/remove system-reserved IP addresses, see tables below)

no security-suite deny martian-addresses（このコマンドは、**security-suite deny martian-addresses** *{***add** *{ip-address {mask | /prefix-length}} |* ***remove*** *{ip-address {mask | /prefix-length}}* により予約されたアドレスを削除し、ユーザにより追加されたすべてのエントリを削除します。**remove** *ip-address {mask | /prefix-length}* パラメータを使用することで、ユーザは特定のエントリを削除できます）。

security-suite deny martian-addresses ***reserved*** *{***add** | **remove***}* コマンドの **no** 形式はありません。保護を削除するには（そして、ハードウェア リソースを解放するには）、代わりに **security-suite deny martian-addresses reserved** *remove* コマンドを使用します。

パラメータ

- **reserved add/remove**：以下の予約済みアドレスの表に対して追加または削除を行います。
- **ip-address**：指定された IP 送信元または宛先アドレスを持つパケットを追加または破棄します。
- **mask**：IP アドレスのネットワーク マスクを指定します。
- **prefix-length**：IP アドレス プレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。
- **reserved**：予約済み（Martian）IP アドレスのブロック内の送信元または宛先 IP アドレスを持つパケットを破棄します。予約済みアドレスのリストについては、ユーザ ガイドラインを参照してください。

デフォルト設定

Martian アドレスは許可されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （342 ページ） がグローバルに有効である必要があります。

security-suite deny martian-addresses *reserved* は、次の表のアドレスを追加または削除します。

アドレス ブロック	現在の使用
0.0.0.0/8（0.0.0.0/32 が送信元アドレスの場合を除く）	このブロック内のアドレスは、「この」ネットワーク上の送信元ホストを参照します。
127.0.0.0/8	このブロックは、インターネット ホスト ループバック アドレスとして使用するために割り当てられています。
192.0.2.0/24	このブロックは、ドキュメンテーションとサンプル コードで使用するための「TEST-NET」として割り当てられています。
224.0.0.0/4（送信元として）	以前はクラス D アドレス空間として知られていたこのブロックは、IPv4 マルチキャスト アドレス割り当てで使用するために割り当てられています。
240.0.0.0/4（255.255.255.255/32 が宛先アドレスの場合を除く）	以前はクラス E アドレス空間として知られていたこのブロックは、予約済みです。

（注） 予約済みのアドレスが含まれている場合は、個々の予約済みのアドレスは削除できません。

例

次の例では、予約済み IP アドレスのブロック内の送信元または宛先アドレスを持つ、すべてのパケットを破棄しています。

```
switchxxxxxx(config)# security-suite deny martian-addresses reserved add
```

security-suite deny syn

特定のインターフェイスからの TCP 接続の作成をブロックするには、**security-suite deny syn** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。このコマンドは、これらの接続を完全にブロックします。

TCP 接続の作成を許可するには、このコマンドの **no** 形式を使用します。

構文

security-suite deny syn {*[***add** *{tcp-port* | **any***} {ip-address* | **any***} {mask* | */prefix-length}]* | *[***remove** *{tcp-port* | **any***} {ip-address* | **any***} {mask* | */prefix-length}]}*

no security-suite deny syn

パラメータ

- **ip-address** | **any**：宛先 IP アドレスを指定します。**any** を使用して、すべての IP アドレスを指定します。
- **mask**：宛先 IP アドレスのネットワーク マスクを指定します。
- **prefix-length**：宛先IPアドレスプレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。
- **tcp-port** | **any**：宛先 TCP ポートを指定します。使用できる値は、**http**、**ftp-control**、**ftp-data**、**ssh**、**telnet**、**smtp**、または **port number** です。すべてのポートを指定するには **any** を使用します。

デフォルト設定

TCP 接続の作成は、すべてのインターフェイスから許可されます。

mask が指定されていない場合、デフォルトは 255.255.255.255 です。

prefix-length を指定しない場合は、デフォルトで 32 が使用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （342 ページ） がグローバルとインターフェイスの両方で有効である必要があります。

インターフェイスからの TCP 接続の作成のブロックは、指定された宛先 IP アドレスと宛先 TCP ポートについて、「SYN=1」、「ACK=0」、および「FIN=0」の入力 TCP パケットを破棄することで行われます。

例

次の例では、インターフェイスからの TCP 接続の作成のブロックを試みています。これは、セキュリティ スイートがインターフェイスごとではなく、グローバルに有効になっているため、失敗します。

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite deny syn add any /32 any
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny syn-fin

SYN と FIN の両方が設定されているすべての入力 TCP パケットをドロップするには、**security-suite deny syn-fin** グローバル コンフィギュレーション モード コマンドを使用します。

SYN と FIN の両方が設定されている TCP パケットを許可するには、このコマンドの **no** 形式を使用します。

構文

security-suite deny syn-fin

no security-suite deny syn-fin

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

この機能は、デフォルトで有効に設定されています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、SYN フラグと FIN フラグの両方が設定されている TCP パケットをブロックしています。

```
switchxxxxxx(config)# security-suite deny syn-fin
```

security-suite dos protect

特定の既知のサービス妨害（DoS）攻撃からシステムを保護するには、**security-suite dos protect** グローバル コンフィギュレーション モード コマンドを使用します。3 つのタイプの攻撃に保護を提供できます（以下のパラメータを参照）。

DoS 保護を無効にするには、このコマンドの **no** 形式を使用します。

構文

security-suite dos protect {**add** *attack* | **remove** *attack*}

no security-suite dos protect

パラメータ

add/remove *attack*：追加または削除する攻撃タイプを指定します。攻撃を追加すると、その攻撃に対する保護が提供されます。攻撃を削除すると、保護が削除されます。

使用できる攻撃タイプは次のとおりです。

- **stacheldraht**：送信元 TCP ポートが 16660 の TCP パケットを破棄します。
- **invasor-trojan**：宛先 TCP ポートが 2140、送信元 TCP ポートが 1024 の TCP パケットを破棄します。
- **back-orifice-trojan**：宛先 UDP ポートが 31337、送信元 UDP ポートが 1024 の UDP パケットを破棄します。

デフォルト設定

保護は設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （342 ページ） がグローバルに有効である必要があります。

例

次の例では、Invasor トロイの木馬 DoS 攻撃からシステムを保護しています。

```
switchxxxxxx(config)# security-suite dos protect add invasor-trojan
```

security-suite dos syn-attack

サービス妨害（DoS）SYN 攻撃をレート制限するには、**security-suite dos syn-attack** インターフェイス コンフィギュレーション モード コマンドを使用します。このコマンドにより、SNY パケットが部分的にブロックされます（最大で、ユーザが指定したレートまで）。

レート制限を無効にするには、このコマンドの **no** 形式を使用します。

構文

security-suite dos syn-attack *syn-rate* {***any*** **|** *ip-address*} {*mask* | *prefix-length*}

no security-suite dos syn-attack {***any*** **|** *ip-address*} {*mask* | *prefix-length*}

パラメータ

- **syn-rate**：1 秒あたりの最大接続数を指定します。（範囲：199 ～ 1000）
- **any | ip-address**：宛先 IP アドレスを指定します。**any** を使用して、すべての IP アドレスを指定します。
- **mask**：宛先 IP アドレスのネットワーク マスクを指定します。
- **prefix-length**：宛先 IP アドレス プレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。

デフォルト設定

レート制限は設定されていません。

ip-address が指定されていない場合、デフォルトは 255.255.255.255 です。

prefix-length が指定されていない場合、デフォルトは 32 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドが動作するためには、show security-suite configuration （342 ページ） がグローバルとインターフェイスの両方で有効である必要があります。このコマンドは、指定された宛先 IP アドレスについて、「SYN=1」、「ACK=0」、および「FIN=0」の入力 TCP パケットをレート制限します。SYN 攻撃のレート制限は、セキュリティ スイートのルールがパケットに適用された後に実装されます。ACL ルールと QoS ルールは、これらのパケットには適用されません。ハードウェア レート制限はバイト数をカウントするため、「SYN」パケットのサイズは短いと見なされます。

例

次の例では、ポートでの DoS SYN 攻撃のレート制限を試みています。これは、セキュリティスイートがインターフェイスごとではなく、グローバルに有効になっているため、失敗します。

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite enable

セキュリティスイート機能と設定を有効にするには、**security-suite enable** グローバル コンフィギュレーション モード コマンドを使用します。セキュリティスイート機能は、さまざまなタイプの攻撃に対する保護をサポートします。デフォルト設定を復元するには、このコマンドの **no** 形式を使用します。

構文

security-suite enable [**global-rules-only | interface-rules-only**]

no security-suite enable

パラメータ

- **global-rules-only**：（オプション）デバイスがグローバルレベル（インターフェイスレベルではない）のセキュリティスイートコマンドのみをサポートするように指定します。この設定により、Ternary Content Addressable Memory（TCAM）のスペースを節約できます。このキーワードを使用しない場合、security-suite コマンドはグローバルに使用することもインターフェイスごとに使用することもできます。
- **interface-rules-only**：（オプション）デバイスがインターフェイスレベルのセキュリティスイートコマンドのみをサポートするように指定します（詳細については、次のユーザガイドラインを参照してください）。このモードは、デバイス上のいずれかのインターフェイスに ACL が適用されている場合は有効にできません。
- **(none)**：キーワードを使用しない場合、セキュリティスイートのコマンドはグローバルにもインターフェイスごとにも使用できます。このモードは、ACL がデバイス上のインターフェイスに適用されている場合は有効にできません。

デフォルト設定

セキュリティ スイート機能は無効になっています。

global-rules-only または **interface-rules-only** のいずれも指定されていない場合、デフォルトではセキュリティスイートをグローバルとインターフェイスごとに有効にします。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

セキュリティスイートの設定を定義し、有効にできる設定のタイプ（グローバルレベルルールのみ、インターフェイス レベル ルールのみ、または両方のタイプ）を決定する機能を有効にするには、このコマンドを使用します。セキュリティスイートが有効になっている場合、ユーザが設定したモードに応じて、次のコマンドを使用できます。

このコマンドを使用すると、ハードウェア リソースが予約されます。予約するリソースの数はコマンドに指定したモード（**global-rules-only**、**interface-rules-only**、または no mode（両方のタイプ））によって異なります。リソースは、**no security-suite enable** コマンドが入力されると解放されます。

セキュリティ スイートを有効にする前に、MAC ACL を削除する必要があります。このルールは、セキュリティ スイートを有効にした後に再入力できます。インターフェイスに ACL またはポリシー マップが割り当てられている場合は、インターフェイスのセキュリティ スイートのルールごとに有効にすることはできません。

例 1：次の例では、セキュリティ スイート機能を有効にし、security-suite コマンドがグローバル コマンドのみであることを指定しています。ポート上でセキュリティ スイートを設定しようとすると失敗します。

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

例 2：次の例では、セキュリティ スイート機能をグローバルに、およびインターフェイスで有効にしています。ポートに対する security-suite コマンドは成功します。

```
switchxxxxxx(config)# security-suite enable
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
switchxxxxxx(config-if)#
```

security-suite syn protection mode

TCP SYN 保護モードを設定するには、**security-suite syn protection mode** グローバル コンフィギュレーション モード コマンドを使用します。

TCP SYN 保護モードをデフォルトに設定するには、このコマンドの **no** 形式を使用します。

構文

security-suite syn protection mode {disabled | report | block}

no security-suite syn protection mode

パラメータ

- **disabled**：この機能が無効になります。
- **report**：この機能でポートごとの TCP SYN トラフィックに関して報告されます（攻撃が識別された場合のレート制限 SYSLOG メッセージを含む）。
- **block**：ローカル システム宛ての攻撃ポートからの TCP SYN トラフィックがブロックされ、レート制限 SYSLOG メッセージ（1 分ごとに 1 回）が生成されます。

デフォルト設定

デフォルト モードは block です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

（ユーザ定義 ACL などの）ACL が定義されているポートでは、この機能は TCP SYN パケットをブロックできません。保護モードがブロックされて SYN トラフィックをブロックできない場合、関連する SYSLOG メッセージ（port gi1/0/1 is under TCP SYN attack など）が作成されます。TCP SYN traffic cannot be blocked on this port since the port is bound to an ACL.」というメッセージが作成されます。

例 1：次の例では、ポートから攻撃が識別された場合に、ポートに対する TCP SYN 攻撃を報告するように TCP SYN 保護機能を設定しています。

```
switchxxxxxx(config)# security-suite syn protection mode report
```

例 2：次の例では、ポートから攻撃が識別された場合に、ポートに対する TCP SYN 攻撃をブロックするように TCP SYN 保護機能を設定しています。

```
switchxxxxxx(config)# security-suite syn protection mode block
```

security-suite syn protection recovery

攻撃されたインターフェイスをSYN保護機能がブロックする期間を設定するには、**security-suite syn protection period** グローバル コンフィギュレーション モード コマンドを使用します。

期間をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

構文

security-suite syn protection recovery timeout

no security-suite syn protection recovery

パラメータ

timeout：SYN パケットのブロック元のインターフェイスでブロックを解除するタイムアウト（秒単位）を定義します。このインターフェイスで SYN 攻撃が引き続きアクティブな場合には、再度ブロックされる可能性があることに注意してください。（範囲：10 ～ 600）

デフォルト設定

デフォルトのタイムアウト値は 60 秒です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

タイムアウトが変更された場合、新しい値は現在攻撃を受けていないインターフェイスでのみ使用されます。

例

次の例では、TCP SYN 期間を 100 秒に設定しています。

```
switchxxxxxx(config)# security-suite syn protection recovery 100
```

security-suite syn protection threshold

SYN 保護機能のしきい値を設定するには、**security-suite syn protection threshold** グローバル コンフィギュレーション モード コマンドを使用します。

しきい値をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

構文

security-suite syn protection threshold syn-packet-rate

no security-suite syn protection threshold

パラメータ

syn-packet-rate：TCP SYN 攻撃の識別をトリガーする、特定の各ポートからのレート（1 秒あたりのパケット数）を定義します。（範囲：20 ～ 200）

デフォルト設定

デフォルトのしきい値は 80 pps（1 秒あたりのパケット数）です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、TCP SYN 保護のしきい値を 40 pps に設定しています。

```
switchxxxxxx(config)# security-suite syn protection threshold 40
```

show security-suite configuration

セキュリティスイート設定を表示するには、**show security-suite configuration** switchxxxxxx> コマンドを使用します。

構文

show security-suite configuration

コマンド モード

ユーザ EXEC モード

例

次の例では、セキュリティ スイート設定を表示しています。

```
switchxxxxxx# show security-suite configuration
```

セキュリティスイートが有効になっています（インターフェイスごとのルールが有効になっている）。

```
Denial Of Service Protect: stacheldraht, invasor-trojan, back-office-trojan.
Denial Of Service SYN-FIN Attack is enabled
Denial Of Service SYN Attack
```

Interface	IP Address	SYN Rate (pps)
gi1/0/1	176.16.23.0\24	100

```
Martian addresses filtering
Reserved addresses: enabled.
Configured addresses: 10.0.0.0/8, 192.168.0.0/16
SYN filtering
```

Interface	IP Address	TCP port
gi1/0/2	176.16.23.0\24	FTP

```
ICMP filtering
```

Interface	IP Address	
gi1/0/2	176.16.23.0\24	

```
Fragmented packets filtering
```

Interface	IP Address	
gi1/0/2	176.16.23.0\24	

show security-suite syn protection

SYN 保護機能の設定と、インターフェイスごとの最後の攻撃の時間を含むインターフェイス ID ごとの動作ステータスを表示するには、**show security-suite syn protection** switchxxxxxx> コマンドを使用します。

構文

show security-suite syn protection [interface-id]

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

インターフェイス ID を使用して、特定のインターフェイスに関する情報を表示します。

例

次の例では、TCP SYN 保護機能の設定と、すべてのインターフェイスの現在のステータスを表示しています。この例では、ポート gi1/0/2 が攻撃されていますが、このポートにはユーザ ACL が存在するため、ブロックできません。そのため、ステータスは Blocked and Reported ではなく Reported になっています。

```
switchxxxxxx# show security-suite syn protection
Protection Mode: Block
Threshold: 40 Packets Per Second
Period: 100 Seconds
```

Interface Name	Current Status	Last Attack
gi1/0/1	Attacked	19:58:22.289 PDT Feb 19 2012 Blocked and Reported
gi1/0/2	Attacked	19:58:22.289 PDT Feb 19 2012 Reported
gi1/0/3	Attacked	19:58:22.289 PDT Feb 19 2012 Blocked and Reported

DHCP リレー コマンド

この章は、次の項で構成されています。

- ip dhcp relay enable（グローバル） （346 ページ）
- ip dhcp relay enable（インターフェイス） （347 ページ）
- ip dhcp relay address（グローバル） （348 ページ）
- show ip dhcp relay （349 ページ）
- ip dhcp information option （350 ページ）
- ip dhcp information option numeric-token-format （351 ページ）
- ip dhcp information option circuit-id （352 ページ）
- ip dhcp information option remote-id （357 ページ）
- show ip dhcp information option tokens （362 ページ）
- show ip dhcp information option （365 ページ）

ip dhcp relay enable（グローバル）

デバイスの DHCP リレー機能を有効にするには、**ip dhcp relay enable** グローバル コンフィギュレーション モード コマンドを使用します。DHCP リレー機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip dhcp relay enable

no ip dhcp relay enable

デフォルト設定

DHCP リレー機能は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、デバイスの DHCP リレー機能を有効にしています。

```
switchxxxxxx(config)# ip dhcp relay enable
```

ip dhcp relay enable（インターフェイス）

インターフェイスの DHCP リレー機能を有効にするには、**ip dhcp relay enable** インターフェイス コンフィギュレーション モード コマンドを使用します。インターフェイスの DHCP リレー エージェント機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip dhcp relay enable

no ip dhcp relay enable

デフォルト設定

無効

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

次のいずれかの条件を満たすと、インターフェイスの DHCP リレーの動作ステータスがアクティブになります。

- DHCP リレーがグローバルに有効になっており、インターフェイスで IP アドレスが定義されている。

または

- DHCP リレーがグローバルに有効になっており、インターフェイスで IP アドレスが定義されておらず、インターフェイスが VLAN であり、オプション 82 が有効になっている。

例

次の例では、VLAN 21 で DHCP リレーを有効にしています。

```
switchxxxxxx(config)# interface vlan 21
switchxxxxxx(config-if)# ip dhcp relay enable
```

ip dhcp relay address（グローバル）

DHCP リレーで利用可能な DHCP サーバを定義するには、**ip dhcp relay address** グローバル コンフィギュレーション モード コマンドを使用します。リストから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。

構文

ip dhcp relay address *ip-address*

no ip dhcp relay address [*ip-address*]

パラメータ

- ***ip-address***：DHCP サーバ IP アドレスを指定します。サーバは最大で 8 つまで定義できます。

デフォルト設定

サーバは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

グローバル DHCP サーバの IP アドレスを定義するには、**ip dhcp relay address** コマンドを使用します。複数の *DHCP* サーバを定義するには、このコマンドを複数回使用します。

DHCP サーバを削除するには、このコマンドの **no** 形式に *ip-address* 引数を指定して使用します。

ip-address 引数を指定しないこのコマンドの **no** 形式は、グローバルに定義されたすべての DHCP サーバを削除します。

例

次の例では、デバイスで DHCP サーバを定義します。

```
switchxxxxxx(config)# ip dhcp relay address 176.16.1.1
```

show ip dhcp relay

DHCP リレーの情報を表示するには、**show ip dhcp relay** EXEC モード コマンドを使用します。

構文

show ip dhcp relay

コマンド モード

ユーザ EXEC モード

例

次に、オプション 82 が無効になっている場合の例を示します。

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally disabled
Option 82 is disabled
Maximum number of supported VLANs without IP Address: 0
Number of DHCP Relays enabled on VLANs without IP Address: 4
DHCP relay is enabled on Ports: gi1/0/1,po1-2
 Active:
 Inactive: gi1/0/1, po1-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
 Active:
 Inactive: 1, 2, 4, 5
Global Servers: 1.1.1.1 , 2.2.2.2
```

次に、オプション 82 が有効になっている場合の例を示します。

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: gi1/0/1,po1-2
 Active: gi1/0/1
 Inactive: po1-2
DHCP relay is enabled on VLANs: 1, 2, 4, 5
 Active: 1, 2, 4, 5
 Inactive:
Global Servers: 1.1.1.1 , 2.2.2.2
```

ip dhcp information option

DHCP オプション 82 のデータ挿入を有効にするには、**ip dhcp information option** グローバル コンフィギュレーション モード コマンドを使用します。DHCP オプション 82 データ挿入を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip dhcp information option

no ip dhcp information option

デフォルト設定

DHCP オプション 82 データ挿入は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

DHCP オプション 82 は、DHCP スヌーピングまたは DHCP リレーが有効になっている場合にのみ有効になります。

例

```
switchxxxxxx(config)# ip dhcp information option
```

ip dhcp information option numeric-token-format

回線 ID およびリモート ID サブオプションのペイロードテンプレートに含める数値トークンの形式を定義するには、**ip dhcp information option number-token-format** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト形式に戻すには、このコマンドの **no** 形式を使用します。

構文

ip dhcp information optionnumeric-token-format {hex | ascii}

no ip dhcp information option numeric-token-format

パラメータ

- **hex**：16 進数（数値）形式は、回線 ID およびリモート ID のペイロードテンプレートに含まれる数値トークンのパケットで使用されます。
- **ascii**：ASCII 形式は、回線 ID および リモート ID のペイロードテンプレートに含まれる数値トークンのパケットで使用されます。このオプションを選択した場合、数値トークンの個々の数字は ASCII テーブルの値で表示されます。

デフォルト設定

使用されるデフォルトの形式は、16 進数/数値形式です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

回線 ID またはリモート ID のサブオプションのペイロード テンプレート コマンドに含まれる数値トークン形式を設定するには、ip dhcp information option circuit-id と ip dhcp information option remote-id コマンドを使用します。

次に、このコマンドの影響を受ける数値トークンを示します。

- $int-ifindex$
- $int-portid$
- $switch-moduleid$
- $vlan-id$

例

次に、数値トークンの挿入にASCII形式を使用するようにデバイスを設定する例を示します。

```
switchxxxxxx(config)# ip dhcp information option numeric-token-format ascii
```

ip dhcp information option circuit-id

DHCP オプション 82 回線 ID サブオプションのペイロードテンプレートを設定するには、**ip dhcp information option circuit-id** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトのテンプレートに戻すには、このコマンドの **no** 形式を使用します。

構文

ip dhcp information option circuit-id *text*

no ip dhcp information option circuit-id

パラメータ

- ***text***：フリーテキストと $tokenname$ 形式の 1 つ以上のトークンの連結（長さ 1 ～ 160）

デフォルト設定

デフォルトの回線 ID のペイロードテンプレートは *$vlan-id$$switch-moduleid$$int-portid$* です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用して、デバイスによって挿入された オプション 82 回線 ID サブオプションのペイロードテンプレートを設定します。回線 ID サブオプションのペイロードセクションには、サブオプションのすべてのバイトの他に、次のようにデバイスによって値が設定されたサブオプションの最初の 4 バイトが含まれています。

回線 ID サブオプションのタイプ（値 = 1）

- サブオプションの合計長（1 バイト目と合計バイト数を除く）

  回線 ID タイプ（値= 1）：デフォルトのサブオプションテンプレートが使用されている場合、このフィールドの値は 0 になります。

  サブオプションのペイロード長

text フィールドは、フリーテキストと *$tokenname$* 形式の 1 つ以上のトークンを連結したものになります。トークンは指定した正確な形式で入力する必要があります（次の表を参照）。そうしないと、トークンとして認識されません。

text は、フリーテキストまたはトークンで開始または終了できます。トークンは連続して連結することも、フリーテキストで区切ることもできます。フリーテキストにスペース文字が含まれている場合は、*text* パラメータを引用符の間に配置する必要があります（例："*text1 text2*"）。

回線 ID のペイロードテンプレートには、インターフェイスパラメータ（*$int-xxx$*で始まるトークン）に関連するトークンを 1 つ以上含める必要があります。さらに、文字列に VLAN 関連トークンが含まれていない場合、ユーザは設定の確認を求められます。

コマンドの *text* フィールドの合計長は 160 バイトを超えることはできません。バイトカウントには、テキストパラメータのすべてのバイト（*text* フィールドに書き込まれたすべてのフリーテキストとトークンを含む）が含まれます。

回線 ID のペイロードリモート ID ペイロードの合計長は 247 バイトを超えることはできません。ペイロードバイトカウントは、フリーテキスト文字数（各 1 バイト）と各トークン用に予約された定義済みの長さを考慮します（次の表を参照）。

次の表に、サポートされているトークン、それらが表すデバイスパラメータ、および各トークンの予約済みバイト数と実際のバイト数の詳細を示します。

トークン名	説明	予約済みの長さ	実際の長さ
$int-ifindex$	送信元インターフェイスの ifIndex 値	4 バイト	16 進形式：2 バイト ASCII 形式：4 バイト
$int-portid$	特定のモジュール（スタック内）の送信元インターフェイスの連続番号。LAG 送信元インターフェイスの場合：LAG ID	2 バイト	16 進形式：1 バイト ASCII 形式：2 バイト
$int-name$	CLI コマンドで使用される送信元インターフェイスの完全な名前。	32 バイト	インターフェイスの完全な名前の ASCII 表現に必要な実際のバイト数。
$int-abrvname$	CLI コマンドで使用する送信元インターフェイスの省略名。	8 バイト	インターフェイスの完全な名前の ASCII 表現に必要な実際のバイト数。
$int-desc-16$	送信元インターフェイスでユーザが設定した説明。説明が 16 バイトを超える場合：最初の 16 バイトのみが使用されます。 説明を設定しない場合は、省略されたインターフェイス名が使用されます。	16 バイト	インターフェイスの説明の ASCII 表現に必要な実際のバイト数（最大 16 バイト）。

トークン名	説明	予約済みの長さ	実際の長さ
$int-desc-32$	送信元インターフェイスでユーザが設定した説明。説明が32バイトを超える場合：最初の32バイトのみが使用されます。 説明を設定しない場合は、省略されたインターフェイス名が使用されます。	32 バイト	インターフェイスの説明の ASCII 表現に必要な実際のバイト数（最大 32 バイト）。
$int-desc-64$	送信元インターフェイスでユーザが設定した説明。 説明を設定しない場合は、省略されたインターフェイス名が使用されます。	64 バイト	インターフェイスの説明の ASCII 表現に必要な実際のバイト数。
$int-mac$	送信元インターフェイスの MAC アドレス（デリミタなしの16進数値）	6 バイト	6 バイト
$switch-mac$	DHCP パケットをリレー/転送するスイッチの MAC アドレス（デリミタなしの 16 進数値）	6 バイト	6 バイト
$switch-hostname-16$	DHCP パケットをリレー/転送するスイッチのホスト名。 ホスト名が16バイトを超える場合：最初の16バイトのみが使用されます。	16 バイト	ホスト名の ASCII 表現に必要な実際のバイト数（最大16バイト）。

トークン名	説明	予約済みの長さ	実際の長さ
$switch-hostname-32$	DHCP パケットをリレー/転送するスイッチのホスト名。 ホスト名が 32 バイトを超える場合：最初の 32 バイトのみが使用されます。	32 バイト	ホスト名の ASCII 表現に必要な実際のバイト数（最大 32 バイト）。
$switch-hostname-58$	DHCP パケットをリレー/転送するスイッチのホスト名。	58 バイト	ホスト名の ASCII 表現に必要な実際のバイト数。
$switch-moduleid$	DHCP クライアント要求を受信した送信元インターフェイスのユニット ID。	2 バイト	16 進形式：1 バイト ASCII 形式：2 バイト
$vlan-id$	送信元 VLAN ID（1 ー 4094）	4 バイト	16 進形式：2 バイト ASCII 形式：4 バイト
$vlan-name-16$	ユーザが VLAN に割り当てた VLAN 名。名前が 16 バイトを超える場合：最初の 16 バイトのみが使用されます。 VLAN に名前を設定しない場合は、関連する VLAN ifDescr MIB フィールドから値が取得されます。	16 バイト	VLAN 名の ASCII 表現に必要な実際のバイト数（最大 16）。
$vlan-name-32$	ユーザが VLAN に割り当てた VLAN 名。 VLAN に名前を設定しない場合は、関連する VLAN ifDescr MIB フィールドから値が取得されます。	32 バイト	VLAN 名の ASCII 表現に必要な実際のバイト数（最大 32）。

注：

- 送信元インターフェイスまたは VLAN int テーブルは、（オプション 82 が追加された）DHCP クライアントパケットを受信したインターフェイスまたは VLAN を参照します。

- 予約済みの（バイト）長さ：トークンがパケットで「消費」する最大長。この値は、247 バイト制限の計算に使用されます（すべてのサブオプションペイロードを組み合わせた場合）。数値トークンを 16 進数値または ASCII 値として入力した場合、予約済みの長さは変更されません。
- 実際の（バイト）長さ：トークンがパケット自体で「消費」する実際のバイト数。トークンを exadecimal 値または ASCII 値として入力した場合、（関連するトークンの場合）実際のバイト長が変更される可能性があります。

例

次に、回線 ID のペイロードテンプレートを、インターフェイス名と VLAN 名を表すフリーテキストとトークンの連結に設定する例を示します（最大 16 文字）。

```
switchxxxxxx(config)# ip dhcp information option circuit-id
aaa$int-name$bbb$vlan-name-16$ccc
```

次に、回線 ID のペイロードテンプレートを設定する例を示します。ここでは、テキストパラメータにインターフェイスに関連するトークンは含まれません。

```
switchxxxxxx(config)# ip dhcp information option circuit-id aaa
Illegal Circuit-ID payload: Cicuit-ID must include at least 1 interface related Token
```

次に、フリーテキストとトークンの連結を使用するように回線 ID のペイロードテンプレートを設定する例を示します。ここでは、テンプレートに VLAN に関連するトークンは含まれません。

```
switchxxxxxx(config)# ip dhcp information option circuit-id aaa$int-name$bbb
Circuit-ID payload does not include a token reflecting DHCP client source VLAN. Continue?
 y/n[n] y
```

次に、フリーテキストとトークンの連結を使用するように回線 ID のペイロードテンプレートを設定し、その結果、回線 ID とリモート ID を組み合わせた予約済みペイロードが 247 バイトを超える例を示します。

```
switchxxxxxx(config)# ip dhcp information option circuit-id
aaa$vlan-name-32$bbb$int-desc-64$ccc$switch-hostname-58$ddd
Illegal Circuit-ID payload: Circuit-ID and Remote-ID payload reserved byte count exceeds
 247 bytes
```

ip dhcp information option remote-id

DHCP オプション 82 リモート ID サブオプションのペイロードテンプレートを設定するには、**ip dhcp information option remote-id** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトのテンプレートに戻すには、このコマンドの **no** 形式を使用します。

構文

ip dhcp information option remote-id *text*

no ip dhcp information option remote-id

パラメータ

- ***text***：フリーテキストと $tokenname$ 形式の 1 つ以上のトークンの連結（長さ 1 ～ 160）

デフォルト設定

デフォルトのリモート ID のペイロードテンプレートは *$switch-mac$* です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

デバイスによって挿入されるオプション 82 リモート ID サブオプションのペイロードテンプレートを設定するには、このコマンドを使用します。リモート ID サブオプションのペイロードセクションには、サブオプションの最初の 4 バイト以外のサブオプションのすべてのバイトが含まれています。値は次のようにデバイスによって設定されます。

リモート ID サブオプションタイプ（値 = 2）

- サブオプションの合計長（1 バイト目と合計バイト数を除く）リモート ID タイプ（値= 1）。注：デフォルトのサブオプションテンプレートを使用する場合は、このフィールドの値は 0 です。サブオプションのペイロード長

text フィールドは、フリーテキストと *$tokenname$* 形式の 1 つ以上のトークンを連結したものになります。トークンは指定した正確な形式で入力する必要があります（次の表を参照）。そうしないと、トークンとして認識されません。

text は、フリーテキストまたはトークンで開始または終了できます。トークンは連続して連結することも、フリーテキストで区切ることもできます。フリーテキストにスペース文字が含まれている場合は、*text* パラメータを引用符の間に配置する必要があります（例：*"text1 text2"*）。

リモート ID のペイロードテンプレートには、1 つのトークンまたは複数のトークンを含めることができます。まったく含めないこともできます。

コマンドの *text* フィールドの合計長は 160 バイトを超えることはできません。バイトカウントには、テキストパラメータのすべてのバイト（*text* フィールドに書き込まれたすべてのフリーテキストとトークンを含む）が含まれます。

回線 ID のペイロードリモート ID ペイロードの合計長は 247 バイトを超えることはできません。ペイロードバイトカウントは、フリーテキスト文字数（各 1 バイト）と各トークン用に予約された定義済みの長さを考慮します（次の表を参照）。

次の表に、サポートされているトークン、それらが表すデバイスパラメータ、および各トークンの予約済みバイト数と実際のバイト数の詳細を示します。

トークン名	説明	予約済みの長さ	実際の長さ
$int-ifindex$	送信元インターフェイスの ifIndex 値	4 バイト	16 進形式：2 バイト ASCII 形式：4 バイト
$int-portid$	特定のモジュール（スタック内）の送信元インターフェイスの連続番号。LAG 送信元インターフェイスの場合：LAG ID	2 バイト	16 進形式：1 バイト ASCII 形式：2 バイト
$int-name$	CLI コマンドで使用される送信元インターフェイスの完全な名前。	32 バイト	インターフェイスの完全な名前の ASCII 表現に必要な実際のバイト数。
$int-abrvname$	CLI コマンドで使用する送信元インターフェイスの省略名。	8 バイト	インターフェイスの完全な名前の ASCII 表現に必要な実際のバイト数。
$int-desc-16$	送信元インターフェイスでユーザが設定した説明。説明が 16 バイトを超える場合：最初の 16 バイトのみが使用されます。 説明を設定しない場合は、省略されたインターフェイス名が使用されます。	16 バイト	インターフェイスの説明の ASCII 表現に必要な実際のバイト数（最大 16 バイト）。

トークン名	説明	予約済みの長さ	実際の長さ
$int-desc-32$	送信元インターフェイスでユーザが設定した説明。説明が32バイトを超える場合：最初の32バイトのみが使用されます。 説明を設定しない場合は、省略されたインターフェイス名が使用されます。	32 バイト	インターフェイスの説明の ASCII 表現に必要な実際のバイト数（最大 32 バイト）。
$int-desc-64$	送信元インターフェイスでユーザが設定した説明。 説明を設定しない場合は、省略されたインターフェイス名が使用されます。	64 バイト	インターフェイスの説明の ASCII 表現に必要な実際のバイト数。
$int-mac$	送信元インターフェイスの MAC アドレス（デリミタなしの16進数値）	6 バイト	6 バイト
$switch-mac$	DHCP パケットをリレー/転送するスイッチの MAC アドレス（デリミタなしの 16 進数値）	6 バイト	6 バイト
$switch-hostname-16$	DHCP パケットをリレー/転送するスイッチのホスト名。 ホスト名が16バイトを超える場合：最初の16バイトのみが使用されます。	16 バイト	ホスト名の ASCII 表現に必要な実際のバイト数（最大16バイト）。

トークン名	説明	予約済みの長さ	実際の長さ
$switch-hostname-32$	DHCP パケットをリレー/転送するスイッチのホスト名。 ホスト名が32バイトを超える場合：最初の32バイトのみが使用されます。	32 バイト	ホスト名の ASCII 表現に必要な実際のバイト数（最大32バイト）。
$switch-hostname-58$	DHCP パケットをリレー/転送するスイッチのホスト名。	58 バイト	ホスト名の ASCII 表現に必要な実際のバイト数。
$switch-moduleid$	DHCP クライアント要求を受信した送信元インターフェイスのユニット ID。	2 バイト	16 進形式：1 バイト ASCII 形式：2 バイト
$vlan-id$	送信元 VLAN ID（1 ー 4094）	4 バイト	16 進形式：2 バイト ASCII 形式：4 バイト
$vlan-name-16$	ユーザが VLAN に割り当てた VLAN 名。名前が16バイトを超える場合：最初の16バイトのみが使用されます。 VLAN に名前を設定しない場合は、関連する VLAN ifDescr MIB フィールドから値が取得されます。	16 バイト	VLAN 名の ASCII 表現に必要な実際のバイト数（最大 16）。
$vlan-name-32$	ユーザが VLAN に割り当てた VLAN 名。 VLAN に名前を設定しない場合は、関連する VLAN ifDescr MIB フィールドから値が取得されます。	32 バイト	VLAN 名の ASCII 表現に必要な実際のバイト数（最大 32）。

注：

- 送信元インターフェイスまたは VLAN int テーブルは、（オプション 82 が追加された）DHCP クライアントパケットを受信したインターフェイスまたは VLAN を参照します。

- 予約済みの（バイト）長さ：トークンがパケットで「消費」する最大長。この値は、247 バイト制限の計算に使用されます（すべてのサブオプションペイロードを組み合わせた場合）。数値トークンを 16 進数値または ASCII 値として入力した場合、予約済みの長さは変更されません。
- 実際の（バイト）長さ：トークンがパケット自体で「消費」する実際のバイト数。実際のバイト長は、トークンが 16 進値または ASCII 値として入力されている場合、（関連するトークンの場合）変更される可能性があります。

例

次に、フリーテキストまたは完全なデバイスホスト名の連結であるリモート ID を使用するようにデバイスを設定する例を示します。

```
switchxxxxxx(config)# ip dhcp information option remote-id aaa$switch-hostname-58$bbb
```

show ip dhcp information option tokens

回線 ID サブオプションとリモート ID サブオプション（DHCP オプション 82）のペイロードを設定するときに使用できるトークンを表示するには、**show ip dhcp information option tokens** ユーザ EXEC モードコマンドを使用します。

構文

show ip dhcp information option tokens [brief]

パラメータ

- **Brief**：トークン情報なしにトークンの名前を表示します。

デフォルト設定

完全なトークン情報が表示されます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

ip dhcp information option circuit-id コマンドまたは ip dhcp information option remote-id コマンドのテキストパラメータの一部として使用できるトークンを表示するには、このコマンドを使用します。このトークンはユーザがサブオプションのペイロードのいずれかに含めることができるさまざまなシステム情報を表示します。これにより、現在のシステム情報と関連インターフェイスにも基づいて値を自動的に更新できます。

トークンには、それらが表す情報に基づいて意味があり、事前に定義された名前が付けられています。$ 記号がトークン名の前後に配置されます（$token-name$）。

トークンは、一般に3つのグループに分けることができます。インターフェイスレベルの情報を表すトークン（$int-xxx$ の形式）、スイッチレベルの情報を表すトークン（$switch-xxx$ の形式）、および VLAN 関連の情報を表すトークン（$vlan-xxx$ の形式）です。

例

次に、サポートされているすべてのトークンと、各トークンに関連するすべての情報を表示する例を示します。

```
switchxxxxxx# show ip dhcp information option tokens
Interface level Tokens - relates to the interface upon which the DHCP client packet was
 received:
Token Name: $int-ifindex$
Token value: ifIndex of the interface
Token format: Hex (default) or ASCII
Token reserved length: 4 bytes.
Token actual payload length: 2(HEX)/4(ASCII) bytes.
Token Name: $int-portid$
```

```
Token value: interface number relative to the specific unit (standalone or stacking unit)
Token format: Hex (default) or ASCII
Token reserved length: 2 bytes
Token actual payload length: 1(HEX)/2(ASCII) bytes
Token Name: $int-name$
Token value: The interface full name based as used in CLI
Token format: ASCII
Token reserved length: 32 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $int-abrvname$
Token value: The interface abbreviated name as used in CLI
Token format: ASCII
Token reserved length: 8 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $int-desc-16$
Token value: (up to) The first 16 bytes of the description user configured for the
interface
Token format: ASCII
Token reserved length: 16 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $int-desc-32$
Token value: (up to) The first 32 bytes of the description user configured for the
interface
Token format: ASCII
Token reserved length: 32 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $int-desc-64$
Token value: The full description user configured for the interface (even if more than
32 bytes)
Token format: ASCII
Token reserved length: 64 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $int-mac$
Token value: The MAC address of the physical interface
Token format: HEX
Token reserved length: 6 bytes
Token actual payload length:6 bytes
Device level Tokens - relates to switch level information:
Token Name: $switch-mac$
Token value: Device base MAC address
Token format: HEX
Token reserved length: 6 bytes
Token actual payload length:6 bytes
Token Name: $switch-hostname-16$
Token value: (Up to) The first 16 bytes of the hostname of the device
Token format: ASCII
Token reserved length: 16 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $switch-hostname-32$
Token value: (Up to) The first 32 bytes of the hostname of the device
Token format: ASCII
Token reserved length: 32 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $switch-hostname-58$
Token value: Device full hostname (even if more than 32 bytes)
Token format: ASCII
Token reserved length: 58 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $switch-moduleid$
Token value: The unit ID of the unit within the stack
Token format: Hex (default) or ASCII
Token reserved length: 2 bytes
Token actual payload length: 1(HEX)/2(ASCII) bytes
VLAN level Tokens - relates to the VLAN upon which the DHCP client packet was received:
```

```
Token Name: $vlan-id$
Token value: VLAN ID (1-4094)
Token format: Hex (default) or ASCII
Token reserved length: 4 bytes
Token actual payload length: 2(HEX)/4(ASCII) bytes
Token Name: $vlan-name-16$
Token value: (Up to) The first 16 bytes of the VLAN name
Token format: ASCII
Token reserved length: 16 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $vlan-name-32$
Token value: The full VLAN name (even if more than 16 bytes)
Token format: ASCII
Token reserved length: 32 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
```

次に、サポートされているトークンの名前のみを表示する例を示します。

```
switchxxxxxx# show ip dhcp information option tokens brief
Interface level Tokens:
$int-ifindex$
$int-portid$
$int-name$
$int-abrvname$
$int-desc-16$
$int-desc-32$
$int-desc-64$
$int-mac$
Device level Tokens:
$switch-mac$
$switch-hostname-16$
$switch-hostname-32$
$switch-hostname-58$
$switch-moduleid$
VLAN level Tokens:
$vlan-id$
$vlan-name-16$
$vlan-name-32$
```

show ip dhcp information option

show ip dhcp information option ユーザ EXEC モードコマンドは DHCP オプション 82 とサブオプションの設定を表示します。

構文

show ip dhcp information option [{interface *interface-id***} {vlan** *vlan***}]**

パラメータ

- **interface** *interface-id*：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。指定したインターフェイスと VLAN で受信した DHCP クライアントメッセージの実際のオプション 82 のペイロードを表示するには、このパラメータを **vlan** パラメータとともに使用します。
- **vlan** *vlan*：VLAN ID を指定します。指定したインターフェイスと VLAN で受信した DHCP クライアントメッセージの実際のオプション 82 のペイロードを表示するには、このパラメータを **interface** パラメータとともに使用します。

デフォルト設定

パラメータを入力しない場合、オプション 82 の一般設定が表示されます。

コマンド モード

ユーザ EXEC モード

例

次に、ユーザがオプション 82 のサブオプションの設定を変更しない場合に DHCP オプション 82 のグローバル情報（サブオプションを含む）を表示する例を示します。

```
switchxxxxxx# show ip dhcp information option
Relay agent Information option is Enabled
Numeric Token format: hex
Circuit-id payload template: (default)
Remote-id payload template: (default)
Total sub Options reserved payload: 14/247 bytes
```

次に、ユーザが回線 ID とリモート ID の両方のサブオプションを変更した場合に DHCP オプション 82 のグローバル情報（サブオプションを含む）を表示する例を示します。

```
switchxxxxxx# show ip dhcp information option
Relay agent Information option is Enabled
Numeric Token format: hex
Circuit-id payload template: aaa$int-name$bbb$vlan-name$ccc
Remote-id payload template: aaa$switch-hostname-58$bbb
Total sub Options reserved payload: 143/247 bytes
```

次に、ユーザが回線 ID とリモート ID の両方のサブオプションを変更した場合に DHCP オプション 82 の特定のインターフェイスと VLAN 情報を表示する例を示します。

```
switchxxxxxx# show ip dhcp information option interface te1/0/1 vlan 2
Relay agent Information option is Enabled
Numeric Token format: hex
Circuit-id payload template: aaa$int-name$bbb$vlan-name$ccc
Remote-id payload template: aaa$switch-hostname-58$bbb
Total sub Options reserved payload: 143/247 bytes
Interface te1/0/1 vlan 2:
Circuit-id header content: 0131012f
Circuit-id payload content: 61616154656e67696761626974457461865726e657431
2f302f3162626241502d564c414e636363
Circuit-id payload textual resolution: aaaTengigabitEthernet1/0/1bbbAP-VLANccc //removed
 support 31-Jul-18//
Circuit-id Total Length: 43
Remote-id header content: 0211010f
Remote-id payload content: 616161466c6f6f72345377769746368626262
Remote-id payload textual resolution: aaaFloor4Switchbbbb //removed support 31-Jul-18//
Remote-id Total Length: 22
```

次に、ユーザが回線 ID サブオプションのみを変更した場合に DHCP オプション 82 の特定のインターフェイスと VLAN 情報（サブオプションを含む）を表示する例を示します。

```
switchxxxxxx# show ip dhcp information option interface te1/0/10 vlan 13
Relay agent Information option is Enabled
Numeric Token format: hex
Circuit-id payload template: $int-portid$aaa$vlan-id$zzz
Remote-id payload template: (default)
Total sub Options reserved payload: 18/247 bytes
Interface te1/0/10 vlan 13:
Circuit-id header content: 010b012f
Circuit-id payload content: 0a616161000d7a7a7a
Circuit-id payload textual resolution: 10aaa13zzz //removed support 31-Jul-18//
Circuit-id Total Length: 13
Remote-id header content: 02080006
Remote-id payload content: 000000112233
Remote-id payload textual resolution: 000000112233 //removed support 31-Jul-18//
Remote-id Total Length: 10
```

次に、ユーザが数値トークン形式を ASCII に設定し、回線 ID サブオプションを設定した場合に DHCP オプション 82 の特定のインターフェイスと VLAN 情報を表示する例を示します。

```
switchxxxxxx# show ip dhcp information option interface te1/0/10 vlan 13
Relay agent Information option is Enabled
Numeric Token format: ascii
Circuit-id payload template: $int-portid$aaa$vlan-id$zzz
Remote-id payload template: (default)
Total sub Options reserved payload: 18/247 bytes
Interface te1/0/10 vlan 13:
Circuit-id header content: 010e012f
Circuit-id payload content: 3130616161303031337a7a7a
Circuit-id payload textual resolution: 10aaa13zzz ////removed support 31-Jul-18//
Circuit-id Total Length: 16
Remote-id header content: 0211000f
Remote-id payload content: 000000112233
Remote-id payload textual resolution: 000000112233 //removed support 31-Jul-18//
Remote-id Total Length: 10
```

次に、$vlan-name-32$ がトークンの 1 つであり、特定の VLAN がデバイスで作成されていない場合に DHCP オプション 82 の特定のインターフェイスと VLAN 情報を表示するように要求した場合の例を示します。

```
switchxxxxxx# show ip dhcp information option interface te1/0/1 vlan 2
Relay agent Information option is Enabled
Numeric Token format: hex
Circuit-id payload template: aaa$int-name$bbb$vlan-name-32$ccc
Remote-id payload template: aaa$switch-hostname-58$bbb
Total sub Options reserved payload: 137/247 bytes
Interface te1/0/1 vlan 2:
Error - Cannot calculate Circuit-ID info - sub-option contains VLAN related Token which
 does not exist on device.
```

DHCP サーバ コマンド

この章は、次の項で構成されています。

- address（DHCP ホスト） （371 ページ）
- address（DHCP ネットワーク） （373 ページ）
- auto-default-router （374 ページ）
- bootfile （375 ページ）
- clear ip dhcp binding （376 ページ）
- client-name （377 ページ）
- default-router （378 ページ）
- dns-server （379 ページ）
- domain-name （380 ページ）
- ip dhcp excluded-address （381 ページ）
- ip dhcp pool host （382 ページ）
- ip dhcp pool network （383 ページ）
- ip dhcp server （384 ページ）
- lease （385 ページ）
- netbios-name-server （386 ページ）
- netbios-node-type （387 ページ）
- next-server （388 ページ）
- next-server-name （389 ページ）
- option （390 ページ）
- show ip dhcp （392 ページ）
- show ip dhcp allocated （393 ページ）
- show ip dhcp binding （394 ページ）
- show ip dhcp declined （396 ページ）
- show ip dhcp excluded-addresses （397 ページ）
- show ip dhcp expired （398 ページ）
- show ip dhcp pool host （399 ページ）
- show ip dhcp pool network （400 ページ）
- show ip dhcp pre-allocated （401 ページ）

- show ip dhcp server statistics （402 ページ）
- time-server （403 ページ）

address（DHCP ホスト）

IP アドレスを DHCP クライアントに手動でバインドするには、DHCP プール ホスト コンフィギュレーション モードで **address** コマンドを使用します。クライアントへの IP アドレスのバインドを削除するには、このコマンドの **no** 形式を使用します。

構文

address *ip-address* {*mask* | *prefix-length*} {**client-identifier** *unique-identifier* | **hardware-address** *mac-address*}

no address

パラメータ

- ***address***：クライアント IP アドレスを指定します。
- ***mask***：クライアント ネットワーク マスクを指定します。
- ***prefix-length***：アドレス プレフィックスを構成するビット数を指定します。プレフィックスはクライアント ネットワーク マスクを指定する代替法です。プレフィックス長は、スラッシュ（/）で開始する必要があります。
- ***unique-identifier***：一意のクライアント ID をドット付き 16 進数表記で指定します。16 進数文字列の各バイトは、2 桁の 16 進数です。バイトは、ピリオドまたはコロンで区切られます。たとえば 01b7.0813.8811.66 などです。
- ***mac-address***：クライアント MAC アドレスを指定します。

デフォルト設定

アドレスはバインドされていません。

コマンド モード

DHCP プール ホスト コンフィギュレーション モード

使用上のガイドライン

DHCP クライアントを分類するために、DHCP サーバは、オプション 61 で渡されたクライアント識別子（**client-identifier** キーワードが設定されている場合）またはクライアント MAC アドレス（**hardware-address** キーワードが設定されている場合）を使用します。

例

次の例では、DHCP クライアントに IP アドレスを手動でバインドしています。

```
switchxxxxxx(config)# ip dhcp pool host aaaa
switchxxxxxx(config-dhcp)# address 10.12.1.99 255.255.255.0 client-identifier
01b7.0813.8811.66
```

```
switchxxxxxx(config-dhcp)# exit
switchxxxxxx(config)# ip dhcp pool host bbbb
switchxxxxxx(config-dhcp)# address 10.12.1.88 255.255.255.0 hardware-address
00:01:b7:08:13:88
switchxxxxxx(config-dhcp)# exit
switchxxxxxx(config)#
```

address（DHCP ネットワーク）

DHCP サーバの DHCP アドレス プールのサブネット番号とマスクを設定するには、DHCP プール ネットワーク コンフィギュレーション モードで **address** コマンドを使用します。サブネット番号とマスクを削除するには、このコマンドの **no** 形式を使用します。

構文

address {*network-number* | **low** *low-address* **high** *high-address*} {*mask* | *prefix-length*}

no address

パラメータ

- ***network-number***：DHCP アドレス プールの IP アドレスを指定します。
- ***mask***：プール ネットワーク マスクを指定します。
- ***prefix-length***：アドレス プレフィックスを構成するビット数を指定します。プレフィックスはクライアント ネットワーク マスクを指定する代替法です。プレフィックス長は、スラッシュ（/）で開始する必要があります。
- **low** *low-address*：アドレス範囲に使用する最初の IP アドレスを指定します。
- **high** *high-address*：アドレスの範囲で使用する、最後の IP アドレスを指定します。

デフォルト設定

DHCP アドレス プールは設定されていません。

low-address が指定されていない場合、デフォルトはネットワークの最初の IP アドレスです。

high-address が指定されていない場合、デフォルトはネットワークの最後の IP アドレスです。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

例

次の例では、DHCP サーバの DHCP アドレス プールのサブネット番号とマスクを設定しています。

```
switchxxxxxx(config-dhcp)# address 10.12.1.0 255.255.255.0
```

auto-default-router

自動デフォルトルータを有効にするには、DHCP プール ネットワーク コンフィギュレーション モードまたは DHCP プール ホスト コンフィギュレーション モードで **auto-default-router** コマンドを使用します。自動デフォルトルータを無効にするには、このコマンドの **no** 形式を使用します。

構文

auto-default-router

no auto-default-router

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

デフォルト設定

有効

使用上のガイドライン

この機能が有効になっており、次の場合にデフォルトルータが設定されていないと、DHCP サーバはデフォルトルータとして入力インターフェイスに定義されている IP アドレスを返します。

- デフォルト ルータが設定できない。
- DHCP クライアントが直接接続されている。
- IP ルーティングが有効になっている。
- デフォルト ルータはクライアントに必要だった。

例

次に、自動デフォルトルータの送信を無効にする例を示します。

```
switchxxxxxx(config-dhcp)# no auto-default-router
```

bootfile

DHCP クライアントにデフォルトのブート イメージ ファイル名を指定するには、DHCP プール ネットワーク コンフィギュレーション モードまたはDHCP プール ホスト コンフィギュレーション モードで**bootfile** コマンドを使用します。ブート イメージ ファイル名を削除するには、このコマンドの **no** 形式を使用します。

構文

bootfile *filename*

no bootfile

パラメータ

- ***filename***：.ブート イメージとして使用されるファイル名を指定します。（長さ：1 ～ 128 文字）。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

例

次の例では、DHCP クライアントのデフォルトのブート イメージ ファイル名として、boot_image_file を指定しています。

```
switchxxxxxx(config-dhcp)# bootfile boot_image_file
```

clear ip dhcp binding

DHCP サーバ データベースからダイナミック アドレス バインドを削除するには、特権 EXEC モードで **clear ip dhcp binding** コマンドを使用します。

構文

clear ip dhcp binding {*address* | *****}

パラメータ

- ***address***：DHCP データベースから削除するバインド アドレスを指定します。
- *****：すべてのダイナミック バインドをクリアします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

通常、指定されるアドレスはクライアント IP アドレスです。アスタリスク（*）文字がアドレス パラメータとして指定された場合、DHCP はすべてのダイナミック バインドをクリアします。

手動のバインドを削除するには、**no ip dhcp pool** グローバル コンフィギュレーション モード コマンドを使用します。

例

次の例では、DHCP サーバ データベースからアドレス バインド 10.12.1.99 を削除しています。

```
switchxxxxxx# clear ip dhcp binding 10.12.1.99
```

client-name

DHCP クライアントの名前を定義するには、DHCP プール ホスト コンフィギュレーション モードで **client-name** コマンドを使用します。クライアント名を削除するには、このコマンドの **no** 形式を使用します。

構文

client-name *name*

no client-name

パラメータ

- ***name***：標準 ASCII 文字を使用して、クライアント名を指定します。クライアント名にドメイン名を含めることはできません。たとえば、Mars という名前を、mars.yahoo.com と指定することはできません。（長さ：1 ～ 32 文字）。

コマンド モード

DHCP プール ホスト コンフィギュレーション モード

デフォルト設定

クライアント名は定義されていません。

例

次の例では、文字列 **client1** をクライアント名として定義しています。

```
switchxxxxxx(config-dhcp)# client-name client1
```

default-router

DHCP クライアントのデフォルト ルータ リストを設定するには、DHCP プール ネットワーク コンフィギュレーション モードまたは DHCP プール ホスト コンフィギュレーション モードで **default-router** コマンドを使用します。デフォルト ルータ リストを削除するには、このコマンドの **no** 形式を使用します。

構文

default-router *ip-address* [*ip-address2 ... ip-address8*]

no default-router

パラメータ

- ***ip-address*** [*ip-address2 ... ip-address8*]：デフォルトルータの IP アドレスを指定します。1 つのコマンド ラインで最大 8 つのアドレスを指定できます。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

デフォルト設定

デフォルト ルータは定義されていません。

使用上のガイドライン

ルータ IP アドレスは、クライアント サブネットと同一のサブネット上に存在する必要があります。

auto-default-router コマンドを設定した場合、DHCP サーバは次の場合にデフォルトルータが設定されていないときにデフォルトルータとして入力インターフェイス上で定義されている IP アドレスに戻ります。

- デフォルト ルータが設定できない。
- DHCP クライアントが直接接続されている。
- IP ルーティングが有効になっている。
- デフォルト ルータはクライアントに必要だった。

例

次の例では、デフォルトのルータ IP アドレスとして 10.12.1.99 を指定しています。

```
switchxxxxxx(config-dhcp)# default-router 10.12.1.99
```

dns-server

DHCP クライアントが利用可能なドメイン ネーム システム（DNS）IP サーバ リストを設定するには、DHCP プール ネットワーク コンフィギュレーション モードまたは DHCP プール ホスト コンフィギュレーション モードで **dns-server** コマンドを使用します。DNS サーバ リストを削除するには、このコマンドの **no** 形式を使用します。

構文

dns-server *ip-address* [*ip-address2 ... ip-address8*]

no dns-server

パラメータ

- ***ip-address*** [*ip-address2 ... ip-address8*]：DNS サーバの IP アドレスを指定します。1 つのコマンド ラインで最大 8 つのアドレスを指定できます。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

デフォルト設定

DNS サーバは定義されていません。

使用上のガイドライン

DHCP クライアント用に DNS IP サーバが設定されていない場合、クライアントはホスト名を IP アドレスに関連付けることができません。

例

次の例では、クライアント ドメイン ネーム サーバ IP アドレスとして 10.12.1.99 を指定しています。

```
switchxxxxxx(config-dhcp)# dns-server 10.12.1.99
```

domain-name

DHCP クライアントのドメイン名を指定するには、DHCP プール ネットワーク コンフィギュレーション モードまたはDHCP プール ホスト コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

構文

domain-name *domain*

no domain-name

パラメータ

- ***domain***：DHCP クライアントのドメイン名文字列を指定します。（長さ：1 ～ 32 文字）。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

デフォルト設定

ドメイン名は定義されていません。

例

次の例では、DHCP クライアントのドメイン名文字列として yahoo.com を指定しています。

```
switchxxxxxx(config-dhcp)# domain-name yahoo.com
```

ip dhcp excluded-address

DHCP サーバが DHCP クライアントに割り当ててはならない IP アドレスを指定するには、グローバル コンフィギュレーション モードで **ip dhcp excluded-address** コマンドを使用します。IP アドレスを除外するには、このコマンドの **no** 形式を使用します。

構文

ip dhcp excluded-address *low-address* [*high-address*]

no ip dhcp excluded-address *low-address* [*high-address*]

パラメータ

- ***low-address***：除外される IP アドレス、または除外されるアドレス範囲の最初の IP アドレスを指定します。
- ***high-address***：（オプション）除外されるアドレス範囲の最後の IP アドレスを指定します。

デフォルト設定

すべての IP プール アドレスが割り当て可能になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

DHCP サーバは、すべてのプールアドレスをクライアントに割り当てることができると想定します。単一の IP アドレスまたは IP アドレスの範囲を除外するには、このコマンドを使用します。

例

次の例では、除外される IP アドレスの範囲を 172.16.1.100 ～ 172.16.1.199 に設定しています。

```
switchxxxxxx(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.199
```

ip dhcp pool host

DHCP サーバで DHCP スタティック アドレスを設定し、DHCP プール ホスト コンフィギュレーション モードにするには、グローバル コンフィギュレーション モードで **ip dhcp pool host** コマンドを使用します。アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

構文

ip dhcp pool host *name*

no ip dhcp pool host *name*

パラメータ

- ***name***：DHCP アドレス プール名。象徴的な文字列（Engineering など）または整数（8 など）を使用できます。（長さ：1 ～ 32 文字）。

デフォルト設定

DHCP ホストは設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドの実行中に、コンフィギュレーション モードが DHCP プール コンフィギュレーション モードに変わります。このモードでは、管理者は IP サブネット番号やデフォルト ルータ リストなどのホスト パラメータを設定できます。

例

次の例では、DHCP アドレス プールとして **station** を設定しています。

```
switchxxxxxx(config)# ip dhcp pool host station
switchxxxxxx(config-dhcp)#
```

ip dhcp pool network

DHCP サーバで DHCP アドレス プールを設定し、DHCP プール ネットワーク コンフィギュレーション モードにするには、グローバル コンフィギュレーション モードで **ip dhcp pool network** コマンドを使用します。アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

構文

ip dhcp pool network *name*

no ip dhcp pool network *name*

パラメータ

- ***name***：DHCP アドレス プール名。象徴的な文字列（「engineering」など）または整数（8 など）を使用できます。（長さ：1 ～ 32 文字）。

デフォルト設定

DHCP アドレス プールは設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドの実行中に、コンフィギュレーション モードが DHCP プール ネットワーク コンフィギュレーション モードに変わります。このモードでは、管理者は IP サブネット番号やデフォルト ルータ リストなどのプール パラメータを設定できます。

例

次の例では、DHCP アドレス プールとして Pool1 を設定しています。

```
switchxxxxxx(config)# ip dhcp pool network Pool1
switchxxxxxx(config-dhcp)#
```

ip dhcp server

デバイスの DHCP サーバ機能を有効にするには、グローバル コンフィギュレーション モードで **ip dhcp server** コマンドを使用します。DHCP サーバを無効にするには、このコマンドの **no** 形式を使用します。

構文

ip dhcp server

no ip dhcp server

デフォルト設定

DHCP サーバは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、デバイス上で DHCP サーバを有効にしています。

```
switchxxxxxx(config)# ip dhcp server
```

lease

DHCP サーバから DHCP クライアントに割り当てられる IP アドレスのリース期間を設定するには、DHCP プール ネットワーク コンフィギュレーション モードで **lease** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

lease *days* [*hours* [*minutes*]] | **infinite**

no lease

パラメータ

- ***days***：リースの日数を指定します。
- ***hours***：（オプション）リースの時間数を指定します。*hours* 値を設定する前に *days* 値を指定する必要があります。
- ***minutes***：（オプション）リースの分数を指定します。*minutes* 値を設定する前に *days* 値および *hours* 値を指定する必要があります。
- **infinite**：リース期間が無期限であることを指定します。

デフォルト設定

デフォルトのリース期間は 1 日です。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

例

次の例は、1 日のリースを示しています。

```
switchxxxxxx(config-dhcp)# lease 1
```

次の例は、1 時間のリースを示しています。

```
switchxxxxxx(config-dhcp)# lease 0 1
```

次の例は、1 分のリースを示しています。

```
switchxxxxxx(config-dhcp)# lease 0 0 1
```

次の例は、無期限（無制限）のリースを示しています。

```
switchxxxxxx(config-dhcp)# lease infinite
```

netbios-name-server

Microsoft DHCP クライアントが利用可能な NetBIOS Windows Internet Naming Service（WINS）サーバ リストを設定するには、DHCP プール ネットワーク コンフィギュレーション モードまたは DHCP プール ホスト コンフィギュレーション モードで **netbios-name-server** を使用します。NetBIOS ネーム サーバ リストを削除するには、このコマンドの **no** 形式を使用します。

構文

netbios-name-server *ip-address* [*ip-address2 ... ip-address8*]

no netbios-name-server

パラメータ

- ***ip-address*** [***ip-address2*** *...* ***ip-address8***]：NetBIOS WINS ネームサーバの IP アドレスを指定します。1 つのコマンド ラインで最大 8 つのアドレスを指定できます。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

デフォルト設定

BIOS サーバは定義されていません。

例

次の例では、DHCP クライアントが利用可能な NetBIOS ネーム サーバの IP アドレスを指定しています。

```
switchxxxxxx(config-dhcp)# netbios-name-server 10.12.1.90
```

netbios-node-type

Microsoft DHCP クライアントの NetBIOS ノード タイプを設定するには、DHCP プール ネットワーク コンフィギュレーション モードまたは DHCP プール ホスト コンフィギュレーション モードで **netbios-node-type** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

netbios-node-type {**b-node** | **p-node** | **m-node** | **h-node**}

no netbios-node-type

パラメータ

- **b-node**：ブロードキャスト NetBIOS ノード タイプを指定します。
- **p-node**：ピアツーピア NetBIOS ノード タイプを指定します。
- **m-node**：混合 NetBIOS ノード タイプを指定します。
- **h-node**：ハイブリッド NetBIOS ノード タイプを指定します。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

デフォルト設定

h-node（ハイブリッド NetBIOS ノード タイプ）

例

次の例では、クライアントの NetBIOS タイプを混合に指定しています。

```
switchxxxxxx(config-dhcp)# netbios node-type m-node
```

next-server

DHCP クライアントの起動プロセスで次のサーバ（siaddr）を設定するには、DHCP プール ネットワーク コンフィギュレーション モードまたは DHCP プール ホスト コンフィギュレーション モードで **next-server** コマンドを使用します。次の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。

構文

next-server *ip-address*

no next-server

パラメータ

- ***ip-address***：起動プロセスでの次のサーバの IP アドレスを指定します。

デフォルト設定

next-server コマンドを使用してブート サーバ リストを設定していない場合、DHCP サーバはインバウンド インターフェイス ヘルパー アドレスをブート サーバとして使用します。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

使用上のガイドライン

クライアントは、コンフィギュレーション ファイルをダウンロードするために、SCP/TFTP プロトコルを使用してこのサーバに接続します。

例

次の例では、次のサーバの IP アドレスとして 10.12.1.99 を指定しています。

```
switchxxxxxx(config-dhcp)# next-server 10.12.1.99
```

next-server-name

DHCP クライアントの起動プロセスで次のサーバ名（sname）を設定するには、DHCP プール ネットワーク コンフィギュレーション モードまたは DHCP プール ホスト コンフィギュレーション モードで **next-server-name** コマンドを使用します。ブート サーバ名を削除するには、このコマンドの **no** 形式を使用します。

構文

next-server-name *name*

no next-server-name

パラメータ

- ***name***：起動プロセスでの次のサーバの名前を指定します。（長さ：1 ～ 64 文字）。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

デフォルト設定

次のサーバ名は定義されていません。

使用上のガイドライン

クライアントは、コンフィギュレーション ファイルをダウンロードするために、SCP/TFTP プロトコルを使用してこのサーバに接続します。

例

次の例では、DHCP クライアントの起動プロセスにおける次のサーバの名前として、www.bootserver.com を指定しています。

```
switchxxxxxx(config-dhcp)# next-server www.bootserver.com
```

option

DHCP サーバ オプションを設定するには、DHCP プール ネットワーク コンフィギュレーション モードまたは DHCP プール ホスト コンフィギュレーション モードで **option** コマンドを使用します。オプションを削除するには、このコマンドの **no** 形式を使用します。

構文

option *code* {**boolean** {**false** | **true**} | **integer** *value* | **ascii** *string* | **hex** {*string* | **none**} | **ip** {*address*} | **ip-list** {*ip-address1* [*ip-address2* …]}} [**description** *text*]

no option *code*

パラメータ

- ***code***：DHCP オプション コードを指定します。サポートされている値は、ユーザ ガイドラインで定義されています。
- **boolean** {**false** | **true**}：ブール値を指定します。この値は、1 オクテットの整数値で符号化されます。0 が false、1 が true です。
- **integer** *value*：整数値を指定します。オプションのサイズはオプション コードに依存しています。
- **ascii** *string*：Network Virtual Terminal（NVT）の ASCII 文字列を指定します。空白を含む ASCII 文字列は、引用符で囲む必要があります。この ASCII 値は、入力された最初の 160 文字から後は切り捨てられます。
- **ip** *address*：IP アドレスを指定します。
- **ip-list** {*ip-address1* [*ip-address2* ...]}：最大で 8 つの IP アドレスを指定します。
- **hex** *string*：ドット付き 16 進データを指定します。この 16 進値は、入力された最初の 320 文字から後は切り捨てられます。16 進数文字列の各バイトは、2 桁の 16 進数です。各バイトは、ピリオド、コロン、または空白で区切ることができます。
- **hex none**：ゼロの長さの 16 進文字列を指定します。
- **description** *text*：ユーザ説明。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

使用上のガイドライン

option コマンドを使用すると、他の独自の CLI コマンドでは定義できないオプションを定義できます。オプションの新しい定義は、そのオプションの前の定義を上書きします。

boolean キーワードは、19、20、27、29 ～ 31、34、36、および 39 のオプションで設定できます。

integer キーワードは、2、13、22 ～ 26、35、37 ～ 38、132 ～ 134、および 211 のオプションで設定できます。スイッチは値の範囲をチェックし、**option** の定義に従ってサイズの値フィールドを構築します。

ascii キーワードは、14、17 ～ 18、40、64、130、209、および 210 のオプションで設定できます。

ip キーワードは、16、28、32、128 ～ 129、131、135、および 136 のオプションで設定できます。

ip-list キーワードは、5、7 ～ 11、33、41、42、45、48、49、65、68 ～ 76 および 150 のオプションで設定できます。

hex キーワードは、1、3 ～ 4、6、12、15、44、46、50 ～ 51、53 ～ 54、56、66 ～ 67、82、および 255 を除く、1 ～ 254 の範囲のオプションに設定できます。スイッチは、この形式で定義されたオプションの構文を検証しません。

例 1。次の例では、クライアントがパケット転送用に IP レイヤを設定する必要があるかどうかを指定する、DHCP オプション 19 を設定しています。

```
switchxxxxxx(config-dhcp)# option 19 boolean true description "IP Forwarding Enable/Disable
 Option"
```

例 2。次の例では、協定世界時（UTC）からのクライアントのオフセットを秒単位で指定する、DHCP オプション 2 を設定しています。

```
switchxxxxxx(config-dhcp)# option 2 integer 3600
```

例 3。次の例では、DHCP クライアント用の WWW サーバを指定する、DHCP オプション 72 を設定しています。WWW サーバ 172.16.3.252 および 172.16.3.253 が次の例では設定されています。

```
switchxxxxxx(config-dhcp)# option 72 ip-list 172.16.3.252 172.16.3.253
```

show ip dhcp

DHCP 設定を表示するには、ユーザ EXEC モードで **show ip dhcp** コマンドを使用します。

構文

show ip dhcp

コマンド モード

ユーザ EXEC モード

例

次の例では、DHCP 設定を表示しています。

```
switchxxxxxx# show ip dhcp
DHCP server is enabled.
```

show ip dhcp allocated

DHCPサーバの特定の割り当て済みアドレスまたはすべての割り当て済みアドレスを表示するには、ユーザ EXEC モードで **show ip dhcp allocated** コマンドを使用します。

構文

show ip dhcp allocated [*ip-address*]

パラメータ

- ***ip-address***：（オプション）IP アドレスを指定します。

コマンド モード

ユーザ EXEC モード

例

次の例では、このコマンドの各種形式の出力を表示します。

```
switchxxxxxx# show ip dhcp allocated
DHCP server enabled
The number of allocated entries is 3
IP address   Hardware address Lease expiration      Type
----------   ---------------- --------------------  ---------
172.16.1.11  00a0.9802.32de   Feb 01 1998 12:00 AM  Dynamic
172.16.3.253 02c7.f800.0422   Infinite              Automatic
172.16.3.254 02c7.f800.0422   Infinite              Static
switchxxxxxx# show ip dhcp allocated 172.16.1.11
DHCP server enabled
The number of allocated entries is 2
IP address   Hardware address Lease expiration      Type
----------   ---------------- --------------------  --------
172.16.1.11  00a0.9802.32de   Feb 01 1998 12:00 AM  Dynamic
switchxxxxxx# show ip dhcp allocated 172.16.3.254
DHCP server enabled
The number of allocated entries is 2
IP address   Hardware address Lease expiration      Type
----------   ---------------- --------------------  -------
172.16.3.254 02c7.f800.0422   Infinite              Static
The following table describes the significant fields shown in the display.
```

フィールド	説明
IP address	DHCP サーバに記録されたホスト IP アドレス。
Hardware address	DHCP サーバに記録されたホストの MAC アドレスまたはクライアント識別子。
Lease expiration	ホスト IP アドレスのリース有効期限。
Type	IP アドレスがホストに割り当てられた方法。

show ip dhcp binding

DHCP サーバの特定のアドレス バインドまたはすべてのアドレス バインドを表示するには、ユーザ EXEC モードで **show ip dhcp binding** コマンドを使用します。

構文

show ip dhcp binding [***ip-address***]

パラメータ

- ***ip-address***：（オプション）IP アドレスを指定します。

コマンド モード

ユーザ EXEC モード

例

次の例では、DHCP サーバのバインド アドレス パラメータを表示しています。

```
switchxxxxxx# show ip dhcp binding
DHCP server enabled
The number of used (all types) entries is 6
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1
IP address Client Identifier  Lease Expiration Type    State
---------- -----------------  -------------    ------- ---------
1.16.1.11  00a0.9802.32de     Feb 01 1998     dynamic allocated
1.16.3.23  02c7.f801.0422     12:00AM         dynamic expired
1.16.3.24  02c7.f802.0422                     dynamic declined
1.16.3.25  02c7.f803.0422                     dynamic pre-allocated
1.16.3.26  02c7.f804.0422                     dynamic declined
switchxxxxxx# show ip dhcp binding 1.16.1.11
DHCP server enabled
IP address Client Identifier  Lease Expiration  Type    State
---------- -----------------  ----------------- ------- ---------
1.16.1.11  00a0.9802.32de     Feb 01 1998      dynamic allocated
                              12:00 AM
switchxxxxxx# show ip dhcp binding 1.16.3.24
IP address Client Identifier   Lease Expiration  Type    State
---------- -----------------   ---------------  ------- ---------
1.16.3.24  02c7.f802.0422                       dynamic declined
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

フィールド	説明
IP address	DHCP サーバに記録されたホスト IP アドレス。

フィールド	説明
Client Identifier	DHCP サーバに記録されたホストの MAC アドレスまたはクライアント識別子。
Lease expiration	ホスト IP アドレスのリース有効期限。
Type	IP アドレスがホストに割り当てられた方法。
State	IP アドレスの状態。

show ip dhcp declined

DHCP サーバの特定の拒否されたアドレスまたはすべての拒否されたアドレスを表示するには、ユーザ EXEC モードで **show ip dhcp declined** コマンドを使用します。

構文

show ip dhcp declined [*ip-address*]

パラメータ

- ***ip-address***：（オプション）IP アドレスを指定します。

コマンド モード

ユーザ EXEC モード

例

次の例では、このコマンドの各種形式の出力を表示します。

```
switchxxxxxx# show ip dhcp declined
DHCP server enabled
The number of declined entries is 2
IP address   Hardware address
172.16.1.11  00a0.9802.32de
172.16.3.254 02c7.f800.0422
switchxxxxxx# show ip dhcp declined 172.16.1.11
DHCP server enabled
The number of declined entries is 2
IP address    Hardware address
172.16.1.11   00a0.9802.32de
```

show ip dhcp excluded-addresses

除外されたアドレスを表示するには、ユーザ EXEC モードで **show ip dhcp excluded-addresses** コマンドを使用します。

構文

show ip dhcp excluded-addresses

コマンド モード

ユーザ EXEC モード

例

次の例では、除外されたアドレスを表示しています。

```
switchxxxxxx# show ip dhcp excluded-addresses
The number of excluded addresses ranges is 2
Excluded addresses:
10.1.1.212- 10.1.1.219, 10.1.2.212- 10.1.2.219
```

show ip dhcp expired

DHCP サーバの特定の期限切れのアドレスまたはすべての期限切れのアドレスを表示するには、ユーザ EXEC モードで **show ip dhcp expired** コマンドを使用します。

構文

show ip dhcp expired [*ip-address*]

パラメータ

- ***ip-address***：（オプション）IP を指定します。

コマンド モード

ユーザ EXEC モード

例

```
switchxxxxxx# show ip dhcp expired
DHCP server enabled
The number of expired entries is 1
IP address   Hardware address
172.16.1.11  00a0.9802.32de
172.16.3.254 02c7.f800.0422
switchxxxxxx# show ip dhcp expired 172.16.1.11
DHCP server enabled
The number of expired entries is 1
IP address  Hardware address
172.16.1.13 00a0.9802.32de
```

show ip dhcp pool host

DHCP プール ホスト設定を表示するには、ユーザ EXEC モードで **show ip dhcp pool host** コマンドを使用します。

構文

show ip dhcp pool host [*address* | *name*]

パラメータ

- ***address***：（オプション）クライアント IP アドレスを指定します。
- ***name***：（オプション）DHCP プール名を指定します。（長さ：1 ～ 32 文字）

コマンド モード

ユーザ EXEC モード

例 1。次の例では、すべての DHCP ホスト プールの設定を表示しています。

```
switchxxxxxx# show ip dhcp pool host
The number of host pools is 1
Name        IP Address  Hardware Address   Client Identifier
----------  ----------  ----------------   -----------------
station 172.16.1.11 01b7.0813.8811.66
```

例 2。次の例では、**station** という名前のプールの DHCP プール ホスト設定を表示しています。

```
switchxxxxxx# show ip dhcp pool host station
Name        IP Address  Hardware Address   Client Identifier
----------  ----------  ----------------   -----------------
station 172.16.1.11 01b7.0813.8811.66

Mask: 255.255.0.0
Auto Default router: enabled
Default router: 172.16.1.1
Client name: client1
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile
Time server 10.12.1.99
Options:
Code Type     Len Value             Description
---  -------  --- ----------------  --------------------------------
2    integer    4 3600
14   ascii     16 qq/aaaa/bbb.txt
19   boolean    1 false                 "IP Forwarding Enable/Disable
                                          Option"
21   ip         4 134.14.14.1
31   ip-list    8 1.1.1.1, 12.23.45.2
47   hex        5 02af00aa00
```

show ip dhcp pool network

DHCP ネットワーク設定を表示するには、ユーザ EXEC モードで **show ip dhcp pool network** コマンドを使用します。

構文

show ip dhcp pool network [*name*]

パラメータ

- ***name***：（オプション）DHCP プール名を指定します。（長さ：1 ～ 32 文字）。

コマンド モード

ユーザ EXEC モード

例 1：次の例では、すべての DHCP ネットワーク プールの設定を表示しています。

```
switchxxxxxx# show ip dhcp pool network
The number of network pools is 2
Name Address range mask Lease
-----------------------------------------------------
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
finance 10.1.2.8-10.1.2.178 255.255.255.0 0d:12h:0m
```

例 2：次の例では、DHCP ネットワーク プール **marketing** の設定を表示しています。

```
switchxxxxxx# show ip dhcp pool network marketing
Name Address range mask Lease
-------------------------------- ------------------------
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
Statistics:
All-range Available Free Pre-allocated Allocated Expired   Declined
---------- ---------   ----- -------------   --------- --------- --------
162 150 68 50 20        3         9
Auto Default router: enabled
Default router: 10.1.1.1
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile
Time server 10.12.1.99
Options:
Code Type     Len Value                Description
---  -------  --- -------------------  --------------------------------
2    integer    4 3600
14   ascii     16 qq/aaaa/bbb.txt
19   boolean    1 false                "IP Forwarding Enable/Disable
                                         Option"
21   ip         4 134.14.14.1
31   ip-list    8 1.1.1.1, 12.23.45.2
47   hex        5 02af00aa00
```

show ip dhcp pre-allocated

DHCPサーバの特定の事前割り当てアドレスまたはすべての事前割り当てアドレスを表示するには、ユーザ EXEC モードで **show ip dhcp pre-allocated** コマンドを使用します。

構文

show ip dhcp pre-allocated [*ip-address*]

パラメータ

- ***ip-address***：（オプション）IP を指定します。

コマンド モード

ユーザ EXEC モード

例

```
switchxxxxxx# show ip dhcp pre-allocated
DHCP server enabled
The number of pre-allocated entries is 1
IP address   Hardware address
172.16.1.11  00a0.9802.32de
172.16.3.254 02c7.f800.0422
switchxxxxxx# show ip dhcp pre-allocated 172.16.1.11
DHCP server enabled
The number of pre-allocated entries is 1
IP address   Hardware address
172.16.1.15  00a0.9802.32de
```

show ip dhcp server statistics

DHCP サーバの統計を表示するには、ユーザ EXEC モードで **show ip dhcp server statistics** コマンドを使用します。

構文

show ip dhcp server statistics

コマンド モード

ユーザ EXEC モード

例

次の例では、DHCP サーバの統計が表示されています。

```
switchxxxxxx# show ip dhcp server statistics
DHCP server enabled
The number of network pools is 7
The number of excluded pools is 2
The number of used (all types) entries is 7
The number of pre-allocated entries is 1
The number of allocated entries is 3
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1
```

time-server

DHCP クライアントのタイム サーバ リストを指定するには、DHCP プール ネットワーク コンフィギュレーション モードまたは DHCP プール ホスト コンフィギュレーション モードで **time-server** コマンドを使用します。タイム サーバ リストを削除するには、このコマンドの **no** 形式を使用します。

構文

time-server *ip-address* [*ip-address2 ... ip-address8*]

no time-server

パラメータ

- ***ip-address*** [*ip-address2 ... ip-address8*]：タイムサーバの IP アドレスを指定します。1 つのコマンド ラインで最大 8 つのアドレスを指定できます。

コマンド モード

DHCP プール ネットワーク コンフィギュレーション モード

DHCP プール ホスト コンフィギュレーション モード

デフォルト設定

タイム サーバは定義されていません。

使用上のガイドライン

タイム サーバの IP アドレスは、クライアント サブネットと同一のサブネット上に存在する必要があります。

例

次の例では、タイム サーバ IP アドレスとして 10.12.1.99 を指定しています。

```
switchxxxxxx(config-dhcp)# time-server 10.12.1.99
```

DHCP スヌーピング コマンド

この章は、次の項で構成されています。

- ip dhcp snooping （406 ページ）
- ip dhcp snooping vlan （407 ページ）
- ip dhcp snooping trust （408 ページ）
- ip dhcp snooping information option allowed-untrusted （409 ページ）
- ip dhcp snooping verify （410 ページ）
- ip dhcp snooping database （411 ページ）
- ip dhcp snooping binding （412 ページ）
- clear ip dhcp snooping database （414 ページ）
- show ip dhcp snooping （415 ページ）
- show ip dhcp snooping binding （416 ページ）
- ip arp inspection （417 ページ）
- ip arp inspection vlan （418 ページ）
- ip arp inspection validate （419 ページ）
- ip arp inspection list create （420 ページ）
- ip mac （421 ページ）
- ip arp inspection list assign （422 ページ）
- ip arp inspection logging interval （423 ページ）
- show ip arp inspection （424 ページ）
- show ip arp inspection list （425 ページ）
- show ip arp inspection statistics （426 ページ）
- clear ip arp inspection statistics （427 ページ）

ip dhcp snooping

Dynamic Host Configuration Protocol（DHCP）スヌーピングをグローバルに有効にするには、**ip dhcp snooping** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ip dhcp snooping

no ip dhcp snooping

デフォルト設定

DHCP スヌーピングは、無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

任意の DHCP スヌーピング設定を有効にするには、DHCP スヌーピングをグローバルに有効にする必要があります。VLAN の DHCP スヌーピングは、VLAN の DHCP スヌーピングが有効になるまでアクティブになりません。

例

次の例では、デバイス上で DHCP スヌーピングを有効にしています。

```
switchxxxxxx(config)# ip dhcp snooping
```

ip dhcp snooping vlan

VLAN で DHCP スヌーピングを有効にするには、**ip dhcp snooping vlan** グローバル コンフィギュレーション モード コマンドを使用します。VLAN で DHCP スヌーピングを無効にするには、このコマンドの **no** 形式を使用します。

構文

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping vlan *vlan-id*

パラメータ

- ***vlan-id***：VLAN ID を指定します。

デフォルト設定

VLAN 上の DHCP スヌーピングは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

VLAN で DHCP スヌーピングを有効にする前に、DHCP スヌーピングをグローバルに有効にする必要があります。

例

次の例では、VLAN 21 で DHCP スヌーピングを有効にしています。

```
switchxxxxxx(config)# ip dhcp snooping vlan 21
```

ip dhcp snooping trust

DHCP スヌーピングを実行するためにポートを信頼できるポートとして設定するには、**ip dhcp snooping trust** インターフェイス コンフィギュレーション（イーサネット、ポート チャネル）モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ip dhcp snooping trust

no ip dhcp snooping trust

デフォルト設定

インターフェイスは、信頼できない状態です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

DHCPサーバ、その他のスイッチ、またはルータに接続されたポートを信頼できるポートとして設定します。DHCPクライアントに接続したポートは、信頼できないポートとして設定します。

例

次に、DHCP スヌーピング用に gi1/0/4 を信頼できるポートとして設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# ip dhcp snooping trust
```

ip dhcp snooping information option allowed-untrusted

信頼できないポートからのオプション 82 情報を持つ DHCP パケットをデバイスが受け入れるようにするには、**ip dhcp snooping information option allowed-untrusted** グローバル コンフィギュレーション モード コマンドを使用します。信頼できないポートからのこのようなパケットをドロップするには、このコマンドの **no** 形式を使用します。

構文

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

デフォルト設定

信頼できないポートからのオプション 82 情報を持つ DHCP パケットは破棄されます。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、信頼できないポートからのオプション 82 情報を持つ DHCP パケットをデバイスが受け入れられるようにしています。

```
switchxxxxxx(config)# ip dhcp snooping information option allowed-untrusted
```

ip dhcp snooping verify

信頼できないポートで受信した DHCP パケットの送信元 MAC アドレスがクライアント ハードウェア アドレスと一致することを確認するようにデバイスを設定するには、**ip dhcp snooping verify** グローバル コンフィギュレーション モード コマンドを使用します。信頼できないポートで受信した DHCP パケットの MAC アドレス検証を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip dhcp snooping verify

no ip dhcp snooping verify

デフォルト設定

スイッチは、パケットのクライアント ハードウェア アドレスと一致する信頼されないポートで受信した DHCP パケットの送信元 MAC アドレスを確認します。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、信頼できないポートで受信した DHCP パケットの送信元 MAC アドレスがクライアント ハードウェア アドレスと一致することを確認するようにデバイスを設定しています。

```
switchxxxxxx(config)# ip dhcp snooping verify
```

ip dhcp snooping database

DHCP スヌーピング バインディング データベース ファイルを有効にするには、**ip dhcp snooping database** グローバル コンフィギュレーション モード コマンドを使用します。DHCP スヌーピング バインディング データベース ファイルを削除するには、このコマンドの **no** 形式を使用します。

構文

ip dhcp snooping database

no ip dhcp snooping database

デフォルト設定

DHCP スヌーピング バインディング データベース ファイルは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

DHCP スヌーピング バインディング データベース ファイルは、Flash 上にあります。データベースのリース時間を正確なものにするために、Simple Network Time Protocol（SNTP）を有効にして設定する必要があります。デバイスのシステム クロックが SNTP と同期している場合にのみ、デバイスはバインディング データベース ファイルにバインディングの変更を書き込みます。

例

次の例では、DHCP スヌーピング バインディング データベース ファイルを有効にしています。

```
switchxxxxxx(config)# ip dhcp snooping database
```

ip dhcp snooping binding

DHCP スヌーピング バインディング データベースを設定して、ダイナミック バインディング エントリをデータベースに追加するには、**ip dhcp snooping binding** 特権 EXEC モード コマンドを使用します。バインディング データベースからエントリを削除するには、このコマンドの **no** 形式を使用します。

構文

ip dhcp snooping binding *mac-address vlan-id ip-address interface-id* **expiry** {*seconds* | **infinite**}

no ip dhcp snooping binding *mac-address vlan-id*

パラメータ

- ***mac-address***：MAC アドレスを指定します。
- ***vlan-id***：VLAN 番号を指定します。
- ***ip-address***：IP アドレスを指定します。
- ***interface-id***：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。
- **expiry**
  - ***seconds***：バインディング エントリが無効になるまでの時間間隔を秒単位で指定します。（範囲：10 ～ 4294967294）。
  - **infinite**：無期限のリース時間を指定します。

デフォルト設定

スタティック バインディングはありません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

DHCP データベースにダイナミック エントリを手動で追加するには、**ip dhcp snooping binding** コマンドを使用します。

このコマンドを入力すると、DHCP スヌーピング データベースにエントリが追加されます。DHCP スヌーピング バインディング ファイルが存在する場合は、そのファイルにもエントリが追加されます。

コンフィギュレーション ファイルには、エントリは追加されません。このエントリは、show コマンドで「DHCP Snooping」エントリとして表示されます。このコマンドにより追加された

エントリは、既存のダイナミック エントリを上書きできます。このエントリは、show コマンドで DHCP Snooping エントリとして表示されます。

DHCP データベースからダイナミック エントリを手動で削除するには、**no ip dhcp snooping binding** コマンドを使用します。

IP アドレスが 0.0.0.0 の一時的なダイナミック エントリは削除できません。

例

次の例では、DHCP スヌーピング バインディング データベースにバインディング エントリを追加しています。

```
switchxxxxxx# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1 gi1/0/4 expiry 900
```

clear ip dhcp snooping database

DHCP スヌーピング バインディング データベースをクリアするには、**clear ip dhcp snooping database** 特権 EXEC モード コマンドを使用します。

構文

clear ip dhcp snooping database

コマンド モード

特権 EXEC モード

例

次の例では、DHCP スヌーピング バインディング データベースをクリアしています。

```
switchxxxxxx# clear ip dhcp snooping database
```

show ip dhcp snooping

すべてのインターフェイスまたは特定のインターフェイスのDHCPスヌーピング設定を表示するには、**show ip dhcp snooping** EXEC モード コマンドを使用します。

構文

show ip dhcp snooping *[interface-id]*

パラメータ

- ***interface-id***：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

ユーザ EXEC モード

例

次の例では、DHCP スヌーピング設定を表示しています。

```
switchxxxxxx# show ip dhcp snooping
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 21
DHCP snooping database is Enabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 6666 seconds
```

Interface	Trusted
---	---
gi1/0/1	対応
gi1/0/2	対応

show ip dhcp snooping binding

すべてのインターフェイスまたは特定のインターフェイスの DHCP スヌーピング バインディング データベースおよび設定情報を表示するには、**show ip dhcp snooping binding** ユーザ EXEC モード コマンドを使用します。

構文

show ip dhcp snooping binding [**mac-address** *mac-address*] [**ip-address** *ip-address*] [**vlan** *vlan-id*] [*interface-id*]

パラメータ

- **mac-address** *mac-address*：MAC アドレスを指定します。
- **ip-address** *ip-address*：IP アドレスを指定します。
- **vlan** *vlan-id*：VLAN ID を指定します。
- ***interface-id***：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

ユーザ EXEC モード

例

次の例では、デバイス上のすべてのインターフェイスの DHCP スヌーピング バインディング データベースと設定情報を表示しています。

```
switchxxxxxx# show ip dhcp snooping binding
Update frequency: 1200
Total number of binding: 2
```

Mac Address	IP Address	Lease (sec)	Type	VLAN	Interface
0060.704C.73FF	10.1.8.1	7983	snooping	3	gi1/0/1
0060.704C.7BC1	10.1.8.2	92332	snooping (s)	3	gi1/0/2

ip arp inspection

Address Resolution Protocol（ARP）インスペクションを有効にするには、**ip arp inspection** グローバル コンフィギュレーション モード コマンドをグローバルに使用します。ARP インスペクションを無効にするには、このコマンドの **no** 形式を使用します。

構文

ip arp inspection

no ip arp inspection

デフォルト設定

ARP インスペクションは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ポートが信頼できないポートとして設定されている場合は、DHCP スヌーピング用に信頼できないポートとしても設定するか、そのポートの IP アドレスと MAC アドレスのバインドをスタティックに設定する必要があることに注意してください。それ以外の場合、このポートに接続されたホストは ARP に応答できません。

例

次の例では、デバイス上で ARP インスペクションを有効にしています。

```
switchxxxxxx(config)# ip arp inspection
```

ip arp inspection vlan

DHCP スヌーピング データベースに基づいて、VLAN 上で ARP インスペクションを有効にするには、**ip arp inspection vlan** グローバル コンフィギュレーション モード コマンドを使用します。VLAN で ARP インスペクションを無効にするには、このコマンドの **no** 形式を使用します。

構文

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan *vlan-id*

パラメータ

- ***vlan-id***：VLAN ID を指定します。

デフォルト設定

VLAN で DHCP スヌーピングに基づく ARP インスペクションが無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、DHCP スヌーピング データベースに基づいて、VLAN 上での ARP インスペクションを有効にします。

例

次の例では、VLAN 23 で DHCP スヌーピング ベースの ARP インスペクションを有効にしています。

```
switchxxxxxx(config)# ip arp inspection vlan 23
```

ip arp inspection validate

ダイナミック Address Resolution Protocol（ARP）インスペクションの特定のチェックを実行するには、**ip arp inspection validate** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ip arp inspection validate

no ip arp inspection validate

デフォルト設定

ARP インスペクションの検証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

次のチェックが行われます。

- **Source MAC address**：イーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本文の送信元 MAC アドレスと比較します。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。
- **Destination MAC address**：イーサネット ヘッダーの宛先 MAC アドレスを、ARP 本文のターゲット MAC アドレスと比較します。この検査は、ARP 応答に対して実行されます。
- **IP addresses**：無効な IP アドレスや予期しない IP アドレスがないか、ARP 本文を比較します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。

例

次の例では、ARP インスペクションの検証を実行しています。

```
switchxxxxxx(config)# ip arp inspection validate
```

ip arp inspection list create

スタティック ARP バインディング リストを作成して、ARP リスト コンフィギュレーション モードを開始するには、**ip arp inspection list create** グローバル コンフィギュレーション モード コマンドを使用します。このリストを削除するには、このコマンドの **no** 形式を使用します。

構文

ip arp inspection list create *name*

no ip arp inspection list create *name*

パラメータ

- ***name***：スタティック ARP バインディング リスト名を指定します。（長さ：1 ～ 32 文字）。

デフォルト設定

スタティック ARP バインディング リストは存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

リストを VLAN に割り当てるには、**ip arp inspection list assign** コマンドを使用します。

例

次の例では、スタティック ARP バインディング リストの「servers」を作成し、ARP リスト コンフィギュレーション モードにしています。

```
switchxxxxxx(config)# ip arp inspection list create servers
```

ip mac

スタティック ARP バインディングを作成するには、**ip mac** ARP リスト コンフィギュレーション モード コマンドを使用します。スタティック ARP バインディングを削除するには、このコマンドの **no** 形式を使用します。

構文

ip *ip-address* **mac** *mac-address*

no ip *ip-address* **mac** *mac-address*

パラメータ

- ***ip-address***：リストに入れる IP アドレスを指定します。
- ***mac-address***：IP アドレスに関連付けられる MAC アドレスを指定します。

デフォルト設定

スタティック ARP バインディングは定義されていません。

コマンド モード

ARP リスト コンフィギュレーション モード

例

次の例では、スタティック ARP バインディングを作成しています。

```
switchxxxxxx(config)# ip arp inspection list create servers
switchxxxxxx(config-arp-list)# ip 172.16.1.1 mac 0060.704C.7321
switchxxxxxx(config-arp-list)# ip 172.16.1.2 mac 0060.704C.7322
```

ip arp inspection list assign

スタティック ARP バインディング リストを VLAN に割り当てるには、**ip arp inspection list assign** グローバル コンフィギュレーション モード コマンドを使用します。割り当てを削除する場合は、このコマンドの **no** 形式を使用します。

構文

ip arp inspection list assign *vlan-id name*

no ip arp inspection list assign *vlan-id*

パラメータ

- ***vlan-id***：VLAN ID を指定します。
- ***name***：スタティック ARP バインディング リスト名を指定します。

デフォルト設定

スタティック ARP バインディング リストは割り当てられていません。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、スタティック ARP バインディング リストの Servers を VLAN 37 に割り当てています。

```
switchxxxxxx(config)# ip arp inspection list assign 37 servers
```

ip arp inspection logging interval

連続する ARP SYSLOG メッセージ間の最小時間間隔を設定するには、**ip arp inspection logging interval** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ip arp inspection logging interval {*seconds* | **infinite**}

no ip arp inspection logging interval

パラメータ

- ***seconds***：連続する ARP SYSLOG メッセージ間の最小時間間隔を指定します。0 の値は、システム メッセージがただちに生成されることを意味します。(範囲：0 ～ 86400)
- **infinite**：SYSLOG メッセージが生成されないことを指定します。

デフォルト設定

デフォルトの ARP SYSLOG メッセージ ロギングの最小間隔は 5 秒です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、ARP SYSLOG メッセージ ロギングの最小時間間隔を 60 秒に設定しています。

```
switchxxxxxx(config)# ip arp inspection logging interval 60
```

show ip arp inspection

すべてのインターフェイスまたは特定のインターフェイスの ARP インスペクション設定を表示するには、**show ip arp inspection** EXEC モード コマンドを使用します。

構文

show ip arp inspection [*interface-id*]

パラメータ

- ***interface-id***：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

ユーザ EXEC モード

例

次の例では、ARP インスペクション設定を表示しています。

```
switchxxxxxx# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 222  seconds
 Interface    Trusted
----------- -----------
gi1/0/1          Yes
gi1/0/2          Yes
```

show ip arp inspection list

スタティック ARP バインディング リストを表示するには、**show ip arp inspection list** 特権 EXEC モード コマンドを使用します。

構文

show ip arp inspection list

コマンド モード

特権 EXEC モード

例

次の例では、スタティック ARP バインディング リストを表示しています。

```
switchxxxxxx# show ip arp inspection list
List name: servers
Assigned to VLANs: 1,2
```

IP	ARP
172.16.1.1	0060.704C.7322
172.16.1.2	0060.704C.7322

show ip arp inspection statistics

この機能により処理された、転送、ドロップ、およびIP/MAC検証エラータイプのパケットの統計を表示するには、**show ip arp inspection statistics** EXEC コマンドを使用します。

構文

show ip arp inspection statistics [*vlan vlan-id*]

パラメータ

- ***vlan-id***：VLAN ID を指定します。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

ARP インスペクション機能を無効にした場合は、カウンタの値は保持されます。

例

```
switchxxxxxx# show ip arp inspection statistics
Vlan   Forwarded Packets Dropped Packets   IP/MAC Failures
----  ----------------- ---------------  ---------------
2     1500           100                        80
```

clear ip arp inspection statistics

ARP インスペクションの統計情報をグローバルにクリアするには、**clear ip arp inspection statistics** 特権 EXEC モード コマンドを使用します。

構文

clear ip arp inspection statistics [**vlan** *vlan-id*]

パラメータ

- ***vlan-id***：VLAN ID を指定します。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# clear ip arp inspection statistics
```

DHCPv6 コマンド

この章は、次の項で構成されています。

- clear ipv6 dhcp client （430 ページ）
- ipv6 address dhcp （431 ページ）
- ipv6 dhcp client information refresh （434 ページ）
- ipv6 dhcp client information refresh minimum （435 ページ）
- ipv6 dhcp duid-en （437 ページ）
- ipv6 dhcp relay destination（グローバル） （438 ページ）
- ipv6 dhcp relay destination（インターフェイス） （440 ページ）
- show ipv6 dhcp （443 ページ）
- show ipv6 dhcp interface （444 ページ）

clear ipv6 dhcp client

インターフェイスで IPv6 クライアントの DHCP を再起動するには、特権 EXEC モードで **clear ipv6 dhcp client** コマンドを使用します。

構文

clear ipv6 dhcp client *interface-id*

パラメータ

- ***interface-id***：インターフェイス識別子。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、前に取得したプレフィックスとその他の設定オプション（たとえば、ドメイン ネーム システム（DNS）サーバ）をまず解放して設定を解除した後に、指定されたインターフェイスで IPv6 クライアントの DHCP を再起動します。

例

次の例では、VLAN 100 で IPv6 クライアントの DHCP を再起動しています。

```
switchxxxxxx# clear ipv6 dhcp client vlan 100
```

ipv6 address dhcp

IPv6 クライアントプロセスの DHCP を有効にし、インターフェイスで IPv6 アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ipv6 address dhcp** コマンドを使用します。インターフェイスから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。

構文

ipv6 address dhcp [**rapid-commit**]

no ipv6 address dhcp

パラメータ

- **rapid-commit**：アドレスの割り当てで、2 メッセージ交換方式を許可します。

デフォルト設定

DHCPv6 サーバから取得した IPv6 アドレスはありません。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

インターフェイス（イーサネット、ポートチャネル、OOB）コンフィギュレーション モード

使用上のガイドライン

このコマンドは、このプロセスがまだ実行されておらず、IPv6 インターフェイスがインターフェイスで有効になっている場合、IPv6 を有効にし（有効になっていない場合）、IPv6 クライアントプロセスの DHCP を開始します。このコマンドは、インターフェイスが DHCPv6 を使用して IPv6 アドレスを動的に学習し、DHCPv6 ステートレスサービスを有効にします。

rapid-commit キーワードは、アドレス割り当ておよびその他の設定について、2 メッセージの交換を使用できるようにします。これを有効にすると、クライアントは送信請求メッセージに rapid-commit オプションを含めます。

このコマンドは、インターフェイスで DHCPv6 を使用し、IPv6 アドレスを動的に学習できるようにします。

DHCPv6 ステートレスサービスは、次のオプションで渡される DHCP サーバからの設定を受信できるようにします。

- オプション 7：OPTION_PREFERENCE：このメッセージ内のサーバのプリファレンス値
- オプション 12：OPTION_UNICAST：ユニキャストを使用して配信されるメッセージをクライアントが送信する IP アドレス
- オプション 23：OPTION_DNS_SERVERS：DNS サーバの IPv6 アドレスのリスト

- オプション 24：OPTION_DOMAIN_LIST：ドメイン検索リスト
- オプション 31：OPTION_SNTP_SERVERS：SNTP サーバの IPv6 アドレスのリスト
- オプション 32：OPTION_INFORMATION_REFRESH_TIME：情報の更新時間オプション
- オプション 41：OPTION_NEW_POSIX_TIMEZONE：新しいタイムゾーンの Posix 文字列
- オプション 59：OPT_BOOTFILE_URL：コンフィギュレーション サーバの URL

  オプション 60：OPT_BOOTFILE_PARAM、最初のパラメータ：コンフィギュレーション ファイルのパス名

DHCPv6 クライアントは、実行中のインターフェイス ID に基づいて次の IAID 形式を使用します。

- オクテット 1、ビット 7ー 4：これらのビットは予約済みであり、0 である必要があります。
- オクテット 1、ビット 3 ー 0：これらのビットには次のインターフェイスタイプが含まれます。

  0：VLAN
  - 1：イーサネットポート
  - 2：ポートチャネル
  - 3：トンネル

- オクテット 2 ー 4：オクテットには、ネットワーク形式のインターフェイスタイプに応じた値が含まれます。
  - VLAN

オクテット 2：予約済み、0 である必要があります

オクテット 3 ー 4：VLAN ID（1 ー 4095）

- イーサネット ポート

オクテット 2、ビット 7 ー 4：スロット番号

オクテット 2、ビット 3 ー 0：ポートタイプ：

0：イーサネット

1：高速イーサネット

2：ギガイーサネット

3：2.5 ギガイーサネット

4 ～ 5 ギガイーサネット

5 ～ 10 ギガイーサネット

6 ～ 12 ギガイーサネット

7 ～ 13.6 ギガイーサネット

8 ～ 16 ギガイーサネット

9 ～ 20 ギガイーサネット

10 ～ 40 ギガイーサネット

11 ～ 100 ギガイーサネット

オクテット 3：ユニット番号

オクテット 4：ポート番号

- ポート チャネル

オクテット 2 ～ 3：予約済み、0 である必要があります。

オクテット 4：ポートチャネル番号

- Tunnel

オクテット 2 ～ 3：予約済み、0 である必要があります。

オクテット 4：トンネル番号

IPv6転送が有効になっている場合、DHCPv6サーバからのステートレス情報のみが必要です。

IPv6 転送が無効から有効に変更されると、DHCPv6 によって割り当てられた IPv6 アドレスが削除されます。

IPv6 転送が有効から無効に変更されると、DHCPv6 サーバからの IPv6 アドレスの受信が再開されます。

DHCPv6クライアント、サーバ、およびリレーの機能は、インターフェイス上で相互排他的です。

例

次に、VLAN 100 で IPv6 を有効にし、IPv6 アドレスを取得する例を示します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 address dhcp
switchxxxxxx(config-if)# exit
```

ipv6 dhcp client information refresh

DHCPv6 サーバの応答に情報の更新時間が含まれていない場合に、指定されたインターフェイスで IPv6 クライアント情報の更新時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp client information refresh** コマンドを使用します。デフォルト値の更新時間に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 dhcp client information refresh *seconds* | **infinite**

no ipv6 dhcp client information refresh

パラメータ

- ***seconds***：更新時間（秒単位）。この値は、**ipv6 dhcp client information refresh** コマンドにより設定された最小許容更新時間よりも短くすることはできません。使用可能な最大値は 4,294967,294 秒（0xFFFFFFFE）です。
- **infinite**：無限の更新時間。

デフォルト設定

デフォルトは 86,400 秒（24 時間）です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ipv6 dhcp client information refresh コマンドは、情報の更新時間を指定します。サーバが情報の更新時間オプションを送信しない場合は、このコマンドによって設定された値が使用されます。

サーバが情報の更新時間オプションを送信しない場合に更新を防止するには、**infinite** キーワードを使用します。

例

次の例では、上限を 2 日に設定します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp client information refresh 172800
switchxxxxxx(config-if)# exit
```

ipv6 dhcp client information refresh minimum

指定したインターフェイスでの最小許容更新時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp client information refresh minimum** コマンドを使用します。設定した更新時間を削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 dhcp client information refresh minimum *seconds* | **infinite**

no ipv6 dhcp client information refresh minimum

パラメータ

- ***seconds***：更新時間（秒単位）。使用可能な最小値は 600 秒です。使用可能な最大値は 4,294,967,294 秒（0xFFFFFFFE）です。
- **infinite**：無限の更新時間。

デフォルト設定

デフォルトは 86,400 秒（24 時間）です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ipv6 dhcp client information refresh minimum コマンドは、情報の最小許容更新時間を指定します。設定された最小更新時間よりも短い情報の更新時間オプションをサーバが送信した場合は、設定された最小更新時間が代わりに使用されます。

このコマンドは、次のような場合に設定できます。

- 予期しない変更が発生する可能性のある、不安定な環境の場合。
- 番号の変更を含む、計画された変更がある場合。管理者は、計画されたイベントが近づくにつれて、徐々に時間を短くすることができます。
- 新しい Simple Network Time Protocol（SNTP）サーバの追加や、ドメインネームシステム（DNS）サーバのアドレス変更などで、新しいサービスまたはサーバがクライアントで利用可能になるまでの時間を制限する場合。

infinite キーワードを設定した場合、クライアントは情報を更新しません。

例

次の例では、上限を 2 日に設定します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp client information refresh 172800
switchxxxxxx(config-if)# exit
```

ipv6 dhcp duid-en

エンタープライズ番号に基づくベンダー DHCPv6 固有 ID（DUID-EN）形式を設定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp duid-en** コマンドを使用します。

デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 dhcp duid-en *enterprise-number identifier*

no ipv6 dhcp duid-en

パラメータ

- ***enterprise-number***：IANA により管理されている、ベンダーの登録済みプライベート エンタープライズ番号。
- ***identifier***：ベンダー定義の空でない 16 進文字列（最大 64 文字の 16 進数文字）。文字数が偶数でない場合は、右側に「0」が追加されます。2 つの 16 進数文字は、それぞれピリオドまたはコロンで区切ることができます。

デフォルト設定

リンク層アドレスに基づく DUID（DUID LL）が使用されます。基本 MAC アドレスがリンク層アドレスとして使用されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

デフォルトでは、DHCPv6 は基本 MAC アドレスを使用したリンク層アドレスに基づく DUID（RFC3315 を参照）を、リンク層アドレスとして使用します。

DUID 形式をエンタープライズ番号に基づくベンダーに変更するには、このコマンドを使用します。

例 1。次の例では、DIID-EN 形式を設定しています。

```
ipv6 dhcp duid-en 9 0CC084D303000912
```

例 2。次の例では、デリミタとしてコロンを使用して DIID-EN 形式を設定しています。

```
switchxxxxxx(config)# ipv6 dhcp duid-en 9 0C:C0:84:D3:03:00:09:12
```

ipv6 dhcp relay destination（グローバル）

クライアント メッセージの転送先のグローバル定義されたリレー宛先アドレスを指定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp relay destination** コマンドを使用します。リレー宛先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。

構文

ipv6 dhcp relay destination {*ipv6-address* [*interface-id*]} | *interface-id*

no ipv6 dhcp relay destination [{*ipv6-address* [*interface-id*]} | *interface-id*]

パラメータ

- ***ipv6-address*** [*interface-id*]：RFC 4291 に記述されている形式のリレー宛先 IPv6 アドレス。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。次のタイプのリレー宛先アドレスがあります。
  - リンクローカル ユニキャスト アドレス。このタイプのアドレスには、*interface-id* 引数を指定する必要があります。
  - グローバルユニキャストIPv6アドレス。*interface-id*引数を省略した場合は、ルーティング テーブルが使用されます。
- ***interface-id***：宛先の出力インターフェイスを指定するインターフェイス識別子。この引数が設定されている場合、クライアントメッセージは、出力インターフェイスが接続されているリンクを介して、既知のリンクローカル マルチキャスト アドレス **All_DHCP_Relay_Agents_and_Servers**（FF02::1:2）に転送されます。

デフォルト設定

グローバルに定義されているリレー宛先はありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ipv6 dhcp relay destination コマンドは、クライアント メッセージが転送される宛先アドレスを指定します。このアドレスは、スイッチで動作しているすべてのDHCPv6リレーで使用されます。アドレスは最大で 100 個まで定義できます。

リレー サービスがインターフェイスで動作している場合、そのインターフェイスに着信するDHCP for IPv6 メッセージは、インターフェイスごとおよびグローバルに設定されたすべてのリレー宛先に転送されます。複数の宛先を1つのインターフェイスに設定でき、複数の出力インターフェイスを1つの宛先に設定することができます。リレー宛先の指定は必須です。ループバックやマルチキャスト アドレスは指定できません。

指定した出力インターフェイスについて、指定したグローバルに定義されているアドレスのみを削除するには、*ipv6-address* 引数および *interface-id* 引数を使用してこのコマンドの **no** 形式を使用します。

すべての出力インターフェイスについて、指定したグローバルに定義されているアドレスのみを削除するには、*ipv6-address* 引数を使用してこのコマンドの **no** 形式を使用します。

引数を使用せずにこのコマンドの **no** 形式を使用すると、すべてのグローバルに定義されているアドレスが削除されます。

例 1。次の例では、VLAN 200 でリレー ユニキャスト リンクローカル宛先アドレスを設定しています。

```
switchxxxxxx(config)# ipv6 dhcp relay destination FE80::1:2 vlan 200
```

例 2。次の例では、クライアント メッセージが VLAN 200 に転送されるように設定しています。

```
switchxxxxxx(config)# ipv6 dhcp relay destination vlan 200
```

例 3。次の例では、ユニキャスト グローバル リレー宛先アドレスを設定しています。

```
switchxxxxxx(config)# ipv6 dhcp relay destination 3002::1:2
```

ipv6 dhcp relay destination（インターフェイス）

クライアント メッセージが転送される宛先アドレスを指定し、そのインターフェイスでDHCP for IPv6 リレー サービスを有効にするには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp relay destination** コマンドを使用します。インターフェイスのリレー宛先を削除するか、または宛先の出力インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 dhcp relay destination [{*ipv6-address* [*interface-id*]} | *interface-id*]

no ipv6 dhcp relay destination [{*ipv6-address* [*interface-id*]} | *interface-id*]

パラメータ

- ***ipv6-address*** [*interface-id*]：RFC 4291 に記述されている形式のリレー宛先 IPv6 アドレス。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。次のタイプのリレー宛先アドレスがあります。
  - リンクローカル ユニキャスト アドレス。このタイプのアドレスには、*interface-id* 引数を指定する必要があります。
  - グローバル ユニキャスト IPv6 アドレス。*interface-id* 引数を省略した場合は、ルーティング テーブルが使用されます。

- ***interface-id***：宛先の出力インターフェイスを指定するインターフェイス識別子。この引数が設定されている場合、クライアント メッセージは、出力インターフェイスが接続されているリンクを介して、既知のリンクローカル マルチキャスト アドレス **All_DHCP_Relay_Agents_and_Servers**（FF02::1:2）に転送されます。

デフォルト設定

リレー機能は無効になっており、インターフェイス上にリレー宛先はありません。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

このコマンドは、クライアント メッセージを転送する宛先アドレスを指定し、インターフェイスで DHCP for IPv6 リレー サービスを有効にします。インターフェイスあたり最大 10 個のアドレスを定義できます。スイッチには最大 100 個のアドレスを定義できます。

IPv6 グローバル アドレスが、リレーが動作するインターフェイスに定義されていない場合、DHCPv6 リレーによって Interface-id オプションが挿入されます。オプションの Interface-id フィー

ルドは、リレーが実行されているインターフェイス名（**ifTable** の **ifName** フィールドの値）です。

リレーサービスがインターフェイス上で実行されている場合、そのインターフェイスで受信された DHCP for IPv6 メッセージは、インターフェイスごとおよびグローバルに設定されたすべてのリレー宛先に転送されます。

着信 DHCP for IPv6 メッセージが、そのインターフェイス上のクライアントから届く場合や、別のリレー エージェントによってリレーされる場合があります。

リレー宛先は、サーバまたは別のリレー エージェントのユニキャスト アドレス、またはマルチキャストアドレスにすることができます。次の2つのタイプのリレー宛先アドレスがあります。

- リンクローカルのユニキャストまたはマルチキャスト IPv6 アドレス。ユーザが出力インターフェイスを指定する必要があります。
- グローバルユニキャスト IPv6 アドレス。このタイプのアドレスには、ユーザがオプションで出力インターフェイスを指定できます。

出力インターフェイスが宛先に設定されていない場合、出力インターフェイスはルーティングテーブルによって決まります。この場合、ユニキャストまたはマルチキャスト ルーティングプロトコルがルータで実行されていることを推奨します。

複数の宛先を 1 つのインターフェイスに設定でき、複数の出力インターフェイスを 1 つの宛先に設定することができます。リレー エージェントは、マルチキャスト アドレスにメッセージをリレーする場合、IPv6 パケット ヘッダーのホップ制限フィールドを 32 に設定します。リレー宛先の指定は必須です。ループバックやノードローカル マルチキャスト アドレスは指定できません。

サーバからの着信リレー応答メッセージを受信して転送するために、インターフェイスのリレー機能を有効にする必要はないことに注意してください。デフォルトでは、リレー機能は無効になっており、インターフェイスにリレー宛先はありません。

特定のアドレスを削除するには、引数を使用してこのコマンドの **no** 形式を使用します。

すべての定義されているアドレスを削除し、インターフェイスのリレーを無効にするには、引数を使用せずにこのコマンドの **no** 形式を使用します。

例 1。次の例では、リレーのユニキャスト リンクローカル宛先アドレスを VLAN 200 で設定し、有効になっていない場合には、VLAN 100 で DHCPv6 リレーを有効にしています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination FE80::1:2 vlan 200
switchxxxxxx(config-if)# exit
```

例 2。次の例では、リレーの既知のマルチキャスト リンクローカル宛先アドレスを VLAN 200 で設定し、有効になっていない場合には、VLAN 100 で DHCPv6 リレーを有効にしています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination vlan 200
switchxxxxxx(config-if)# exit
```

例 3。次の例では、ユニキャスト グローバル リレー宛先アドレスを設定し、有効になっていない場合には、VLAN 100 で DHCPv6 リレーを有効にしています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination 3002::1:2
switchxxxxxx(config-if)# exit
```

例 4。次の例では、VLAN 100 で DHCPv6 リレーを有効にしています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination
switchxxxxxx(config-if)# exit
```

例 5。次の例では、VLAN 100 で DHCPv6 リレーを無効にしています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# no ipv6 dhcp relay destination
switchxxxxxx(config-if)# exit
```

show ipv6 dhcp

指定したデバイスのダイナミック DHCP 固有識別子（DUID）を表示するには、ユーザ EXEC モードで **show ipv6 dhcp** コマンドを使用します。この情報は DHCPv6 クライアントおよび DHCPv6 リレーで使用されます。

構文

show ipv6 dhcp

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

このコマンドは、クライアント識別子とサーバ識別子の両方のリンク層アドレスに基づく DUID を使用します。デバイスは、最も小さい番号のインターフェイスの MAC アドレスを使用して DUID を形成します。

例 1。次は、スイッチの DUID 形式がエンタープライズ番号に基づくベンダーの場合のコマンド出力例です。

```
switchxxxxxx# show ipv6 dhcp
The switch's DHCPv6 unique identifier(DUID)is 0002000000090CC084D303000912
  Format: 2
  Enterprise Number: 9
  Identifier: 0CC084D303000912
```

例 2。次は、スイッチの DUID 形式がリンク層アドレスに基づくベンダーの場合のコマンド出力例です。

```
switchxxxxxx# show ipv6 dhcp
The switch's DHCPv6 unique identifier(DUID)is 000300010024012607AA
  Format: 3
  Hardware type: 1
  MAC Address: 0024.0126.07AA
```

例 3。次は、スイッチの DUID 形式がリンク層アドレスに基づくベンダーで DHCPv6 リレーがサポートされている場合のコマンド出力例です。

```
switchxxxxxx# show ipv6 dhcp
The switch's DHCPv6 unique identifier(DUID)is 000300010024012607AA
  Format: 3
  Hardware type: 1
  MAC Address: 0024.0126.07AA
Relay Destinations:
  2001:001:250:A2FF:FEBF:A056
  2001:1001:250:A2FF:FEBF:A056
  2001:1011:250:A2FF:FEBF:A056 via VLAN 100
  FE80::250:A2FF:FEBF:A056 via VLAN 100
  FE80::250:A2FF:FEBF:A056 via VLAN 200
```

show ipv6 dhcp interface

DHCP for IPv6 インターフェイス情報を表示するには、ユーザ EXEC モードで **show ipv6 dhcp interface** コマンドを使用します。

構文

show ipv6 dhcp interface [*interface-id*]

パラメータ

- ***interface-id***：インターフェイス識別子。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

このコマンドでインターフェイスが指定されていない場合は、IPv6用DHCP（クライアントまたはサーバ）が有効になっているすべてのインターフェイスが表示されます。このコマンドでインターフェイスが指定される場合、指定されているインターフェイスに関する情報だけが表示されます。

注。この新しい出力形式は、ステートフル設定をサポートするSWバージョン以降でサポートされます。

例

次に、DHCPv6 クライアントが有効になっている場合のこのコマンドの出力例を示します。

```
switchxxxxxx# show ipv6 dhcp interface
VLAN 100 is in client mode
  Configuration:
    Statefull Service is enabled (rapid-commit)
    Auto-Configuration is enabled
    Information Refresh Time: 86400 seconds
    Information Refresh Minimum Time: 600 seconds
  State:
    DHCP Operational mode is enabled
    Statefull Service is available
  DHCP server:
    Address: FE80::204:FCFF:FEA1:7439
    DUID: 0003000100002FCA17400
    Preference: 20
  IPv6 Address Information:
    IA NA: IA ID 0x00040001, T1 120, T2 192
    IPv6 Address: 30e0::12:45:11
      preferred lifetime: 300, valid lifetime: 54333
      expires at Nov 08 2002 09:11 (54331 seconds)
      renew for address will be sent in 54301 seconds
    IPv6 Address: 3012::13:af:25
      preferred lifetime: 280, valid lifetime: 51111
      expires at Nov 08 2002 08:17 (51109 seconds)
```

```
      renew for address will be sent in 5101 seconds
  Stateless Information:
    Information Refresh Time:  86400 seconds
    expires at Nov 08 2002 08:17 (51109 seconds)
    DNS Servers: 1001::1, 2001::10
    DNS Domain Search List: company.com beta.org
    SNTP Servers: 2004::1
    POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
    Configuration Server: config.company.com
    Configuration Path Name: qqq/config/aaa_config.dat
    Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 105 is in client mode
 Configuration:
    Statefull Service is enabled
    Auto-Configuration is disabled
    Information Refresh Time: 86400 seconds
    Information Refresh Minimum Time: 600 seconds
  State:
    DHCP Operational mode is enabled
    Statefull Service is not available (IPv6 routing is enabled)
  DHCP server:
    Address: FE80::204:FCFF:FEA1:7439
    DUID: 000300010002FCA17400
    Preference: 20
  Stateless Information:
    Information Refresh Time:  86400 seconds
    expires at Nov 08 2002 08:17 (51109 seconds)
    DNS Servers: 1001::1, 2001::10
    DNS Domain Search List: company.com beta.org
    SNTP Servers: 2004::1
    POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
    Configuration Server: config.company.com
    Configuration Path Name: qqq/config/aaa_config.dat
    Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 107 is in client mode
 Configuration:
    Statefull Service is enabled
    Auto-Configuration is enabled
    Information Refresh Time: 86400 seconds
    Information Refresh Minimum Time: 600 seconds
  State:
    DHCP Operational mode is enabled
    Statefull Service is not available (IPv6 routing is enabled)
  DHCP server:
    Address: FE80::204:FCFF:FEA1:7439
    DUID: 000300010002FCA17400
    Preference: 20
  Stateless Information:
    Information Refresh Time:  86400 seconds
    expires at Nov 08 2002 08:17 (51109 seconds)
    DNS Servers: 1001::1, 2001::10
    DNS Domain Search List: company.com beta.org
    SNTP Servers: 2004::1
    POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
    Configuration Server: config.company.com
    Configuration Path Name: qqq/config/aaa_config.dat
    Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 110 is in client mode
 Configuration:
    Statefull Service is enabled
    Auto-Configuration is disabled
    Information Refresh Time: 86400 seconds
    Information Refresh Minimum Time: 600 seconds
  State:
```

```
    DHCP Operational mode is disabled (IPv6 is not enabled)
VLAN 1000 is in client mode
 Configuration:
    Statefull Service is enabled
    Auto-Configuration is enabled
    Information Refresh Time: 86400 seconds
    Information Refresh Minimum Time: 600 seconds
  State:
    DHCP Operational mode is disabled (Interface status is DOWN)
  DHCP server:
    Address: FE80::204:FCFF:FEA1:7439
    DUID: 000300010002FCA17400
    Preference: 20
  Stateless Information:
    Information Refresh Time:  86400 seconds
    expires at Nov 08 2002 08:17 (51109 seconds)
    DNS Servers: 1001::1, 2001::10
    DNS Domain Search List: company.com beta.org
    SNTP Servers: 2004::1
    POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
    Configuration Server: config.company.com
    Configuration Path Name: qqq/config/aaa_config.dat
    Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 1010 is in relay mode
  DHCP Operational mode is enabled
  Relay source interface: VLAN 101
  Relay destinations:
    2001:001:250:A2FF:FEBF:A056
    FE80::250:A2FF:FEBF:A056 via FastEthernet 1/0/10
```

DNS クライアント コマンド

この章は、次の項で構成されています。

- clear host （448 ページ）
- ip domain lookup （449 ページ）
- ip domain name （450 ページ）
- ip domain polling-interval （451 ページ）
- ip domain retry （452 ページ）
- ip domain timeout （453 ページ）
- ip host （454 ページ）
- ip name-server （456 ページ）
- show hosts （457 ページ）

clear host

DNS クライアントの名前/アドレス キャッシュからダイナミックなホストの名前/アドレス マッピングのエントリを削除するには、特権 EXEC モードで **clear host** コマンドを使用します。

構文

clear host {*hostname* | *****}

パラメータ

- ***hostname***：DNS クライアントの名前/アドレス キャッシュからホストの名前/アドレス マッピングが削除されるホストの名前。
- *****：DNS クライアントの名前/アドレス キャッシュからすべてのダイナミックなホストの名前/アドレス マッピングを削除することを指定します。

デフォルト設定

DNS クライアントの名前/アドレス キャッシュからホストの名前/アドレス マッピングのエントリは削除されません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

単一のホスト名のマッピング情報を提供するダイナミック エントリを削除するには、*hostname* 引数を使用します。すべてのダイナミック エントリを削除するには、***** キーワードを使用します。

DNS ホスト名キャッシュにスタティックなホストの名前/アドレス マッピングを定義するには、ip host （454 ページ） コマンドを使用します。

DNS ホスト名キャッシュのスタティックなホストの名前/アドレス マッピングを削除するには、**no** ip host （454 ページ） コマンドを使用します。

例

次の例では、DNS クライアントの名前/アドレス キャッシュからすべてのダイナミック エントリを削除しています。

```
switchxxxxxx# clear host *
```

ip domain lookup

IP ドメイン ネーム システム（DNS）ベースのホスト名からアドレスへの変換を有効にするには、グローバル コンフィギュレーション モードで **ip domain lookup** コマンドを使用します。

DNS を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip domain lookup

no ip domain lookup

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、DNS ベースのホスト名からアドレスへの変換を有効にしています。

```
switchxxxxxx(config)# ip domain lookup
```

ip domain name

未修飾のホスト名（ドット付き 10 進表記のドメイン名を持たない名前）を完成させるためにスイッチが使用するデフォルトのドメイン名を定義するには、グローバル コンフィギュレーション モードで **ip domain name** コマンドを使用します。

スタティックに定義されたデフォルト ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

構文

ip domain name *name*

no ip domain name

パラメータ

name：未修飾のホスト名を完成させるために使用されるデフォルトのドメイン名。ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。長さは 1 ～ 158 文字です。各ドメイン レベルの最大ラベル長は 63 文字です。

デフォルト設定

デフォルトのドメイン名は定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ドメイン名を含まない IP ホスト名（つまりドットのない名前）にはドットとデフォルトのドメイン名が追加され、その後でホスト テーブルに追加されます。

ドメイン名とホスト名は、A ～ Z の ASCII 文字（大文字と小文字を区別しない）、0 ～ 9 の数字、アンダースコア、およびハイフンに制限されています。ピリオド（.）は、ラベルを区切るために使用されます。

各ドメイン レベルの最大サイズは 63 文字です。名前の最大サイズは 158 バイトです。

例

次の例では、デフォルトのドメイン名を「www.website.com」と定義しています。

```
switchxxxxxx(config)# ip domain name website.com
```

ip domain polling-interval

ポーリング間隔を指定するには、グローバル コンフィギュレーション モードで **ip domain polling-interval** コマンドを使用します。

デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

構文

ip domain polling-interval seconds

no ip domain polling-interval

パラメータ

seconds：ポーリング間隔（秒）。範囲は（2*（R+1）*T）～ 3600 です。

デフォルト設定

デフォルト値は 2 *（R+1）* T です。ここで、

- R は **ip domain retry** コマンドにより設定された値です。
- T は **ip domain timeout** コマンドにより設定された値です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

一部のアプリケーションは、指定された IP アドレスと継続的に通信します。IP アドレスの解決を受信しなかったり、固定回数の再送信を使用して DNS サーバを検出しなかったこのようなアプリケーションの DNS クライアントは、アプリケーションにエラーを返し、ポーリング間隔を使用して IP アドレスに DNS 要求メッセージを送信し続けます。

例

次の例では、ポーリング間隔を 100 秒に設定する方法を示しています。

```
switchxxxxxx(config)# ip domain polling-interval 100
```

ip domain retry

応答がない場合にデバイスがドメイン ネーム システム（DNS）クエリーを送信する回数を指定するには、グローバル コンフィギュレーション モードで **ip domain retry** コマンドを使用します。

デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

構文

ip domain retry *number*

no ip domain retry

パラメータ

number：DNS サーバへの DNS クエリーの送信を再試行する回数。指定できる範囲は 0 ～ 16 です。

デフォルト設定

デフォルト値は 1 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

number 引数は、DNS サーバが存在しないとスイッチが判断するまでに、DNS サーバに DNS クエリーが送信される回数を指定します。

例

次の例では、諦める前に DNS クエリーを 10 回送信するようにスイッチを設定する方法を示しています。

```
switchxxxxxx(config)# ip domain retry 10
```

ip domain timeout

DNS クエリーへの応答を待機する時間を指定するには、グローバル コンフィギュレーション モードで **ip domain timeout** コマンドを使用します。

デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

構文

ip domain timeout seconds

no ip domain timeout

パラメータ

seconds：DNS クエリーへの応答を待機する時間（秒）。指定できる範囲は 1 ～ 60 です。

デフォルト設定

デフォルト値は 2 秒です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

デフォルトのタイムアウト値を変更するには、このコマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

例

次の例では、DNS クエリーへの応答を 50 秒間待機するようにスイッチを設定する方法を示しています。

```
switchxxxxxx(config)# ip domain timeout 50
```

ip host

DNS ホスト名キャッシュのスタティックなホストの名前/アドレス マッピングを定義するには、**ip host** グローバル コンフィギュレーション モード コマンドを使用します。

スタティックなホストの名前/アドレスマッピングを削除するには、このコマンドの **no** 形式を使用します。

構文

ip host *hostname address1* [*address2...address8*]

no ip host *hostname* [*address1...address8*]

パラメータ

- ***hostname***：ホストの名前。（長さ：1 ～ 158 文字、各ドメイン レベルのラベルの最大長は 63 文字です）。
- ***address1***：関連付けられるホスト IP アドレス（IPv4、または IPv6 スタックがサポートされている場合には IPv6）。
- ***address2***...***address8***：単一のスペースで区切られた、最大で 7 つの追加で関連付けられる IP アドレス（IPv4、または IPv6 スタックがサポートされている場合には IPv6）。

デフォルト設定

ホストは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ホスト名は、A ～ Z の ASCII 文字（大文字と小文字を区別しない）、0 ～ 9 の数字、アンダースコア、およびハイフンに制限されています。ピリオド（.）は、ラベルを区切るために使用されます。

IP アプリケーションは、次の順序で IP アドレスを受信します。

1. このコマンドにより指定された順序の IPv6 アドレス。
2. このコマンドにより指定された順序の IPv4 アドレス。

指定したアドレスを削除するには、*address1...address8* 引数を使用してこのコマンドの **no** 形式を使用します。すべてのアドレスが削除されると、そのエントリは削除されます。

例

次の例では、スタティックなホストの名前/アドレス マッピングをホスト キャッシュに定義しています。

```
switchxxxxxx(config)# ip host accounting.website.com 176.10.23.1
```

ip name-server

名前とアドレスの解決に使用する1つ以上のネームサーバのアドレスを指定するには、グローバル コンフィギュレーション モードで **ip name-server** コマンドを使用します。

スタティックに指定された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。

構文

ip name-server *server1-address* [*server-address2...erver-address8*]

no ip name-server [*server-address1...server-address8*]

パラメータ

- ***server-address1***：単一のネーム サーバの IPv4 または IPv6 アドレス。
- ***server-address2...server-address8***：追加のネームサーバの IPv4 または IPv6 アドレス。

デフォルト設定

ネーム サーバの IP アドレスは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

サーバの優先順位は、入力された順序によって決まります。

各 **ip name-server** コマンドは、前のコマンドで定義された設定を置き換えます（存在する場合）。

例

次の例では、ネーム サーバとして IPv4 ホスト 172.16.1.111、172.16.1.2、および IPv6 ホスト 2001:0DB8::3 を指定する方法を示しています。

```
switchxxxxxx(config)# ip name-server 172.16.1.111 172.16.1.2 2001:0DB8::3
```

show hosts

デフォルト ドメイン名、名前検索サービスのスタイル、ネーム サーバ ホストの一覧、およびキャッシュ内にあるホスト名とアドレスの一覧を表示するには、特権 EXEC モードで **show hosts** コマンドを使用します。

構文

show hosts [**all** | *hostname*]

パラメータ

- **all**：指定されたホスト名のキャッシュ情報が、設定されたすべての DNS ビューについて表示されます。これはデフォルトです。
- ***hostname***：表示される指定されたホスト名のキャッシュ情報が、特定のホスト名のエントリに限定されます。

コマンド モード

特権 EXEC モード

デフォルト設定

デフォルトは **all** です。

使用上のガイドライン

このコマンドは、デフォルト ドメイン名、ネーム サーバ ホストの一覧、およびキャッシュ内にあるホスト名とアドレスの一覧を表示します。

例

次に、パラメータを指定しない場合の出力例を示します。

```
switchxxxxxx# show hosts
Name/address lookup is enabled
Domain Timeout: 3 seconds
Domain Retry: 4 times
Domain Polling Interval: 10 seconds
Default Domain Table
Source  Interface Preference Domain
static                       website.com
dhcpv6  vlan 100      1      qqtca.com
dhcpv6  vlan 100      2      company.com
dhcpv6  vlan 1100     1      pptca.com
Name Server Table
Source  Interface Preference  IP Address
static               1        192.0.2.204
static               2        192.0.2.205
static               3        192.0.2.105
DHCPv6      vlan 100 1        2002:0:22AC::11:231A:0BB4
DHCPv4      vlan 1   1        192.1.122.20
```

```
DHCPv4      vlan 1   2        154.1.122.20
Casche Table
Flags: (static/dynamic, OK/Ne/??)
OK - Okay, Ne - Negative Cache, ?? - No Response
Host Flag Address;Age...in preference order
example1.company.com (dynamic, OK) 2002:0:130F::0A0:1504:0BB4;1 112.0.2.10 176.16.8.8;123
 124 173.0.2.30;39
example2.company.com (dynamic, ??)
example3.company.com (static, OK) 120.0.2.27
example4.company.com (dynamic, OK) 24 173.0.2.30;15
example5.company.com (dynamic, Ne); 12
```

EEE コマンド

この章は、次の項で構成されています。

- eee enable（グローバル） （460 ページ）
- eee enable（インターフェイス） （461 ページ）
- eee lldp enable （462 ページ）
- show eee （463 ページ）

eee enable（グローバル）

EEE モードをグローバルに有効にするには、**eee enable** グローバル コンフィギュレーション コマンドを使用します。このモードを無効にするには、このコマンドの **no** 形式を使用します。

構文

eee enable

no eee enable

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

EEE を機能させるには、リンク相手のデバイスも EEE をサポートし、EEE が有効になっている必要があります。また、EEE を適切に機能させるには、自動ネゴシエーションを有効にする必要があります。ただし、ポート速度が 1 ギガとしてネゴシエートされる場合は、自動ネゴシエーション ステータスが有効か無効かにかかわらず、常に EEE が機能します。

ポートで自動ネゴシエーションが有効になっておらず、速度が 1 ギガ未満の場合、EEE の動作ステータスは無効になります。

例

```
switchxxxxxx(config)# eee enable
```

eee enable（インターフェイス）

イーサネット ポートで EEE モードを有効にするには、**eee enable** インターフェイス コンフィギュレーション コマンドを使用します。このモードを無効にするには、このコマンドの **no** 形式を使用します。

構文

eee enable

no eee enable

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

EEE が有効です。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

ポートで自動ネゴシエーションが有効になっておらず、速度が 1 ギガの場合、EEE の動作ステータスは無効になります。

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# eee enable
```

eee lldp enable

イーサネット ポートで LLDP による EEE サポートを有効にするには、**eee lldp enable** インターフェイス コンフィギュレーション コマンドを使用します。このサポートを無効にするには、このコマンドの **no** 形式を使用します。

構文

eee lldp enable

no eee lldp enable

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

有効

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

EEE LLDP アドバタイズメントを有効にすると、最適な省エネルギー モードを実現するために、デバイスがシステムの起動時間を選択および変更できるようになります。

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# eee lldp enable
```

show eee

EEE 情報を表示するには、**show eee** EXEC コマンドを使用します。

構文

show eee *[interface-id]*

パラメータ

interface-id：（オプション）イーサネット ポートを指定します。

デフォルト

なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

ポートが 10 G ポートで、リンク速度が 1 G の場合、EEE リモート ステータスは解決（および表示）できません。

例 1：以下は、すべてのポートに関する簡単な情報を表示しています。

```
switchxxxxxx# show eee
EEE globally enabled
EEE Administrate status is enabled on ports: gi1/0/1-2, gi1/0/4
EEE Operational status is enabled on ports: gi1/0/1-2, gi1/0/4
EEE LLDP Administrate status is enabled on ports: gi1/0/1-3
EEE LLDP Operational status is enabled on ports: gi1/0/1-2
```

例 2：以下は、ポートが Not Present 状態のときに表示される情報です。ポートが EEE をサポートしている場合、情報は表示されません。

```
switchxxxxxx# show eee gi1/0/1
Port Status: notPresent
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

例 3：以下は、ポートが DOWN ステータスのときに表示される情報です。

```
switchxxxxxx# show eee gi1/0/1
Port Status: DOWN
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

例 4：以下は、ポートが UP ステータスで、EEE をサポートしていないときに表示される情報です。

```
switchxxxxxx# show eee gi1/0/2
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

例 5：以下は、ネイバーが EEE をサポートしていないときに表示される情報です。

```
switchxxxxxx# show eee gi1/0/4
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Remote status: disabled
EEE Administrate status: enabled
EEE Operational status: disabled (neighbor does not support)
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: disabled
```

例 6：以下は、ポート上で EEE が無効になっているときに表示される情報です。

```
switchxxxxxx# show eee gi1/0/1
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Administrate status: disabled
EEE Operational status: disabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: disabled
```

例 7：以下は、ポート上で EEE が実行されていて、EEE LLDP が無効になっているときに表示される情報です。

```
switchxxxxxx# show eee gi1/0/2
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: disabled
EEE LLDP Operational status: disabled
Resolved Tx Timer: 10usec
```

```
Local Tx Timer: 10 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
```

例 8：EEE と EEE LLDP がポートで実行されているときに表示される情報を次に示します。

```
switchxxxxxx# show eee gi1/0/3
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec
```

例 9：以下は、ポート上で EEE が実行されていて、EEE LLDP が有効になっているものの、リモート リンク パートナーと同期していないときに表示される情報です。

```
switchxxxxxx# show eee gi1/0/4
Port Status: up
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status:  disabled
Resolved Tx Timer: 64
Local Tx Timer: 64
Resolved Rx Timer: 16
Local Rx Timer: 16
```

例 10：EEE と EEE LLDP がポートで実行されているときに表示される情報を次に示します。

```
switchxxxxxx# show eee gi1/0/3
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
```

```
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec
```

イーサネット コンフィギュレーション コマンド

この章は、次の項で構成されています。

- interface （469 ページ）
- interface range （470 ページ）
- shutdown （471 ページ）
- operation time （473 ページ）
- description （474 ページ）
- speed （475 ページ）
- duplex （476 ページ）
- negotiation （477 ページ）
- flowcontrol （479 ページ）
- mdix （480 ページ）
- back-pressure （481 ページ）
- port jumbo-frame （482 ページ）
- link-flap prevention （483 ページ）
- clear counters （484 ページ）
- set interface active （485 ページ）
- errdisable recovery cause （486 ページ）
- errdisable recovery interval （488 ページ）
- errdisable recovery reset （489 ページ）
- show interfaces configuration （491 ページ）
- show interfaces status （492 ページ）
- show interfaces advertise （493 ページ）
- show interfaces description （495 ページ）
- show interfaces counters （496 ページ）
- show ports jumbo-frame （499 ページ）
- show link-flap prevention （500 ページ）
- show errdisable recovery （501 ページ）

- show errdisable interfaces （502 ページ）
- clear switchport monitor （503 ページ）
- show switchport monitor （504 ページ）

interface

インターフェイスを設定するためにインターフェイス コンフィギュレーション モードにするには、**interface** グローバル コンフィギュレーション モード コマンドを使用します。

構文

interface *interface-id*

パラメータ

interface-id：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポート、ポートチャネル、VLAN、範囲、Bluetooth、IP インターフェイス、またはトンネルのいずれかのタイプを指定できます。

コマンド モード

グローバル コンフィギュレーション モード

例 1：イーサネット ポートの場合：

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)#
```

例 2：ポート チャネル（LAG）の場合：

```
switchxxxxxx(config)# interface po1
switchxxxxxx(config-if)#
```

interface range

コマンドを複数のポートで同時に実行するには、**interface range** コマンドを使用します。

構文

interface range *interface-id-list*

パラメータ

interface-id-list：インターフェイス ID のリストを指定します。インターフェイス ID には、イーサネット ポート、VLAN、またはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル、VLAN）コンフィギュレーション モード

使用上のガイドライン

インターフェイス範囲コンテキストのコマンドは、範囲内の各インターフェイスで独立して実行されます。いずれかのインターフェイスでコマンドがエラーを返した場合も、他のインターフェイスでのコマンドの実行は停止されません。

例

```
switchxxxxxx(config)# interface range gi1/0/1-4
switchxxxxxx(config-if-range)#
```

shutdown

インターフェイスを無効にするには、**shutdown** インターフェイス コンフィギュレーション モードコマンドを使用します。無効にしたインターフェイスを再起動するには、このコマンドの **no** 形式を使用します。

構文

shutdown

no shutdown

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

インターフェイスが有効になります。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

shutdown コマンドは、ifAdminStatus（RFC 2863 を参照）の値を DOWN に設定します。IfAdminStatus が DOWN に変更されると、ifOperStatus も DOWN に変わります。

ifOperStatus の DOWN 状態は、インターフェイスがより高いレベルとの間でメッセージを送受信しないことを意味します。たとえば、IP インターフェイスが設定されている VLAN をシャットダウンすると、VLAN へのブリッジングは継続されますが、スイッチは VLAN 上で IP トラフィックを送受信できません。

注：

- スイッチがイーサネット ポートをシャットダウンする場合は、ポート MAC サブレイヤもシャットダウンします。
- スイッチがポート チャネルをシャットダウンする場合は、ポート チャネルのすべてのポートもシャットダウンします。

例 1：次に、gi1/0/4 の動作を無効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  shutdown
switchxxxxxx(config-if)#
```

例 2：次の例では、無効にされたイーサネット ポートを再起動しています。

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  no shutdown
switchxxxxxx(config-if)#
```

例 3：次の例では、VLAN 100 をシャットダウンしています。

```
switchxxxxxx(config)#  interface vlan 100
switchxxxxxx(config-if)#  shutdown
switchxxxxxx(config-if)#
```

例 4：次の例では、トンネル 1 をシャットダウンしています。

```
switchxxxxxx(config)#  interface tunnel 1
switchxxxxxx(config-if)#  shutdown
switchxxxxxx(config-if)#
```

例 5：次の例では、ポート チャネル 3 をシャットダウンしています。

```
switchxxxxxx(config)#  interface po3
switchxxxxxx(config-if)#  shutdown
switchxxxxxx(config-if)#
```

operation time

ポートがアップしている時間を制御するには、**operation time** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。ポートの稼働時間の時間範囲をキャンセルするには、このコマンドの **no** 形式を使用します。

構文

operation time *time-range-name*

no operation time

パラメータ

- **time-range-name**：ポートが稼働する（アップ状態になる）時間範囲を指定します。時間範囲が有効でない場合、ポートはシャットダウンされます。（範囲：1 ～ 32 文字）

デフォルト設定

ポートの許可ステートに設定されている時間範囲はありません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

認証が成功したらただちにフォワーディング ステートに進むことができるように、802.1x エッジ ポート（エンド ステーションに接続されている **auto** ステートのポート）でスパニング ツリーを無効にするか、スパニング ツリー PortFast モードを有効にすることを推奨します。

例

operation time コマンドは、ポートのステータスがアップの場合にポートに影響を与えます。このコマンドは、ポートがアップ状態のままになる時間枠と、ポートがシャットダウンされる時間を定義します。他の理由でポートがシャットダウンされている間は、このコマンドは影響を与えません。

次に、ポート gi1/0/1 で動作時間範囲（「morning」という）をアクティブにする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  operation time morning
```

description

インターフェイスに説明を追加するには、**description** インターフェイス コンフィギュレーション モード コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

構文

description *string*

no description

パラメータ

string：ユーザに役立つポートのコメントまたは説明を指定します。（長さ：1 ～ 64 文字）。

デフォルト設定

インターフェイスに説明は付加されていません。

コマンド モード

インターフェイス（イーサネット、ポートチャネル、Bluetooth）コンフィギュレーション モード

例

次に、説明「SW#3」を gi1/0/4 に追加する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  description SW#3
```

speed

自動ネゴシエーションを使用していないときに、指定したイーサネットインターフェイスの速度を設定するには、**speed** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

speed {**100** | **1000** | **2500** | **5000** | **10000**}

no speed

パラメータ

- **100**：100 Mbps の動作を強制します
- **1000**：1000 Mbps の動作を強制します
- **2500**：2500 Mbps の動作を適用します。
- **5000**：5000 Mbps の動作を適用します。
- **10000**：10000 Mbps の動作を強制します

デフォルト設定

ポートはそのポートの最大速度で動作します。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

ポート チャネル コンテキストの **no speed** コマンドは、ポート チャネル内の各ポートをそのポートの最大速度に戻します。

例

次に、gi1/0/4 の速度を 100 Mbps の動作に設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  speed 100
```

duplex

自動ネゴシエーションを使用していないときに、指定したイーサネットインターフェイスの全二重通信または半二重通信を設定するには、**duplex**インターフェイス（イーサネット、ポートチャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

duplex *{***half** | **full***}*

no duplex

パラメータ

- **half**：半二重通信を強制します。
- **full**：全二重通信を強制します。

デフォルト設定

インターフェイスは全二重モードで動作します。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、全二重モードで動作するように gi1/0/1 を設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  duplex full
```

negotiation

指定したインターフェイスの速度およびデュプレックスパラメータの自動ネゴシエーションとマスター スレーブ モードを有効にするには、**negotiation** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。自動ネゴシエーションを無効にするには、このコマンドの **no** 形式を使用します。

構文

negotiation [*capability* [*capability2... capability5*]] [***preferred*** {***master*** | ***slave***}]

no negotiation

パラメータ

- **Capability**：（オプション）アドバタイズする機能を指定します。（使用可能な値：10h、10f、100h、100f、1000f、2500f、5000f、10000f）。

  10h：10 半二重をアドバタイズします。

  10f：10 全二重をアドバタイズします。

  100h：100 半二重をアドバタイズします。

  100f：100 全二重をアドバタイズします。

  1000f：1000 全二重をアドバタイズします。

  2500f：2500 全二重をアドバタイズします。

  - **5000f**：5000 全二重をアドバタイズします。
  - **10000f**：10000 全二重をアドバタイズします。

- **Preferred**：（オプション）マスター スレーブ設定を指定します。

  Master：マスター設定をアドバタイズします。

  Slave：スレーブ設定をアドバタイズします。

デフォルト設定

機能が指定されていない場合、デフォルトではポートのすべての機能のリストと、スレーブモードが指定されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、gi1/0/1 で自動ネゴシエーションを有効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  negotiation
```

flowcontrol

指定したインターフェイスでのフロー制御を設定するには、**flowcontrol**インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。フロー制御を無効にするには、このコマンドの **no** 形式を使用します。

構文

flowcontrol *{***on** | **off***}*

no flowcontrol

パラメータ

- **on**：フロー制御を有効にします。
- **off**：フロー制御を無効にします。

デフォルト設定

フロー制御は無効に設定されています。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、ポート gi1/0/1 でフロー制御を有効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  flowcontrol on
```

mdix

指定したインターフェイスでケーブル クロスオーバーを有効にするには、**mdix** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。ケーブル クロスオーバーを無効にするには、このコマンドの **no** 形式を使用します。

構文

mdix *{***on** | **auto***}*

no mdix

パラメータ

- **on**：手動 MDIX を有効にします。
- **auto**：自動 MDI/MDIX を有効にします。

デフォルト設定

デフォルト設定は auto です。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、ポート gi1/0/1 で自動クロスオーバーを有効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  mdix auto
```

back-pressure

特定のインターフェイスでバック プレッシャを有効にするには、**back-pressure** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。バック プレッシャを無効にするには、このコマンドの **no** 形式を使用します。

構文

back-pressure

no back-pressure

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

バック プレッシャは無効になっています。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

EEE が有効になっている場合は、バック プレッシャを有効にできません。

例

次に、ポート gi1/0/1 でバックプレッシャを有効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  back-pressure
```

port jumbo-frame

デバイス上でジャンボ フレームを有効にするには、**port jumbo-frame** グローバル コンフィギュレーション モード コマンドを使用します。ジャンボ フレームを無効にするには、このコマンドの **no** 形式を使用します。

構文

port jumbo-frame

no port jumbo-frame

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

デバイス上でジャンボ フレームは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、デバイスをリセットした後に有効になります。

例

次の例では、デバイス上でジャンボ フレームを有効にしています。

```
switchxxxxxx(config)#  port jumbo-frame
```

link-flap prevention

過剰なリンクフラッピングにより物理インターフェイスを err-disable に設定できるようにするには、**link-flap prevention** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

link-flap prevention {**enable** | **disable**}

no link-flap prevention

パラメータ

enable：リンクフラップ防止を有効にします。

disable：リンクフラップ防止を無効にします。

デフォルト設定

デバイスでリンクフラップ防止が有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、インターフェイスが 10 秒の間に 1 秒以内のリンクフラップ（リンクステータスの変更）が3回発生した場合、イーサネット（物理）インターフェイスをシャットダウンします。

例

次に、デバイスでリンクフラップ防止を有効にする例を示します。

```
switchxxxxxx(config)#  link-flap prevention
```

clear counters

すべてのインターフェイスまたは特定のインターフェイスでカウンタをクリアするには、**clear counters** 特権 EXEC モード コマンドを使用します。

構文

clear counters *[interface-id]*

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。

デフォルト設定

すべてのカウンタがクリアされます。

コマンド モード

特権 EXEC モード

例

次に、gi1/0/1 の統計情報カウンタをクリアする例を示します。

```
switchxxxxxx#  clear counters gi1/0/1
```

set interface active

シャットダウンされたインターフェイスを再アクティブ化するには、**set interface active** 特権 EXEC モード コマンドを使用します。

構文

set interface active *interface-id*

パラメータ

interface-id：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、アクティブに設定されていた、システムによりシャットダウンされたインターフェイスをアクティブ化するために使用します。

例

次に、gi1/0/1 を再アクティブ化する例を示します。

```
switchxxxxxx#  set interface active gi1/0/1
```

errdisable recovery cause

Err-Disable シャットダウン後のインターフェイスの自動再アクティブ化を有効にするには、**errdisable recovery cause** グローバル コンフィギュレーション モード コマンドを使用します。自動再アクティブ化を無効にするには、このコマンドの **no** 形式を使用します。

構文

errdisable recovery cause {**all** | **port-security** | **dot1x-src-address** | **acl-deny** | **stp-bpdu-guard** | **stp-loopback-guard** | **loopback-detection | udld | storm-control | link-flap** }

no errdisable recovery cause {**all** | **port-security** | **dot1x-src-address** | **acl-deny** | **stp-bpdu-guard** | **stp-loopback-guard** | **loopback-detection** | **udld | storm-control | link-flap** }

パラメータ

- **all**：以下に説明するすべての理由のエラー リカバリ メカニズムを有効にします。
- **port-security**：ポート セキュリティ Err-Disable 状態のエラー リカバリ メカニズムを有効にします。
- **dot1x-src-address**：802.1x Err-Disable 状態のエラー リカバリ メカニズムを有効にします。
- **acl-deny**：ACL 拒否 Err-Disable 状態のエラー リカバリ メカニズムを有効にします。
- **stp-bpdu-guard**：STP BPDU ガード Err-Disable 状態のエラーリカバリメカニズムを有効にします。
- **stp-loopback-guard**：STP ループバックガード Err-Disable 状態のエラーリカバリメカニズムを有効にします。
- **loopback-detection**：ループバック検出 Err-Disable 状態のエラーリカバリメカニズムを有効にします。
- **udld**：UDLD シャットダウン状態に対しエラー リカバリ メカニズムを有効にします。
- **storm-control**：ストーム制御シャットダウン状態に対しエラー リカバリ メカニズムを有効にします。
- **link-flap**：リンクフラップ防止 Err-Disable 状態のエラーリカバリメカニズムを有効にします。

デフォルト設定

自動再アクティブ化は、自動再作成がデフォルトで有効になっている場合のリンクフラップが理由の場合を除き、無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、すべての状態の後のインターフェイスの自動再アクティブ化を有効にしています。

```
switchxxxxxx(config)#  errdisable recovery cause all
```

errdisable recovery interval

エラー リカバリのタイムアウト間隔を設定するには、**errdisable recovery interval** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

構文

errdisable recovery interval *seconds*

no errdisable recovery interval

パラメータ

seconds：エラーリカバリのタイムアウト間隔を秒単位で指定します。（範囲：30 ～ 86400）

デフォルト設定

デフォルトのエラー リカバリのタイムアウト間隔は 300 秒です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、エラー リカバリのタイムアウト間隔を 10 分に設定しています。

```
switchxxxxxx(config)#  errdisable recovery interval 600
```

errdisable recovery reset

指定されたアプリケーションによってシャットダウンされた1つ以上のインターフェイスを再アクティブ化するには、**errdisable recovery reset** 特権 EXEC モード コマンドを使用します。単一のインターフェイス、複数のインターフェイス、またはすべてのインターフェイスを指定できます。

構文

errdisable recovery reset {**all** | **port-security** | **dot1x-src-address** | **acl-deny** |**stp-bpdu-guard** | **stp-loopback-guard** | l**oopback-detection | udld | storm-control | link-flap | interface** *interface-id*}

パラメータ

- **all**：状態に関係なく、すべてのインターフェイスを再アクティブ化します。
- **port-security**：ポート セキュリティ Err-Disable 状態のすべてのインターフェイスを再アクティブ化します。
- **dot1x-src-address**：802.1x Err-Disable 状態のすべてのインターフェイスを再アクティブ化します。
- **acl-deny**：ACL 拒否 Err-Disable 状態のすべてのインターフェイスを再アクティブ化します。
- **stp-bpdu-guard**：STP BPDU ガード Err-Disable 状態のすべてのインターフェイスを再アクティブ化します。
- **stp-loopback-guard**：STP ループバック ガード Err-Disable 状態のすべてのインターフェイスを再アクティブ化します。
- **loopback-detection**：ループバック検出 Err-Disable 状態のすべてのインターフェイスを再アクティブ化します。
- **udld**：UDLD シャットダウン状態のすべてのインターフェイスを再アクティブ化します。
- **storm-control**：ストーム制御シャットダウン状態のすべてのインターフェイスを再アクティブ化します。
- **link-flap**：リンクフラップ防止 Err-Disable 状態のすべてのインターフェイスを再アクティブ化します。
- **interface** *interface-id*：アクティブに設定されていた、システムによりシャットダウンされたインターフェイスを再アクティブ化します。

コマンド モード

特権 EXEC モード

例 1：インターフェイス gi1/0/1 を再アクティブ化する例を示します。

```
switchxxxxxx# errdisable recovery reset interface gi1/0/1
```

例 2：次の例では、状態に関係なく、すべてのインターフェイスを再アクティブ化しています。

```
switchxxxxxx# errdisable recovery reset all
```

例 3：次の例では、ポート セキュリティ Err-Disable 状態のすべてのインターフェイスを有効にしています。

```
switchxxxxxx# errdisable recovery reset port-security
```

show interfaces configuration

設定済みのすべてのインターフェイスまたは特定のインターフェイスの設定を表示するには、**show interfaces configuration** 特権 EXEC モード コマンドを使用します。

構文

show interfaces configuration *[interface-id* | **detailed**]

パラメータ

- **interface-id**：（オプション）インターフェイス ID を指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのインターフェイスを表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

例

次の例では、すべての設定済みインターフェイスの設定を表示しています。

```
switchxxxxxx#  show interfaces configuration
                                          Flow     Admin  Back      Mdix
Port   Type     Duplex  Speed  Neg      control  State  Pressure  Mode
------ -------- ------  -----  -------- -------  -----  --------  ----
gi1/0/1 1G-Copper   Full    1000   Enabled  Off      Up     Disabled  Off
gi1/0/2 1G-Copper   Full    1000   Disabled Off      Up     Disabled  Off
gi1/0/2 10G-Copper  Full    10000  Disabled Off      Up     Disabled  Off
gi1/0/3 10G-Copper  Full    2500   Disabled Off      Up     Disabled  Off
gi1/0/4 10G-Copper  Full    5000   Disabled Off      Up     Disabled  Off
                                  Flow      Admin
PO      Type   Speed  Neg        Control   State
------  ------ -----  --------   -------   -----
Po1                   Disabled   Off       Up
```

show interfaces status

すべてのインターフェイスまたは特定のインターフェイスのステータスを表示するには、**show interfaces status** 特権 EXEC モード コマンドを使用します。

構文

show interfaces status *[interface-id* | **detailed**]

パラメータ

- **interface-id**：（オプション）インターフェイス ID を指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

コマンド モード

特権 EXEC モード

デフォルト設定

すべてのインターフェイスについて表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

例

次の例では、すべての設定済みインターフェイスのステータスを表示しています。

```
switchxxxxxx#  show interfaces status
                                          Flow  Link   Back     Mdix
Port   Type      Duplex  Speed Neg       ctrl  State  Pressure Mode
------ --------- ------  ----- --------- ----  ------ -------- --
gi1/0/1  1G-Copper  Full   1000  Disabled Off   Up     Disabled Off
gi1/0/2  1G-Copper  --     --     --       --    Down   --       --
te1/0/1  10G-Copper --     2500   --       --    Down   --       --
                                        Flow     Link
PO     Type      Duplex Speed  Neg     control  State
-----  -------   ------ -----  ------- ----     ------
Po1    1G        Full   10000  Disabled Off     Up
*: The interface was suspended by the system.
```

show interfaces advertise

設定済みのすべてのインターフェイスまたは特定のインターフェイスの自動ネゴシエーション アドバタイズメント情報を表示するには、**show interfaces advertise** 特権 EXEC モード コマンドを使用します。

構文

show interfaces advertise *[interface-id* **| detailed**]

パラメータ

- **interface-id**：（オプション）インターフェイス ID を指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのインターフェイスについて表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

例

次の例では、自動ネゴシエーション情報を表示しています。

```
switchxxxxxx#  show interfaces advertise

Port    Type        Neg     Prefered Operational Link Advertisement
----    ----------- ------- -------- ---------------------------
gi1/0/1 1G-Copper   Enable  Master   1000f, 100f, 10f, 10h
gi1/0/2 1G-Copper   Enable  Slave    1000f
tw1/03  2.5G-Copper Enable           2500f, 1000f, 100f, 100h
                            Slave
te1/0/1 10G-Copper  Enable  Slave    10000f, 5000f, 2500f,1000f
```

```
switchxxxxxx#  show interfaces advertise gi1/0/1
Port:gi1/0/1
Type: 1G-Copper
Link state: Up
Auto Negotiation: enabled
Preference: Master
```

Admin Local link Advertisement		10h	10f	100h	100f	1G	2.5G
Oper Local link Advertisement		---	---	----	----	-----	-----
Remote Local link Advertisement		yes	yes	yes	yes	yes	no
Priority Resolution		yes	yes	yes	yes	yes	no
		no	no	yes	yes	yes	no
		-	-	-	-	yes	-

```
switchxxxxxx#  show interfaces advertise gi1/0/1
Port: gi1/0/1
Type: 1G-Copper
Link state: Up
Auto negotiation: disabled.
```

show interfaces description

設定済みのすべてのインターフェイスまたは特定のインターフェイスの説明を表示するには、**show interfaces description** 特権 EXEC モード コマンドを使用します。

構文

show interfaces description *[interface-id* | **detailed**]

パラメータ

- **interface-id**：（オプション）インターフェイス ID を指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのインターフェイスの説明を表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

例

次の例では、すべての設定済みインターフェイスの説明を表示しています。

```
switchxxxxxx#  show interfaces description
```

```
Port          Descriptions
------        -----------------------------------------------
gi1/0/1       Port that should be used for management only
gi1/0/2
gi1/0/3
gi1/0/4
```

```
PO            Description
----          -----------
Po1           Output
```

show interfaces counters

すべての物理インターフェイスまたは特定のインターフェイスにより見られたトラフィックを表示するには、**show interfaces counters** 特権 EXEC モード コマンドを使用します。

構文

show interfaces counters *[interface-id* | **detailed**]

パラメータ

- **interface-id**：（オプション）インターフェイス ID を指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのインターフェイスのカウンタを表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

例

次の例では、すべての物理インターフェイスで見られたトラフィックを表示しています。

```
switchxxxxxx#  show interfaces counters gi1/0/1
Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------- ------------ ------------ ------------ ------------
gi1/0/1           0            0            0            0
Port       OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------- ------------ ------------ ------------ ------------
gi1/0/1           0            1            35          7051
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

次の表で、この出力で表示されるフィールドについて説明します。

フィールド	説明
InOctets	受信したオクテットの数。
InUcastPkts	受信ユニキャスト パケット数。
InMcastPkts	受信ユニキャスト パケット数。
InBcastPkts	受信したブロードキャスト パケットの数。
OutOctets	送信したオクテットの数。
OutUcastPkts	送信ユニキャスト パケット数。
OutMcastPkts	送信ユニキャスト パケット数。
OutBcastPkts	送信ブロードキャスト パケット数。
FCS Errors	長さがオクテットの整数で、FCS チェックに合格しない受信フレームの数。
Single Collision Frames	単一の衝突に関与し、その後正常に送信されたフレームの数。
Multiple Collision Frames	複数の衝突に関与し、その後正常に送信されたフレームの数。
SQE Test Errors	SQE TEST ERROR が受信された回数。SQE TEST ERROR は PLS キャリア検知機能の SQE 検出メカニズムの検証規則に従って設定されます。IEEE 規格 802.3 の 2000 エディション、セクション 7.2.4.6 を参照してください。
Deferred Transmissions	メディアがビジーなために最初の伝送試行が遅延したフレームの数。
Late Collisions	パケットの伝送までの 1 スロット時間よりも遅れて衝突が検出された回数。
Excessive Collisions	過度の衝突により伝送が失敗したフレームの数。
Oversize Packets	最大許容フレーム サイズを超える、受信したフレームの数。
Internal MAC Rx Errors	内部 MAC サブレイヤ受信エラーにより受信が失敗したフレームの数。
Received Pause Frames	PAUSE 操作を示す演算コードを含む、受信された MAC 制御フレームの数。

フィールド	説明
Transmitted Pause Frames	PAUSE操作を示す演算コードを含む、このインターフェイスで送信した MAC 制御フレームの数。

show ports jumbo-frame

デバイスでジャンボフレームが有効になっているかどうかを表示するには、**show ports jumbo-frame** 特権 EXEC モードコマンドを使用します。

構文

show ports jumbo-frame

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

次の例では、デバイスでジャンボ フレームが有効になっているかどうかを表示しています。

```
switchxxxxxx#  show ports jumbo-frame
Jumbo frames are disabled
Jumbo frames will be enabled after reset
```

show link-flap prevention

デバイスでリンクフラップ防止が有効になっているかどうかを表示するには、**show link-flap prevention** 特権 EXEC モードコマンドを使用します。

構文

show link-flap prevention

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

次に、デバイスでリンクフラップ防止が有効になっているかどうかを表示する例を示します。

```
switchxxxxxx#  show link-flap prevention
link-flap prevention is currently enabled on device
```

show errdisable recovery

デバイスの Err-Disable 設定を表示するには、**show errdisable recovery** 特権 EXEC モード コマンドを使用します。

構文

show errdisable recovery

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

次の例では、Err-Disable 設定を表示しています。

```
switchxxxxxx#  show errdisable recovery
Timer interval: 300 Seconds
Reason                 Automatic Recovery
---------------------- ------------------
port-security          Disable
dot1x-src-address      Disable
acl-deny               Enable
stp-bpdu-guard         Disable
stp-loopback-guard     Disable
loop-detection         Disable
udld                   Disable
storm control          Disable
link-flap             Disable
```

show errdisable interfaces

すべてのインターフェイスまたは特定のインターフェイスの Err-Disable 状態を表示するには、**show errdisable interfaces** 特権 EXEC モード コマンドを使用します。

構文

show errdisable interfaces [*interface-id*]

パラメータ

- **interface**：（オプション）ポートまたはポート チャネルの番号。

デフォルト設定

すべてのインターフェイスについて表示します。

コマンド モード

特権 EXEC モード

例

次に、gi1/0/1 の Err-Disable 状態を表示する例を示します。

```
switchxxxxxx#  show errdisable interfaces
Interface                 Reason                       Time to recovery
(sec)
------------          ------------------               -------------
gi1/0/1                   port-security                       250
gi1/0/5                   acl-deny                            NA
```

clear switchport monitor

すべてまたは特定のインターフェイスまたはインターフェイスリストのモニタ対象の統計情報をクリアするには、**clear switchport monitor** 特権 EXEC モードコマンドを使用します。

構文

clear switchport monitor *[interface-id-list]*

パラメータ

interface-id-list：（オプション）インターフェイス ID のリストを指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。

デフォルト設定

すべてのモニタ対象の統計情報がクリアされます。

コマンド モード

特権 EXEC モード

例

次に、gi1/0/1 のモニタ対象の統計情報をクリアする例を示します。

```
switchxxxxxx#  clear switchport monitor gi1/0/1
```

show switchport monitor

特定のインターフェイスによって収集されたモニタ対象の統計情報を表示するには、**show switchport monitor** 特権 EXEC モードコマンドを使用します。

構文

show switchport monitor *interface-id* {**seconds** | **minutes** | **hours** | **days** |**weeks**} *[***utilization** | **tx** | **rx** | **frames]**

show switchport monitor *interface-id* {***days*** |**weeks**}

show switchport monitor utilization *[interface-id]*

パラメータ

- **interface-id**：（オプション）インターフェイス ID を指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。
- **seconds**：最新の 20 個のサンプル。15 秒ごとにサンプリングされます。
- **minutes**：最新の 60 個のサンプル。60 秒ごとにサンプリングされます（システム時刻に従って 1 分間隔）。
- **hours**：最新の 24 個のサンプル。60 分ごとにサンプリングされます（システム時刻に基づく 1 時間ごと）。
- **days**：最新の 7 個のサンプル。24 時間ごとにサンプリングされます（システム時刻に従って午前 0 時から午前 0 時まで）。
- **weeks**：最新の 12 個のサンプル。7 日ごとにサンプリングされます（土曜日の午前 0 時から土曜日の午前 0 時まで）。
- **utilization**：時間枠ごとに計算された使用率を表示します。
- **rx**：受信カウンタの統計情報を表示します。
- **tx**：送信カウンタの統計情報を表示します。
- **frames**：パケットサイズごとに収集された受信カウンタの統計情報を表示します。

デフォルト設定

show switchport monitor *utilization* コマンドの場合に、1 つのインターフェイスまたはすべてのインターフェイスのモニタ対象の統計情報を表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

show switchport monitor *utilization* は、各時間枠（最後の分、最後の時間、最後の日、および最後の週の最後の時間枠のインターフェイスごとの使用率の概要を表示するために使用されます。

show switchport monitor *interface-id* は、時間枠およびカウンタタイプごとに収集されたモニタ対象の統計情報サンプルを表示するために使用されます。

例 1：次に、インターフェイス gi1/0/1 で確認されたモニタ対象の統計情報の使用状況を表示する例を示します。

```
switchxxxxxx#  show switchport monitor utilization gi1/0/1
```

Interface --------- gi1/0/1	Minutes Rx/TX utilization ------------ 95%	Hours Rx/TX utilization ----------- 80%	Days Rx/TX utilization ----------- 60%	Weeks Rx/TX utilization ----------- 20%

例 2：次に、インターフェイス gi1/0/1 で確認され、分単位で収集されたモニタ対象の Tx 統計情報を表示します。

```
switchxxxxxx#  show switchport monitor gi1/0/1 minutes tx
```

Time ---------- 04:22:00(~) 04:23:00	Unicast frames Sent -------------- 95% 80%	Broadcast frames Sent ----------- 80% 70%	Multicast frames Sent ----------- 60% 60%	Good Octet Sent ------- 20% 50%

（ー）すべてのサンプルが使用できるわけではありません。

次の表で、この出力で表示されるフィールドについて説明します。

フィールド	説明
Time	システムのリアルタイムクロックの現在のサンプルのタイムスタンプ。 秒、分、時間の形式は hh:mm:ss です。 日と週の形式は次のとおりです。 <day of week> dd/mm/yy。
Good Octets Received	受信したオクテットの数。
Good Unicast frames Received	受信ユニキャスト パケット数。
Good Multicast frames Received	受信ユニキャスト パケット数。
Good Broadcast frames Received	受信したブロードキャスト パケットの数。
Good Octets Sent	送信したオクテットの数。

フィールド	説明
Good Unicast frames Sent	送信ユニキャスト パケット数。
Good Multicast frames Sent	送信ユニキャスト パケット数。
Good Broadcast frames Sent	送信ブロードキャスト パケット数。
Frames of 64 bytes	64 バイトの受信パケットサイズの数。
Frames of 65-127 bytes	65 ー 127 バイトの受信パケットサイズの数。
Frames of 128-255 bytes	128 ー 255 バイトの受信パケットサイズの数。
Frames of 256-511 bytes	256 ー 511 バイトの受信パケットサイズの数。
Frames of 512-1023 bytes	512 ～ 1023 バイトの受信パケットサイズの数。
Frames of 1024-1518 bytes	1024 ～ 1518 バイトの受信パケットサイズの数。
Rx Error Frames Received	長さがオクテットの整数で、FCS チェックに合格しない受信フレームの数。
Rx Utilization	インターフェイスの受信フレームの使用率（パーセンテージ）。
Tx Utilization	インターフェイスの送信フレームの使用率（パーセンテージ）。
Rx/Tx Utilization	インターフェイス上の Rx 使用率と Tx 使用率の平均（パーセンテージ）。

ファイル システム コマンド

この章は、次の項で構成されています。

- ファイル仕様 （508 ページ）
- システム フラッシュ ファイル （511 ページ）
- スタック上のフラッシュ ファイル システム （512 ページ）
- boot config （513 ページ）
- boot localization （515 ページ）
- boot system （517 ページ）
- cd （519 ページ）
- copy （520 ページ）
- delete （523 ページ）
- dir （524 ページ）
- mkdir （525 ページ）
- more （526 ページ）
- pwd （527 ページ）
- reload （528 ページ）
- rename （530 ページ）
- rmdir （532 ページ）
- service mirror-configuration （533 ページ）
- show bootvar / show version （534 ページ）
- show mirror-configuration service （537 ページ）
- show reload （538 ページ）
- show running-config （539 ページ）
- show startup-config （541 ページ）
- write （542 ページ）

ファイル仕様

ファイルは次の場所にある可能性があります。

- ネットワーク：TFTP サーバおよび/または SCP サーバ - ネットワーク ファイル
- アクティブフラッシュ：フラッシュファイル
- アクティブの USB ポートに接続されている大容量ストレージ：USB ファイル1 つの大容量ストレージだけがサポートされます。

注。スイッチ内ではすべてのスタックユニットのフラッシュ上のファイルシステムがサポートされますが、ファイルシステム CLI コマンドは、アクティブユニット上のフラッシュファイルへのアクセスのみを許可します。アクティブユニットと他のユニット間で必要なファイル同期は、スイッチによって自動的に実行されます。

ファイルまたはディレクトリの場所の指定には、Uniform Resource Locator（URL）が使用されます。URL には次のシンタックスがあります。

<*url*> ::= **tftp://**<*location*>/<*file-path*> | **scp://**[<*username*>**:**<*password*>**@**]<*location*>/<*file-path*> | **usb://**<*file-path*> | **flash://**<*file-path*> | <*current-directory*>[/<*file-path*>] | <*higher-directory*>[/<*file-path*>] | <*file-path*>

<*username*> ::= 文字列（70 文字以内）

<*password*> ::= 文字列（70 文字以内）

<*location*> ::= <*ipv4-address*> | <*ipv6-address*> | <*dns-name*>

<*current-directory*> ::= [{**usb** | **flash**}**:**][**.**]

<*higher-directory*> ::= [{**usb** | **flash**}**:**]**..**

<*file-path*> ::= [<*directories-path*>/]<*filename*>

<*directories-path*> ::= <*directory-name*> | <*directories-path*>/<*directory-name*>

<*directories-path*> の最大ディレクトリ数は 16 です。

<*directory-name*> ::= 文字列（63 文字以内）

<*filename*> ::= 文字列（63 文字以内）

ファイル名およびディレクトリ名は、ポータブルファイル名文字セットの文字だけで構成されます。このセットには次の文字が含まれます。

- A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- a b c d e f g h i j k l m n o p q r s t u v w x y z
- <スペース>
- 0 1 2 3 4 5 6 7 8 9 . _ -

最後の 3 つの文字はそれぞれ、<ピリオド>、<下線>、および <ハイフン> の文字です。

URL にスペースが含まれている場合、" 文字で囲む必要があります。

次に例を示します。

"flash://aaa it/alpha/file 125"

URL の最大長は 160 文字です

USB では次のファイル システムがサポートされています。

- **FAT32**：完全サポート。
- **NTFS**：部分的にサポート（読み取り専用）。

スイッチでは、次の事前に定義された URL エイリアスがサポートされています。

- **active-image**：事前に定義された URL エイリアスはアクティブイメージファイルを指定します。このファイルには、次の権限があります。

  readable

  executable

- **inactive-image**：事前に定義された URL エイリアスは、非アクティブイメージファイルを指定します。このファイルには、次の権限があります。

  readable

  executable

- **running-config**：事前に定義された URL エイリアスは、実行コンフィギュレーション ファイルを指定します。
- **startup-config**：事前に定義された URL エイリアスは、スタートアップ コンフィギュレーション ファイルを指定します。このファイルには、次の権限があります。

  readable

- **localization**。事前に定義された URL エイリアスは、セカンダリ言語ディクショナリファイルを指定します。これらのファイルには次の権限があります。

  readable

- **logging**。事前に定義された URL エイリアスは、Syslog ファイルを指定します。このファイルには、次の権限があります。

  readable

- **mirror-config**。事前に定義された URL エイリアスは、ミラー設定ファイルを指定します。このファイルには、次の権限があります。

  readable

例 1。次の例では、IPv4 アドレスを使用して TFTP サーバ上のファイルを指定します。

```
tftp://1.1.1.1/aaa/dat/file.txt
```

例 2。次の例では、IPv6 アドレスを使用して TFTP サーバ上のファイルを指定します。

```
tftp://3000:1:2::11/aaa/dat/file.txt
```

例 3。次の例では、DNS 名を使用して TFTP サーバ上のファイルを指定します。

```
tftp://files.export.com/aaa/dat/file.txt
```

例 4。次の例では、フラッシュ上のファイルを指定します。

```
flash://aaa/dat/file.txt
```

例 5。次の例では、現在のディレクトリを使用してファイルを指定します。

```
./dat/file.txt
```

```
dat/file.txt
```

例 6。次の例では、上位のディレクトリを使用してファイルを指定します。

```
../dat/file.txt
```

例 7。次の例では、USB ポートに接続された大容量ストレージ デバイス上のファイルを指定します。

```
usb://aaa/dat/file.txt
```

例 8。次の例では、現在のディレクトリを使用して、USB ポートに接続された大容量ストレージ デバイス上のファイルを指定します。

```
usb:aaa/dat/file.txt
```

```
usb:./aaa/dat/file.txt
```

例 9。次の例では、上位のディレクトリを使用して、USB ポートに接続された大容量ストレージ デバイス上のファイルを指定します。

```
usb:../aaa/dat/file.txt
```

システム フラッシュ ファイル

スイッチが使用するシステム ファイルは、**flash://system/** ディレクトリにあります。ユーザはシステム ファイルおよびディレクトリを追加、削除、および名前変更できません。ユーザはシステム ディレクトリの下に新しいディレクトリを作成できません。

システム ファイルは、次のグループに分類されます。

- 内部のシステム ファイル。ファイルは、スイッチ自体によって作成されます。例として、Syslog ファイルを挙げることができます。
- ユーザによってインストール/アンインストールされたファイル。このグループには次のファイルが含まれます。

  アクティブおよび非アクティブ イメージ

  スタートアップ コンフィギュレーション

  セカンダリ言語辞書

また、次の以前のバージョンからのコマンドも使用できます。

注。工場出荷時のデフォルトにリセットすると、次のファイルを除いて、フラッシュからすべてのファイルが削除されます。

- active-image
- inactive-image
- mirror-config
- localization

flash://system/ ディレクトリには次のディレクトリが含まれます。

- **flash://system/images/**：このディレクトリにはアクティブと非アクティブのイメージファイルが含まれています。
- **flash://system/configuration/**：このディレクトリには、スタートアップとミラーのコンフィギュレーション ファイルが含まれています。
- **flash://system/localization/**：このディレクトリには、セカンダリ言語ディクショナリファイルが含まれています。
- **flash://system/syslog/**：このディレクトリには、syslog ファイルが含まれています。
- **flash://system/applications/**：このディレクトリには、スイッチアプリケーションによって管理される内部システムファイルが含まれています。

スタック上のフラッシュ ファイル システム

CLI コマンドは、アクティブユニットのフラッシュにあるファイルにのみアクセスを提供します。スイッチは、アクティブユニットとメンバーユニット間の自動同期を実行します。

- スタンバイユニットのフラッシュファイルシステムは、アクティブユニットのフラッシュファイルシステムと完全に同期されます。
- 非スタンバイメンバーユニットのファイルシステムの場合、次のファイルのみが同期されます。
  - アクティブなイメージ ファイル
  - 非アクティブなイメージ ファイル
  - セカンダリ言語ディクショナリファイル
  - その他のすべてのファイルおよびディレクトリは削除されます。

boot config

リロード後にスタートアップ コンフィギュレーションとしてファイルをインストールするには、特権EXECモードで**boot config**コマンドを使用します。スタートアップ コンフィギュレーション ファイルをアンインストールするには、このコマンドの **no** 形式を使用します。

構文

boot config *startup-config-url*

boot config running-config

boot config mirror-config

no boot config

パラメータ

- ***startup-config-url***：ファイルの URL。事前に定義された URL は設定できません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

startup-config-url ファイルからスタートアップ コンフィギュレーションをインストールするには、**boot config** *startup-config-url* コマンドを使用します。ファイルは、CLI コマンドを含むテキスト ファイルである必要があります。コマンドは次の処理を実行します。

- システムのディレクトリ **flash://system/configuration/** にファイルをコピーします
- テキスト形式から内部のバイナリ形式へファイル形式を変換します。
- 変換後のファイルをスタートアップ コンフィギュレーションとしてインストールします。前のスタートアップ コンフィギュレーション ファイルは削除されます。
- スタンバイユニットにスタートアップ コンフィギュレーションをインストールします。

実行コンフィギュレーションからスタートアップコンフィギュレーションをインストールするには、**boot config running-config** コマンドを使用します。

ミラー コンフィギュレーション ファイルからスタートアップ コンフィギュレーションをインストールするには、**boot config mirror-config** コマンドを使用します。

スタートアップ コンフィギュレーションをアンインストールするには、**no boot config** コマンドを使用します。アンインストールされたファイルは削除されます。

例1。次の例では、TFTPサーバからスタートアップコンフィギュレーションをインストールします。

```
switchxxxxxx#  boot config tftp://1.1.1./confiration-files/config-v1.9.dat
```

例 2。次に、フラッシュからスタートアップ コンフィギュレーションをインストールする例を示します。

```
switchxxxxxx#  boot config flash://confiration-files/config-v1.9.dat
```

例 3。次の例では、現在のスタートアップ コンフィギュレーションを設定解除します。

```
switchxxxxxx#  no boot config
```

例 4。次の例では、実行コンフィギュレーション ファイルからスタートアップ コンフィギュレーションをインストールします。

```
switchxxxxxx#  boot config running-config
```

例 5。次の例では、ミラー コンフィギュレーション ファイルからスタートアップ コンフィギュレーションをインストールします。

```
switchxxxxxx#  boot config mirror-config
```

boot localization

ファイルをセカンダリ言語辞書ファイルとしてインストールするには、特権 EXEC モードで **boot localization** コマンドを使用します。インストールした言語ファイルを削除するには、このコマンドの **no** 形式を使用します。

構文

boot localization *dictionary-url*

no boot localization

パラメータ

- ***dictionary***-url：ファイルの URL。事前に定義された URL は設定できません。

デフォルト設定

デフォルト言語。

コマンド モード

特権 EXEC モード

使用上のガイドライン

セカンダリ言語ディクショナリを *dictionary-url* ファイルからインストールするには、**boot localization** *dictionary-url* コマンドを使用します。コマンドは次の処理を実行します。

- システムのディレクトリ **flash://system/localization/** にファイルをコピーします
- インストールしたファイル形式とファイル言語がデバイスでサポートされているかどうかを検証します。ファイルの形式が正しくない場合、またはファイルの言語がデバイスでサポートされていない場合、ファイルはコピーされず、コマンドはエラーで終了します。
- デバイス上の関連する言語ファイルを、インストールしたファイルに置き換えます。言語ファイルを更新しても、Web GUI ユーザが使用するアクティブなセカンダリ言語は変更されません。
- 他のすべてのスタックユニットにセカンダリ言語ディクショナリの関連ファイルをインストールします。

セカンダリ言語辞書をアンインストールするには、**no boot dictionary** コマンドを使用します。アンインストールしたファイルは削除されます。

例 1。次の例では、TFTP サーバからセカンダリ言語辞書ファイルをインストールします。

```
switchxxxxxx#  boot localization tftp://196.1.1.1/web-dictionaries/germany-dictionary.lang
```

例 2。次の例では、フラッシュからセカンダリ言語辞書ファイルをインストールします。

```
switchxxxxxx#  boot localization flash://web-dictionaries/germany-dictionary.lang
```

boot system

スタートアップ時にスイッチがロードするシステム（アクティブ）イメージをインストールするには、特権 EXEC モードで **boot system** コマンドを使用します。

構文

boot system *image-url*

boot system inactive-image

パラメータ

- ***image-url***：ファイルの URL。事前に定義された URL は設定できません。

デフォルト設定

デフォルトなし。

コマンド モード

特権 EXEC モード

使用上のガイドライン

image-url ファイルから新しいアクティブ イメージをインストールするには、**boot system** *image-url* コマンドを使用します。コマンドは次の処理を実行します。

- システムのディレクトリ **flash://system/image/** にファイルをコピーします
- その形式を検証します。ファイルが正しいイメージ形式ではない場合、ファイルは削除され、コマンドはエラーで終了します。
- コピーしたファイルを、スタートアップ時にロードするために使用されるアクティブ イメージとしてインストールします。前のアクティブ イメージ ファイルは、非アクティブ イメージとして保存されます。前の（非アクティブな）イメージは削除されます。
- すべてのスタック ユニットで新しいアクティブ イメージをインストールします。

非アクティブイメージをアクティブイメージとして、アクティブイメージを非アクティブイメージとして設定するには、**boot system inactive-image** コマンドを使用します。

コマンドは、すべてのスタック ユニットで非アクティブ イメージをアクティブとしてインストールします。

例 1。次の例では、TFTP サーバから新しいアクティブ イメージを設定します。

```
switchxxxxxx#  boot system tftp://145.21.2.3/image/image-v1-1.ros
```

例 2。次の例では、フラッシュから新しいアクティブ イメージを設定します。

```
switchxxxxxx#  boot system flash://images/image-v1-1.ros
```

例 3。次の例では、非アクティブ イメージを設定します。

```
switchxxxxxx#  boot system inactive-image
```

cd

現在のディレクトリまたはファイル システムを変更するには、ユーザ EXEC モードで **cd** コマンドを使用します。

構文

cd *url*

パラメータ

- ***url***：フラッシュまたは USB のディレクトリを指定します。

デフォルト設定

フラッシュのルート ディレクトリ（**flash://**）

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

ターミナル セッションが開始されると、セッションの現在のディレクトリが **flash://** に設定されます。現在のディレクトリを変更するには、**cd** コマンドを使用します。

例 1。次の例では、フラッシュで新しい現在のディレクトリを設定します。

```
switchxxxxxx>  pwd
flash://
switchxxxxxx>  cd date/aaa
switchxxxxxx> pwd
flash://date/aaa
```

例 2。次の例では、USB で新しい現在のディレクトリを設定します。

```
switchxxxxxx> pwd
flash://
switchxxxxxx> cd usb://
switchxxxxxx> pwd
usb://
```

copy

ファイルをコピー元からコピー先にコピーするには、特権 EXEC モードで **copy** コマンドを使用します。

構文

copy *src-url dst-url*

***copy** {**running-config** | **startup-config**} *dst-url*

copy {**running-config** | **startup-config**} *dst-url* [**exclude** | **include-encrypted** | **include-plaintext**]

copy *src-url* **running-config**

copy running-config startup-config

copy tech-support cbd usb://<*file-path*>

パラメータ

- ***src-url***：コピー元ファイルの場所の URL。事前に定義された URL エイリアスを設定できます。
- ***dst-url***：コピー先のファイルまたはディレクトリの URL。事前に定義された URL エイリアスは設定できません。
- **exclude**：ファイルは、コピーするファイルのセンシティブ データを含みません。
- **include-encrypted**：ファイルは、暗号化された形式でセンシティブ データを含みます。安全性オプションが設定されていない場合、デフォルトではこの安全性オプションが適用されます。
- **include-plaintext**：ファイルは、プレーンテキスト形式でセンシティブ データを含みます。
- **tech-support cbd**：ソースが Cisco Business Dashboard（CBD）テクニカルサポート情報であることを示します。このソースが選択されている場合、宛先は USB のみです。指定したファイル名に「.zip」サフィックスが含まれていない場合、このサフィックスはコピーされたファイル名に自動的に追加されます（完全なパス長は最大 160 文字）。

コマンド モード

特権 EXEC モード

使用上のガイドライン

次に関連するガイドラインを示します。

- 1 つのネットワーク ファイルを、別のネットワーク ファイルにコピーすることはできません。
- **Localization** は、事前に定義された *src-url* または *dst-url* としてサポートされていません。

- 任意のファイルをコピーするには、**copy** *src-url dst-url* コマンドを使用します。*dst-url* 引数が既存のフラッシュ ファイルを定義している場合、このファイルに書き込み権限がないとコマンドは失敗します。*dst-url* 引数がディレクトリ ファイルを定義している場合、ファイルは同じ名前のディレクトリにコピーされます。ファイル形式の検証または変換は行われません。*src-url* 引数と *dst-url* 引数がフラッシュ ファイルを定義している場合、*dst-url* ファイルは *src-url* ファイルのアクセス権を持ちます。*src-url* 引数が非フラッシュ ファイルを定義し、*dst-url* 引数がフラッシュ ファイルを定義している場合、*dst-url* ファイルは次の権限を持ちます。
  - readable
  - writable
- 実行コンフィギュレーション ファイルにファイルを追加するには、**copy** *src-url* **running-config** コマンドを使用します。

例 1。次の例では、ファイル file1 を TFTP サーバー 172.16.101.101 から **flash://aaa/file1** ファイルへコピーします。

```
switchxxxxxx# copy tftp://172.16.101.101/file1 flash://aaa/file1
```

例 2。次の例では、スタートアップ コンフィギュレーション ファイルを **tftp://172.16.101.101/config.txt** ファイルに保存します。

```
*switchxxxxxx# copy startup-config tftp://172.16.101.101/config.txt or switchxxxxxx#
copy startup-config tftp://172.16.101.101/config.txt include-encrypted
```

例 3。次の例では、実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーションにコピーします。

```
switchxxxxxx# copy running-config startup-config
```

（注） *

show running-config または startup-config の ssd 設定に「file SSD Indicator **plaintext**」と表示されている場合、コピーされたファイルには**プレーンテキスト**の機密情報が含まれています。

show running-config または startup-config の ssd 設定に「file SSD Indicator **encrypted**」と表示されている場合、コピーされたファイルには**暗号化された**機密情報が含まれています。

show running-config または startup-config の ssd 設定に「file SSD Indicator **exclude**」と表示されている場合、コピーされたファイルには機密情報が含まれず、**除外されます。**

例 4。次の例では、TFTP サーバに Syslog ファイルをコピーします。

```
switchxxxxxx# copy logging tftp://1.1.1.1/syslog.txt
```

例 5。次の例では、USB ポートに接続された大容量ストレージ デバイスからフラッシュにファイルをコピーします。

```
switchxxxxxx# copy usb://aaa/file1.txt flash://dir1/file2
```

delete

ローカル ファイルを削除するには、特権 EXEC モードで **delete** コマンドを使用します。

構文

delete *url*

delete startup-config

パラメータ

- ***url***：削除するローカル ファイルのローカル URL を指定します。事前に定義された URL およびネットワーク URL は設定できません。
- ***file-name***：削除する SNA ユーザファイルの名前を指定します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

delete *url* コマンドは、ネットワーク ファイルを削除できません。

スタートアップ コンフィギュレーション ファイルを削除するには、**delete startup-config** コマンドを使用します。

例 1。次の例では、フラッシュから「backup/config」というファイルを削除します。

```
switchxxxxxx# cd flash://backup/
switchxxxxxx# delete aaa.ttt
Delete flash://backup/aaa.ttt? [Y/N]Y
```

例 2。次の例では、USB ポートに接続された大容量ストレージ デバイスから「aaa/config」というファイルを削除します。

```
switchxxxxxx# delete usb://aaa/config
Delete usb://aaa/config? [Y/N]Y
```

dir

ファイルまたはファイル システムのリストを表示するには、ユーザ EXEC モードで **dir** コマンドを使用します。

構文

dir [*url*]

パラメータ

- ***url***：表示するディレクトリのローカル URL を指定します。事前に定義された URL およびネットワーク URL は設定できません。引数を指定しない場合、現在のディレクトリが使用されます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

このコマンドは、ネットワーク ディレクトリには適用できません。

現在のディレクトリを表示するには、**dir** コマンドを引数なしで使用します。

例

次の例では、**flash://mng/** ディレクトリを表示します。

```
switchxxxxxx> dir flash://mng/
Permissions
  d-directory
  r-readable
  w-writable
  x-executable
134560K of 520000K are free
Directory of flash://mng/
Permission  File Size     Last Modified      File Name
----------  ---------  --------------------  ------------------
 drw-         4720148  Dec 12 2010 17:49:36  bin
 -r--              60  Dec 12 2011 17:49:36  config-list
 -r--             160  Feb 12 2011 17:49:36  image-list
 -r-x         6520148  Nov 29 2010  7:12:30  image1
 -rw-            2014  Nov 20 2010  9:12:30  data
```

mkdir

新規ディレクトリを作成するには、特権 EXEC モードで **mkdir** コマンドを使用します。

構文

mkdir *url*

パラメータ

- *url*：作成したディレクトリの URL を指定します。事前に定義された URL およびネットワーク URL は設定できません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

mkdir コマンドは、ネットワーク ディレクトリには適用できません。

mkdir コマンドは、**flash://system/** ディレクトリにはディレクトリを作成できません。

作成したものを除き、*url* 引数で定義されているすべてのディレクトリが存在している必要があります。

例 1。次の例では、フラッシュにディレクトリを作成します。

```
switchxxxxxx# mkdir flash://date/aaa/
```

例 2。次の例では、USB ポートに接続された大容量ストレージ デバイスにディレクトリを作成します。

```
switchxxxxxx# mkdir usb://newdir/
```

more

ファイルの内容を表示するには、ユーザ EXEC モードで **more** コマンドを使用します。

構文

more *url*

パラメータ

- ***url***：表示するファイルのローカルURLまたは事前に定義されたファイル名を指定します。

コマンド モード

ユーザ EXEC モード

例

次の例では、実行コンフィギュレーション ファイルの内容を表示します。

```
switchxxxxxx> more running-config
no spanning-tree
interface range gi/11-48
speed 1000
exit
no lldp run
line console
exec-timeout 0
```

pwd

現在のディレクトリを表示するには、ユーザ EXEC モードで **pwd** コマンドを使用します。

構文

pwd [usb: I flash:]

パラメータ

- **usb:**：USB ドライバの現在のディレクトリを表示します。
- **flash:**：フラッシュ ドライバの現在のディレクトリを表示します。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

指定されたドライバの現在のディレクトリを表示するには、**pwd usb:** I **flash:** コマンドを使用します。

最近 **cd** コマンドによって設定された現在のディレクトリを表示するには、**pwd** コマンドを使用します。

例

次の例では、**cd** コマンドを使用して現在のディレクトリを変更し、次に **pwd** コマンドを使用してその現在のディレクトリを表示します。

```
switchxxxxxx> pwd
flash://
switchxxxxxx> cd date/aaa
switchxxxxxx> pwd
flash://date/aaa
```

reload

オペレーティング システムをリロードするには、特権 EXEC モードで **reload** コマンドを使用します。

構文

reload [**in** [hhh:mm | mmm] | **at** hh:mm [day month]] | **cancel**]

reload cancel

パラメータ

- **in** *hhh*:*mm* | *mmm*：指定した分数、または時間および分数が経過したときにイメージがリロードされるようにスケジューリングします。リロードは、約 24 日以内に実行する必要があります。
- **at** *hh*:*mm*：イメージのリロードが（24 時間制で）指定された時間に有効になるようにスケジューリングします。月日を指定すると、指定された日時にリロードが行われるようにスケジュールが設定されます。月日を指定しなかった場合、リロードは当日の指定時刻に行われます（指定時刻が現時刻より後の場合）。または翌日の指定時刻に行われます（指定時刻が現在時刻よりも前の場合）。00:00 を指定すると、深夜 0 時のリロードが設定されます。リロードは、24 時間以内に実行される必要があります。
- ***day***：1 ～ 31 の範囲で日付を指定します。
- ***month***：月を指定します。（範囲：Jan ～ Dec）
- **cancel**：スケジューリングされているリロードをキャンセルします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

スイッチをリロードするには、**reload** コマンドを使用します。

スケジューリングされたスイッチのリロードを指定するには、**reload** {**in** *hhh*:*mm* | *mmm* | **at** *hh*:*mm* [*day month*]} コマンドを使用します。

at キーワードは、スイッチでシステム クロックが設定されている場合にのみ設定できます。

at キーワードを使用してリロード時刻を指定するときに月日を指定した場合は、指定された日時にリロードが実行されます。月日が指定されていない場合は、リロードが（指定された時間が現在の時間よりも遅い場合は）現在の日の指定された時間、または（指定された時間が現在の時間よりも早い場合は）翌日の指定された時間に行われます。00:00 を指定すると、深夜 0 時のリロードが設定されます。リロードは、24 日以内に実行される必要があります。

スケジューリングされたリロードを取り消すには、**reload cancel** コマンドを使用します。

例 1。次に、スイッチをリロードする例を示します。

```
switchxxxxxx# reload
This command will reset the whole system and disconnect your current session. Do you
want to continue? (Y/N) [Y]
```

例 2。次に、10 分でイメージをリロードする例を示します。

```
switchxxxxxx# reload in 10
This command will reset the whole system and disconnect your current session. Reload is
 scheduled for 11:57:08 UTC Fri Apr 21 2012 (in 10 minutes). Do you want to continue?
(Y/N) [Y]
```

例 3。次に、8 月 24 日 12:10 にイメージをリロードする例を示します。

```
switchxxxxxx# reload at 12:10 24 Aug
This command will reset the whole system and disconnect your current session. Reload is
 scheduled for 12:10:00 UTC Sun Aug 24 2014 (in 1 hours and 12 minutes). Do you want to
 continue ? (Y/N)[N]
```

例 4。次に、13:00 にイメージをリロードする例を示します。

```
switchxxxxxx# reload at 13:00 soft
This command will reset the whole system and disconnect your current session. Reload is
 scheduled for 13:00:00 UTC Fri Apr 21 2012 (in 1 hour and 3 minutes). Do you want to
continue? (Y/N) [Y]
```

例 5。次に、リロードを取り消す例を示します。

```
switchxxxxxx# reload cancel
Reload cancelled.
```

rename

ローカル ファイルまたはディレクトリの名前を変更するには、特権 EXEC モードで **rename** コマンドを使用します。

構文

rename *url new-url*

パラメータ

- *url*：名前を変更するファイルまたはディレクトリの URL を指定します。事前に定義された URL およびネットワーク URL は設定できません。
- *new-url*：名前が変更されたファイルまたはディレクトリの新しい URL を指定します。事前に定義された URL およびネットワーク URL は設定できません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

url および *new-url* 引数は、同じドライバを指定する必要があります。

このコマンドは、ネットワーク ファイルまたはネットワーク ディレクトリの名前を変更することはできません。

このコマンドは、ファイルまたはディレクトリの名前を **flash://system** ディレクトリに変更することはできません。

例 1。次に、**flash://bin/text1.txt** ファイルの名前を **flash://archive/text1sav.txt** に変更する例を示します。

```
switchxxxxxx# cd flash://archive
switchxxxxxx# rename flash://bin/text1.txt ./text1sav.txt
```

例 2。次に、**flash://a/b** ディレクトリの名前を **flash://e/g/h** ディレクトリに変更する例を示します。

```
switchxxxxxx# pwd
flash://a/b/c/d
switchxxxxxx> dir flash://a
Permissions
  • d-directory
  • r-readable
  • w-writable
  • x-executable
134560K of 520000K are free
Directory of flash://a
File Name     Permission  File Size      Last Modified
---------     ----------  ---------   --------------------
b                drw-        472148   Dec 13 2010 15:49:36
```

```
switchxxxxxx> dir flash://e/g/h
Permissions
  • d-directory
  • r-readable
  • w-writable
  • x-executable
134560K of 520000K are free
Directory of flash://e/g/h
File Name     Permission  File Size      Last Modified
---------     ----------  ---------   --------------------
switchxxxxxx# rename flash://a/b flash://e/g/h
switchxxxxxx# pwd
flash://e/g/h/c/d
switchxxxxxx> dir flash://a
Permissions
  • d-directory
  • r-readable
  • w-writable
  • x-executable
134560K of 520000K are free
Directory of flash://mng/
File Name     Permission  File Size      Last Modified
---------     ----------  ---------   --------------------
switchxxxxxx> dir flash://e/g/h
Permissions
  • d-directory
  • r-readable
  • w-writable
  • x-executable
134560K of 520000K are free
Directory of flash://e/g/h
File Name     Permission  File Size      Last Modified
---------     ----------  ---------   --------------------
c                drw-        720148   Dec 12 2010 17:49:36
```

rmdir

ローカル ディレクトリを削除するには、特権 EXEC モードで **rmdir** コマンドを使用します。

構文

rmdir *url*

パラメータ

- *url*：削除するファイルまたはディレクトリの URL を指定します。事前に定義された URL およびネットワーク URL は設定できません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

空のディレクトリのみが削除できます。

このコマンドは、ネットワーク ディレクトリを削除できません。

このコマンドは、**flash://system** ディレクトリ内のディレクトリを削除できません。

例 1。次の例では、フラッシュから「backup/config」というディレクトリを削除します。

```
switchxxxxxx# rmdir flash://backup/config/
Remove flash://backup/config? [Y/N]Y
```

例 2。次の例では、USB ポートに接続された大容量ストレージ デバイスから「aaa/config」というディレクトリを削除します。

```
switchxxxxxx# rmdir usb://aaa/config/
Remove directory usb://aaa/config? [Y/N]Y
```

service mirror-configuration

ミラー コンフィギュレーション サービスを有効にするには、**service mirror-configuration** グローバル コンフィギュレーション モード コマンドを使用します。このサービスを無効にするには、**no service mirror-configuration** コマンドを使用します。

構文

service mirror-configuration

no service mirror-configuration

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

デフォルト設定では、ミラー コンフィギュレーション サービスは有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ミラー設定サービスは、最後の既知の安定した設定（24時間変更されていないスタートアップコンフィギュレーション）のコピーを自動的に保持します。

このサービスを無効にすると、ミラー設定ファイルが削除されます。

例 1：次の例は、ミラー設定サービスを無効にします。

```
switchxxxxxx(config)# no service mirror-configuration
```

This operation will delete the mirror-config file if exists. Do you want to continue? (Y/N) [N]

例 2：次の例では、ミラー コンフィギュレーション サービスを有効にしています。

```
switchxxxxxx(config)# service mirror-configuration
```

サービスが有効になりました。

show bootvar / show version

スタートアップ時にデバイスによってロードされたアクティブなシステム イメージ ファイルを表示し、またスイッチをリブート後にロードされるシステム イメージ ファイルを表示するには、ユーザ EXEC モードで **show bootvar** または **show version** コマンドを使用します。

構文

show bootvar

show version

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

Show bootvar と **show version** コマンドには同じ機能があります。

例 1。次の例では、リロード後のコマンドの出力例を示します。

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 04-Jul-2014
  Time: 15:03:07
Inactive-image: flash://system/images/image_v12-01.ros
  Version: 12.01
  MD5 Digest: 3FA000012857D8855AABC7577AB8999
  Date: 04-Feb-2001
  Time: 11:13:17
```

例 2。この例では、**boot system tftp://1.1.1.1/image_v14-01.ros** コマンドの適用後に、非アクティブを継続します。

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
  Inactive after reboot
Inactive-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
  Active after reboot
```

例 3。この例では、システムリロード後に、非アクティブを継続します。

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
Inactive-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
```

例 4。この例では、**boot system inactive-image** コマンドの適用後に、非アクティブを継続します。

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
  Inactive after reboot
Inactive-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
Active after reboot
```

例 5。この例では、システムリロード後に、非アクティブを継続します。

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
Inactive-image: flash://system/images/_image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
```

例 7。次の例では、**boot system** コマンドを 2 回適用した後のコマンド出力例を示します。

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
Inactive-image: flash://system/images/image_v12-01.ros
  Version: 12.01
  MD5 Digest: 3FA000012857D8855AABC7577AB8999
  Date: 04-Feb-2001
  Time: 11:13:17
switchxxxxxx# boot system tftp://1.1.1.1/image_v14-01.ros
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
```

```
  Inactive after reboot
Inactive-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
  Active after reboot
switchxxxxxx# boot system tftp://1.1.1.1/image_v14-04.ros
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
  Inactive after reboot
Inactive-image: flash://system/images/image_v14-04.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
  Active after reboot
```

例 8。次の例では、**boot system tftp://1.1.1.1/image_v14-01.ros** コマンドと **boot system inactive-image** コマンドを適用した後のコマンド出力例を示します。

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
Inactive-image: flash://system/images/image_v12-01.ros
  Version: 12.01
  MD5 Digest: 3FA000012857D8855AABC7577AB8999
  Date: 04-Feb-2001
  Time: 11:13:17
switchxxxxxx# boot system tftp://1.1.1.1/image_v14-01.ros
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
  Inactive after reboot
Inactive-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
  Active after reboot
switchxxxxxx# boot system inactive-image
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
Inactive-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
```

show mirror-configuration service

ミラー設定サービスのステータスを表示するには、ユーザ EXEC モードで **show mirror-configuration service** コマンドを使用します。

構文

show mirror-configuration service

コマンド モード

ユーザ EXEC モード

例

次の例では、ミラー コンフィギュレーション サービスのステータスを表示しています。

```
switchxxxxxx# show mirror-configuration service
Mirror-configuration service is enabled
```

show reload

スイッチのリロードのステータスを表示するには、ユーザ EXEC モードで **show reload** コマンドを使用します。

構文

show reload

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

show reload コマンドを使用すると保留中のイメージのリロードを表示できます。

例 1。次の例では、スケジュール済みリロードが設定されているときの情報を表示します。

```
switchxxxxxx> show reload
Image reload scheduled for 00:00:00 UTC Sat April 20 (in 3 hours and 12 minutes)
```

例 2。次の例では、スケジュール済みリロードが設定されていないときの情報を表示します。

```
switchxxxxxx> show reload
No scheduled reload
```

show running-config

現在の実行コンフィギュレーション ファイルの内容を表示するには、特権 EXEC モードで **show running-config** コマンドを使用します。

show running-config [**interface** i***nterface-id-list*** **| detailed** | **brief**]

パラメータ

- **interface** interface-id-list：インターフェイス ID のリストを指定します。インターフェイス ID には次のタイプのいずれかを指定できます：イーサネット ポート、ポート チャネルまたは VLAN。
- **detailed**：SSL キーと SSH キー、および証明書を含む設定を表示します。
- **brief**：SSL キーと SSH キー、および証明書なしで設定を表示します。

デフォルト設定

すべてのインターフェイスが表示されます。**detailed** または **brief** キーワードが指定されていない場合、**brief** キーワードが適用されます。

コマンド モード

特権 EXEC モード

例

次の例では、実行コンフィギュレーション ファイルの内容を表示しています。

```
switchxxxxxx# show running-config
config-file-header
AA307-02
v1.2.5.76 / R750_NIK_1_2_584_002
CLI v1.0
file SSD indicator encrypted
@
ssd-control-start
ssd config
ssd file passphrase control unrestricted
no ssd file integrity control
ssd-control-end cb0a3fdb1f3a1af4e4430033719968c0
!
unit-type unit 1 network te uplink none
unit-type unit 2 network te uplink none
unit-type unit 3 network te uplink none
unit-type unit 4 network te uplink none
unit-type-control-end
!
no spanning-tree
interface range gi1/0/1-4
speed 1000
exit
no lldp run
interface vlan 1
```

```
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
switchxxxxxx#
```

show startup-config

スタートアップ コンフィギュレーション ファイルの内容を表示するには、特権 EXEC モードで **show startup-config** コマンドを使用します。

構文

show startup-config [**interface** ***interface-id-list***]

パラメータ

- **interface** interface-id-list：インターフェイス ID のリストを指定します。インターフェイス ID には次のタイプのいずれかを指定できます：イーサネット ポート、ポート チャネルまたは VLAN。

コマンド モード

特権 EXEC モード

例

次の例では、スタートアップ コンフィギュレーション ファイルの内容を表示します。

```
switchxxxxxx# show startup-config
config-file-header
AA307-02
v1.2.5.76 / R750_NIK_1_2_584_002
CLI v1.0
file SSD indicator encrypted
@
ssd-control-start
ssd config
ssd file passphrase control unrestricted
no ssd file integrity control
ssd-control-end cb0a3fdb1f3a1af4e4430033719968c0
!
no spanning-tree
interface range gi1/0/1-4
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
switchxxxxxx#
```

write

実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに保存するには、特権 EXEC モードで **write** コマンドを使用します。

構文

write

write memory

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルに保存するには **write** コマンドまたは **write memory** コマンドを使用します。

例

次の例では、write コマンドを使用して startup-config ファイルを running-config ファイルで上書きする方法を示します。

```
switchxxxxxx# write
Overwrite file [startup-config] ?[Yes/press any key for no]....15-Sep-2010 11:27
:48 %COPY-I-FILECPY: Files Copy - source URL running-config destination URL
flash://startup-config
15-Sep-2010 11:27:50 %COPY-N-TRAP: The copy operation was completed successfully
Copy succeeded
```

GVRP コマンド

この章は、次の項で構成されています。

- clear gvrp statistics （544 ページ）
- gvrp enable（グローバル） （545 ページ）
- gvrp enable（インターフェイス） （546 ページ）
- gvrp registration-forbid （547 ページ）
- gvrp vlan-creation-forbid （548 ページ）
- show gvrp configuration （549 ページ）
- show gvrp error-statistics （550 ページ）
- show gvrp statistics （551 ページ）

clear gvrp statistics

すべてのインターフェイスまたは特定のインターフェイスの GVRP 統計情報をクリアするには、**clear gvrp statistics** 特権 EXEC モード コマンドを使用します。

構文

clear gvrp statistics *[interface-id]*

パラメータ

Interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

デフォルト設定

すべての GVRP 統計情報がクリアされます。

コマンド モード

特権 EXEC モード

例

次に、gi1/0/4 のすべての GVRP 統計情報をクリアする例を示します。

```
switchxxxxxx#  clear gvrp statistics gi1/0/4
```

gvrp enable（グローバル）

Generic Attribute Registration Protocol（GARP）VLAN 登録プロトコル（GVRP）をグローバルに有効にするには、**gvrp enable** グローバル コンフィギュレーション モード コマンドを使用します。デバイスの GVRP を無効にするには、このコマンドの **no** 形式を使用します。

構文

gvrp enable

no gvrp enable

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

GVRP はグローバルに無効となっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、デバイスの GVRP をグローバルに有効となっています。

```
switchxxxxxx(config)#  gvrp enable
```

gvrp enable（インターフェイス）

インターフェイスでGVRPを有効にするには、**gvrp enable**インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。インターフェイスで GVRP を無効にするには、このコマンドの **no** 形式を使用します。

構文

gvrp enable

no gvrp enable

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

すべてのインターフェイスで GVRP は無効です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

アクセス ポートは常に単一の VLAN のみのメンバーであるため、VLAN に動的に参加しません。タグなしVLANのメンバーシップはタグ付きVLANと同じ方法で反映されます。つまり、PVID をタグなし VLAN ID として手動で定義する必要があります。

例

次に、gi1/0/4 で GVRP を有効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  gvrp enable
```

gvrp registration-forbid

ポートのすべてのダイナミック VLAN を登録解除し、ポートでの VLAN の作成または登録を防止するには、**gvrp registration-forbid** インターフェイス コンフィギュレーション モード コマンドを使用します。ポートで VLAN を動的に登録できるようにするには、このコマンドの **no** 形式を使用します。

構文

gvrp registration-forbid

no gvrp registration-forbid

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

ポートでの VLAN の動的登録が許可されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、gi1/0/2 の VLAN のダイナミック登録を禁止する例を示します。

```
switchxxxxxx(config-if)#  interface gi1/0/2
switchxxxxxx(config-if)#  gvrp registration-forbid
```

gvrp vlan-creation-forbid

ダイナミック VLAN 作成または変更を無効にするには、**gvrp vlan-creation-forbid** インターフェイス コンフィギュレーション モード コマンドを使用します。ダイナミック VLAN の作成または変更を有効にするには、このコマンドの **no** 形式を使用します。

構文

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

有効

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、gi1/0/3 でのダイナミック VLAN の作成を無効にする例を示します。

```
switchxxxxxx(config-if)#  interface gi1/0/3
switchxxxxxx(config-if)#  gvrp vlan-creation-forbid
```

show gvrp configuration

タイマー値などの GVRP コンフィギュレーション情報、GVRP とダイナミック VLAN の作成を有効にするかどうか、GVRP を実行しているポートを表示するには、**show gvrp configuration** EXEC モード コマンドを使用します。

構文

show gvrp configuration *[interface-id* | **detailed**]

パラメータ

- **interface-id**：（オプション）インターフェイス ID を指定します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポートまたはポート チャネル。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべての GVRP 統計情報は、すべてのインターフェイスに対して表示されます。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

ユーザ EXEC モード

例

次に、GVRP の設定を表示する例を示します。

```
switchxxxxxx#  show gvrp configuration
GVRP Feature is currently Enabled on the device.
Maximum VLANs: 4094
Port(s) GVRP-Status  Regist-    Dynamic          Timers(ms)
                     ration     VLAN Creation    Join   Leave   Leave All
----    ----------- --------   -------------    ----    -----   ----------
gi1/0/1     Enabled     Forbidden   Disabled         600     200    10000
gi1/0/2     Enabled     Normal      Enabled          1200    400    20000
```

show gvrp error-statistics

show gvrp error-statistics EXEC モード コマンドを使用すると、すべてのインターフェイスまたは特定のインターフェイスの GVRP エラーの統計情報が表示されます。

構文

show gvrp error-statistics *[interface-id]*

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

デフォルト設定

すべての GVRP エラーの統計情報が表示されます。

コマンド モード

ユーザ EXEC モード

例

次の例では、GVRP エラー統計情報を表示します。

```
switchxxxxxx#  show gvrp error-statistics
GVRP Error Statistics:
----------------------
Legend:
  INVPROT  : Invalid Protocol Id
  INVATYP  : Invalid Attribute Type  INVALEN : Invalid Attribute Length
  INVAVAL  : Invalid Attribute Value INVEVENT: Invalid Event
  Port   INVPROT INVATYP INVAVAL INVALEN INVEVENT
-------- ------- ------- ------- ------- --------
 gi1/0/1      0       0       0       0       0
 gi1/0/2      0       0       0       0       0
 gi1/0/3      0       0       0       0       0
 gi1/0/4      0       0       0       0       0
```

show gvrp statistics

すべてのインターフェイスまたは特定のインターフェイスのGVRP統計情報を表示するには、**show gvrp statistics** EXEC モード コマンドを使用します。

構文

show gvrp statistics *[interface-id]*

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

デフォルト設定

すべての GVRP 統計情報が表示されます。

コマンド モード

ユーザ EXEC モード

例

次に、GVRP 統計情報を表示する例を示します。

```
switchxxxxxx#  show gvrp statistics
GVRP statistics:
----------------
Legend:
```

rJE :	Join Empty Received	rJIn: Join In Received
rEmp:	Empty Received	rLIn: Leave In Received
rLE :	Leave Empty Received	rLA : Leave All Received
sJE :	Join Empty Sent	sJIn: Join In Sent
sEmp:	Empty Sent	sLIn: Leave In Sent
sLE :	Leave Empty Sent	sLA : Leave All Sent

Port	rJE	rJIn	rEmp	rLIn	rLE	rLA	sJE	sJIn	sEmp	sLIn	sLE	sLA
-----	----	----	----	----	----	----	----	----	----	----	----	---
gi1/0/1	0	0	0	0	0	0	0	0	0	0	0	0
gi1/0/2	0	0	0	0	0	0	0	0	0	0	0	0
gi1/0/3	0	0	0	0	0	0	0	0	0	0	0	0
gi1/0/4	0	0	0	0	0	0	0	0	0	0	0	0

グリーン イーサネット コマンド

この章は、次の項で構成されています。

- green-ethernet energy-detect（グローバル） （554 ページ）
- green-ethernet energy-detect（インターフェイス） （555 ページ）
- green-ethernet short-reach（グローバル） （556 ページ）
- green-ethernet short-reach（インターフェイス） （557 ページ）
- green-ethernet power-meter reset （558 ページ）
- show green-ethernet （559 ページ）

green-ethernet energy-detect（グローバル）

Green-Ethernet Energy-Detect モードをグローバルに有効にするには、**green-ethernet energy-detect** グローバル コンフィギュレーション モード コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

green-ethernet energy-detect

no green-ethernet energy-detect

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)#  green-ethernet energy-detect
```

green-ethernet energy-detect（インターフェイス）

ポートで Green Ethernet-Energy-Detect モードを有効にするには、**green-ethernet energy-detect** インターフェイス コンフィギュレーション モード コマンドを使用します。ポートで無効にするには、このコマンドの no 形式を使用します。

構文

green-ethernet energy-detect

no green-ethernet energy-detect

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

無効

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

Energy-Detect は銅線ポートのみで動作します。ポートの自動選択が有効の場合、銅/ファイバの Energy-Detect は動作しません。

通常動作後にリンクが失われると、スリープ モードに移行するまで PHY ～ 5 秒かかります。

例

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  green-ethernet energy-detect
```

green-ethernet short-reach（グローバル）

Green-Ethernet Short-Reach モードをグローバルに有効にするには、**green-ethernet short-reach** グローバル コンフィギュレーション モード コマンドを使用します。これを無効にするには、このコマンドの **no** 形式を使用します。

構文

green-ethernet short-reach

no green-ethernet short-reach

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)#  green-ethernet short-reach
```

green-ethernet short-reach（インターフェイス）

ポートで green-ethernet short-reach モードを有効にするには、**green-ethernet short-reach** インターフェイス コンフィギュレーション モード コマンドを使用します。ポートで無効にするには、このコマンドの **no** 形式を使用します。

構文

green-ethernet short-reach

no green-ethernet short-reach

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

無効

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

VCT 長の確認は、速度が 1000 Mbps で動作する銅線ポートのみで実行できます。メディアが銅線以外の場合、またはリンク速度が 1000 Mbps 以外の場合、Short-Reach モードは適用されません。

インターフェイスを強化モードに設定した場合、VCT長の確認が完了し、電力が低に設定されると、エラーのアクティブなモニタリングが継続的に実行されます。特定のしきい値の超過エラーの場合、PHY は長距離に戻されます。

Short-Reach モードが有効の場合は、EEE を有効にすることはできません。

例

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  green-ethernet short-reach
```

green-ethernet power-meter reset

省電力メーターをリセットするには、**green-ethernet power meter reset** 特権 EXEC モードを使用します。

構文

green-ethernet power-meter reset

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx#  green-ethernet power-meter reset
```

show green-ethernet

green-ethernet のコンフィギュレーションおよび情報を表示するには、**show green-ethernet** 特権 EXEC モード コマンドを使用します。

構文

show green-ethernet [*interface-id* | ***detailed***]

パラメータ

- **interface-id**：（オプション）イーサネット ポートを指定します
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのポートについて表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

表示された省電力は、次の項目で節約した電力に関連しています。

- ポート LED
- Energy detect
- Short reach

ポート使用率に基づいていますが、考慮されていないため、EEE省電力は本質的に動的です。

次に、このコマンドで表示される操作以外の理由について説明します。

いくつかの理由がある場合は、優先度の最も高い理由のみが表示されます。

Energy-Detect 操作以外の理由		
Priority	**理由**	**説明**
1	NP	ポートが存在しません
2	LT	リンクのタイプがサポートされていません（光、自動メディア選択）
3	LU	ポート リンクは稼働しています。該当しません

Short-Reach 操作以外の理由		
Priority	理由	説明
1	NP	ポートが存在しません
2	LT	リンク タイプがサポートされていません（ファイバ）
3	LS	リンク速度がサポートされていません（10 mbps、100 mbps）
4	LL	VCTテストから受信したリンク長がしきい値を超えています
6	LD	ポート リンクがダウン状態です – 該当なし

例

```
switchxxxxxx#  show green-ethernet
Energy-Detect mode: Enabled
Short-Reach mode: Disabled
Disable Port LEDs mode: Enabled
Power Savings: 24% (1.08W out of maximum 4.33W)
Cumulative Energy Saved: 33 [Watt*Hour]
* Estimated Annual Power saving: 300 [Watt*Hour]
* Annual estimate is based on the saving during the previous week
NA - information for previous week is not available
Short-Reach cable length threshold: 50m
Port     Energy-Detect       Short-Reach           VCT Cable
      Admin Oper Reason   Admin Force Oper Reason   Length
----  ----- ---- -------  ----- ----- ---- -------  ------
gi1/0/1   on    on            off  off   off
gi1/0/2   on    off  LU       on   off   on           < 50
gi1/0/3   on    off  LU       off  off   off
```

IGMP コマンド

この章は、次の項で構成されています。

- clear ip igmp counters （562 ページ）
- ip igmp last-member-query-count （563 ページ）
- ip igmp last-member-query-interval （564 ページ）
- ip igmp query-interval （565 ページ）
- ip igmp query-max-response-time （566 ページ）
- ip igmp robustness （567 ページ）
- ip igmp version （568 ページ）
- show ip igmp counters （569 ページ）
- show ip igmp counters （570 ページ）
- show ip igmp groups （571 ページ）
- show ip igmp groups summary （573 ページ）
- show ip igmp interface （574 ページ）

clear ip igmp counters

Internet Group Management Protocol（IGMP）インターフェイスのカウンタをクリアするには、**clear ip igmp counters** コマンドを特権 EXEC モードで使用します。

構文

clear ip igmp counters [interface-id]

パラメータ

- ***interface-id***：（オプション）インターフェイス識別子

コマンド モード

特権 EXEC モード

使用上のガイドライン

clear ip igmp counters コマンドを使用して、受信した参加および脱退の数を追跡する IGMP カウンタをクリアします。オプションの *interface-id* 引数を省略した場合、**clear ip igmp counters** コマンドはすべてのインターフェイスのカウンタをクリアします。

例

次の例では、VLAN 100 のカウンタをクリアします。

```
switchxxxxxx# clear ip igmp counters vlan 100
```

ip igmp last-member-query-count

Internet Group Management Protocol（IGMP）の最後のメンバーのクエリー カウンタを設定するには、**ip igmp last-member-query-count** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ip igmp last-member-query-count count

no ip igmp last-member-query-count

パラメータ

count：脱退を示すメッセージの受信時にグループまたはグループ送信元固有のクエリーを送信した回数。（範囲：1 ～ 7）

デフォルト設定

IGMP 堅牢性変数の値。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ip igmp robustness コマンドを使用して、IGMP の最後のメンバーのクエリー カウンタを変更します。

例

次の例では、IGMP の最後のメンバーのクエリー カウンタの値を 3 に変更します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp last-member-query-count 3
switchxxxxxx(config-if)# exit
```

ip igmp last-member-query-interval

Internet Group Management Protocol（IGMP）の最後のメンバーのクエリー間隔を設定するには、**ip igmp last-member-query-interval** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトの IGMP クエリー間隔に戻すには、このコマンドの **no** 形式を使用します。

構文

ip igmp last-member-query-interval *milliseconds*

no ip igmp last-member-query-interval

パラメータ

- ***milliseconds***：インターフェイスで IGMP グループ固有のホスト クエリー メッセージが送信されたミリ秒単位の間隔。（範囲：100 ～ 25500）。

デフォルト設定

IGMP の最後のメンバーのデフォルトのクエリー間隔は 1000 ミリ秒です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ip igmp last-member-query-interval コマンドを使用して、インターフェイスで IGMP の最後のメンバーのクエリー間隔を設定します。

例

次に、IGMP の最後のメンバーのクエリー間隔を 1500 ミリ秒に増加する例を示します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp last-member-query-interval 1500
switchxxxxxx(config-if)# exit
```

ip igmp query-interval

IGMP クエリアが Internet Group Management Protocol（IGMP）のホスト クエリー メッセージをインターフェイスから送信する頻度を設定するには、**ip igmp query-interval** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトの IGMP クエリー間隔に戻すには、このコマンドの **no** 形式を使用します。

構文

ip igmp query-interval *seconds*

no ip igmp query-interval

パラメータ

- ***seconds***：スイッチがインターフェイスから IGMP クエリー メッセージを送信する頻度（秒単位）。範囲は 30 ～ 18000 です。

デフォルト設定

デフォルトの IGMP クエリー間隔は 125 秒です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ip igmp query-interval コマンドを使用して、IGMP クエリアがインターフェイスから IGMP ホスト クエリー メッセージを送信する頻度を設定します。ルータの接続されたネットワーク上にメンバーがいるマルチキャスト グループを検出するために、IGMP クエリアはクエリー ホスト メッセージを送信します。

クエリー間隔は、クエリーの最大応答時間よりも長い必要があります。

例

次に、IGMP クエリアが IGMP ホスト クエリー メッセージを送信する頻度を 180 秒に増加する例を示します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp query-interval 180
switchxxxxxx(config-if)# exit
```

ip igmp query-max-response-time

Internet Group Management Protocol（IGMP）クエリーにアドバタイズされる最大応答時間を設定するには、**ip igmp query-max-response-time** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

パラメータ

- ***seconds***：IGMP クエリーでアドバタイズされる最大応答時間（秒単位）。（範囲：5 ～ 20）

デフォルト設定

10 秒。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

このコマンドは、応答側がIGMPクエリー メッセージに応答できる期間を制御します。この期間を過ぎると、ルータはグループを削除します。

このコマンドは、ルータがグループを削除する前に、どれくらいの時間でホストがIGMPクエリー メッセージに応答する必要があるかを制御します。10 秒未満の値を設定すると、ルータはグループをすばやくプルーニングすることができます。

クエリーの最大応答時間はクエリー間隔よりも短い必要があります。

注。ホストが十分な速さで応答しない場合、誤ってプルーニングされる可能性があります。したがって、ホストは10秒（または設定した値）よりも早く、応答を認識する必要があります。

例

次に、最大応答時間を 8 秒に設定する例を示します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp query-max-response-time 8
switchxxxxxx(config-if)# exit
```

ip igmp robustness

Internet Group Management Protocol（IGMP）堅牢性変数を設定するには、**ip igmp robustness** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ip igmp robustness count

no ip igmp robustness

パラメータ

- ***count***：リンク上で予期されるパケット損失の数。パラメータの範囲。（範囲：1 ～ 7）。

デフォルト設定

デフォルト値は 2 です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ip igmp robustness コマンドを使用して、IGMP 堅牢性変数を変更します。

例

次の例では、IGMP の堅牢性変数の値を 3 に変更します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp robustness 3
switchxxxxxx(config-if)# exit
```

ip igmp version

ルータが使用する Internet Group Management Protocol（IGMP）のバージョンを設定するには、**ip igmp version** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ip igmp version {**1** | **2** | **3**}

no ip igmp version

パラメータ

- **1**：IGMP バージョン 1。
- **2**：IGMP バージョン 2。
- **3**：IGMP バージョン 3。

デフォルト設定

3

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

コマンドを使用して、IGMP のデフォルトのバージョンを変更します>

例

次の例では、IGMP バージョン 2 を使用するようにルータを設定します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp version 2
switchxxxxxx(config-if)# exit
```

show ip igmp counters

Internet Group Management Protocol（IGMP）トラフィック カウンタを表示するには、**show ip igmp counters** コマンドをユーザ EXEC モードで使用します。

構文

show ip igmp counters [*interface-id*]

パラメータ

- ***interface-id***：（オプション）インターフェイス識別子。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

show ip igmp counters コマンドを使用して、予想される数の IGMP プロトコル メッセージが受信および送信されたかどうかを確認します。

オプションの *interface-id* 引数を省略した場合、**show ip igmp counters** コマンドはすべてのインターフェイスのカウンタを表示します。

例

次の例では、送受信された IGMP プロトコル メッセージを表示します。

```
switchxxxxxx# show ip igmp counters vlan 100
VLAN 100
Elapsed time since counters cleared:00:00:21
Failed received Joins: 0
Total IGMPv1 received messages: 0
Total IGMPv2 received messages: 10
Total IGMPv3 received messages: 0
Total invalid received messages: 0
General Sent Queries: 0
Specific Sent Queries: 0
```

show ip igmp counters

Internet Group Management Protocol（IGMP）トラフィック カウンタを表示するには、**show ip igmp counters** コマンドをユーザ EXEC モードで使用します。

構文

show ip igmp counters [*interface-id*]

パラメータ

- ***interface-id***：（オプション）インターフェイス識別子。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

show ip igmp counters コマンドを使用して、予想される数の IGMP プロトコル メッセージが受信および送信されたかどうかを確認します。

オプションの *interface-id* 引数を省略した場合、**show ip igmp counters** コマンドはすべてのインターフェイスのカウンタを表示します。

例

次の例では、送受信された IGMP プロトコル メッセージを表示します。

```
switchxxxxxx# show ip igmp counters vlan 100
VLAN 100
Elapsed time since counters cleared:00:00:21
Failed received Joins: 0
Total IGMPv1 received messages: 0
Total IGMPv2 received messages: 10
Total IGMPv3 received messages: 0
Total invalid received messages: 0
General Sent Queries: 0
Specific Sent Queries: 0
```

show ip igmp groups

ルータに直接接続され Internet Group Management Protocol（IGMP）を通じて学習されたマルチキャスト グループを表示するには、**show ip igmp groups** コマンドを EXEC モードで使用します。

構文

show ip igmp groups [*group-name* | *group-address* | *interface-id*] [**detail**]

パラメータ

- ***group-name*** **|** *group-address*：（オプション）IP アドレスまたはマルチキャスト グループの名前。
- ***interface-id***：（オプション）インターフェイス識別子。
- **detail**：（オプション）個々のソースに関する詳細情報が表示されます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

show ip igmp groups [**detail**] コマンドを使用して、直接接続されたすべてのグループを表示します。

show ip igmp groups [*group-name* | *group-address*] [**detail**] コマンドを使用して、指定した 1 つの直接接続されたグループを表示します。

show ip igmp groups *interface-id* [**detail**] コマンドを使用して、指定したインターフェイスに直接接続されたすべてのグループを表示します。

例 1。次に、**show ip igmp groups** コマンドの出力例を示します。VLAN 100 により参加しているすべてのグループが表示されます。

```
switchxxxxxx# show ip igmp groups vlan 100
```

IGMP Connected Group Membership

```
Expires: never - switch itself has joined the group
Group Address Interface Expires
224.1.1.1 VLAN 100 00:01:30
224.10.12.79 VLAN 100 never
225.1.1.1 VLAN 100 00:00:27
```

例 2。次に、**detail** キーワードを指定した **show ip igmp groups** コマンドの出力例を示します。

```
switchxxxxxx# show ip igmp groups detail
Expires: zero value - INCLUDE state; non-zero value - EXCLUDE state
Interface: VLAN 100
```

```
Group: 225.1.1.1
Router mode: INCLUDE
Last reporter: 10.0.119.133
Group Timer Expires: 00:20:11
Group source list:
Source Address Expires
20.1.1.1 00:04:08
120.1.1.1 00:02:01
Group: 226.1.1.2
Router mode: EXCLUDE
Last reporter: 100.1.12.130
Group Timer Expiry: 00:22:12
Exclude Mode Expiry (Filter) Timer: 00:10:11
Group source list:
Source Address Expires
2.2.2.1 00:04:08
192.168.1.1 00:04:08
12.1.1.10 00:00:00
40.3.4.2 00:00:00
```

show ip igmp groups summary

Internet Group Management Protocol（IGMP）キャッシュ内に存在する、(*,G) および (S,G) メンバーシップ レポートの数を表示するには、**show ip igmp groups summary** コマンドをユーザ EXEC モードで使用します。

構文

show ip igmp groups summary

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

show ip igmp groups summary コマンドは、直接接続のマルチキャスト グループの数を表示します。

例

次に、**show ip igmp groups summary** コマンドの出力例を示します。

```
switchxxxxxx# show ip igmp groups summary
GMP Route Summary
No. of (*,G) routes = 5
No. of (S,G) routes = 0

Field Descriptions:
No. of (*,G) routes = 5—Displays the number of groups present in the IGMP cache.
No. of (S,G) routes = 0—Displays the number of include and exclude mode sources present
 in the IGMP cache.
```

show ip igmp interface

インターフェイスのマルチキャスト関連情報を表示するには、**show ip igmp interface** コマンドを特権 EXEC モードで使用します。

構文

show ip igmp interface [*interface-id*]

パラメータ

- ***interface-id***：（オプション）インターフェイス識別子。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

オプションの *interface-id* 引数を省略した場合、**show ip igmp interface** コマンドはすべてのインターフェイスの情報を表示します。

例

次に、イーサネット インターフェイス 2/1/1 に対する **show ip igmp interface** コマンドの出力例を示します。

```
switchxxxxxx# show ip igmp interface vlan 100
VLAN 100 is up
 Administrative IGMP Querier IP address is 1.1.1.1
 Operational IGMP Querier IP address is 1.1.1.1
 Current IGMP version is 3
 Administrative IGMP robustness variable is 2 seconds
 Operational IGMP robustness variable is 2 seconds
 Administrative IGMP query interval is 125 seconds
 Operational IGMP query interval is 125 seconds
 Administrative IGMP max query response time is 10 seconds
 Operational IGMP max query response time is 10 seconds
 Administrative Last member query response interval is 1000 milliseconds
 Operational Last member query response interval is 1000 milliseconds
```

IGMP プロキシ コマンド

この章は、次の項で構成されています。

- ip igmp-proxy （576 ページ）
- ip igmp-proxy downstream protected （577 ページ）
- ip igmp-proxy downstream protected interface （578 ページ）
- ip igmp-proxy ssm （579 ページ）
- show ip igmp-proxy interface （580 ページ）

ip igmp-proxy

IGMP プロキシ ツリーに、ダウンストリーム インターフェイスを追加するには、**ip igmp-proxy** コマンドをインターフェイス コンフィギュレーション モードで使用します。インターフェイスから IGMP プロキシ ツリーへのダウン ストリームを削除するには、このコマンドの **no** 形式を使用します。

構文

ip igmp-proxy *upstream-interface-id*

no ip igmp-proxy

パラメータ

- ***upstream-interface-id***：アップストリーム インターフェイス識別子。

デフォルト設定

プロトコルはインターフェイスで無効です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ip igmp-proxy コマンドを使用して、IGMP プロキシ ツリーへのダウンストリーム インターフェイスを追加します。プロキシ ツリーが存在しない場合は、作成されます。

ダウンストリーム インターフェイスを削除するには、このコマンドの **no** 形式を使用します。最後のダウン ストリーム インターフェイスがプロキシ ツリーから削除されると、プロキシ ツリーも削除されます。

例 1。次の例では、vlan 200 をアップストリーム インターフェイスとする、IGMP プロキシ プロセスに、ダウンストリーム インターフェイスを追加します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp-proxy vlan 200
switchxxxxxx(config-if)# exit
```

例 2。次の例では、vlan 200 をアップストリーム インターフェイスとする、IGMP プロキシ プロセスに、ダウンストリーム インターフェイスの範囲を追加します。

```
switchxxxxxx(config)# interface range vlan 100-105
switchxxxxxx(config-if)# ip igmp-proxy vlan 200
switchxxxxxx(config-if)# exit
```

ip igmp-proxy downstream protected

ダウンストリーム インターフェイスから IP マルチキャスト トラフィックの転送を無効にするには、**ip igmp-proxy downstream protected** コマンドをグローバル コンフィギュレーション モードで使用します。ダウンストリームインターフェイスからの転送を許可するには、このコマンドの **no** 形式を使用します。

構文

ip igmp-proxy downstream protected

no ip igmp-proxy downstream protected

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

ダウンストリーム インターフェイスからの転送を許可します。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ip igmp-proxy downstream protected コマンドを使用して、ダウンストリーム インターフェイスからの転送をブロックします。

例

次の例では、ダウンストリーム インターフェイスからの転送を禁止します。

```
switchxxxxxx(config)# ip igmp-proxy downstream protected
```

ip igmp-proxy downstream protected interface

指定したダウンストリーム インターフェイスからの IP マルチキャスト トラフィックの転送を有効または無効にするには、**ip igmp-proxy downstream protected interface** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

ip igmp-proxy downstream protected interface {enabled | disabled}

no ip igmp-proxy downstream protected interface

パラメータ

- **enabled**：インターフェイスでのダウンストリーム インターフェイスの保護が有効です。インターフェイスに到着する IPv4 マルチキャスト トラフィックは転送されません。
- **disabled**：インターフェイスでのダウンストリーム インターフェイスの保護が無効です。インターフェイスに到着する IPv4 マルチキャスト トラフィックは転送されます。

デフォルト設定

グローバル ダウンストリームの保護の設定（**ip igmp-proxy downstream protected** コマンドを参照）

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ip igmp-proxy downstream protected interface disabled コマンドを使用して、指定したダウンストリーム インターフェイスからの転送をブロックします。

ip igmp-proxy downstream protected interface enabled コマンドを使用して、指定したダウンストリーム インターフェイスからの転送を許可します。

このコマンドは、ダウンストリーム インターフェイスに対してのみ設定できます。ダウンストリーム インターフェイスが IGMP プロキシ ツリーから削除されると、設定も削除されます。

例

次の例では、ダウンストリーム インターフェイス vlan 100 からの転送を禁止します。

```
switchxxxxxx(config)# interface vlan100
switchxxxxxx(config-if)# ip igmp-proxy downstream protected interface enabled
switchxxxxxx(config-if)# exit
```

ip igmp-proxy ssm

IP マルチキャスト アドレスの送信元特定マルチキャスト（SSM）範囲を定義するには、**ip igmp-proxy ssm** コマンドをグローバル コンフィギュレーション モードで使用します。SSM 範囲を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip igmp-proxy ssm {**default** | **range** *access-list*}

no ip igmp-proxy ssm

パラメータ

- **default**：232.0.0.0/8 への SSM 範囲のアクセス リストを定義します（rfc4607 を参照）。
- **range** *access-list*：SSM 範囲を定義する標準の IP アクセス リスト名を指定します。

デフォルト設定

このコマンドは無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

新しい **ip igmp-proxy ssm** コマンドは、以前の **ip igmp-proxy ssm** コマンドをオーバーライドします。

定義したすべての範囲を削除するには、**no ip igmp-proxy ssm** コマンドを使用します。

例

次に、アクセス リスト **list1** によって定義された IP アドレスの範囲およびデフォルトの IP アドレスの範囲の SSM サービスを設定する方法の例を示します。

```
switchxxxxxx(config)# ip access-list list1 permit 224.2.151.0/24
switchxxxxxx(config)# ip access-list list1 deny 224.2.152.141
switchxxxxxx(config)# ip access-list list1 permit 224.2.152.0/24
switchxxxxxx(config)# ip igmp-proxy ssm range list1
```

show ip igmp-proxy interface

IGMPプロキシの設定されたインターフェイスに関する情報を表示するには、**show ip igmp-proxy interface** コマンドをユーザ EXEC モードまたは特権 EXEC モードで使用します。

構文

show ip igmp-proxy interface [*interface-id*]

パラメータ

- ***interface-id***：（オプション）インターフェイスに関する IGMP プロキシ情報を表示します。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

show ip igmp-proxy interface コマンドを使用して、IGMP プロキシが有効になっているすべてのインターフェイスを表示するか、指定したインターフェイスのIGMPプロキシ設定を表示します。

例 1。次の例では、IGMP プロキシが有効になっているすべてのインターフェイスの IGMP プロキシ ステータスを表示します。

```
switchxxxxxx# show ip igmp-proxy interface
```

* - the switch is the Querier on the interface

```
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downdtream interfaces protection is disabled
SSM Access List Name:list1
Interface  Type         Interface Protection
 vlan 100  upstream
*vlan 102  downstream   enabled
*vlan 110  downstream   default
 vlan 113  downstream   disabled
```

例 2。次に、指定したアップストリームインターフェイスに対する **show ip igmp-proxy interface** コマンドの出力例を示します。

```
switchxxxxxx# show ip igmp-proxy interface vlan 100
```

* - the switch is the Querier on the interface

```
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downdtream interfaces protection is disabled
```

```
SSM Access List Name:
IP Multicast Tarffic Discarding from Downdtream interfaces is disabled
vlan 100 is a Upstream interface
Downstream interfaces:
 *vlan 102, *vlan 110, vlan 113
```

例 3。次に、指定したダウンストリームインターフェイスに対する **show ip igmp-proxy interface** コマンドの出力例を示します。

```
switchxxxxxx# show ip igmp-proxy interface vlan 102
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downdtream interfaces protection is disabled
vlan 102 is a Downstream interface
The switch is the Querier on vlan 102
Downsteam Interface protection is enabled
SSM Access List Name: default
Upstream interface: vlan 100
```

例 4。次に、IGMP プロキシが無効になっているインターフェイスに対する **show ip igmp-proxy interface** コマンドの出力例を示します。

```
switchxxxxxx# show ip igmp-proxy interface vlan 1
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is disabled
```

IGMP スヌーピング コマンド

この章は、次の項で構成されています。

- ip igmp snooping（グローバル） （584 ページ）
- ip igmp snooping vlan （585 ページ）
- ip igmp snooping vlan mrouter （586 ページ）
- ip igmp snooping vlan mrouter interface （587 ページ）
- ip igmp snooping vlan forbidden mrouter （588 ページ）
- ip igmp snooping vlan static （589 ページ）
- ip igmp snooping vlan multicast-tv （590 ページ）
- ip igmp snooping map cpe vlan （591 ページ）
- ip igmp snooping querier （592 ページ）
- ip igmp snooping vlan querier （593 ページ）
- ip igmp snooping vlan querier address （594 ページ）
- ip igmp snooping vlan querier election （595 ページ）
- ip igmp snooping vlan querier version （596 ページ）
- ip igmp snooping vlan immediate-leave （597 ページ）
- ip igmp snooping map cpe vlan （598 ページ）
- show ip igmp snooping groups （599 ページ）
- show ip igmp snooping interface （600 ページ）
- show ip igmp snooping mrouter （601 ページ）
- show ip igmp snooping multicast-tv （602 ページ）

ip igmp snooping（グローバル）

Internet Group Management Protocol（IGMP）スヌーピングを有効にするには、**ip igmp snooping** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping

no ip igmp snooping

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

例

次に、IGMP スヌーピングを有効にする例を示します。

```
switchxxxxxx(config)# ip igmp snooping
```

ip igmp snooping vlan

特定の VLAN で IGMP スヌーピングを有効にするには、**ip igmp snooping vlan** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

パラメータ

- ***vlan-id***：VLAN を指定します。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

IGMP スヌーピングは、スタティック VLAN 上でのみ有効にできます。

IGMPv1、IGMPv2、および IGMPv3 スヌーピングがサポートされています。

例

```
switchxxxxxx(config)# ip igmp snooping vlan 2
```

ip igmp snooping vlan mrouter

VLAN でマルチキャスト ルータ ポートの自動学習を有効にするには、**ip igmp snooping vlan mrouter** コマンドをグローバル コンフィギュレーション モードで使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

構文

ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**

no ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**

パラメータ

- ***vlan-id***：VLAN を指定します。

デフォルト設定

pim-dvmrp の学習が有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

マルチキャスト ルータ ポートは次の項目に従って学習します。

- ポートで受信したクエリ
- ポートで受信した PIM/PIMv2
- ポートで受信した DVMRP
- ポートで受信した MRDISC

  ポートで受信した MOSPF

VLAN を作成する前に、このコマンドを実行できます。

例

```
switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

ip igmp snooping vlan mrouter interface

マルチキャスト ルータ ポートに接続されたポートを定義するには、**ip igmp snooping mrouter interface** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping vlan *vlan-id* **mrouter interface** i*nterface-list*

no ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-list*

パラメータ

- ***vlan-id***：VLAN を指定します。
- ***interface-list***：インターフェイスのリストを指定します。インターフェイスには、イーサネット ポートまたはポートチャネルのいずれかのタイプを指定できます。

デフォルト設定

ポートは定義されません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

マルチキャストルータ ポートとして定義されているポートでは、すべてのマルチキャストデータとすべての IGMP パケット（レポートおよびクエリー）を受信します。VLAN を作成する前に、このコマンドを実行できます。

例

```
switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter interface gi1/0/1
```

ip igmp snooping vlan forbidden mrouter

スタティック設定または自動学習でポートがマルチキャスト ルータ ポートとして定義されないようにするには、**ip igmp snooping vlan forbidden mrouter** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping vlan *vlan-id* **forbidden mrouter interface** *interface-list*

no ip igmp snooping vlan vlan-id **forbidden mrouter interface** interface-list

パラメータ

- ***vlan-id***：VLAN を指定します。
- ***interface-list***：インターフェイスのリストを指定します。インターフェイスには、イーサネット ポートまたはポートチャネルのいずれかを指定できます。

デフォルト設定

ポートは定義されていません.

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

マルチキャスト ルータ ポートが禁止されたポートにマルチキャスト ルータ ポートを指定できません（つまり、動的に学習したり、静的に割り当てたりすることはできません）。

VLAN を作成する前に、このコマンドを実行できます。

例

```
switchxxxxxx(config)# ip igmp snooping vlan 1 forbidden mrouter interface gi1/0/1
```

ip igmp snooping vlan static

ブリッジ テーブルに IP 層マルチキャスト アドレスを登録して、このアドレスで定義されるグループに静的なポートを追加するには、**ip igmp snooping vlan static** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping vlan *vlan-id* **static** *ip-address* [**interface** *interface-list*]

no ip igmp snooping vlan *vlan-id* **static** *ip-address* [**interface** *interface-list*]

パラメータ

- ***vlan-id***：VLAN を指定します。
- ***ip-address***：IP マルチキャスト アドレスを指定します。
- **interface** *interface-list*：（オプション）インターフェイスのリストを指定します。インターフェイスには、イーサネット ポートまたはポートチャネルのいずれかを指定できます。

デフォルト設定

マルチキャスト アドレスは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

スタティック マルチキャスト アドレスは、スタティック VLAN 上でのみ定義できます。

VLAN を作成する前に、このコマンドを実行できます。

インターフェイスを指定せずにエントリを登録できます。

ポートリストを指定せずに **no** コマンドを使用すると、エントリが削除されます。

例

```
switchxxxxxx(config)# ip igmp snooping vlan 1 static 239.2.2.2 interface gi1/0/1
```

ip igmp snooping vlan multicast-tv

マルチキャスト TV VLAN に関連付けられたマルチキャスト IP アドレスを定義するには、**ip igmp snooping vlan multicast-tv** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping vlan *vlan-id* **multicast-tv** *first-ip-multicast-address* [*last-ip-multicast-address* | {**count** *number*}]

no ip igmp snooping vlan *vlan-id* **multicast-tv** *first-ip-multicast-address* [*last-ip-multicast-address* | {**count** *number*}]

パラメータ

- ***vlan-id***：VLAN を指定します。
- ***first-ip-multicast-address***：範囲の最初のマルチキャスト IP アドレス。
- ***last-ip-multicast-address***：範囲の最後のマルチキャスト IP アドレス。
- **count** *number*：（オプション）複数の連続マルチキャスト IP アドレスを設定します。インターフェイスを指定しない場合、デフォルト値は 1 です。

デフォルト設定

マルチキャスト IP アドレスが関連付けられていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、マルチキャスト TV VLAN 上のマルチキャスト伝送を定義できます。設定に関連するのは、マルチキャスト TV VLAN として設定されている VLAN のメンバーであるアクセス ポートのみです。

このようなアクセス ポートで IGMP メッセージを受信すると、このメッセージがマルチキャスト TV VLAN に関連付けられたマルチキャスト IP アドレスのいずれかのためである場合のみ、マルチキャスト TV VLAN に関連付けられます。

最大 256 の VLAN を設定できます。

例

```
switchxxxxxx(config)# ip igmp snooping vlan 1 multicast-tv 239.2.2.2 count 3
```

ip igmp snooping map cpe vlan

CPE VLAN をマルチキャスト TV VLAN にマップするには、**ip igmp snooping map cpe vlan** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping map cpe vlan *cpe-vlan-id* **multicast-tv vlan** *vlan-id*

no ip igmp snooping map cpe vlan *vlan-id*

パラメータ

- ***cpe-vlan-id***：CPE VLAN ID を指定します。
- **vlan-id**：マルチキャスト TV VLAN ID を指定します。

デフォルト設定

マッピングが存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、CPE VLAN とマルチキャスト TV VLAN を関連付けられます。

CPE VLAN のタグ付き顧客ポートで IGMP メッセージを受信し、この CPE VLAN をマルチキャスト TV VLAN にマッピングした場合、IGMP メッセージはマルチキャスト TV VLAN に関連付けられます。

例

次の例では、CPE VLAN 2 をマルチキャスト TV VLAN 31 にマッピングします。

```
switchxxxxxx(config)# ip igmp snooping map cpe vlan 2 multicast-tv vlan 31
```

ip igmp snooping querier

IGMP スヌーピング クエリアをグローバルに有効にするには、**ip igmp snooping querier** コマンドをグローバル コンフィギュレーション モードで使用します。IGMP スヌーピング クエリアをグローバルに無効にするには、このコマンドの **no** 形式を使用します。

構文

ip igmp snooping querier

no ip igmp snooping querier

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

VLAN で IGMP スヌーピング クエリアを実行するには、VLAN 上でグローバルに有効にします。

例

次の例では、IGMP スヌーピング クエリアをグローバルに無効にしています。

```
switchxxxxxx(config)# no ip igmp snooping querier
```

ip igmp snooping vlan querier

特定の VLAN 上で IGMP スヌーピング クエリアを有効にするには、**ip igmp snooping vlan querier** コマンドをグローバル コンフィギュレーション モードで使用します。VLAN インターフェイスで IGMP スヌーピング クエリアを無効にするには、このコマンドの **no** 形式を使用します。

構文

ip igmp snooping vlan *vlan-id* **querier**

no ip igmp snooping vlan *vlan-id* **querier**

パラメータ

- ***vlan-id***：VLAN を指定します。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

IGMP スヌーピング クエリアは、その VLAN に IGMP スヌーピングが有効になっている場合にのみ、VLAN 上で有効にできます。

例

次の例では、VLAN 1 上で IGMP スヌーピング クエリアを有効にしています。

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier
```

ip igmp snooping vlan querier address

IGMP スヌーピング クエリアで使用される送信元 IP アドレスを定義するには、**ip igmp snooping vlan querier address** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping vlan *vlan-id* **querier address** *ip-address*

no ip igmp snooping vlan *vlan-id* **querier address**

パラメータ

- ***vlan-id***：VLAN を指定します。
- ***ip-address***：IP アドレスを指定します。

デフォルト設定

VLAN の IP アドレスが設定されている場合は、IGMP スヌーピング クエリアの送信元アドレスとして使用されます。複数の IP アドレスがある場合は、VLAN で定義されている最低限の IP アドレスが使用されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドで IP アドレスが設定されておらず、クエリアの VLAN の IP アドレスが設定されていない場合、クエリアは無効です。

例

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier address 10.5.234.205
```

ip igmp snooping vlan querier election

特定の VLAN 上で IGMP スヌーピング クエリア選択メカニズムを有効にするには、**ip igmp snooping vlan querier election** コマンドをグローバル コンフィギュレーション モードで使用します。クエリア選択メカニズムを無効にするには、このコマンドの **no** 形式を使用します。

構文

ip igmp snooping vlan *vlan-id* **querier election**

no ip igmp snooping vlan *vlan-id* **querier election**

パラメータ

- ***vlan-id***：VLAN を指定します。

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ip igmp snooping vlan querier election コマンドの **no** 形式を使用すると、VLAN で IGMP クエリア選択メカニズムを無効にできます。IGMP クエリア選定メカニズムが有効の場合、IGMP スヌーピング クエリアは RFC2236 と RFC3376 で指定された標準的な IGMP クエリア選定メカニズムをサポートします。IGMP クエリア選定メカニズムが無効の場合、IGMP スヌーピング クエリアは有効になってから 60 秒間、一般的なクエリー メッセージの送信を遅らせます。このときにスイッチが別クエリアから IGMP クエリーを受信しなかった場合は、一般的なクエリー メッセージの送信を開始します。スイッチがクエリアとして動作する場合、VLAN で別のクエリアが検出されると、一般的なクエリー メッセージの送信を停止します。この場合、スイッチが次の式に等しいクエリー パッシブ間隔で別のクエリアを受信すると、一般的なクエリー メッセージの送信を再開します

<堅牢性>*<クエリー間隔> + 0.5*<クエリー応答間隔>。

VLAN に IPM マルチキャスト ルータがある場合は、IGMP クエリア選定メカニズムを無効にすることをお勧めします。

例

次の例では、VLAN 1 で IGMP スヌーピング クエリア選定を無効にしています。

```
switchxxxxxx(config)# no ip igmp snooping vlan 1 querier election
```

ip igmp snooping vlan querier version

特定の VLAN で IGMP スヌーピング クエリアの IGMP バージョンを設定するには、**ip igmp snooping vlan querier version** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping vlan *vlan-id* **querier version** {**2** | **3**}

no ip igmp snooping vlan *vlan-id* **querier version**

パラメータ

- ***vlan-id***：VLAN を指定します。
- **querier version 2**：IGMP バージョンが IGMPv2 になることを指定します。
- **querier version 3**：IGMP バージョンが IGMPv3 になることを指定します。

デフォルト設定

IGMPv2.

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、IGMP スヌーピング クエリア VLAN 1 ～ 3 のバージョンを設定しています。

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier version 3
```

ip igmp snooping vlan immediate-leave

VLAN で IGMP スヌーピング即時脱退処理を有効にするには、**ip igmp snooping vlan immediate-leave** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

パラメータ

- ***vlan-id***：VLAN ID 値を指定します。（範囲：1 ～ 4094）。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

VLAN を作成する前に、このコマンドを実行できます。

例

次の例では、VLAN 1 で IGMP スヌーピング即時脱退機能を有効にしています。

```
switchxxxxxx(config)# ip igmp snooping vlan 1 immediate-leave
```

ip igmp snooping map cpe vlan

CPE VLAN をマルチキャスト TV VLAN にマップするには、**ip igmp snooping map cpe vlan** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ip igmp snooping map cpe vlan *cpe-vlan-id* **multicast-tv vlan** *vlan-id*

no ip igmp snooping map cpe vlan *vlan-id*

パラメータ

- ***cpe-vlan-id***：CPE VLAN ID を指定します。
- **vlan-id**：マルチキャスト TV VLAN ID を指定します。

デフォルト設定

マッピングが存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、CPE VLAN とマルチキャスト TV VLAN を関連付けられます。

CPE VLAN のタグ付き顧客ポートで IGMP メッセージを受信し、この CPE VLAN をマルチキャスト TV VLAN にマッピングした場合、IGMP メッセージはマルチキャスト TV VLAN に関連付けられます。

例

次の例では、CPE VLAN 2 をマルチキャスト TV VLAN 31 にマッピングします。

```
switchxxxxxx(config)# ip igmp snooping map cpe vlan 2 multicast-tv vlan 31
```

show ip igmp snooping groups

IGMP スヌーピングで学習したマルチキャスト グループを表示するには、**show ip igmp snooping groups** コマンドをユーザ EXEC モードで使用します。

構文

show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*] [**source** *ip-address*]

パラメータ

- **vlan** *vlan-id*：（オプション）VLAN ID を指定します。
- **ip-multicast-address** *ip-multicast-address*：（オプション）IP マルチキャストアドレスを指定します。
- **ip-address** *ip-address*：（オプション）IP 送信元アドレスを指定します。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

IGMP スヌーピングで学習したすべてのマルチキャスト グループを確認するには、**show ip igmp snooping groups** コマンドをパラメータを指定せずに使用します。

show ip igmp snooping groups コマンドをパラメータを指定して使用すると、IGMP スヌーピングで学習したすべてのマルチキャスト グループの必要なサブセットが表示されます

例

次の例では、サンプル出力をいくつか示します。

```
switchxxxxxx# show ip igmp snooping groups vlan 1
```

```
switchxxxxxx# show ip igmp snooping groups

Vlan  Group            Source       Include Ports    Exclude Ports  Comp-Mode
----  Address          Address      ---------        --------       ---------
1     ---------------  ----------   gi1/0/1                         v2
      239.255.255.250  *
```

show ip igmp snooping interface

特定の VLAN で IGMP スヌーピング設定を表示するには、**show ip igmp snooping interface** コマンドをユーザ EXEC モードで使用します。

構文

show ip igmp snooping interface *vlan-id*

パラメータ

- ***vlan-id***：VLAN ID を指定します。

コマンド モード

ユーザ EXEC モード

例

次の例では、VLAN 1000 上の IGMP スヌーピング設定を表示します

```
switchxxxxxx# show ip igmp snooping interface 1000
IGMP Snooping is globally enabled
IGMP Snooping Querier is globally enabled
VLAN 1000
IGMP Snooping is enabled
IGMP snooping last immediate leave: enable
Automatic learning of Multicast router ports is enabled
IGMP Snooping Querier is enabled
IGMP Snooping Querier operation state: is not running
IGMP Snooping Querier version: 2
IGMP Snooping Querier election is enabled
IGMP Snooping Querier address: 194.12.10.166
IGMP snooping robustness: admin 2  oper 2
IGMP snooping query interval: admin 125 sec oper 125 sec
IGMP snooping query maximum response: admin 10 sec oper 10 sec
IGMP snooping last member query counter: admin 2 oper 2
IGMP snooping last member query interval: admin 1000 msec oper 500 msec
IGMP Snooping interface active Querier address: 194.12.100.100 (remote)
Groups that are in IGMP version 1 compatibility mode:
231.2.2.3, 231.2.2.3
```

show ip igmp snooping mrouter

すべての VLAN または特定の VLAN で動的に学習したマルチキャスト ルータ インターフェイスの情報を表示するには、**show ip igmp snooping mrouter** コマンドをユーザ EXEC モードで使用します。

構文

show ip igmp snooping mrouter [**interface** *vlan-id*]

パラメータ

- **interface** *vlan-id*：（オプション）VLAN ID を指定します。

コマンド モード

ユーザ EXEC モード

例

次の例では、VLAN 1000 で動的に学習したマルチキャスト ルータ インターフェイスの情報を表示します。

```
switchxxxxxx# show ip igmp snooping mrouter interface 1000
```

VLAN	Dynamic	Static	Forbidden
----	---------	---------	----------
1000	gi1/0/1	gi1/0/2	gi1/0/3 ～ 4

show ip igmp snooping multicast-tv

マルチキャスト TV VLAN に関連付けられた IP アドレスを表示するには、**show ip igmp snooping multicast-tv** コマンドをユーザ EXEC モードで使用します。

構文

show ip igmp snooping multicast-tv [**vlan** *vlan-id*]

パラメータ

- **vlan** *vlan-id*：（オプション）VLAN ID を指定します。

コマンド モード

ユーザ EXEC モード

例

次の例では、すべてのマルチキャスト TV VLAN に関連付けられた IP アドレスを表示します。

```
switchxxxxxx# show ip igmp snooping multicast-tv
VLAN First IP Address Last IP Address
---- ---------------- ---------------
1000 238.2.5.5 238.2.5.5
1000 239.255.0.0 239.255.1.1
1010 232.0.0.0 239.0.0.255
1010 239.0.1.2 239.255.4.5
```

IP アドレッシング コマンド

この章は、次の項で構成されています。

- ip address （604 ページ）
- ip address dhcp （606 ページ）
- renew dhcp （607 ページ）
- ip default-gateway （608 ページ）
- show ip interface （609 ページ）
- arp （610 ページ）
- arp timeout（グローバル） （611 ページ）
- ip arp proxy disable （612 ページ）
- ip proxy-arp （613 ページ）
- clear arp-cache （614 ページ）
- show arp （615 ページ）
- show arp configuration （616 ページ）
- interface ip （617 ページ）
- ip helper-address （618 ページ）
- show ip helper-address （620 ページ）
- show ip dhcp client interface （621 ページ）

ip address

ip address インターフェイス コンフィギュレーション（イーサネット、VLAN、ポート チャネル）モード コマンドを使用すると、インターフェイスの IP アドレスを定義できます。IP アドレスの定義を削除するには、このコマンドの **no** 形式を使用します。

構文

Bluetooth インターフェイス

ip address *ip-address* {*mask* | */prefix-length*}

no ip address

インバンド インターフェイス：

ip address *ip-address* {*mask* | */prefix-length*}

no ip address [*ip-address*]

パラメータ

- ***ip-address***：IP アドレスを指定します。
- ***mask***：IP アドレスのネットワーク マスクを指定します。
- ***prefix-length***：IP アドレス プレフィックスを構成するビットの数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。（範囲：8 ～ 30）

デフォルト設定

IP アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス（イーサネット、ポートチャネル、Bluetooth）コンフィギュレーション モード

使用上のガイドライン

ip address コマンドを使用して、インターフェイスにスタティック IP アドレスを定義します。

インバンド インターフェイス

複数の IP アドレスがサポートされます。新しく定義した IP アドレスはインターフェイスに追加されます。

インターフェイスでスタティック IP アドレスを定義すると、インターフェイスで実行されている DHCP クライアントが停止し、DHCP クライアントによって割り当てられた IP アドレスが削除されます。

設定済み IP アドレスが別の設定済みアドレスと重複する場合は、警告メッセージが表示されます。既存の IP アドレスを変更するには、既存のアドレスを削除し、新しいアドレスを追加します。

DHCP クライアントまたは手動で IP アドレスを割り当てていない場合は、IP アドレス 192.168.1.254 がデフォルトの VLAN に割り当てられます。

Bluetooth インターフェイス

1 つの IP アドレスがサポートされています。Bluetooth インターフェイスで定義した新しい IP アドレスは、以前に定義した IP アドレスを上書きします。Bluetooth インターフェイスに設定されている IP アドレスを、インバンドインターフェイスに設定されているアドレスと同じサブネット上に置くことはできません。Bluetooth インターフェイスの IP アドレスは、ルーティング機能をサポートしていません。

例 1。次の例では、IP アドレス 131.108.1.27 とサブネットマスク 255.255.255.0 で VLAN 1 を設定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 131.108.1.27 255.255.255.0
```

例 2。次の例では、3 つの重複した IP アドレスを設定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 1.1.1.1 255.0.0.0
switchxxxxxx(config)# exit
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ip address 1.2.1.1 255.255.0.0
switchxxxxxx(config)# This IP address overlaps IP address 1.1.1.1/8 on vlan1, are you
sure? [Y/N]Y
switchxxxxxx(config)# exit
switchxxxxxx(config)# interface vlan 3
switchxxxxxx(config-if)# ip address 1.3.1.1 255.255.0.0
switchxxxxxx(config)# This IP address overlaps IP address 1.1.1.1/8 on vlan1, are you
sure? [Y/N]Y
switchxxxxxx(config)# exit
```

ip address dhcp

p address dhcp インターフェイス コンフィギュレーション（イーサネット、VLAN、ポート チャネル）モード コマンドを使用すると、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバからイーサネット インターフェイスの IP アドレスを取得できます。このコマンドで **no** を使用すると、取得した IP アドレスを解放できます。

構文

ip address dhcp

no ip address dhcp

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ip address dhcp コマンドを使用して、インターフェイスで DHCP クライアントを有効にします。

ip address dhcp コマンドは、インターフェイスに手動で設定されているすべてのアドレスを削除します。

DHCP ルータオプション（オプション 3）で受信したデフォルトルート（デフォルトゲートウェイ）は、インバンドインターフェイスには 8、OOB には 6 のメトリックが割り当てられます。

このコマンドで **no** を使用すると、インターフェイスで DHCP クライアントを無効にできます。

例

次の例では、DHCP から VLAN 100 の IP アドレスを取得します。

```
switchxxxxxx(config)# interface vlan100
switchxxxxxx(config-if)# ip address dhcp
```

renew dhcp

renew dhcp 特権 EXEC モード コマンドを使用すると、特定のインターフェイスの DHCP サーバから取得した IP アドレスを更新できます。

構文

renew dhcp *interface-id* **[force-autoconfig**]

パラメータ

- ***interface-id***：インターフェイスを指定します。
- **force-autoconfig**：DHCP サーバが割り当てられた IP アドレスの DHCP オプション 67 レコードを保持している場合、レコードは既存のデバイス設定を上書きします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

renew dhcp コマンドを使用して、インターフェイスで DHCP アドレスを更新します。

このコマンドでは、インターフェイスでの DHCP クライアントは有効になりません。DHCP クライアントがインターフェイスで有効でない場合、コマンドはエラーメッセージを返します。

例

次の例では、DHCP サーバから取得された VLAN 19 で IP アドレスを更新します。

```
switchxxxxxx# renew dhcp vlan 19
```

ip default-gateway

ip default-gateway グローバル コンフィギュレーション モード コマンドは、デフォルト ゲートウェイ（デバイス）を定義します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ip default-gateway *ip-address*

no ip default-gateway [***ip-address***]

パラメータ

- ***ip-address***：デフォルト ゲートウェイの IP アドレスを指定します。

コマンド モード

グローバル コンフィギュレーション モード

デフォルト設定

デフォルト ゲートウェイは定義されていません。

使用上のガイドライン

ip default-gateway コマンドを使用すると、デフォルト ゲートウェイ（デフォルト ルート）を定義できます。

ip default-gateway コマンドは、インバンドインターフェイスで接続されているゲートウェイでは4、OOB で接続されているゲートウェイでは2のメトリックを使用して、デフォルトルートを追加します。

no ip default-gateway *ip-address* コマンドを使用すると、デフォルト ゲートウェイを 1 つ削除できます。

no ip default-gateway コマンドを使用すると、すべてのデフォルト ゲートウェイを削除できます。

例

次の例では、デフォルト ゲートウェイ 192.168.1.1 を定義しています。

```
switchxxxxxx(config)# ip default-gateway 192.168.1.1
```

show ip interface

show ip interface EXEC モード コマンドを使用すると、設定した IP インターフェイスの利便性の状態を表示できます。

構文

show ip interface [i*nterface-id*]

パラメータ

- ***interface-id***：IP アドレスを定義するインターフェイス ID を指定します。

デフォルト設定

すべての IP アドレス。

コマンド モード

ユーザ EXEC モード

例 1 - 次の例では、設定されているすべての IP アドレスとそのタイプを表示します。

```
switchxxxxxx# show ip interface

IP Address       I/F     I/F Status  Type   Directed   Redirect  Status
                          admin/oper        Broadcast
-------------    ------  ----------- ------- --------  --------- -----
10.5.230.232/24  vlan 1  UP/UP       Static  disable   Enabled   Valid
10.5.234.202/24 vlan 4 UP/DOWN Static disable Disabled Valid
10.5.240.200/24 oob UP/UP Static Valid
```

例 2：次の例では、特定の L2 インターフェイスに設定されている IP アドレスとそのタイプを表示します。

```
switchxxxxxx# show ip interface vlan 1

IP Address       I/F     I/F Status  Type   Directed   Redirect  Status
                          admin/oper        Broadcast
-------------    ------  ----------- ------- --------  --------- -----
10.5.230.232/24  vlan 1  UP/UP       Static  disable   Enabled   Valid
```

arp

arp グローバル コンフィギュレーション モード コマンドを使用すると、アドレス解決プロトコル（ARP）キャッシュに固定エントリを追加できます。このコマンドで **no** 形式を使用すると、ARP キャッシュからエントリを削除できます。

構文

arp *ip-address mac-address* **[***interface-id***]**

no arp *ip-address*

パラメータ

- ***ip-address***：指定した MAC アドレスにマップする IP アドレスまたは IP エイリアス。
- ***mac-address***：指定された IP アドレスまたは IP エイリアスにマップされる MAC アドレス。
- ***interface-id***：アドレス ペアが指定したインターフェイスに追加されます。

コマンド モード

グローバル コンフィギュレーション モード

デフォルト設定

固定エントリは定義されません。

インターフェイス ID が入力されていない場合、アドレス ペアはすべてのインターフェイスに関連します。

使用上のガイドライン

ソフトウェアは ARP キャッシュ エントリを使用して 32 ビット IP アドレスを 48 ビット ハードウェア アドレス（MAC）に変換します。多くのホストはダイナミック アドレス解決をサポートしているため、通常はスタティック ARP キャッシュ エントリを指定する必要はありません。

例

次の例では、IP アドレス 198.133.219.232 と MAC アドレス 00:00:0c:40:0f:bc を ARP テーブルに追加します。

```
switchxxxxxx(config)# arp 198.133.219.232 00:00:0c:40:0f:bc vlan100
```

arp timeout（グローバル）

arp timeout グローバル コンフィギュレーション モード コマンドを使用すると、エントリがARPキャッシュに残っているときの間隔を設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

arp timeout *seconds*

no arp timeout

パラメータ

- ***seconds***：エントリがARPキャッシュに残っているときの間隔を（秒単位で）指定します。（範囲：1 ～ 40000000）。

デフォルト設定

デフォルトの ARP タイムアウトは、IP ルーティングが有効になっている場合は 60000 秒、IP ルーティングが無効になっている場合は、300 秒です。

コマンド モード

グローバル コンフィギュレーション モード

例

次に、ARP タイムアウトを 12000 秒に設定する例を示します。

```
switchxxxxxx(config)# arp timeout 12000
```

ip arp proxy disable

ip arp proxy disable グローバル コンフィギュレーション モード コマンドを使用すると、プロキシのアドレス解決プロトコル（ARP）をグローバルに無効にできます。このコマンドで **no** 形式を使用すると、プロキシの ARP をもう一度有効にできます。

構文

ip arp proxy disable

no ip arp proxy disable

デフォルト

デフォルトでは、無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、プロキシ ARP のインターフェイス設定を上書きします。

このコマンドは IP ルーティングが有効な場合にのみサポートされます。

例

次の例では、ARP プロキシをグローバルに無効にします。

```
switchxxxxxx(config)# ip arp proxy disable
```

ip proxy-arp

ip proxy-arp インターフェイス コンフィギュレーション モード コマンドを使用すると、特定のインターフェイスで ARP プロキシを有効にできます。このコマンドで **no** 形式を使用すると、プロキシを無効にできます。

構文

ip proxy-arp

no ip proxy-arp

デフォルト設定

ARP プロキシが有効になっています。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

この設定は、少なくとも 1 つの IP アドレスが、特定のインターフェイス上で定義されている場合にのみ適用できます。

このコマンドは IP ルーティングが有効な場合にのみサポートされます。

例

次に、スイッチがルータ モードのときに ARP プロキシを有効にする例を示します。

```
switchxxxxxx(config-if)# ip proxy-arp
```

clear arp-cache

clear arp-cache 特権 EXEC モード コマンドを使用すると、ARP キャッシュからすべてのダイナミック エントリを削除できます。

構文

clear arp-cache

コマンド モード

特権 EXEC モード

例

次の例では、ARP キャッシュからすべてのダイナミック エントリを削除します。

```
switchxxxxxx# clear arp-cache
```

show arp

show arp 特権 EXEC モード コマンドを使用すると、ARP テーブルのエントリを表示できます。

構文

show arp *[***ip-address** *ip-address] [***mac-address** *mac-address] [interface-id]*

パラメータ

- **ip-address** *ip-address*：IP アドレスを指定します。
- **mac-address** *mac-address*：MAC アドレスを指定します。
- ***interface-id***：インターフェイス ID を指定します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

FDB テーブルの MAC アドレスに関連付けられているインターフェイスが期限切れになるため、インターフェイス フィールドを空にできます。

ARP エントリがポートまたはポートチャネルで定義されている IP インターフェイスに関連付けられている場合、VLAN フィールドは空です。

例

次の例では、ARP テーブル内のエントリを表示します。

```
switchxxxxxx# show arp
ARP timeout: 80000 Seconds

VLAN      Interface          IP Address    HW Address          Status
-------   ---------------    ----------    -----------------   -------
VLAN 1    gi1/0/1            10.7.1.102    00:10:B5:04:DB:4B   Dynamic
VLAN 1    gi1/0/2            10.7.1.135    00:50:22:00:2A:A4   Static
VLAN 2    gi1/0/1            11.7.1.135    00:12:22:00:2A:A4   Dynamic
          gi1/0/2            12.10.1.13    00:11:55:04:DB:4B   Dynamic
```

show arp configuration

show arp configuration 特権 EXEC コマンドを使用すると、ARP プロトコルのグローバルおよびインターフェイス設定を表示できます。

構文

show arp configuration

パラメータ

このコマンドには、引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# show arp configuration
Global configuration:
 ARP Proxy: enabled
 ARP timeout:    80000 Seconds
Interface configuration:
VLAN 1:
 ARP Proxy: disabled
 ARP timeout:60000 Seconds
VLAN 10:
 ARP Proxy: enabled
 ARP timeout: 70000 Seconds
VLAN 20:
 ARP Proxy: enabled
 ARP timeout: 80000 Second (Global)
```

interface ip

interface ip グローバル コンフィギュレーション モード コマンドを使用すると、IP インターフェイス コンフィギュレーション モードを入力できます。

構文

interface ip *ip-address*

パラメータ

- ***ip-address***：デバイスの IP アドレスの 1 つを指定します。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、IP インターフェイス コンフィギュレーション モードを入力します。

```
switchxxxxxx(config)# interface ip 192.168.1.1
switchxxxxxx(config-ip)#
```

ip helper-address

ip helper-address グローバル コンフィギュレーション モード コマンドを使用すると、インターフェイスで受信した UDP ブロードキャスト パケットを特定の（ヘルパー）アドレスを転送できます。このコマンドで **no** 形式を使用すると、特定の（ヘルパー）アドレスへのブロードキャスト パケットの転送を無効にできます。

構文

ip helper-address {*ip-interface* | all} *address* [*udp-port-list*]

no ip helper-address {*ip-interface* | all} *address*

パラメータ

- ***ip-interface***：IP インターフェイスを指定します。
- **all**：すべての IP インターフェイスを指定します。
- ***address***：UDP ブロードキャスト パケットの転送先である宛先ブロードキャストまたはホスト アドレスを指定します。値を 0.0.0.0 に指定すると、UDP ブロードキャスト パケットがホストに転送されません。
- ***udp-port-list***：ブロードキャストパケットの転送先である宛先 UDP ポート番号を指定します（範囲：1 ～ 59999）。これはスペースで区切られたポート番号のリストです。

デフォルト設定

インターフェイスで受信した UDP ブロードキャスト パケットを特定の（ヘルパー）アドレスに転送できません。

udp-port-list が指定されていない場合は、デフォルト サービスのパケットがヘルパー アドレスに転送されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、UDP ブロードキャスト パケットの転送先 UDP ポート番号を指定することにより、UDP ブロードキャスト パケットを、あるインターフェイスから別のインターフェイスへ転送します。デフォルトでは、UDP ポート番号が指定されていない場合、デバイスは次の 6 個のサービスの UDP ブロードキャスト パケットを転送します。

- IEN-116 ネーム サービス（ポート 42）
- DNS（ポート 53）
- NetBIOS ネーム サーバ（ポート 137）

- NetBIOS データグラム サーバ（ポート 138）
- TACACS サーバ（ポート 49）
- タイム サービス（ポート 37）

多くのヘルパーアドレスを定義できます。ただし、デバイスのアドレスとポートのペアの合計数は 128 に制限されています。

特定のインターフェイスに対するヘルパーアドレスの設定は、すべてのインターフェイスに対するヘルパー アドレスの設定より優先されます。

このコマンドを使用しても、BOOTP/DHCP（ポート 67、68）を転送することはできません。BOOTP/DHCP パケットをリレーするには、DHCP リレー コマンドを使用します。

ip-interface 引数を OOB ポートにすることはできません。

例

次の例では、すべてのインターフェイスで受信した UDP ブロードキャスト パケットを宛先 IP アドレスの UDP ポートおよび UDP ポート 1 と 2 に転送できます。

```
switchxxxxxx(config)# ip helper-address all 172.16.9.9 49 53 1 2
```

show ip helper-address

show ip helper-address 特権 EXEC モード コマンドを使用すると、システムの IP ヘルパー アドレス設定を表示できます。

構文

show ip helper-address

パラメータ

このコマンドには、引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

例

次の例では、システムの IP ヘルパー アドレス設定が表示されます。

```
switchxxxxxx# show ip

Interface            Helper Address       UDP Ports
------------         --------------       -------------------------
192.168.1.1          172.16.8.8           37, 42, 49, 53, 137, 138
192.168.2.1          172.16.9.9           37, 49
```

show ip dhcp client interface

show ip dhcp client interface コマンドをユーザ EXEC または特権 EXEC モードで使用すると、DHCP クライアント インターフェイス情報を表示できます。

構文

show ip dhcp client interface [*interface-id*]

パラメータ

- ***interface-id***：インターフェイス識別子。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

インターフェイスが指定されていない場合は、DHCPクライアントが有効になっているすべてのインターフェイスが表示されます。インターフェイスが指定される場合、指定されているインターフェイスに関する情報だけが表示されます。

例

次に、**show ip dhcp client interface** コマンドの出力例を示します。

```
switchxxxxxx# show ip dhcp client interface
VLAN 100 is in client mode
Address: 170.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
Default Gateway: 170.10.100.1
DNS Servers: 115.1.1.1, 87.12.34.20
DNS Domain Search List: company.com
Host Name: switch_floor7
Configuration Server Addresses: 192.1.1.1 202.1.1.1
Configuration Path Name: qqq/config/aaa_config.dat
Image Path Name: qqq/image/aaa_image.ros
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
VLAN 1200 is in client mode
Address: 180.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
Default Gateway: 180.10.100.1
DNS Servers: 115.1.1.1, 87.12.34.20
DNS Domain Search List: company.com
Host Name: switch_floor7
Configuration Server Addresses: configuration.company.com
Configuration Path Name: qqq/config/aaa_config.dat
Image Path Name: qqq/image/aaa_image.ros
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
Option 43: 5A1N;K4;B3;IFE80::2E0:81FF:FE2D:3799;J6088
```

IP ルーティング プロトコル独立型コマンド

この章は、次の項で構成されています。

- accept-lifetime （624 ページ）
- directed-broadcast （626 ページ）
- ip policy route-map （627 ページ）
- ip redirects （629 ページ）
- ip route （630 ページ）
- ip routing （632 ページ）
- key-string （633 ページ）
- key（キーチェーン） （634 ページ）
- key chain （636 ページ）
- send-lifetime （638 ページ）
- show ip protocols （640 ページ）
- show ip route （641 ページ）
- show ip route summary （645 ページ）
- show key chain （646 ページ）

accept-lifetime

キーチェーンの認証キーが有効なキーとして受信される期間を設定するには、キーチェーン キー コンフィギュレーション モードで **accept-lifetime** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

accept-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no accept-lifetime

パラメータ

- ***start-time***：key コマンドで指定したキーが受信できる開始時刻です。構文は次のいずれかにすることができます。
  - *hh*:*mm*:*ss Month date year*
  - *hh*:*mm*:*ss date Month year*
  - *hh*：時間（0 ～ 23）
  - *mm*：分（0 ～ 59）
  - *ss*：秒（0 ～ 59）
  - *Month*：月の最初の 3 文字
  - date：日（1 ～ 31）
  - year：年（4 桁）

許容される年の範囲は 2020 ～ 2037 年で、デフォルトの開始時刻および許容される最も早い日付は、許容される最初の年の 1 月 1 日です。

- **infinite**：キーは *start-time* 値以降、受信可能です。
- ***end-time***：キーは、*start-time* 値から *end-time* 値まで、受信可能です。構文は、*start-time* 値と同じです。*end-time* 値は *start-time* 値の後である必要があります。デフォルトの終了時刻は無限の期間です。
- **duration** *seconds*：キーが受信可能な時間の長さ（秒単位）。値の範囲は 1 ～ 2147483646 です。

デフォルト設定

認証キーが着信パケットを認証できるデフォルトの期間は**Forever**に設定されます。

Foreverの定義：開始時刻は 2000 年 1 月 1 日、終了時刻は無期限です。

コマンド モード

キー チェーン キー コンフィギュレーション モード

使用上のガイドライン

Time-of-Date のデフォルト値は常に過去の時間のため、**Time-of-Date** が管理または SNTP で設定されていないことに関係なく、スイッチは再度 **Time-of-Date** と *start-time* 引数の値をチェックします。

start-time 引数の値の検証に成功し、*end-time* 引数が設定され、その値が **infinite** の場合、**Time-of-Date** が管理または SNTP によって設定されていないことに関係なく、キーは有効と見なされます。

Time-of-Date が管理または SNTP によって設定されておらず、*end-time* 引数が **infinite** または **duration** パラメータと異なる値で設定されている場合、キーは期限切れと見なされます。

Time-of-Date が管理または SNTP によって設定されている場合、スイッチは再度 **Time-of-Date** と、*end-time* 引数または **duration** パラメータの値をチェックします。

最後のキーの期限が切れると、認証はエラーで終了します。

例

次の例では、keychain1 という名前のキー チェーンが設定されます。string1 という名前のキーが午後 1 時 30 分から午後 3 時 30 分まで承認され、午後 2 時 00 分から午後 3 時 00 分まで送信されます。string2 という名前のキーが午後 2 時 30 分から午後 4 時 30 分まで承認され、午後 3 時 00 分から午後 4 時 00 分まで送信されます。ルータの設定時間内でのキーの移行または不一致に対して重複が許されます。時間の違いを処理するために、各側に 30 分間の余裕があります。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)#  ip rip authentication key-chain keychain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# key chain keychain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string string1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string string2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
```

directed-broadcast

directed-broadcast IP インターフェイス コンフィギュレーション モード コマンドを使用して、物理ブロードキャストにダイレクト ブロードキャストの変換を有効にします。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

directed-broadcast

no directed-broadcast

デフォルト設定

物理ブロードキャストへのダイレクト ブロードキャストの変換が無効です。すべての IP ダイレクト ブロードキャストがドロップされます。

コマンド モード

IP コンフィギュレーション モード

例

次の例では、ダイレクト ブロードキャストの物理ブロードキャストへの変換を有効にします。

```
switchxxxxxx(config)# interface ip 192.168.1.1
switchxxxxxx(config-ip)# directed-broadcast
```

ip policy route-map

インターフェイスでポリシールーティングを有効にし、ルートマップを識別するには、インターフェイス コンフィギュレーション モードで **ip policy route-map** コマンドを使用します。ポリシールーティングを無効にするには、このコマンドの **no** 形式を使用します。

構文

ip policy route-map *map-tag*

no ip policy route-map

パラメータ

- ***map-tag***：ポリシールーティングに使用するルートマップの名前。

デフォルト設定

インターフェイスでポリシールーティングは実行されません。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

インターフェイスでポリシールーティングを有効にするには、**ip policy route-map** コマンドを使用します。実際のポリシールーティングは、IPアドレスがインターフェイスで定義されている場合に実行されます。

map-tag 名を持つルートマップで指定されたルートマップ条件に一致する IP パケットは、一致した ACL のアクションに応じてルートを取得します。

- **permit**：set コマンドのポリシールーティングで指定されたルート。
- **deny**：IP 転送テーブルで指定されたルート（通常のルーティング）。
- ポリシールーティングに使用するルートマップの名前。

一致しない IP パケットは、明らかな最短パスを使用して転送されます。

レイヤ2インターフェイスでのIPポリシールーティングは、IPインターフェイスが定義され、そのステータスが UP で、ネクストホップが到達可能である場合にのみ実行されます。IP ポリシールーティングが適用されていない場合、一致した IP パケットは明らかな最短パスを使用して転送されます。

注。当然ながら、通常の IP ルーティング ポリシー ベースの IP ルータは、MAC「tome」IP フレームのみをルーティングします。IPポリシールーティングは、インターフェイスで次の機能とともに設定できません。

- VLAN ACL

例

次に、ポリシールーティングを設定する例を示します。

```
switchxxxxxx(config)# ip access-list extended pr-acl1
switchxxxxxx(config-ip-al)# permit tcp any any 156.12.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# ip access-list extended pr-acl2
switchxxxxxx(config-ip-al)# permit tcp any any 156.122.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr 10
switchxxxxxx(config-route-map)# match ip address access-list pr-acl1
switchxxxxxx(config-route-map)# set ip next-hop 56.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# route-map pbr 20
switchxxxxxx(config-route-map)# match ip address access-list pr-acl2
switchxxxxxx(config-route-map)# set ip next-hop 50.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip policy route-map pbr
switchxxxxxx(config-if)# exit
```

ip redirects

ip redirects コマンドを IP インターフェイス コンフィギュレーション モードで使用すると、ICMP リダイレクト メッセージを送信し、受信したパケットと同じインターフェイスを介してパケットを再送信できます。リダイレクト メッセージの送信を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip redirects

no ip redirects

デフォルト設定

ICMP リダイレクト メッセージの送信が有効になっています。

コマンド モード

IP コンフィギュレーション モード

例

次の例では、IP インターフェイス 1.1.1.1 で ICMP リダイレクト メッセージの送信を無効にし、IP インターフェイス 2.2.2.2 でメッセージを再度有効にします。

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# no ip redirects
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 2.2.2.2
switchxxxxxx(config-ip)# ip redirects
switchxxxxxx(config-ip)# exit
```

ip route

スタティック ルートを確立するには、**ip route** コマンドをグローバル コンフィギュレーション モードで使用します。スタティック ルートを削除するには、このコマンドの **no** 形式を使用します。

構文

ip route *prefix* {*mask* | */prefix-length*} {{*ip-address* [**metric** *value*]} | **reject-route**}

no ip route *prefix* {*mask* | */prefix-length*} [*ip-address*]

パラメータ

- ***prefix***：宛先の IP ルート プレフィックス。
- ***mask***：宛先のプレフィックス マスク。
- ***/ prefix-length***：宛先のプレフィックスマスク。IP アドレスのプレフィックスを構成するビット数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。（範囲：0 ～ 32）
- ***ip-address***：ネットワークに到達するために使用可能なネクスト ホップの IP アドレス。
- **metric** *value*：ルートのメトリック。デフォルトのメトリックは、インバンドインターフェイスのネクストホップでは 4、OOB のネクストホップでは 2 です。範囲：1 ～ 255。
- **reject-route**：宛先ネットワークへのルーティングを停止します。

デフォルト設定

スタティック ルートは確立されません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

特定のサブネットへのすべての静的ルートを削除するには、*ip-address* パラメータを指定せずに **no ip route** コマンドを使用します。

特定のネクストホップを介した特定のサブネットへの 1 つの静的ルートをのみを削除するには、*ip-address* パラメータを指定して **no ip route** コマンドを使用します。

例 1：次の例では、マスクを使用してネットワーク 172.31.0.0 のパケットを 172.31.6.6 のルータにルーティングする方法を示します。

```
switchxxxxxx(config)# ip route 172.31.0.0 255.255.0.0 172.31.6.6 metric 2
```

例 2：次の例では、プレフィックス長を使用してネットワーク 172.31.0.0 のパケットを 172.31.6.6 のルータにルーティングする方法を示します。

```
switchxxxxxx(config)# ip route 172.31.0.0 /16 172.31.6.6 metric 2
```

例 3：次の例では、ネットワーク 194.1.1.0 のパケットを拒否する方法を示します。

```
switchxxxxxx(config)# ip route 194.1.1.0 255.255.255.0 reject-route
```

例 4：次の例では、ネットワーク 194.1.1.0/24 へのすべてのスタティック ルートを削除する方法を示します。

```
switchxxxxxx(config)# no ip route 194.1.1.0 /24
```

例 5：次の例では、1.1.1.1 を介してネットワーク 194.1.1.0/24 へのスタティック ルートを 1 つ削除する方法を示します。

```
switchxxxxxx(config)# no ip route 194.1.1.0 /24 1.1.1.1
```

ip routing

IP ルーティングを有効にするには、グローバル コンフィギュレーション モードで **ip routing** コマンドを使用します。IP ルーティングを無効にするには、このコマンドの **no** 形式を使用します。

構文

ip routing

no ip routing

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

IP ルーティングが有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

コマンドを使用して IP ルーティングを有効にします。

スイッチは、インバンドインターフェイスと OOB ポートで 1 つの IPv4 スタックをサポートしています。

IP ルーティングが有効になっているかどうかに関係なく、IP スタックは常に OOB ポートで IP ホストとして実行しています。

スイッチは、インバンド インターフェイスと OOB インターフェイス間のルーティングをブロックします。

2 つの最適なルート（インバンド経由で 1 つと、OOB ポート経由で 1 つ）がある場合、スイッチは OOB ポート経由のルートを使用します。

OOB ポートでは、DHCP リレーと IP ヘルパーを有効にすることはできません。

OOB ポートでは、ルーティング プロトコルを有効にすることはできません。

OOB ポートで定義されている IP サブネットは、インバンドインターフェイスで実行されているルーティング プロトコルに再配布されません。

例：次の例では、IP ルーティングを有効にします

```
switchxxxxxx(config)# ip routing
```

key-string

キーに認証文字列を指定するには、キー チェーン キー コンフィギュレーション モードで **key-string** コマンドを使用します。認証文字列を削除するには、このコマンドの **no** 形式を使用します。

構文

key-string *text*

no key-string

パラメータ

- ***text***：認証文字列を指定します。文字列には、1 ～ 16 文字を使用できます。

デフォルト設定

キーは存在しません。

コマンド モード

キー チェーン キー コンフィギュレーション モード

例

次の例では、chain1 という名前のキー チェーンが設定されます。Key1 という名前のキーは、午後 1 時 30 分から午後 3 時 30 分まで承認され、午後 2 時から午後 3 時まで送信されます。Key2 という名前のキーは、午後 2 時 30 分から午後 4 時 30 分まで承認され、午後 3 時から午後 4 時まで送信されます。この重複により、キーの移行またはルータの設定時間の不一致に対処できます。時間の違いを処理するために、各側に 30 分間の余裕があります。

```
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# version 2
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# exit
```

key（キーチェーン）

キーチェーンの認証キーを識別するには、キーチェーン コンフィギュレーション モードで **key** コマンドを使用します。キー チェーンから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。

構文

key *key-id*

no key *key-id*

パラメータ

- ***key-id***：キー チェーンの認証キーの識別番号。キーの範囲は 1 ～ 255 です。キーの ID 番号は連続している必要はありません。キーの識別番号の範囲は、キーが定義されているキー チェーンです。

デフォルト設定

キー チェーンにキーは存在しません。

コマンド モード

キーチェーン キー コンフィギュレーション モード

使用上のガイドライン

キー チェーンに複数のキーを設定し、**accept-lifetime** および **send-lifetime** キー チェーン キー コマンド設定に基づいてキーが将来無効になるように、ソフトウェアでキーを配列できるようにすると便利です。

各キーには、ローカルに格納される独自のキー識別子があります。キー識別子とメッセージに関連付けられたインターフェイスの組み合わせによって、使用中の認証アルゴリズムと 認証キーが一意に識別されます。有効なキーの数にかかわらず、1 つの認証パケットのみが送信されます。ソフトウェアは、最小のキー識別番号の検索を開始し、最初の有効なキーを使用します。

最後のキーの期限が切れると、認証はエラーで終了します。

すべてのキーを削除するには、**no keychain** コマンドを使用してキー チェーンを削除します。

例

次の例では、chain1 という名前のキー チェーンが設定されます。Key1 という名前のキーは、午後 1 時 30 分から午後 3 時 30 分まで承認され、午後 2 時から午後 3 時まで送信されます。Key2 という名前のキーは、午後 2 時 30 分から午後 4 時 30 分まで承認され、午後 3 時から午後 4 時まで送信されます。この重複により、キーの移行またはルータの設定時間の不一致に対処できます。時間の違いを処理するために、各側に 30 分間の余裕があります。

```
switchxxxxxx(config)# key 1
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
```

key chain

ルーティング プロトコルの認証を有効にするには、**key chain** コマンドをグローバル コンフィギュレーション モードで使用して、認証キーのグループを識別します。キー チェーンを削除するには、このコマンドの **no** 形式を使用します

構文

key chain *name-of-chain*

no key chain *name-of-chain*

パラメータ

- ***name-of-chain***：キー チェーンの名前。チェーン名は 1 ～ 32 文字にすることができます。キー チェーンには、少なくとも 1 つのキーを含める必要がありますが、最大 256 個のキーを含めることができます。

デフォルト設定

キー チェーンは存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

認証を有効にするには、キーでキー チェーンを設定する必要があります。

複数のキー チェーンの識別が可能ですが、ルーティング プロトコルごとのインターフェイスごとに 1 つのキー チェーンを使用することを推奨します。キー チェーン コマンドを指定するときは、**キーチェーン** コンフィギュレーション モードに入ります。

例

次の例では、chain1 という名前のキー チェーンが設定されます。Key1 という名前のキーは、午後 1 時 30 分から午後 3 時 30 分まで承認され、午後 2 時から午後 3 時まで送信されます。Key2 という名前のキーは、午後 2 時 30 分から午後 4 時 30 分まで承認され、午後 3 時から午後 4 時まで送信されます。この重複により、キーの移行またはルータの設定時間の不一致に対処できます。時間の違いを処理するために、各側に 30 分間の余裕があります。

```
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
```

```
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
```

send-lifetime

キーチェーンの認証キーが送信できる期間を設定するには、キー チェーン キー コンフィギュレーション モードで**send-lifetime** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

send-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no send-lifetime

パラメータ

- ***start-time***：**key** コマンドで指定したキーが受信できる開始時刻です。構文は次のいずれかにすることができます。
  - *hh*:*mm*:*ss Month date year*
  - *hh*:*mm*:*ss date Month year*
  - *hh*：時間（0 ～ 23）
  - *mm*：分（0 ～ 59）
  - *ss*：秒（0 ～ 59）
  - *Month*：月の最初の 3 文字
  - date：日（1 ～ 31）
  - year：年（4 桁）

デフォルトの開始時刻と許容可能な最も古い日付は、2000 年 1 月 1 日です。

- **infinite**：キーは *start-time* 値以降、受信可能です。
- ***end-time***：キーは、*start-time* 値から *end-time* 値まで、受信可能です。構文は、*start-time* 値と同じです。*end-time* 値は *start-time* 値の後である必要があります。デフォルトの終了時刻は無限の期間です。
- **duration** *seconds*：キーが受信可能な時間の長さ（秒単位）。値の範囲は 1 ～ 2147483646 です。

デフォルト設定

認証キーが着信パケットを認証できるデフォルトの期間は期限なしに設定されます。

期限なし（開始時刻は 2000 年 1 月 1 日、終了時刻は infinite）

コマンド モード

キー チェーン キー コンフィギュレーション モード

使用上のガイドライン

start-time 値と、次の値のいずれかを指定します：**infinite** *end-time*、または **duration** *seconds*。

Time-of-Date が管理または SNTP で設定されていない場合、キーは期限切れと見なされます。

最後のキーの期限が切れると、認証はエラーで終了します。

例

次の例では、chain1 という名前のキー チェーンが設定されます。key1 という名前のキーが午後 1 時 30 分から午後 3 時 30 分まで承認され、午後 2 時 00 分から午後 3 時 00 分まで送信されます。key2 という名前のキーが午後 2 時 30 分から午後 4 時 30 分まで承認され、午後 3 時 00 分から午後 4 時 00 分まで送信されます。ルータの設定時間内でのキーの移行または不一致に対して重複が許されます。時間の違いを処理するために、各側に 30 分間の余裕があります。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
```

show ip protocols

アクティブな IP ルーティング プロトコル プロセスのパラメータおよび現在の状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip protocols** コマンドを使用します。

構文

show ip protocols [**summary**]

パラメータ

- **summary**：設定されているルーティング プロトコル プロセス名が表示されます。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

show ip protocols コマンドにより表示される情報は、ルーティング動作のデバッグに役立ちます。

例 1。次に、アクティブなルーティング プロトコルを示す、**show ip protocols** コマンドの出力例を示します。

```
switchxxxxxx# show ip protocols
IP Routing Protocol is "rip"
Interfaces  IP Addresses
VLAN 1    12.1.1.1
VLAN 1    150.23.12.2
VLAN 11   1.1.1.1
```

例 2。次に、**show ip protocols** コマンドに **summary** キーワードを指定した場合の出力例を示します。

```
switchxxxxxx# show ipv6 protocols summary
IP Routing Protocol is "rip"
```

show ip route

ルーティング テーブルの現在の状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip route** コマンドを使用します。

構文

show ip route [**address** *ip-address* {*mask* [**longer-prefixes**]} [*protocol* | **static** | **rejected** | **icmp** | **connected**]

パラメータ

- **address** *ip-address*：ルーティング情報が表示されるネットワーク IP アドレス。
- ***mask***：サブネットマスクの値。
- **longer-prefixes**：IP アドレスとマスクのペアに一致するルートのみを表示するように指定します。
- ***protocol***：表示されるプロトコルの送信元の名前。次のいずれかの引数を使用します。
- **rip**：RIP により追加されたルートが表示されます
- **connected**：接続ルートが表示されます。
- **icmp**：ICMP ダイレクトで追加されたルートを表示します。
- **rejected**：拒否したルートを表示します。
- **static**：スタティック ルートを表示します。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

パラメータを指定せずにこのコマンドを使用すると、IPv6 ルーティング テーブル全体を表示できます。

パラメータを指定してこのコマンドを使用すると、必要なルートを指定できます。

例 1。次に、IP ルーティングが無効になっている場合の **show ip route** コマンドの出力例を示します。

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)IP Forwarding: disabled
Codes: > - best, C - connected, S - static, I - ICMP
IP Routing Table - 5 entries
Code IP Route Distance/ Next Hop Last Time Outgoing
 Metric IP Address Updated Interface
```

```
------ ------------------- ----------- --------------- ------------- ------------
S 10.10.0.0/16 1/2 10.119.254.244 00:02:22 vlan2
S> 10.10.0.0/16 1/1 10.120.254.244 00:02:22 vlan3
S> 10.16.2.0/24 1/1 10.119.254.244 00:02:22 vlan2
C> 10.119.0.0/16 0/1 0.0.0.0 vlan2
C> 10.120.0.0/16 0/1 0.0.0.0 vlan3
```

例 2。次に、IP ルーティングが有効になっている場合の **show ip route** コマンドの出力例を示します。

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)
Directed Broadcast Forwarding: disabled
Codes: > - best, C - connected, S - static
Codes: > - best, C - connected, S - static
R - RIP
Policy Routing
VLAN 1
Route Map: BPR1
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.1
Next Hop Status: Active
ACL Name: ACLTCPTELNET
Next Hop: 2.2.2.2
Next Hop Status: Not Active (Unreachable)
ACL Name: ACL_AA
Next Hop: 3.3.3.3
Next Hop Status: Not Active (Not direct)
VLAN 100
Route Map: BPR_10
Status: Not Active (No IP interface on VLAN 100)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
VLAN 110
Route Map: BPR_20
Status: Not Active (VLAN 110 status is DOWN)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
VLAN 200
Route Map: BPR_A0
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
IP Routing Table - 5 entries
Code IP Route Distance/ Next Hop Last Time Outgoing
Metric IP Address Updated Interface
------ ------------------- ----------- --------------- ------------- ------------
R> 10.7.10.0/24 120/5 10.119.254.244 00:02:22 vlan2
S> 10.175.0.0/16 1/1 10.119.254.240 00:02:22 vlan2
S> 10.180.0.0/16 1/1 10.119.254.240 00:02:42 vlan3
C> 10.119.0.0/16 0/1 0.0.0.0 vlan2
C> 10.120.0.0/16 0/1 0.0.0.0 vlan3
```

例 3。次の例では、アドレス 10.16.0.0 とマスク 255.255.0.0 で論理 AND 演算が実行され、10.16.0.0 となります。ルーティング テーブルの各宛先では、マスクを使用して論理 AND 演算が実行されるため、結果は 10.16.0.0 と比較されます。この範囲に含まれるすべての宛先が出力に表示されます。

```
switchxxxxxx# show ip route 10.16.0.0 255.255.0.0 longer-prefix
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled Directed Broadcast Forwarding: disabled
Codes: > - best, C - connected, S - static
R - RIP
Policy Routing
VLAN 1
Route Map: BPR1
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.1
Next Hop Status: Active
ACL Name: ACLTCPTELNET
Next Hop: 2.2.2.2
Next Hop Status: Not Active (Unreachable)
ACL Name: ACL_AA
Next Hop: 3.3.3.3
Next Hop Status: Not Active (Not direct)
VLAN 100
Route Map: BPR_10
Status: Not Active (No IP interface on VLAN 100)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
VLAN 110
Route Map: BPR_20
Status: Not Active (VLAN 110 status is DOWN)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
VLAN 200
Route Map: BPR_A0
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
IP Routing Table - 6 entries
Code IP Route Distance/ Next Hop Last Time Outgoing
Metric IP Address Updated Interface
------ ------------------ ----------- --------------- ------------- ------------
S> 10.16.2.0/24 1/1 10.119.254.244 00:02:22 vlan2
S> 10.16.2.64/26 1/1 100.1.14.244 00:02:22 vlan1
S> 10.16.2.128/26 1/1 110.9.2.2 00:02:22 vlan3
S> 10.16.208.0/24 1/1 120.120.5.44 00:02:22 vlan2
S> 10.16.223.0/24 1/1 20.1.2.24 00:02:22 vlan5
S> 10.16.236.0/24 1/1 30.19.54.240 00:02:23 vlan
C> 10.119.0.0/16 0/1 0.0.0.0 vlan2
C> 10.120.0.0/16 0/1 0.0.0.0 vlan3
C> 20.1.0.0/16 0/1 0.0.0.0 vlan5
C> 30.19.0.0/16 0/1 0.0.0.0 vlan2
C> 100.1.0.0/16 0/1 0.0.0.0 vlan1
C> 110.9.0.0/16 0/1 0.0.0.0 vlan3
C> 120.120.0.0/16 0/1 0.0.0.0 vlan2
```

例 4。次に、IP ルーティングが有効になっており、ハードウェア転送がアクティブになっていない場合の **show ip route** コマンドの出力例を示します。

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled (hardware forwarding is not active)
Directed Broadcast Forwarding: disabled
Codes: > - best, C - connected, S - static
Codes: > - best, C - connected, S - static
R - RIP
```

```
Policy Routin
VLAN 1
Route Map: BPR1
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.1
Next Hop Status: Active
ACL Name: ACLTCPTELNET
Next Hop: 2.2.2.2
Next Hop Status: Not Active (Unreachable)
ACL Name: ACL_AA
Next Hop: 3.3.3.3
Next Hop Status: Not Active (Not direct)
VLAN 100
Route Map: BPR_10
Status: Not Active (No IP interface on VLAN 100)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
VLAN 110
Route Map: BPR_20
Status: Not Active (VLAN 110 status is DOWN)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Activ
VLAN 200
Route Map: BPR_A0
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
IP Routing Table - 5 entries
Code IP Route Distance/ Next Hop Last Time Outgoing
Metric IP Address Updated Interface
------ ------------------ ----------- --------------- ------------- ------------
R> 10.7.10.0/24 120/5 10.119.254.244 00:02:22 vlan2
S> 10.175.0.0/16 1/1 10.119.254.240 00:02:22 vlan2
S> 10.180.0.0/16 1/1 10.119.254.240 00:02:42 vlan3
C> 10.119.0.0/16 0/1 0.0.0.0 vlan2
C> 10.120.0.0/16 0/1 0.0.0.0 vlan3
```

show ip route summary

show ip route summary コマンドをユーザ EXEC または特権 EXEC モードで使用すると、サマリー形式で IP ルーティング テーブルの現在の内容を表示できます。

構文

show ip route summary

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

例

次に、**show ip route summary** コマンドの出力例を示します。

```
switchxxxxxx# show ip route summary
IP Routing Table Summary - 90 entries
35 connected, 25 static, 12 RIP
Number of prefixes:
/16: 16, /18: 10, /22: 15, /24: 15, /28: 2, /30: 12
```

show key chain

認証キー情報を表示するには、**show key chain** コマンドを特権 EXEC モードで使用します。

構文

show key chain [*name-of-chain*]

パラメータ

- ***name-of-chain***：key chain コマンドで命名された表示対象のキー チェーン名。

デフォルト設定

すべてのキー チェーンの情報が表示されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

例

例 1。次に、現在の時刻が定義されている場合の **show key chain** コマンドの出力例を示します。

```
switchxxxxxx# show key chain
Current Time of Date is Feb 8 2023
Accept lifetime is configured to ignore
Key-chain trees:
key 1 -- text "chestnut"
accept lifetime (always valid) - (always valid) [valid now]
send lifetime (always valid) - (always valid) [valid now]
key 2 -- text "birch"
accept lifetime (00:00:00 Dec 5 2021) - (23:59:59 Dec 5 2025)
send lifetime (06:00:00 Dec 5 2021) - (18:00:00 Dec 5 2026)[valid now]
```

例 2。次に、現在の時刻が定義されていない場合の **show key chain** コマンドの出力例を示します。

```
switchxxxxxx# show key chain
Current Time of Date is not defined
Accept lifetime is ignored
Key-chain trees:
key 1 -- text "chestnut"
accept lifetime (always valid) - (always valid) [valid now]
send lifetime (always valid) - (always valid) [valid now]
key 2 -- text "birch"
accept lifetime (00:00:00 Dec 5 2010) - (23:59:59 Dec 5 2010)
send lifetime (06:00:00 Dec 5 2010) - (18:00:00 Dec 5 2016)
```

IP システム管理コマンド

この章は、次の項で構成されています。

- ping （648 ページ）
- ssh （651 ページ）
- telnet （653 ページ）
- traceroute （657 ページ）

ping

ping EXEC モード コマンドを使用すると、ICMP エコー要求パケットをネットワーク上の別のノードに送信できます。

構文

ping [ip] {*ipv4-address* | *hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *source-address*]

ping ipv6 {*ipv6-address* | *hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *source-address*]

パラメータ

- **ip**：IPv4 を使用してネットワーク接続を確認します。
- **ipv6**：IPv6 を使用してネットワーク接続を確認します。
- ***ipv4-address***：ping する IPv4 アドレス。
- ***ipv6-address***：ping するユニキャストまたはマルチキャスト IPv6 アドレス。IPv6 アドレスがリンク ローカル アドレス（IPv6Z アドレス）である場合、発信インターフェイス名を指定する必要があります。
- ***hostname***：ping するホスト名（長さ：1 ～ 158 文字。ホスト名の各部分の最大ラベル サイズ：58）
- **size** *packet_size*：VLAN タグを含まないパケット内のバイト数。デフォルト値は 64 バイトです。（IPv4：64 ～ 1518、IPv6：68 ～ 1518）
- **count** ***packet_count***：送信するパケット数。1 ～ 65535 パケット。デフォルトは 4 パケットです。0 を入力すると、停止するまで ping します（0 ～ 65535）。
- **time** ***time-out***：各返信に対して待機するまでのタイムアウト（ミリ秒単位）。50 ～ 65535 ミリ秒。デフォルトは 2000 ミリ秒です（50 ～ 65535）。
- **source** *source-address*：送信元アドレス（ユニキャスト IPv4 アドレスまたはグローバルユニキャスト IPv6 アドレス）。

コマンド モード

特権 EXEC モード

使用上のガイドライン

ping を停止するには **Esc** を押します。次に、ping コマンド結果の例を示します。

- **Destination does not respond**：ホストが応答しない場合は、10 秒以内に「ホストから返答がありません」と表示されます。

- **Destination unreachable**：この宛先のゲートウェイには、宛先が到達不能であることが表示されます。
- **Network or host unreachable**：スイッチのルート テーブルに対応するエントリが見つかりません。

リンク ローカル アドレスを使用して直接接続されたホストのネットワークの接続性を確認するために、**ping ipv6** コマンドを使用する場合、出力インターフェイスは **IPv6Z** 形式で指定します。出力インターフェイスが指定されていない場合、デフォルトのインターフェイスが選択されます。

マルチキャスト アドレスが指定された **ping ipv6** コマンドを使用する場合、表示される情報は受信したすべてのエコー応答から取得されます。

キーワードに **source** を設定したのに、宛先アドレスがスイッチのアドレスではない場合、コマンドは停止し、エラー メッセージが表示され、ping は送信されません。

例 1：IP アドレスに ping します。

```
switchxxxxxx> ping ip 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

例 2：サイトに ping します。

```
switchxxxxxx> ping ip yahoo.com
Pinging yahoo.com [66.218.71.198] with 64 bytes of data:
64 bytes from 66.218.71.198: icmp_seq=0. time=11 ms
64 bytes from 66.218.71.198: icmp_seq=1. time=8 ms
64 bytes from 66.218.71.198: icmp_seq=2. time=8 ms
64 bytes from 66.218.71.198: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

例 3：IPv6 アドレスに ping します。

```
switchxxxxxx> ping ipv6 3003::11
Pinging 3003::11 with 64 bytes of data:
64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::11: icmp_seq=2. time=50 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
64 bytes from 3003::11: icmp_seq=4. time=0 ms
----3003::11 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/12/50
switchxxxxxx> ping ipv6 FF02::1
Pinging FF02::1 with 64 bytes of data:
64 bytes from FF02::1: icmp_seq=1. time=0 ms
64 bytes from FF02::1: icmp_seq=1. time=70 ms
64 bytes from FF02::1: icmp_seq=2. time=0 ms
64 bytes from FF02::1: icmp_seq=1. time=1050 ms
64 bytes from FF02::1: icmp_seq=2. time=70 ms
64 bytes from FF02::1: icmp_seq=2. time=1050 ms
```

```
64 bytes from FF02::1: icmp_seq=3. time=0 ms
64 bytes from FF02::1: icmp_seq=3. time=70 ms
64 bytes from FF02::1: icmp_seq=4. time=0 ms
64 bytes from FF02::1: icmp_seq=3. time=1050 ms
64 bytes from FF02::1: icmp_seq=4. time=70 ms
64 bytes from FF02::1: icmp_sq=4. time=1050 ms
---- FF02::1 PING Statistics----
4 packets transmitted, 12 packets received
```

ssh

暗号化セッションをリモート ネットワーキング デバイスで開始するには、ユーザ EXEC モードか、または特権 EXEC モードで **ssh** コマンドを使用します。

構文

ssh {*ip-address* | *hostname*} [*port*] [*keyword...*]

パラメータ

- ***ip-address***：宛先ホスト IP アドレス（IPv4 または IPv6）を指定します。
- ***hostname***：ping するホスト名（長さ：1 ～ 158 文字。ホスト名の各部分の最大ラベル サイズ：58）
- ***port***：10 進数の TCP ポート番号を指定します。デフォルトポートは SSH ポート（22）です。
- ***keyword***：ユーザ ガイドラインのキーワード テーブルに記載されているキーワードを 1 つ以上指定します。

キーワード テーブル

オプション	説明
/password *password*	SSH サーバを実行しているリモート ネットワーキング デバイスにログインするときに使用するパスワードを指定します。キーワードを指定しない場合は、**ip ssh-client password** コマンドで設定したパスワードが使用されます。このキーワードを指定する場合は、**/user** キーワードも指定する必要があります。
/source-interface *interface-id*	最小 IPv4/v6 アドレスが送信元 IPv4/v6 アドレスとして使用される送信元インターフェイスを指定します。キーワードを指定しない場合は、**ip ssh-client source-interface** コマンドで設定した送信元 IPv4/IPv6 アドレスが使用されます。
/user *user-name*	SSH サーバを実行しているリモート ネットワーキング デバイスにログインするときに使用するユーザ名を指定します。キーワードを指定しない場合は、**ip ssh-client username** コマンドで設定したユーザ名が使用されます。このキーワードを指定する場合は、**/password** キーワードも指定する必要があります。

デフォルト設定

デフォルトポートは、ホストの SSH ポート（22）です。

コマンド モード

特権 EXEC モード

使用上のガイドライン

ssh コマンドを使用すると、スイッチは SSH サーバを実行している別のスイッチへのセキュアな暗号化通信を確立できます。この接続は、接続が暗号化される点を除き、Telnet 接続の機能と同様です。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。

同時にアクティブにできる SSH 端末接続は 1 つのみです。

例 1。次に、ローカルデバイスとエッジデバイス HQedge の間にセキュアなセッションを設定する例を示します。

```
switchxxxxxx> ssh HQedge
```

例 2。次に、ローカルデバイスとエッジデバイス 1.1.1.1 の間にセキュアなセッションを設定する例を示します。ユーザ名は HQhost、パスワードは **ip ssh-client password** コマンドで設定したパスワードです。

```
switchxxxxxx> ssh 1.1.1.1 /user HQhost
```

例 3。次に、ローカルデバイスとエッジデバイス HQedge の間にセキュアなセッションを設定する例を示します。ユーザ名は HQhost、パスワードは ar3245ddd です。

```
switchxxxxxx> ssh HQedge /user HQhost /password ar3245ddd
```

例 4。次に、送信元インターフェイスとしてルックバック インターフェイスを設定する例を示します。

```
switchxxxxxx> ssh HQedge /source-interface loopback1
```

telnet

telnet EXEC モード コマンドで Telnet をサポートするホストにログオンします。

構文

telnet {*ip-address* | *hostname*} [*port*] [*keyword...*]

パラメータ

- ***ip-address***：宛先ホスト IP アドレス（IPv4 または IPv6）を指定します。
- ***hostname***：ping するホスト名（長さ：1 ～ 158 文字。ホスト名の各部分の最大ラベル サイズ：58）
- ***port***：10 進数の TCP ポート番号またはユーザ ガイドラインのポート テーブルに記載されているキーワードの 1 つを指定します。
- ***keyword***：ユーザ ガイドラインのキーワード テーブルに記載されているキーワードを 1 つ以上指定します。

デフォルト設定

デフォルトのポートはホストの Telnet ポート（23）です。

コマンド モード

特権 EXEC モード

使用上のガイドライン

Telnet ソフトウェアは Telnet シーケンス形式の特殊な Telnet コマンドをサポートします。このシーケンスは、一般的な端末制御機能をオペレーティング システム固有の機能にマッピングします。Telnet シーケンスを入力するには、エスケープ シーケンス キー（Ctrl-shift-6）の後に Telnet コマンド文字を押します。

特殊な Telnet のシーケンス

Telnet シーケンス	目的
Ctrl-shift-6-b	ブレーク
Ctrl-shift-6-c	プロセスの割り込み（IP）
Ctrl-shift-6-h	文字の消去（EC）
Ctrl-shift-6-o	出力の中断（AO）
Ctrl-shift-6-t	応答確認（AYT）

Telnet シーケンス	目的
Ctrl-shift-6-u	行の消去（EL）

アクティブな Telnet セッション中は、システム プロンプトで ?/help キーを押すと、利用可能な Telnet コマンドが表示されます。

次に、この一覧の例を示します。

```
switchxxxxxx> ?/help
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
?/help suspends the session (return to system command prompt)
```

複数の Telnet セッションを同時に開くと、セッション間を切り替えることができます。後続のセッションを開くには、エスケープ シーケンス キー（Ctrl-shift-6）と x を押してシステム コマンド プロンプトに戻り、現在の接続を停止する必要があります。その後、telnet EXEC コマンドで新しい接続を開きます。

このコマンドは、ローカル デバイスとの現在の Telnet セッションで開かれたリモート ホストとの Telnet 同時接続を表示します。他の Telnet セッションで開かれたリモート ホストとの Telnet 接続は表示されません。

キーワード テーブル

オプション	説明
/echo	ローカル エコーを有効にします。
/quiet	ソフトウェアからのすべてのメッセージが画面上に表示されないようにします。
/source-interface	送信元インターフェイスを指定します。
/stream	ストリーム処理をオンにします。これにより、Telnet の制御シーケンスなしの raw TCP ストリームが有効になります。ストリーム接続は Telnet オプションを処理せず、UNIX-to-UNIX Copy Program（UUCP; UNIX 間コピー プログラム）や他の非 Telnet プロトコルを実行するポート接続に適している場合があります。
Ctrl-shift-6 x	システム コマンド プロンプトに戻ります。

ポート テーブル

キーワード	説明	ポート番号
BGP	ボーダー ゲートウェイ プロトコル	179

キーワード	説明	ポート番号
chargen	キャラクタ ジェネレータ	19
cmd	リモート コマンド	514
daytime	日時	13
discard	廃棄	9
domain	ドメイン ネーム サービス	53
echo	Echo	7
exec	EXEC	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP データ接続	20
gopher	Gopher	70
hostname	NIC ネームサーバ	101
ident	Ident プロトコル	113
irc	インターネット リレー チャット	194
klogin	Kerberos ログイン	543
kshell	Kerberos シェル	544
login	ログイン	513
lpd	印刷サービス	515
nntp	ネットワーク ニュース トランスポート プロトコル	119
pim-auto-rp	PIM Auto-RP	496
pop2	POP v2	109
pop3	POP v3	110
smtp	シンプル メール転送プロトコル	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC アクセス コントロール システム	49

キーワード	説明	ポート番号
talk	Talk	517
Telnet	Telnet	23
time	Time	37
uucp	UNIX 間コピー プログラム	540
whois	ニックネーム	43
www	ワールドワイド ウェブ	80

例

次に、Telnet 経由で IP アドレス 176.213.10.50 にログインしたときの例を示します。

```
switchxxxxxx>  telnet 176.213.10.50
```

traceroute

宛先に転送するときにパケットが通るルートを表示するには、**traceroute** EXEC モード コマンドを使用します。

構文

traceroute ip {*ipv4-address* | *hostname*} [**size** *packet_size*] [**ttl** *max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*]

traceroute ipv6 {*ipv6-address* | *hostname*} [**size** *packet_size*] [**ttl** *max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*]

パラメータ

- **ip**：IPv4 を使用してルートを検出します。
- **ipv6**：IPv6 を使用してルートを検出します。
- ***ipv4-address***：宛先ホストの IPv4 アドレス。
- ***ipv6-address***：宛先ホストの IPv6 アドレス。
- ***hostname***：ping するホスト名（長さ：1 ～ 158 文字。ホスト名の各部分の最大ラベル サイズ：58）
- **size** *packet_size*：VLAN タグを含まないパケット内のバイト数。デフォルト値は 64 バイトです。（IPv4：64 ～ 1518、IPv6：68 ～ 1518）
- **ttl** *max-ttl*：使用可能な最大 TTL 値。デフォルトは 30 です。**traceroute** コマンドは、宛先に到達した場合、またはこの値に到達した場合に終了します。（範囲：1 ～ 255）
- **count** *packet_count*：各 TTL レベルで送信されるプローブ数。デフォルトの数は 3 です。（範囲：1 ～ 10）
- **timeout** *time_out*：プローブ パケットへの応答を待機する秒数。デフォルトは 3 秒です。(範囲：1 ～ 60)
- **source** *ip-address*：プローブの送信元アドレスとして使用するデバイスのインターフェイス アドレスの 1 つ。デバイスはデフォルトで最適な送信元アドレスを選択します。（範囲：有効な IP アドレス）

コマンド モード

特権 EXEC モード

使用上のガイドライン

traceroute コマンドは、データグラムが存続可能時間（TTL）の値を超過するとルートで生成されるエラー メッセージを活用して動作します。

traceroute コマンドは最初に TTL 値が 1 のプローブ データグラムを送信します。これにより、1 つめのルータによってプローブ データグラムが廃棄され、エラー メッセージが返信されます。traceroute コマンドは、TTL レベルごとに複数のプローブを送信し、それぞれのラウンドトリップ時間を表示します。

traceroute コマンドでは 1 回に送信されるプローブは 1 つです。各発信パケットから 1 つまたは 2 つのエラー メッセージが生成される可能性があります。「time exceeded」エラー メッセージは、中間ルータがプローブを検出し、廃棄したことを示します。「destination unreachable」エラーメッセージは、宛先ノードがプローブを受信して、パケットを配信できないためにそれを破棄したことを示します。応答が着信する前にタイマーがオフになった場合、traceroute コマンドはアスタリスク（*）を出力します。

宛先が応答する、最大 TTL を超過する、またはユーザが Esc でトレースを中断すると **traceroute** コマンドは終了します。

Traceroute ipv6 コマンドは、IPv6 リンク ローカル アドレスには関連ありません。

例

```
switchxxxxxx> traceroute ip umaxp1.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxp1.physics.lsa.umich.edu (141.211.101.64)
1 i2-gateway.stanford.edu (192.68.191.83)  0 msec 0 msec 0 msec
2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162)  1 msec 1 msec 1 msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103)  33 msec 35 msec 35 msec
6 iplsng-kscyng.abilene.ucaid.edu (198.32.8.80)   47 msec 45 msec 45 msec
7 so-0-2-0x1.aa1.mich.net (192.122.183.9)  56 msec  53 msec 54 msec
8 atm1-0x24.michnet8.mich.net (198.108.23.82)  56 msec 56 msec 57 msec
9 * * *
10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu(141.211.5.22)58 msec 58msec 58 msec
11 umaxp1.physics.lsa.umich.edu (141.211.101.64)  62 msec 63 msec 63 msec
Trace completed
```

次の表に、この出力で表示される重要なフィールドについて説明します。

フィールド	説明
1	ホストへのパスのルータのシーケンス番号を示します。
i2-gateway.stanford.edu	このルータのホスト名。
192.68.191.83	このルータの IP アドレス。
1 msec 1 msec 1 msec	送信される各プローブのラウンドトリップ時間。

次に、traceroute コマンド出力に表示される文字を示します。

フィールド	説明
*	プローブがタイムアウトになりました。
?	パケット タイプが不明です。

フィールド	説明
A	管理上、到達不能です。通常、この出力は、アクセス リストがトラフィックをブロックしていることを表しています。
F	フラグメンテーションが必要で、DF が送信されます。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	発信元。
R	フラグメント再組み立て時間を超過しました
S	送信元ルートに障害が発生しました。
U	ポートが到達不能です。

IPv4 IPM ルータ コマンド

この章は、次の項で構成されています。

- ip multicast-routing （662 ページ）
- ip multicast ttl-threshold （663 ページ）
- show ip mroute （664 ページ）
- show ip multicast （666 ページ）

ip multicast-routing

ルータのすべての IP が有効なインターフェイスで IPv4 マルチキャスト ルーティングを有効にし、マルチキャスト転送を有効にするには、**ip multicast-routing** コマンドをグローバル コンフィギュレーション モードで使用します。マルチキャスト ルーティングおよび転送を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip multicast-routing igmp-proxy

no ip multicast-routing

パラメータ

- **igmp-proxy**：IGMP プロキシを使用して、マルチキャスト ルーティングを有効にします。

デフォルト設定

マルチキャスト ルーティングが有効になっていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ip multicast-routing コマンドを、必要な IP マルチキャスト ルーティング プロトコルを指定するパラメータと使用します。

インターフェイスで IPv4 マルチキャスト パケットを転送するには、IPv4 マルチキャスト転送をグローバルに有効にし、IPMv4 ルーティング プロトコルをインターフェイスで有効にする必要があります。

例

次の例では、IGMP プロキシを使用して IP マルチキャスト ルーティングを有効にします。

```
switchxxxxxx(config)# ip multicast-routing igmp-proxy
```

ip multicast ttl-threshold

インターフェイスから転送されるパケットの存続可能時間（TTL）しきい値を設定するには、インターフェイス コンフィギュレーション モードで **ip multicast ttl-threshold** コマンドを使用します。デフォルトの TTL しきい値に戻すには、このコマンドの **no** 形式を使用します。

構文

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold

パラメータ

- ***ttl-value***：ホップでの存続可能時間の値。値の範囲は 0 ～ 256 です。

デフォルト設定

デフォルトの TTL 値は 0 です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

しきい値未満の TTL 値を持つマルチキャスト パケットは、インターフェイスで転送されません。デフォルト値の 0 は、すべてのマルチキャスト パケットがインターフェイスで転送されることを意味します。

256 の値は、インターフェイスでマルチキャスト パケットが転送されないことを意味します。

TTL しきい値は、境界ルータでのみ設定する必要があります。逆に、TTL しきい値を自動的に設定するルータは、境界ルータになります。

例

次の例では、境界ルータの TTL しきい値を 200 に設定します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip multicast ttl-threshold 200
switchxxxxxx(config-if)# exit
```

show ip mroute

マルチキャスト ルーティング（mroute）テーブルの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip mroute** コマンドを使用します。

構文

show ip mroute [*group-address* [*source-address*]] [**summary**]

パラメータ

- ***group-address***：宛先マルチキャスト IP アドレス。
- ***source-address***：送信元 IP アドレス。
- **summary**：出力をフィルタして、mroute テーブルの各エントリに対し、1 行の簡略サマリーを表示します。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

show ip mroute コマンドを使用して、mroute テーブルの Mroute エンティティに関する情報を表示します。スイッチは、(*,G) エントリから (S,G) エントリを作成することで、マルチキャスト ルーティング テーブルに値を代入します。アスタリスク（*）は、すべての送信元アドレスを示し、「S」は単一ソース アドレスを示し、「G」は宛先マルチキャスト グループ アドレスを示します。(S,G) エントリの作成時に、スイッチはユニキャスト ルーティング テーブルで見つかった（つまり、Reverse Path Forwarding（RPF）によって）、該当する宛先グループへの最適なパスを使用します。

例

次の例の重要なフィールドの説明

Timers:Uptime/Expires：「Uptime」は、エントリが IP マルチキャスト ルーティング テーブルに格納されていた期間（時間、分、秒）をインターフェイスごとに示します。「Expires」は、IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間（時間、分、秒）をインターフェイスごとに示します。

(*, 224.0.255.1) と (192.168.37.100/32, 224.0.255.1)：IP マルチキャスト ルーティング テーブルのエントリ。エントリは、送信元ルータの IP アドレスと、それに続くマルチキャスト グループの IP アドレスで構成されます。送信元ルータの位置に置かれたアスタリスク（*）は、すべての送信元を意味します。

最初の形式のエントリは、(*,G) または「スター カンマ G」エントリと呼ばれます。2 番目の形式のエントリは、(S,G) または「S カンマ G」エントリと呼ばれます。(*,G) エントリは、(S,G) エントリを作成するために使用されます。

Incoming interface：送信元からのマルチキャスト パケットが着信する予定のインターフェイス。パケットがこのインターフェイスに着信しなかった場合、廃棄されます。

Outgoing Interface List（OIF）：パケット転送時に使用されるインターフェイス。

例 1。次に、**show ip mroute** コマンドに summary キーワードを指定した場合の出力例を示します。

```
switchxxxxxx# show ip mroute summary
Timers: Uptime/Expires
IP Multicast Routing Table
(172.16.160.67/32, 224.2.127.254), 00:02:46/00:00:12, OIF count:2
(172.16.244.217/32, 224.2.127.254), 00:02:15/00:00:40, OIF count:
(172.16.8.33/32, 224.2.127.254), 00:00:25/00:02:32, OIF count:2
(172.16.2.62/32, 224.2.127.254), 00:00:51/00:02:03, OIF count:2
(172.16.8.3/32, 224.2.127.254), 00:00:26/00:02:33, OIF count:2
(172.16.60.189/32, 224.2.127.254), 00:03:47/00:00:46, OIF count:2
```

例 2。次に、**show ip mroute** コマンドの出力例を示します。

```
switchxxxxxx# show ip mroute
Timers: Uptime/Expires
IP Multicast Routing Table
(*, 224.0.255.3), 5:29:15/00:03:01
Incoming interface: vlan2
Outgoing interface list:
vlan100, 5:29:15/0:02:57
(192.168.46.0/24, 224.0.255.3), 05:29:15/00:02:59
Incoming interface: vlan2
Outgoing interface list:
vlan5, 05:29:15/00:02:57
```

show ip multicast

IP マルチキャスト構成に関する一般情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip multicast** コマンドを使用します。

構文

show ip multicast [**interface** *interface-id*]

パラメータ

- **interface**：IP マルチキャスト用に設定されたインターフェイスに関する、IP マルチキャスト関連情報を表示します。
- ***interface-id***：IP マルチキャスト情報を表示するインターフェイス識別子。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

show ip multicast コマンドを **interface** キーワードを指定せずに使用して、ルータの IP マルチキャストの状態に関する一般情報を表示します。

show ip multicast コマンドを **interface** キーワードを指定して使用して、指定したインターフェイスに関する IP マルチキャスト情報を表示します。

例 1。次に、IP マルチキャスト ルーティング プロトコルが有効でないときに、**interface** キーワードなしでの **show ip multicast** コマンドの出力例を示します。

```
switchxxxxxx# show ip multicast
IP Unicast Forwarding: enabled
IP Multicast Protocol: No
```

例 2。次に、IGMP プロキシが有効なときに、**interface** キーワードなしでの **show ip multicast** コマンドの出力例を示します。

```
switchxxxxxx# show ip multicast
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
```

例 3。次に、指定したインターフェイスに関する **show ip multicast** コマンドの出力例を示します。IGMP プロキシがインターフェイスで有効になっており、そのインターフェイスは IGMP プロキシ アップストリーム インターフェイスです。

```
switchxxxxxx# show ip multicast interface vlan 200
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
vlan 200
TTL-threshold: 0
```

```
IGMP Protocol: IGMPv3
IGMP Proxy: Upstream
```

例 4。次に、指定したインターフェイスに関する **show ip multicast** コマンドの出力例を示します。IGMP プロキシがインターフェイスで有効になっており、そのインターフェイスは IGMP プロキシ ダウンリンク インターフェイスです。

```
switchxxxxxx# show ip multicast interface vlan 100
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGP Proxy
vlan 200
TTL-threshold: 0
IGMP Protocol: IGMPv3
IGMP Proxy: DownStream (Upstream: vlan 200)
```

例 5。次に、指定したインターフェイスに関する **show ip multicast** コマンドの出力例を示します。IGMP プロキシはインターフェイスで無効です。

```
switchxxxxxx# show ip multicast interface vlan 100
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
vlan 200
IP Status: enabled
hop-threshold: 100
IGMP Protocol: IGMPv3
IGMP Proxy: disabled
```

IPv6 コマンド

この章は、次の項で構成されています。

- clear ipv6 neighbors （671 ページ）
- ipv6 address （672 ページ）
- ipv6 address anycast （673 ページ）
- ipv6 address autoconfig （675 ページ）
- ipv6 address eui-64 （676 ページ）
- ipv6 address link-local （678 ページ）
- ipv6 default-gateway （679 ページ）
- ipv6 enable （680 ページ）
- ipv6 hop-limit （681 ページ）
- ipv6 icmp error-interval （682 ページ）
- ipv6 link-local default zone （684 ページ）
- ipv6 nd advertisement-interval （685 ページ）
- ipv6 nd dad attempts （686 ページ）
- ipv6 nd hop-limit （688 ページ）
- ipv6 nd managed-config-flag （689 ページ）
- ipv6 nd prefix （690 ページ）
- ipv6 nd ra interval （693 ページ）
- ipv6 nd ra lifetime （694 ページ）
- ipv6 nd ra suppress （695 ページ）
- ipv6 nd reachable-time （696 ページ）
- ipv6 nd router-preference （697 ページ）
- ipv6 redirects （698 ページ）
- ipv6 route （699 ページ）
- ipv6 unicast-routing （701 ページ）
- ipv6 unreachables （702 ページ）
- show ipv6 interface （703 ページ）
- show ipv6 link-local default zone （710 ページ）
- show ipv6 nd prefix （711 ページ）

- show ipv6 neighbors （712 ページ）
- show ipv6 route （714 ページ）
- show ipv6 route summary （717 ページ）
- show ipv6 static （718 ページ）

clear ipv6 neighbors

clear ipv6 neighbors コマンドを特権 EXEC モードで使用すると、スタティック エントリを除く、すべてのエントリを IPv6 ネイバー探索キャッシュを削除できます。

構文

clear ipv6 neighbors

コマンド モード

特権 EXEC モード

使用上のガイドライン

例

次に、ネイバー探索キャッシュのすべてのエントリ（スタティック エントリは除く）を削除する例を示します。

```
switchxxxxxx# clear ipv6 neighbors
```

ipv6 address

ipv6 address コマンドをインターフェイス コンフィギュレーション モードで使用すると、IPv6 一般プレフィックスに基づいてグローバルユニキャスト IPv6 アドレスを設定し、インターフェイスで IPv6 アドレッシングを有効にできます。インターフェイスから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。

構文

ipv6 address *ipv6-address*/*prefix-length*

no ipv6 address [*ipv6-address*/*prefix-length*]

パラメータ

- ***ipv6-address***：インターフェイスに割り当てられたグローバル ユニキャスト IPv6 アドレスを指定します。この引数は RFC4293 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
- ***prefix-length***：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。

デフォルト設定

IP アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ipv6 address コマンドは、ISATAP インターフェイス上の IPv6 アドレスの定義には適用できません。

no IPv6 address コマンドを引数なしで使用すると、手動で設定されたリンクローカル アドレスを含む、手動で設定されたすべての IPv6 アドレスがインターフェイスから削除されます。

例

次の例では、VLAN 100 上の IPv6 グローバル アドレス 2001:DB8:2222:7272::72 を定義します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
switchxxxxxx(config-if)# exit
```

ipv6 address anycast

ipv6 address anycast コマンドをインターフェイス コンフィギュレーション モードで使用して、グローバル ユニキャスト IPv6 エニーキャスト アドレスを設定し、インターフェイスでの IPv6 処理を有効にします。インターフェイスから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。

構文

ipv6 address *ipv6-prefix*/*prefix-length* **anycast**

no ipv6 address [*ipv6-prefix*/*prefix-length*]

パラメータ

- ***ipv6-address***：インターフェイスに割り当てられたグローバル ユニキャスト IPv6 アドレスを指定します。この引数は RFC4293 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
- ***prefix-length***：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。

デフォルト設定

IP アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

エニーキャスト アドレスは、通常は異なるノードに属するインターフェイスのセットに割り当てられます。エニーキャスト アドレスに送信されたパケットは、使用しているルーティング プロトコルの定義に従って、そのエニーキャスト アドレスが示す最も近いインターフェイスに送信されます。エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられるため、その構文ではユニキャスト アドレスと区別できません。エニーキャスト アドレスを割り当てるノードには、そのアドレスがエニーキャスト アドレスとはっきり分かるように設定する必要があります。

エニーキャスト アドレスを使用できるのはルータだけです。ホストでは使用できません。エニーキャスト アドレスは、IPv6 パケットの送信元アドレスとして使用できません。

サブネット ルータのエニーキャスト アドレスには、一連のゼロで連結されたプレフィックスがあります（インターフェイス ID）。サブネット ルータ エニーキャスト アドレスを使用すると、サブネット ルータ エニーキャスト アドレスのプレフィックスが示すリンク上のルータに到達できます。

ipv6 address anycast コマンドは、ISATAP インターフェイスで IPv6 アドレスを定義することに適用できません。

例

次の例では、インターフェイスでの IPv6 の処理を可能にし、プレフィックス 2001:0DB8:1:1::/64 をインターフェイスに割り当て、IPv6 エニー キャスト アドレス 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE を設定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
switchxxxxxx(config-if)# exit
```

ipv6 address autoconfig

ipv6 address autoconfig コマンドをインターフェイス コンフィギュレーション モードで使用すると、ステートレス自動設定を使用してIPv6アドレスの自動設定を有効にして、インターフェイスで IPv6 処理を有効にできます。アドレスは、ルータ アドバタイズメント メッセージで受信されたプレフィックスによって設定されます。IPv6アドレスの自動設定を無効にして、インターフェイスから設定済みアドレスを自動的に削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 address autoconfig

no ipv6 address autoconfig

デフォルト設定

ステートレス自動設定は有効になっています。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

このコマンドにより、インターフェイス上のIPv6を有効になると（無効になっている場合）、スイッチは IPv6 ステートレス アドレス自動設定を実行し、リンク上のプレフィックスを検出して、eui-64 ベースのアドレスがインターフェイスに追加されます。

ステートレス自動設定は、IPv6 転送が無効になっている場合にのみ適用されます。

IPv6 転送を無効から有効に変更して、ステートレス自動設定が有効になると、スイッチはステートレス自動設定を停止し、すべてのインターフェイスからステートレス自動設定済みのすべての ipv6 アドレスを削除します。

IPv6 転送を有効から無効に変更して、ステートレス自動設定が有効になると、スイッチはステートレス自動設定を再開します。

さらに、**ipv6 address autoconfig** コマンドは、DHCPv6 ステートレスクライアントがインターフェイス上で DHCP ステートレス情報を受信できるようにします。この情報は、IPv6 転送が有効かどうかに関係なく、DHCPv6 サーバから受信します。

例

次の例では、IPv6 アドレスが自動的に割り当てられます。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 address autoconfig
switchxxxxxx(config-if)# exit
```

ipv6 address eui-64

ipv6 address eui-64 コマンドをインターフェイス コンフィギュレーション モードで使用すると、インターフェイスのグローバル ユニキャスト IPv6 アドレスを設定し、アドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して IPv6 処理を有効にできます。インターフェイスから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。

構文

ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

no ipv6 address [*ipv6-prefix*/*prefix-length* **eui-64**]

パラメータ

- ***ipv6-prefix***：インターフェイスに割り当てられているグローバル ユニキャスト IPv6 アドレスを指定します。この引数は RFC4293 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
- ***prefix-length***：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。

デフォルト設定

IP アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

prefix-length 引数に指定されている値が 64 ビットを超えている場合は、プレフィックス ビットがインターフェイス ID よりも優先されます。

IPv6 アドレスは次の方法で *ipv6-prefix* と EUI-64 インターフェイス ID から作成されます。

- 最初の *prefix-length* ビットは *ipv6-prefix* から取得されます。
- *prefix-length* が 64 より小さい場合、

  次の（64-*prefix-length*）ビットは 0 で埋められます。

  - 最後の 64 ビットは EUI-64 インターフェイス ID から取得されます。

- *prefix-length* が 64 に等しい場合、次の 64 ビットは、EUI-64 インターフェイス ID から取得されます。

- *prefix-length* が 64 より大きい場合、次の（128-*prefix-length*）ビットは EUI-64 インターフェイス ID の最後の（64-(*prefix-length*-64)）ビットから取得されます。

スイッチはその IPv6 アドレスのいずれかを使用している別のホストを検出すると、その IPv6 アドレスを追加し、コンソールにエラー メッセージを表示します。

例

次の例では、VLAN 1 で IPv6 アドレッシングを有効にして、IPv6 グローバル アドレス 2001:0DB8:0:1::/64 を設定し、アドレスの低位 64 ビットの EUI-64 インターフェイスを指定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
switchxxxxxx(config-if)# exit
```

ipv6 address link-local

ipv6 address link-local コマンドをインターフェイス コンフィギュレーション モードで使用すると、インターフェイスの IPv6 リンク ローカル アドレスを設定し、インターフェイスで IPv6 処理を有効にできます。手動設定済みのリンク ローカル アドレスをインターフェイスから削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 address *ipv6-prefix* **link-local**

no ipv6 address [**link-local**]

パラメータ

- ***ipv6-address***：インターフェイスに割り当てられている IPv6 ネットワークを指定します。この引数は RFC4293 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。

デフォルト設定

デフォルトのリンクローカル アドレスが定義されています。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

IPv6 処理がインターフェイスで有効であり、通常、IPv6 アドレスがインターフェイスで設定されている場合、スイッチはインターフェイスのリンクローカルアドレスが自動的に生成します。インターフェイスで使用されるリンク ローカル アドレスを手動で指定するには、**ipv6 address link-local** コマンドを使用します。

ipv6 address link-local コマンドは、ISATAP インターフェイス上の IPv6 アドレスの定義には適用できません。

例

次の例では、VLAN 1 で IPv6 アドレッシングを有効にし、FE80::260:3EFF:FE11:6770 を VLAN 1 のリンク ローカル アドレスとして設定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
switchxxxxxx(config-if)# exit
```

ipv6 default-gateway

ipv6 default-gateway グローバル コンフィギュレーション モード コマンドを使用すると、IPv6 デフォルト ゲートウェイを定義できます。IPv6 デフォルト ゲートウェイを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 default-gateway {*ipv6-address* [*outgoing-interface-id*]} | *interface-id*

no ipv6 default-gateway *[{ipv6-address* [*outgoing-interface-id*]} | *interface-id*]

パラメータ

- ***ipv6-address***：ネットワークへのアクセスに使用可能な IPv6 ルータの IPv6 アドレスを指定します。
- ***outgoing-interface-id***：発信インターフェイス識別子。
- ***interface-id***：ネットワークに到達するために使用可能な発信インターフェイスのインターフェイス識別子を指定します。この引数は、ポイントツーポイントインターフェイス（手動 IPv6 over IPv4 トンネル）にのみ適用できます。

デフォルト設定

デフォルト ゲートウェイは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

例 1。次の例では、グローバル IPv6 アドレスのデフォルト ゲートウェイを定義しています。

```
switchxxxxxx(config)# ipv6 default-gateway 5::5
```

例 2。次の例では、リンクローカル IPv6 アドレスを指定したデフォルト ゲートウェイが定義されています。

```
switchxxxxxx(config)# ipv6 default-gateway  FE80::260:3EFF:FE11:6770%vlan1
```

例 3。次の例では、手動 tunnel 1 のデフォルト ゲートウェイが定義されています。

```
switchxxxxxx(config)# ipv6 default-gateway tunnel1
```

ipv6 enable

ipv6 enable コマンドをインターフェイス コンフィギュレーション モードで使用すると、インターフェイスで IPv6 処理を有効にできます。

明示的な IPv6 アドレスでまだ設定されていないインターフェイスで IPv6 処理を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 enable

no ipv6 enable

デフォルト設定

IPv6 インターフェイスは無効です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

このコマンドを実行すると、インターフェイスで IPv6 リンクローカル ユニキャスト アドレスが自動的に設定され、IPv6 処理のインターフェイスも有効になります。明示的な IPv6 アドレスで設定されているインターフェイスで **no ipv6 enable** コマンドを実行しても、IPv6 処理は無効になりません。

例

次の例では、IPv6 アドレッシング モードの VLAN 1 を有効にします。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 enable
switchxxxxxx(config-if)# exit
```

ipv6 hop-limit

ipv6 hop-limit コマンドをグローバル コンフィギュレーション モードで使用して、ルータによって発信されたすべての IPv6 パケットで使用されるホップの最大数を設定します。

ホップ制限をそのデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 hop-limit *value*

no ipv6 hop-limit

パラメータ

- ***value***：ホップの最大数。指定できる範囲は 1 ～ 255 です。

デフォルト設定

デフォルトのホップ カウントは 64 です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、ルータから発信されたすべての IPv6 パケットに対しホップの最大数 15 を設定します。

```
switchxxxxxx(config)# ipv6 hop-limit 15
```

ipv6 icmp error-interval

ipv6 icmp error-interval コマンドをグローバル コンフィギュレーション モードで使用すると、IPv6 ICMP エラー メッセージの間隔およびバケット サイズを設定できます。間隔をそのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 icmp error-interval *milliseconds* [*bucketsize*]

no ipv6 icmp error-interval

パラメータ

- ***milliseconds***：バケットに格納されるトークン間の間隔。各トークンは、1 つの ICMP エラー メッセージを表します。指定できる範囲は 0 ～ 2147483647 です。値を 0 にすると、ICMP レート制限が無効になります。
- ***bucketsize***：バケットに格納されるトークンの最大数。指定できる範囲は 1 ～ 200 です。

デフォルト設定

デフォルトの間隔は 100 ms で、デフォルト バケットサイズは 10 です。つまり、1 秒間に 100 個の ICMP エラー メッセージが送信されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

次のコマンドを使用すると、IPv6 ICMP エラー メッセージが送信されるレートを制限できます。トークン バケット アルゴリズムは、1 件の IPv6 ICMP エラー メッセージを表す 1 つのトークンで使用されます。トークンは、バケットで許可されているトークンの最大数に達するまで、指定された間隔で、仮想バケットに保存されます。

milliseconds 引数は、バケットに届くトークン間の間隔を指定します。省略可能な *bucketsize* 引数は、バケットに許容されたトークンの最大数を定義するために使用されます。トークンは、IPv6 ICMP エラー メッセージが送信されるとバケットから削除されます。たとえば、*bucketsize* 引数を 20 に設定すると、20 の IPv6 ICMP エラー メッセージを連続して送信することができます。トークンのバケットが空になると、新しいトークンがバケットに配置されるまで、IPv6 ICMP エラー メッセージは送信されません。

1 秒間あたりの平均パケット数 = (1000/ *milliseconds*) * *bucketsize*.

ICMP レート制限を無効にするには、*milliseconds* 引数をゼロに設定します。

例

次の例は、50 ミリ秒の間隔と 20 トークンのバケット サイズが IPv6 ICMP エラー メッセージに対して設定されていることを示します。

```
switchxxxxxx(config)# ipv6 icmp error-interval 50 20
```

ipv6 link-local default zone

Ipv6 link-local default zone コマンドを使用すると、インターフェイスを指定せずに、またはデフォルト ゾーンを 0 に指定してリンク ローカル パケットを出力するようにインターフェイスを設定できます。

このコマンドの **no** 形式を使用すると、デフォルトのリンク ローカル インターフェイスをデフォルト値に戻します。

構文

Ipv6 link-local default zone interface-id

no Ipv6 link-local default zone

パラメータ

- ***interface-id***：IPv6Z インターフェイス識別子を指定せずに、またはデフォルト 0 の識別子を指定して送信されるパケットの出力インターフェイスとして使用されるインターフェイスを指定します。

デフォルト

デフォルトでは、**link local default zone** は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、デフォルト ゾーンとして VLAN 1 を定義しています。

```
switchxxxxxx(config)# ipv6 link-local default zone vlan1
```

ipv6 nd advertisement-interval

ipv6 nd advertisement-interval をインターフェイス コンフィギュレーション モードで使用して、ルータ アドバタイズメント（RA）のアドバタイズメント間隔オプションを設定します。

間隔をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd advertisement-interval

no ipv6 nd advertisement-interval

デフォルト設定

アドバタイズ間隔オプションは送信されません。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ipv6 nd advertisement-interval コマンドを使用して、訪問モバイル ノードにそのノードが RA の受信を想定する間隔を示します。ノードは、移動検出アルゴリズムでこの情報を使用できます。

例

次の例では、RA で送信されるアドバタイズメント間隔オプションが有効になります。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd advertisement-interval
switchxxxxxx(config-if)# exit
```

ipv6 nd dad attempts

ipv6 nd dad attempts コマンドをインターフェイス コンフィギュレーション モードで使用すると、インターフェイスのユニキャストIPv6アドレスで重複アドレス検出を実行中に、インターフェイスで送信されたネイバー送信要求メッセージの連続数を設定できます。

メッセージ数をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts

パラメータ

- ***value***：ネイバー送信要求メッセージの数。指定できる範囲は0～600です。値0を設定すると、指定されたインターフェイスでの重複アドレス検出処理が無効になります。値1を設定すると、追加送信のない単一送信が行われます。

デフォルト設定

1

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャストIPv6アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャストIPv6アドレスの一意性を確認します。

DupAddrDetectTransmitsノード設定変数（『IPv6 Stateless Address Autoconfiguration』のRFC 4862で指定されています）は、tentativeユニキャストIPv6アドレスで重複アドレス検出が実行されているときに、インターフェイスで送信されるネイバー送信要求メッセージの連続数を自動的に判別するときに使用されます。

重複アドレス検出のネイバー送信要求メッセージの間隔（重複アドレス検出タイムアウト間隔）は、ネイバー探索に関連する変数RetransTimer（RFC 4861『Neighbor Discovery for IPv6』で指定されています）により指定されます。この変数は、アドレスが解決されるとき、または隣接の到達可能性がプローブされるときに、ネイバー送信要求メッセージが再隣接に転送される間隔を決定するために使用されます。これは、アドレス解決およびネイバー到達不能検出中のネイバー要請メッセージの間隔を指定するときに使用される管理変数と同じです。

重複アドレス検出は、管理上ダウンしているインターフェイスでは停止します。インターフェイスが管理上ダウンしている間、そのインターフェイスに割り当てられたユニキャストIPv6

アドレスは保留状態に設定されます。インターフェイスが管理上アップ状態に戻ると、そのインターフェイスで重複アドレス検出が自動的に再起動されます。

管理上アップ状態に戻っているインターフェイスでは、インターフェイス上のすべてのユニキャスト IPv6 アドレスを対象に重複アドレス検出が再起動されます。インターフェイスのリンクローカル アドレスで重複アドレス検出が実行されている間、他の IPv6 アドレスの状態は仮承諾に設定されたままとなります。リンクローカルアドレスで重複アドレス検出が完了すると、残りの IPv6 アドレスで重複アドレス検出が実行されます。

重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態はDUPLICATEに設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカル アドレスである場合、インターフェイス上での IPv6 パケットの処理は無効になり、エラー SYSLOG メッセージが発行されます。

重複アドレスがインターフェイスのグローバルアドレスである場合、そのアドレスは使用されず、エラー SYSLOG メッセージが発行されます。

アドレスの状態がDUPLICATEに設定されている間、重複アドレスに関連付けられたコンフィギュレーション コマンドはすべて設定済みのままとなります。

インターフェイスのリンクローカル アドレスが変更された場合、新しいリンクローカル アドレスで重複アドレス検出が実行され、インターフェイスに関連付けられた他のすべての IPv6 アドレスが再生成されます（重複アドレス検出は新規のリンクローカルアドレスでのみ実行されます）。

注。DAD が NBMA インターフェイスでサポートされていないため、コマンドは許可されていますが、影響のないISATAPタイプのIPv6トンネルインターフェイスには影響を与えません。インターフェイス タイプがDADをサポートしている別のタイプで変更される場合、設定は保存され、影響を与えます（IPv6 手動トンネルに対してなど）。

例

次に、重複アドレス検出がインターフェイスの仮承諾のユニキャスト IPv6 アドレスで実行された場合に、VLAN 1 で 5 つ連続して送信されるネイバー送信要求メッセージを設定する例を示します。また、この例では、VLAN 2 で重複アドレス検出処理も無効です。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd dad attempts 5
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ipv6 nd dad attempts 0
switchxxxxxx(config-if)# exit
```

ipv6 nd hop-limit

ipv6 nd hop-limit コマンドをグローバル コンフィギュレーション モードで使用して、ルータ アドバタイズメントで使用されるホップの最大数を設定します。

ホップ制限をそのデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd hop-limit *value*

no ipv6 nd hop-limit

パラメータ

- ***value***：ホップの最大数。指定できる範囲は 1 ～ 255 です。

デフォルト設定

デフォルト値が **ipv6 hop-limit** コマンドにより定義されます。コマンドが設定されていない場合は、64 ホップに設定されます。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

デフォルト値を変更する場合は、このコマンドを使用します。デフォルト値は **ipv6 hop-limit** コマンドで定義されます。

例

次の例では、VLAN 2 のルータ アドバタイズメントに 15 の最大ホップ数を設定します。

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ipv6 nd hop-limit 15
switchxxxxxx(config-if)# exit
```

ipv6 nd managed-config-flag

ipv6 nd managed-config-flag コマンドをインターフェイス コンフィギュレーション モードで使用して、IPv6 ルータ アドバタイズメントに「managed address configuration flag フラグ」を設定します。

IPv6 ルータ アドバタイズメントからこのフラグをクリアするには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

デフォルト設定

「managed address configuration flag」フラグは、IPv6 ルータ アドバタイズメントで設定されません。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

Managed Address Configuration フラグを IPv6 ルータ アドバタイズメントで設定すると、アドレスの取得にステートフル自動設定を使用するかどうかを、接続ホストに示すことができます。このフラグが設定されている場合、添付されているホストは、ステートフル自動設定を使用してアドレスを取得する必要があり、設定されていない場合は、添付されているホストは、ステートフル自動設定を使用してアドレスを取得できません。

ホストは、ステートフルおよびステートレス オートコンフィギュレーションを同時に使用できます。

例

次の例では、VLAN 1 の IPv6 ルータ アドバタイズメントに、Managed Address Configuration フラグを設定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd managed-config-flag
switchxxxxxx(config-if)# exit
```

ipv6 nd prefix

ipv6 nd prefix コマンドをインターフェイス コンフィギュレーション モードで使用して、IPv6 ネイバー探索（ND）ルータ アドバタイズメントに含まれる IPv6 プレフィックスを設定します。

プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd prefix {*ipv6-prefix*/*prefix-length* | **default**} [**no-advertise** | {[*valid-lifetime preferred-lifetime*] [**no-autoconfig**] [**off-link** | **no-onlink**]}]

no ipv6 nd prefix [*ipv6-prefix*/*prefix-length* | **default**]

パラメータ

- ***ipv6-prefix***：ルータ アドバタイズメントに含まれる IPv6 ネットワーク番号。この引数は RFC4293 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
- ***prefix-length***：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
- **default**：ipv6 address コマンドを使用して、インターフェイスのアドレスとして設定される、自動アドバタイズされたプレフィックスに使用されるデフォルト値。
- **no-advertise**：プレフィックスはアドバタイズされません。
- ***valid-lifetime***：このプレフィックスが継続して有効な残りの時間の長さ（秒単位）。つまり無効化されるまでの時間です。4,294,967,295 の値は無限を表します。無効化されたプレフィックスから生成されたアドレスは、パケットの宛先または発信元アドレスとして表示されません。
- ***preferred-lifetime***：このプレフィックスが継続して優先される残りの時間の長さ（秒単位）。つまり廃止されるまでの時間です。4,294,967,295 の値は無限を表します。廃止されたプレフィックスから生成されたアドレスは、新しい通信の発信元アドレスとして使用できなくなりますが、このようなインターフェイスで受信されたパケットは意図したとおりに処理されます。*preferred-lifetime* は *valid-lifetime* より大きくする必要があります。
- **no-autoconfig**：指定したプレフィックスは、IPv6 自動設定には使用できないことを、ローカル リンク上のホストに示します。プレフィックスは A ビット クリアでアドバタイズされます。
- **off-link**：指定したプレフィックスをオフリンクとして設定します。プレフィクスは L ビット クリアでアドバタイズされます。プレフィクスは、接続されたプレフィクスとしてルーティングテーブルに挿入されません。プレフィックスが接続されたプレフィックスとして

ルーティング テーブルにすでに存在する場合（たとえば、**ipv6 address** コマンドを使用してプレフィックスも設定された場合など）、そのプレフィックスは削除されます。

- **no-onlink**：指定したプレフィクスをオンリンクでないものとして設定します。プレフィクスは L ビット クリアでアドバタイズされます。

デフォルト設定

IPv6 ルータ アドバタイズメントを生成する、インターフェイスで設定されたすべてのプレフィックスは、有効期間 2,592,000 秒（30 日）と推奨期間 604,800 秒（7 日）でアドバタイズされます。

デフォルトで、次に注意してください。

- すべてのプレフィックスは、接続されているプレフィックスとしてルーティングテーブルに挿入されます。
- すべてのプレフィックスは、オンリンクとしてアドバタイズされます（たとえばLビットがアドバタイズメントに設定されます）
- すべてのプレフィックスが自動設定プレフィックスとしてアドバタイズされます（たとえば A ビットがアドバタイズメントに設定されます）

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、プレフィックスをアドバタイズするかどうかなど、プレフィックスごとに個々のパラメータを制御できます。

ipv6 nd prefix *ipv6-prefix*/*prefix-length* コマンドを使用して、プレフィックスをプレフィックス テーブルに追加します。

no ipv6 nd prefix *ipv6-prefix*/*prefix-length* コマンドを使用して、プレフィックスをプレフィックス テーブルから削除します。

no ipv6 nd prefix コマンドを *ipv6-prefix*/*prefix-length* 引数を指定しないで使用すると、すべてのプレフィックスがプレフィックステーブルから削除されます。

注。no ipv6 nd prefix コマンドは、デフォルト値を元のデフォルト値に戻しません。

スイッチは、次のアドバタイズメント アルゴリズムをサポートします。

- **ipv6 nd prefix default** コマンドによって定義されたパラメータを使用して、プレフィックス テーブルに配置（**ipv6 nd prefix** コマンドにより変更（設定））されているプレフィックスを除く、インターフェイスのアドレスとして設定されている（またはコマンドが設定されていない場合はデフォルト値）すべてのプレフィックスをアドバタイズします。

  ipv6 nd prefix コマンドを **no-advertise** キーワードなしで使用して、設定されているすべてのプレフィックスをアドバタイズします。

default キーワード

default キーワードは、**ipv6 address** コマンドを使用して、インターフェイスのアドレスとして設定されている自動アドバタイズされるプレフィックスのデフォルト値を設定するために使用できます。

注。これらのデフォルト値はipv6 nd prefix コマンドのデフォルト値としては使用されません。

デフォルト値を元のデフォルト値に戻すには、**no ipv6 nd prefix default** コマンドを使用します。

オンリンク

オンリンクが「オン」（デフォルト）のときは、指定されたプレフィックスがそのリンクに割り当てられます。指定されたプレフィックスを含むそのようなアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。オンリンク プレフィックスは、接続されたプレフィックスとしてルーティング テーブルに挿入されます。

自動設定

自動設定がオン（デフォルト）のときは、指定されたプレフィックスがローカル リンク上のホストの IPv6 自動設定に使用されます。

設定オプションは、次のように、IPv6 ND ルータ アドバタイズメントのプレフィックスに関連付けられている L ビットおよび A ビット設定と、ルーティング テーブル内のプレフィックスの有無に影響します。

- **Default** L=1、A=1、ルーティング テーブルにあり
- **no-onlink** L=0、A=1、ルーティング テーブルにあり
- **no-autoconfig** L=1、A=0、ルーティング テーブルにあり
- **no-onlink no-autoconfig** L=0、A=0、ルーティング テーブルにあり
- **off-link** L=0、A=1、ルーティング テーブルになし
- **off-link no-autoconfig** L=0、A=0、ルーティング テーブルになし

例 1。次に、有効期間 1000 秒、推奨期間 900 秒で、VLAN 1 から送信されるルータ アドバタイズメントに IPv6 プレフィックス 2001:0DB8::/35 を含める例を示します。プレフィックスは、ルーティング テーブルに挿入されます。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
switchxxxxxx(config-if)# exit
```

例 2。次に、L ビット クリアでプレフィックスをアドバタイズする例を示します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address 2001::1/64
switchxxxxxx(config-if)# ipv6 nd prefix 2001::/64 3600 3600 no-onlink
switchxxxxxx(config-if)# exit
```

ipv6 nd ra interval

ipv6 nd ra interval コマンドをインターフェイス コンフィギュレーション モードで使用して、インターフェイスで IPv6 ルータ アドバタイズメント（RA）伝送間隔を設定します。

デフォルトの間隔に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd ra interval *maximum-secs* [*minimum-secs*]

no ipv6 nd ra interval

パラメータ

- ***maximum-secs***：IPv6 RA 伝送の最大間隔（秒単位）。範囲は 4 ～ 1800 です。
- ***minimum-secs***：IPv6 RA 伝送の最小間隔（秒単位）。範囲は 3 ～ 1350 です。

デフォルト設定

maximum-secs は 600 秒です。

値が 3 秒以上の場合、*minimum-secs* は 0.33**maximum-sec* で、値が 3 秒未満の場合、3 秒です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用してルータがデフォルト ルータとして設定されている場合、送信間隔は IPv6 ルータ アドバタイズメントの有効期間以内でなければなりません。他の IPv6 ノードとの同期を防ぐために、実際に使用される間隔は最小値と最大値の間の値からランダムに選択されます。

RA の間隔の最小値は、最大値の 75% 以上および 3 秒未満にはできません。

例 1。次の例では、VLAN 1 での IPv6 ルータ アドバタイズメント間隔を 201 秒に設定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd ra interval 201
switchxxxxxx(config-if)# exit
```

例 2。次の例では、200 秒の最大 RA 間隔および 50 秒の最小 RA 間隔を示します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd ra interval 200 50
switchxxxxxx(config-if)# exit
```

ipv6 nd ra lifetime

ipv6 nd ra lifetime コマンドをインターフェイス コンフィギュレーション モードで使用して、インターフェイスで IPv6 ルータ アドバタイズメントにルータの有効期間の値を設定します。

デフォルトの有効期間に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd ra lifetime *seconds*

no ipv6 nd ra lifetime

パラメータ

- ***seconds***：このルータが継続してデフォルト ルータとして有効な、秒単位の残りの時間の長さ（ルータの有効期間の値）。ゼロの値は、デフォルトルータとして有効ではなくなったことを示します。許容範囲は 0 または <Maximum RA Interval> から 9000 秒までです。

デフォルト設定

デフォルトの有効期間の値は 3*<Maximum RA Interval> 秒です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ルータの有効期間の値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。この値は、このインターフェイスでのデフォルト ルータとしてルータの有用性を示します。値を 0 に設定すると、ルータは、このインターフェイスでデフォルト ルータとは見なされません。ルータがこのインターフェイスでデフォルト ルータと見なされるようにするには、ルータの有効期間の値にゼロ以外の値を設定します。ルータの有効期間の値としてゼロ以外の値を設定する場合は、その値がルータ アドバタイズメント間隔以上でなければなりません。

例

次の例では、VLAN 1 での IPv6 ルータ アドバタイズメント有効期間を 1801 秒に設定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd ra lifetime 1801
switchxxxxxx(config-if)# exit
```

ipv6 nd ra suppress

ipv6 nd ra suppress コマンドをインターフェイス コンフィギュレーション モードで使用して、インターフェイスでの IPv6 ルータ アドバタイズメント伝送を抑制します。インターフェイスでの IPv6 ルータ アドバタイズメントの送信を再び有効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd ra suppress

no ipv6 nd ra suppress

デフォルト設定

LAN インターフェイス：IPv6 ルータ アドバタイズメントは自動的に送信されます。

ポイントツーポイント インターフェイス：IPv6 ルータ アドバタイズメントは抑制されます。

NBMA インターフェイス：IPv6 ルータ アドバタイズメントは抑制されます。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

no ipv6 nd ra suppress コマンドを使用して、ポイントツーポイントインターフェイスでの IPv6 ルータ アドバタイズメントの送信を有効にします（手動トンネルなど）。

NBMA インターフェイス：IPv6 ルータ アドバタイズメントは抑制されます。

no ipv6 nd ra suppress コマンドを使用して、NBMA インターフェイスでの IPv6 ルータ アドバタイズメントの送信を有効にします（ISATAP トンネルなど）。

例 1。次の例では、vlan 1 での IPv6 ルータ アドバタイズメントを抑制します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd ra suppress
switchxxxxxx(config-if)# exit
```

例 2。次の例では、tunnel 1 での IPv6 ルータ アドバタイズメントの送信を有効にします。

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# no ipv6 nd ra suppress
switchxxxxxx(config-if)# exit
```

ipv6 nd reachable-time

ipv6 nd reachable-time コマンドをインターフェイス コンフィギュレーション モードで使用して、いくつかの到達可能性の確認イベントが発生した後に、リモート IPv6 ノードが到達可能と考えられる時間を設定します。

デフォルトの時間に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

パラメータ

- ***milliseconds***：リモート IPv6 ノードが到達可能と考えられる時間（ミリ秒単位）。許容範囲は 0 ～ 3600000 ミリ秒です。

デフォルト設定

0 ミリ秒（未指定）の場合、ルータ アドバタイズメントでアドバタイズされます。値 30000（30 秒）は、ルータ自体のネイバー探索アクティビティに使用されます。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

設定時間により、ルータは、利用不可隣接を検出できます。設定時間を短くすると、ルータは、より速く利用不可隣接を検出できます。ただし、設定時間を短くすると、すべての IPv6 ネットワーク デバイスで消費される IPv6 ネットワーク帯域幅および処理リソースが多くなります。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

設定時間は、インターフェイスから送信されるすべてのルータ アドバタイズメントに含まれるため、同じリンクのノードは同じ時間値を共有します。値に 0 を設定すると、設定時間がこのルータで指定されていないことを示します。

例

次の例では、VLAN 1 での IPv6 到達可能時間を 1,700,000 ミリ秒に設定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd reachable-time 1700000
switchxxxxxx(config-if)# exit
```

ipv6 nd router-preference

ipv6 nd router-preference コマンドをインターフェイス コンフィギュレーション モードで使用して、特定のインターフェイス上での、ルータのデフォルト ルータ設定（DRP）を設定します。

デフォルトの DRP に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd router-preference {**high** | **medium** | **low**}

no ipv6 nd router-preference

パラメータ

- **high**：インターフェイスで指定したルータの優先度は高くなります。
- **medium**：インターフェイスで指定したルータの優先度は中程度です。
- **low**：インターフェイスで指定したルータの優先度は低くなります。

デフォルト設定

ルータ アドバタイズメント（RA）は中程度の優先度で送信されます。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

RA メッセージは、このコマンドによって設定されている DRP とともに送信されます。DRP が設定されていない場合は、RA は中小規模のプリファレンスとともに送信されます。

たとえば、リンク上の2つのルータが等価ではあっても、等コストではないルーティングを提供する可能性がある場合、およびポリシーでホストがいずれかのルータを選択するよう指示された場合は、DRP が有効です。

例

次の例では、VLAN 1 上のルータに高い DRP を設定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd router-preference high
switchxxxxxx(config-if)# exit
```

ipv6 redirects

ipv6 redirects コマンドをインターフェイス コンフィギュレーション モードで使用して、パケットを受信したのと同じインターフェイスを介してパケットを再送信する、ICMP IPv6 リダイレクト メッセージの送信を有効にします。

リダイレクト メッセージの送信を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 redirects

no ipv6 redirects

デフォルト設定

ICMP IPv6 リダイレクト メッセージの送信は有効です。

コマンド モード

インターフェイス コンフィギュレーション モード

例

次の例では、VLAN 100 での ICMP IPv6 リダイレクト メッセージの送信を無効にし、VLAN 2 上のメッセージを再度有効にします。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# no ipv6 redirects
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ipv6 redirects
switchxxxxxx(config-if)# exit
```

ipv6 route

ipv6 route コマンドをグローバル コンフィギュレーション モードで使用して、IPv6 のスタティック ルートを確立します。

以前設定したスタティック ルートを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 route *ipv6-prefix*/*prefix-length* {{*next-ipv6-address* [*outgoing-interface-id*]} | *interface-id*} [*metric*]

no ipv6 route *ipv6-prefix*/*prefix-length* [{*next-ipv6-address* [*outgoing-interface-id*]} | *interface-id*]

パラメータ

- ***ipv6-prefix***：スタティック ルートの宛先となる IPv6 ネットワーク。スタティック ホスト ルートを設定する場合は、ホスト名も設定できます。
- ***prefix-length***：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
- ***next-ipv6-address***：指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。*next-ipv6-address* 引数がリンクローカルアドレスの場合、ゾーン形式で定義する必要があります（IPv6 Zone Format> ::= *IPv6-Link-Local-Address***%***Interface-ID*）。*interface-id* 引数は、スペースなしでコード化する必要があります。
- ***outgoing-interface-id***：発信インターフェイス識別子。
- ***interface-id***：発信インターフェイス識別子。この引数は、ポイントツーポイントインターフェイス（手動 IPv6 over IPv4 トンネル）にのみ適用できます。
- ***metric***：スタティック ルートのメトリック。指定できる値は 1 ～ 65535 です。デフォルト値は 1 です。

デフォルト設定

スタティック エントリは、IPv6 ネイバー探索キャッシュに設定されません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

発信インターフェイスが手動トンネルの場合に静的ルートを定義するには、**ipv6 route** *ipv6-prefix*/*prefix-length interface-id* [*metric*] コマンドを使用します。

next-ipv6-address 引数がオンリンクプレフィックスに属するグローバル IPv6 アドレスの場合、*outgoing-interface-id* 引数を省略できます。この場合、このオンリンクプレフィックスが定義さ

れているL2インターフェイスが発信インターフェイスとして使用されます。*outgoing-interface-id* 引数を設定した場合、このスイッチの決定がオーバーライドされます。

next-ipv6-address 引数が設定する必要があるオンリンクプレフィックスに属していないグローバル IPv6 アドレスの場合、*outgoing-interface-id* 引数を設定する必要があります。

next-ipv6-address 引数がリンクローカル IPv6 アドレスで、*outgoing-interface-id* 引数を省略する場合、*next-ipv6-address* 引数のゾーンは発信インターフェイスとして使用されます。*outgoing-interface-id* 引数を設定した場合は、このゾーンがオーバーライドされます。

例 1。次の例では、グローバルのネクスト ホップを含むスタティック ルートを定義します。

```
switchxxxxxx(config)# ipv6 route 2001::/64 5::5 10
```

例 2。次の例では、リンクローカルのネクスト ホップを含むスタティック ルートを定義します。

```
switchxxxxxx(config)# ipv6 route 2001:DB8:2222::/48 FE80::260:3EFF:FE11:6770%vlan1 12
```

例 3。次の例では、手動 tunnel 1 のスタティック ルートを定義します。

```
switchxxxxxx(config)# ipv6 route 2001:DB8:2222::/48 tunnel1
```

例 4。次に、発信インターフェイスで静的ルートを定義する例を示します。

```
switchxxxxxx(config)# ipv6 route 2001::/64 5::5 vlan10 10
```

ipv6 unicast-routing

ipv6 unicast-routing コマンドをグローバル コンフィギュレーション モードで使用して、IPv6 ユニキャスト データグラムの転送を有効にします。

IPv6 ユニキャスト データグラムの転送を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 unicast-routing

no ipv6 unicast-routing

デフォルト設定

IPv6 ユニキャスト ルーティングは無効です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、IPv6 ユニキャスト データグラムの転送を有効にします。

```
switchxxxxxx(config)# ipv6 unicast-routing
```

ipv6 unreachables

ipv6 unreachables コマンドをインターフェイス コンフィギュレーション モードで使用すると、指定したインターフェイスで受信したパケットの IPv6（ICMPv6）到達不能メッセージで Internet Control Message Protocol の生成を有効にできます。

到達不能メッセージが生成されないようにするには、このコマンドの **no** 形式を使用します。

構文

ipv6 unreachables

no ipv6 unreachables

デフォルト設定

ICMP IPv6 到達不能メッセージの送信が有効になっています。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

スイッチは、認識できないプロトコルを使用する自分宛てのユニキャスト パケットを受信すると、その送信元に ICMPv6 到達不能メッセージを送信します。

宛先アドレスまでのルートが不明なため最終的な宛先に配信できないデータグラムを受信した場合、スイッチはそのデータグラムの発信者に ICMP ホスト到達不能メッセージで応答します。

例

次に、必要に応じて、インターフェイス上の ICMPv6 到達不能メッセージの生成を無効にする例を示します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# no ipv6 unreachables
switchxxxxxx(config-if)# exit
```

show ipv6 interface

show ipv6 interface コマンドをユーザ EXEC または特権 EXEC モードで使用すると、IPv6 用に設定したインターフェイスの利便性の状態を表示できます。

構文

show ipv6 interface [**brief**] | [[*interface-id*] [**prefix**]]

パラメータ

- **brief**：IPv6 が定義されている各インターフェイスの IPv6 ステータスおよび設定の概要を表示します。
- ***interface-id***：情報を表示するインターフェイス識別子。
- **prefix**：ローカルの IPv6 プレフィックス プールから生成されるプレフィックス。

デフォルト設定

オプション **brief**：すべての IPv6 インターフェイスが表示されます。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

このコマンドを使用すると、インターフェイスの IPv6 ステータスとそこで設定したアドレスを検証できます。また、このコマンドは、このインターフェイスと設定されている機能での操作に対して IPv6 が使用するパラメータも表示します。

インターフェイスのハードウェアが使用できる場合、インターフェイスは up とマークされます。

省略可能なインターフェイス識別子を指定する場合、コマンドは特定のインターフェイスの情報のみを表示します。特定のインターフェイスでは、インターフェイスに設定されている IPv6 ネイバー探索（ND）プレフィックスを表示するプレフィックスのキーワードを入力できます。

キーワードは IPv6 ユニキャスト ルーティングが有効な場合にのみサポートされます。

例 1。show ipv6 interface コマンドは指定したインターフェイスの情報を表示します。

```
switchxxxxxx# show ipv6 interface vlan 1
VLAN 1 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
IPv6 Forwarding is enabled
Global unicast address(es):
Ipv6 Global Address                          Type
2000:0DB8::2/64 (ANY)                        Manual
```

```
2000:0DB8::2/64                                 Manual
2000:1DB8::2011/64                              Manual
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF11:6770
MTU is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router maximum advertisement interval is 600 seconds
ND router minimum advertisement interval is 198 seconds (DEFAULT)
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Stateless autoconfiguration is enabled.
Stateless autoconfiguration is not available (IPv6 Forwarding is enabled).
MLD Version is 2
Field Descriptions:
```

- **vlan 1 is up/up**：インターフェイスの管理/動作ステータスを示します。
- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**：IPv6 がインターフェイスで有効になっている、停止している、または無効になっていることを示します。IPv6 が有効になっている場合は、インターフェイスのステータスが Enabled と表示されます。重複アドレス検出でインターフェイスのリンクローカル アドレスが重複していると特定された場合は、そのインターフェイスでの IPv6 パケットの処理が無効になり、インターフェイスのステータスが Stalled になります。IPv6 が有効になっていない場合は、インターフェイスのステータスが Disabled と表示されます。
- **link-local address**：インターフェイスに割り当てられているリンクローカル アドレスを表示します。
- **Global unicast address(es):**：インターフェイスに割り当てるグローバル ユニキャスト アドレスを表示します。タイプは **manual** または **autoconfig** です。
- **Joined group address(es)**：このインターフェイスが属するマルチキャスト グループを示します。
- **MTU is 1500 bytes**：インターフェイスの最大転送単位。
- **ICMP error messages**：このインターフェイス上で送信されるエラー メッセージの最小間隔（ミリ秒単位）を指定します。
- **ICMP redirects**：インターフェイスでの ICMP IPv6 リダイレクト メッセージの状態（メッセージの送信が有効または無効）。
- **ND DAD**：インターフェイスでの重複アドレス検出の状態（有効または無効）。
- **number of DAD attempts**：重複アドレス検出が実行されているときに、インターフェイスで送信されるネイバー要請メッセージの連続数。

- **ND reachable time**：このインターフェイスに割り当てられているネイバー探索到達可能時間（ミリ秒単位）を表示します。
- **ND advertised reachable time**：このインターフェイスでアドバタイズされるネイバー探索到達可能時間（ミリ秒単位）を表示します。
- **ND advertised retransmit interval**：このインターフェイスでアドバタイズされるネイバー探索再送信間隔（ミリ秒単位）を表示します。
- **ND router advertisements**：このインターフェイスで送信されるネイバー探索ルータ アドバタイズメントの間隔（秒単位）およびアドバタイズメントが期限切れになるまでの時間数を指定します。
- **ND advertised default router preference is Medium**：特定のインターフェイス上のルータの DRP。
- **MLD Version**：MLD のバージョン

例 2。show ipv6 interface コマンドは、指定した手動 Ipv6 トンネルの情報を表示します。

```
switchxxxxxx# show ipv6 interface tunnel 2
Tunnel 2 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
IPv6 Forwarding is enabled
Global unicast address(es):
Ipv6 Global Address                          Type
2000:0DB8::2/64 (ANY)                        Manual
2000:0DB8::2/64                              Manual
2000:1DB8::2011/64                           Manual
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF11:6770
MTU is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
Stateless autoconfiguration is disabled.
MLD Version is 2
Tunnel mode is manual
Tunnel Local IPv4 address : 10.10.10.1(auto)
Tunnel Remote Ipv4 address : 10.1.1.1
Field Descriptions:
```

- **vlan 1 is up/up**：インターフェイスの管理/動作ステータスを示します。
- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**：IPv6 がインターフェイスで有効になっている、停止している、または無効になっていることを示します。IPv6 が有効になっている場合は、インターフェイスのステータスが「enabled」と表示されます。重複アドレス検出でインターフェイスの

リンクローカル アドレスが重複していると特定された場合は、そのインターフェイスでの IPv6 パケットの処理が無効になり、インターフェイスのステータスが「stalled」になります。IPv6 が有効になっていない場合は、インターフェイスのステータスが「disabled」と表示されます。

- **link-local address**：インターフェイスに割り当てられているリンクローカル アドレスを表示します。
- **Global Unicast address(es)**：インターフェイスに割り当てられているグローバル ユニキャスト アドレスを表示します。タイプは **manual** または **autoconfig** です。
- **Joined group address(es)**：このインターフェイスが属するマルチキャスト グループを示します。
- ：インターフェイスの最大伝送単位。
- **ICMP error messages**：このインターフェイス上で送信されるエラー メッセージの最小間隔（ミリ秒単位）を指定します。
- **ICMP redirects**：インターフェイスでのインターネット制御メッセージ プロトコル（ICMP）IPv6 リダイレクト メッセージの状態（メッセージの送信が有効か無効か）。
- **ND DAD**：インターフェイスでの重複アドレス検出の状態（有効または無効）。
- **number of DAD attempts**：重複アドレス検出が実行されているときに、インターフェイスで送信されるネイバー要請メッセージの連続数。
- **ND reachable time**：このインターフェイスに割り当てられているネイバー探索到達可能時間（ミリ秒単位）を表示します。
- **ND advertised reachable time**：このインターフェイスでアドバタイズされるネイバー探索到達可能時間（ミリ秒単位）を表示します。
- **ND advertised retransmit interval**：このインターフェイスでアドバタイズされるネイバー探索再送信間隔（ミリ秒単位）を表示します。
- **ND router advertisements**：このインターフェイスで送信されるネイバー探索ルータ アドバタイズメントの間隔（秒単位）およびアドバタイズメントが期限切れになるまでの時間数を指定します。
- **ND advertised default router preference is Medium**：特定のインターフェイス上のルータの DRP。
- **MLD Version**：MLD のバージョン
- **Tunnel mode**：トンネルモードを **manual** に指定します。
- **Tunnel Local IPv4 address**：トンネルのローカル IPv4 アドレスを、次の形式のいずれかで指定します。

  ipv4-address

ipv4-address（auto）

ipv4-address(interface-id)

Tunnel Remote Ipv4 address：トンネルのリモート IPv4 アドレスを指定します

例 3。show ipv6 interface コマンドは、指定した ISATAP トンネルの情報を表示します。

```
switchxxxxxx# show ipv6 interface tunnel 1
Tunnel 1 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
ICMP redirects are disabled
Global unicast address(es):
Ipv6 Global Address                          Type
2000:0DB8::2/64 (ANY)                        Manual
2000:0DB8::2/64                              Manual
2000:1DB8::2011/64                           Manual
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF11:6770
 is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ICMP redirects are enabled
ND DAD is disabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Stateless autoconfiguration is disabled.
MLD Version is 2
Tunnel mode is ISATAP
Tunnel Local IPv4 address : 10.10.10.1(VLAN 1)
ISATAP Router DNS name is isatap
Field Descriptions:
```

- **ND DAD**：インターフェイスでの重複アドレス検出の状態（有効または無効）。**注。**DAD が NBMA インターフェイスでサポートされていないため、**number of DAD attempts** パラメータの値に関係なく、ISATAP タイプの IPv6 トンネル インターフェイス上の重複アドレス検出の状態が disabled として常に表示されます。パラメータ値が 0 より大きく、ユーザがトンネルのタイプを手動に変更した場合は、スイッチが DAD を自動的に有効にします。
- **number of DAD attempts**：重複アドレス検出が実行されているときに、インターフェイスで送信されるネイバー要請メッセージの連続数。
- **vlan 1 is up/up**：インターフェイスの管理/動作ステータスを示します。
- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**：IPv6 がインターフェイスで有効になっている、停止している、または無効になっていることを示します。IPv6 が有効になっている場合は、インターフェイスのステータスが「enabled」と表示されます。重複アドレス検出でインターフェイスのリンクローカルアドレスが重複していると特定された場合は、そのインターフェイスでの IPv6 パケットの処理が無効になり、インターフェイスのステータスが

「stalled」になります。IPv6 が有効になっていない場合は、インターフェイスのステータスが「disabled」と表示されます。

- **link-local address**：インターフェイスに割り当てられているリンクローカル アドレスを表示します。
- **Global Unicast address(es)**：インターフェイスに割り当てられているグローバル ユニキャスト アドレスを表示します。タイプは **manual** または **autoconfig** です。
- **Joined group address(es)**：このインターフェイスが属するマルチキャスト グループを示します。
- ：インターフェイスの最大伝送単位。
- **ICMP error messages**：このインターフェイス上で送信されるエラー メッセージの最小間隔（ミリ秒単位）を指定します。
- **ICMP redirects**：インターフェイスでのインターネット制御メッセージ プロトコル（ICMP）IPv6 リダイレクト メッセージの状態（メッセージの送信が有効か無効か）。
- **number of DAD attempts**：重複アドレス検出が実行されているときに、インターフェイスで送信されるネイバー要請メッセージの連続数。
- **ND reachable time**：このインターフェイスに割り当てられているネイバー探索到達可能時間（ミリ秒単位）を表示します。
- **ND advertised reachable time**：このインターフェイスでアドバタイズされるネイバー探索到達可能時間（ミリ秒単位）を表示します。
- **ND advertised retransmit interval**：このインターフェイスでアドバタイズされるネイバー探索再送信間隔（ミリ秒単位）を表示します。
- **ND router advertisements**：このインターフェイスで送信されるネイバー探索ルータ アドバタイズメントの間隔（秒単位）およびアドバタイズメントが期限切れになるまでの時間数を指定します。
- **ND advertised default router preference is Medium**：特定のインターフェイス上のルータの DRP。
- **MLD Version**：MLD のバージョン
- **Tunnel mode**：トンネルモードを **isatap** に指定します。
- **Tunnel Local IPv4 address**：トンネルのローカル IPv4 アドレスを、次の形式のいずれかで指定します。
  - ipv4-address
  - *ipv4-address*（auto）
  - *ipv4-address(interface-id*)

- **Tunnel Remote Ipv4 address**：トンネルのリモート IPv4 アドレスを指定します
- **ISATAP Router DNS name is**：ISATAP ルータの DNS 名

例 4。brief キーワードを指定して次のコマンドを実行すると、IPv6 が定義されているすべてのインターフェイスに関する情報が表示されます。

```
switchxxxxxx# show ipv6 interface brief
Interface  Interface  IPv6     Link Local        MLD        Number of
             State     State   IPv6 Address     Version  Global Addresses
---------  --------- -------  ----------------- -------   ----------------
vlan 1     up/up     enabled  FE80::0DB8:12AB:FA01        1
1
vlan 2     up/up     stalled  FE80::0DB8:12AB:FA01        1
1
vlan 3     up/down   enabled  FE80::0DB8:12AB:FA01        1
 3
vlan 4     down/down enabled  FE80::0DB8:12AB:FA01         2
 2
vlan 5     up/up     enabled  FE80::0DB8:12AB:FA01        1
 1
vlan 100   up/up     enabled  FE80::0DB8:12AB:FA01        1
 1
vlan 1000  up/up     stalled  FE80::0DB8:12AB:FA01        1
 1
```

例 5。この出力例は、ローカル IPv6 プレフィックス プールからプレフィックスを生成した VLAN 1 の特性を示しています。

```
switchxxxxxx# configure terminal
switchxxxxxx(config)# interface vlan1
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:1::1/64
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:2::1/64
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:3::1/64
switchxxxxxx(config-if)# ipv6 nd prefix 2001:0DB8:1::/64 no-advertise
switchxxxxxx(config-if)# ipv6 nd prefix 2001:0DB8:3::/64 2912000 564900 off-link
switchxxxxxx(config-if)# ipv6 nd prefix 2001:0DB8:4::/64
switchxxxxxx(config-if)# ipv6 nd prefix 2001:0DB8:5::/64 2912000 564900 off-link
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# exit
switchxxxxxx# show ipv6 interface vlan 1 prefix
IPv6 Prefix Advertisements VLAN 1
Codes: A - Address, P - Prefix is advertised, R is in Routing Table
Code Prefix              Flags  Valid Lifetime    Preferred Lifetime
---- ----------------    ----  ---------------    ----------------------
     default             LA      2592000          604800
AR   2001:0DB8:1::/64    LA      infinite         infinite
APR  2001:0DB8:2::/64    LA      infinite         infinite
AP   2001:0DB8:3::/64    A       infinite         infinite
PR   2001:0DB8:4::/64    LA      2592000          604800
P    2001:0DB8:5::/64    A       2912000          564900
```

show ipv6 link-local default zone

show ipv6 link-local default zone コマンドをユーザ EXEC または特権 EXEC モードで使用すると、IPv6 リンク ローカル デフォルト ゾーンを表示できます。

構文

show ipv6 link-local default zone

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

例 1。次の例では、デフォルト ゾーンが定義されている場合はそのゾーンを表示します。

```
switchxxxxxx# show ipv6 link-local default zone
Link Local Default Zone is VLAN 1
```

例 2。次の例では、デフォルト ゾーンが定義されていない場合はそのゾーンを表示します。

```
switchxxxxxx# show ipv6 link-local default zone
Link Local Default Zone is not defined
```

show ipv6 nd prefix

show ipv6 nd prefix コマンドをユーザ EXEC モードまたは特権 EXEC モードで使用して、IPv6 ネイバー探索（ND）ルータ アドバタイズメントに含まれる IPv6 プレフィックスを表示します。

構文

show ipv6 nd prefix [***interface-id***]

パラメータ

- ***interface-id***：プレフィックスがアドバタイズされる、インターフェイス識別子。

デフォルト設定

プレフィックスは表示されません。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

how ipv6 nd prefix コマンドに、*interface-id* 引数を指定して使用すると、1 つのインターフェイス上でアドバタイズされるプレフィックスが表示されます。

例

次の例では、IPv6 プレフィックスが表示されます。

```
switchxxxxxx# show ipv6 nd prefix vlan 100
vlan 100
default
valid-lifetime 2,592,000 secs
preferred-lifetime 604,800 secs
on-link
auto-config
prefix 2001::1/64
valid-lifetime 3,600 secs
preferred-lifetime 2,700 secs
prefix 2001:2:12/64
no advertise
prefix 2002::1/64
valid-lifetime 3,600 secs
preferred-lifetime 2,700 secs
on-link
prefix 2011::1/64
valid-lifetime 3,600 secs
preferred-lifetime 2,700 secs
off-link
auto-config
```

show ipv6 neighbors

IPv6 ネイバー探索（ND）キャッシュ情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ipv6 neighbors** コマンドを使用します。

構文

show ipv6 neighbors [*interface-id* | *ipv6-address* | *ipv6-hostname*]

パラメータ

- ***interface-id***：IPv6 ネイバー情報が表示されるインターフェイスの識別子を指定します。
- ***ipv6-address***：ネイバーの IPv6 アドレスを指定します。この引数は RFC4293 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
- ***ipv6-hostname***：リモート ネットワーク デバイスの IPv6 ホスト名を指定します。

デフォルト設定

すべての IPv6 ND キャッシュ エントリがリスト表示されます。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

interface-id 引数が指定されていない場合、すべての IPv6 ネイバーのキャッシュ情報が表示されます。*interface-id* 引数を指定すると、指定したインターフェイスのキャッシュ情報のみが表示されます。

例 1。次に、interface-id を指定して入力された show ipv6 neighbors コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 neighbors vlan 1
IPv6 Address                Age Link-layer Addr     State  Interface Router
2000:0:0:4::2                0    0003.a0d6.141e    REACH  VLAN1       Yes
3001:1::45a                  -    0002.7d1a.9472    REACH  VLAN1       -
FE80::203:A0FF:FED6:141E     0    0003.a0d6.141e    REACH  VLAN1       No
```

例 2。次に、IPv6 アドレスを指定して入力された show ipv6 neighbors コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 neighbors 2000:0:0:4::2
IPv6 Address                Age Link-layer Addr     State  Interface Router
2000:0:0:4::2                0    0003.a0d6.141e    REACH  VLAN1       Yes
Field Descriptions:
```

- **Total number of entries**：キャッシュのエントリ（ピア）の数。

- **IPv6 Address**：ネイバーまたはインターフェイスの IPv6 アドレス。
- **Age**：アドレスが到達可能と確認されてから経過した時間（分）。ハイフン（-）はスタティック エントリを示します。
- **Link-layer Addr**：MAC アドレス。アドレスが不明の場合、ハイフン（-）が表示されます。
- **Interface**：ネイバーが接続されているインターフェイス。
- **Router**：ネイバーがルータかどうかを指定します。スタティック エントリのハイフン（-）が表示されます。

show ipv6 route

show ipv6 route コマンドをユーザ EXEC または特権 EXEC モードで使用すると、IPv6 ルーティング テーブルの現在のコンテンツを表示できます。

構文

show ipv6 route [*ipv6-address* | *ipv6-prefix/prefix-length* | *protocol* | **interface** *interface-id*]

パラメータ

- ***ipv6-address***：特定の IPv6 アドレスのルーティング情報を表示します。この引数は RFC4293 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
- ***ipv6-prefix***：特定の IPv6 ネットワークのルーティング情報を表示します。この引数は RFC4293 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
- ***prefix-length***：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
- **protocol**：**bgp**、**isis**、**ospf**、または **rip** の各キーワードを使用して指定したルーティング プロトコルのルートを表示し、**connected**、**static**、**nd**、または **icmp** の各キーワードを使用してルートの指定したタイプのルートを表示します。
- **interface** *interface-id*：インターフェイスの識別子。

デフォルト設定

すべてのアクティブなルーティング テーブルのすべての IPv6 ルーティング情報が表示されます。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

IPv6 に固有の情報である点を除いて、このコマンドの出力は、**show ip route** コマンドの出力と類似しています。

ipv6-address または *ipv6-prefix*/*prefix-length* 引数が指定されている場合、最長一致ルックアップがルーティング テーブルから実行され、このアドレスまたはネットワークのルート情報のみが表示されます。**icmp**、**nd**、**connected**、**local**、または **static** の各キーワードが指定されている

場合、このタイプのルートのみが表示されます。*interface-id* 引数が指定されている場合、指定したインターフェイス固有のルートのみが表示されます。

例 1。次に、IPv6 ルーティングが有効になっていないときに、IPv6 アドレスまたはプレフィックスを指定せずに **show ipv6 route** コマンドを入力した場合の出力例を示します。

```
switchxxxxxx# show ipv6 route
Codes: > - Best
       S - Static, C - Connected(from ipv6 address), I - ICMP Redirect, ND - Router
Advertisment
[d/m]: d - route’s distance, m - route’s metric
IPv6 Forwarding is disabled
IPv6 Routing Table - 4 entries
S> ::/0 [1/1]
   via:: fe80::77  VLAN 1
ND> ::/0   [3/2]
   via:: fe80::200:cff:fe4a:dfa8 VLAN 1 Lifetime 1784 sec
C> 3002:1:1:1:1/64   [0/0]
   via:: VLAN 1
ND> 3004:1:1:1:1/64   [0/0]
   via:: VLAN 100 Lifetime 1784 sec
```

例 2。次に、IPv6 ルーティングが有効になっており、IPv6 アドレスまたはプレフィックスを指定せずに **show ipv6 route** コマンドを入力した場合の出力例を示します。

```
switchxxxxxx# show ipv6 route
Codes: > - Best
    S - Static, C - Connected(from ipv6 address),
   L - Local(on-link prefixes defined by the ipv6 nd prefix command with on-link keyword,
[d/m]: d - route’s distance, m - route’s metric
IPv6 Forwarding is enabled (hardware forwarding is not active)
IPv6 Policy Routing
VLAN 1
   Route Map:   BPR1
   Status:   Active
      ACL Name: ACLTCPHTTP
         Next Hop: fe80::77
         Next Hop Status: Active
      ACL Name: ACLTCPTELNET
          Next Hop: 4001::27
          Next Hop Status: Not Active (Unreachable)
      ACL Name: ACL_AA
         Next Hop: 301a:23:24
         Next Hop Status: Not Active (Not direct)
VLAN 100
   Route Map:   BPR_10
   Status:   Not Active (No IP interface on VLAN 100)
      ACL Name: ACLTCPHTTP
        Next Hop: 4214::10
        Next Hop Status: Active
VLAN 110
   Route Map:   BPR_20
   Status:   Not Active (VLAN 110 status is DOWN)
      ACL Name: ACLTCPHTTP
        Next Hop: 3004:1241::73
        Next Hop Status: Active
VLAN 200
   Route Map:   BPR_A0
   Status:   Active
      ACL Name: ACLTCPHTTP
         Next Hop: 3004:1241::73
```

```
         Next Hop Status: Active
IPv6 Routing Table - 3 entries
S>   3000::/64 [1/1]
       via:: FE80::A8BB:CCFF:FE02:8B00   VLAN 100
C>   4001::/64 [0/0]
       via::   VLAN 100
L>   4002::/64 [0/0]
       via::   VLAN 100 Lifetime 9000 sec
```

show ipv6 route summary

show ipv6 route summary コマンドをユーザ EXEC または特権 EXEC モードで使用すると、サマリー形式で IPv6 ルーティング テーブルの現在の内容を表示できます。

構文

show ipv6 route summary

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

例

次に、show ipv6 route summary コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 route summary
IPv6 Routing Table Summary - 97 entries
37 local, 35 connected, 25 static
Number of prefixes:
/16: 1, /28: 10, /32: 5, /35: 25, /40: 1, /64: 9
/96: 5, /112: 1, /127: 4, /128: 36
```

show ipv6 static

show ipv6 static コマンドをユーザ EXEC モードまたは特権 EXEC モードで使用して、IPv6 ルーティング テーブルの現在のスタティック ルートを表示します。

構文

show ipv6 static [*ipv6-address* | *ipv6-prefix*/*prefix-length*] [**interface** *interface-id*][**detail**]

パラメータ

- ***ipv6-address***：特定の IPv6 アドレスのルーティング情報を提供します。この引数は RFC4293 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
- ***ipv6-prefix***：特定の IPv6 ネットワークのルーティング情報を提供します。この引数は RFC4293 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
- ***prefix-length***：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
- **interface** *interface-id*：インターフェイスの識別子。
- **detail**：無効なルートの場合、ルートが無効な理由。

デフォルト設定

すべてのアクティブなルーティング テーブルのすべての IPv6 スタティック ルーティングの情報が表示されます。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

ipv6-address または *ipv6-prefix*/*prefix-length* 引数が指定される場合、ルーティング テーブルから、最長一致の検索が実行され、そのアドレスまたはネットワークのルート情報のみが表示されます。コマンドシンタックスで指定された条件に一致する情報だけが表示されます。たとえば、*interface-id* 引数を指定すると、指定したインターフェイス固有のルートのみが表示されます。

detail キーワードを指定すると、無効な直接または完全に指定したルートの、無効な理由が表示されます。

例 1。次に、オプションを指定しない場合の **show ipv6 static** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 static
IPv6 Static routes   Code: * - installed in Forwarding Information Base (FIB)
IPv6 Static routes distance is 1
* 3000::/16, via outgoing interface tunnel1, metric 1
  5000::/16, via outgoing interface tunnel2, metric 1
* 5555::/16, via outgoing interface VLAN100 nexthop 4000::1 metric 1
  5555::/16, via outgoing interface VLAN10 nexthop 9999::1 vlan100 metric 1
* 5555::/16, via outgoing interface VLAN100 nexthop 4001:AF00::1,  metric 1
* 6000::/16, via outgoing interface VLAN1 nexthop 2007::1 metric 1
```

例 2。次に、IPv6 プレフィックス 2001:200::/35 を指定して入力した **show ipv6 static** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 static 2001:200::/35
IPv6 Static routes   Code: * - installed in Forwarding Information Base (FIB)
IPv6 Static routes distance is 1
* 2001:200::/35, via outgoing interface VLAN100 nexthop 4000::1, metric 1
   2001:200::/35, via outgoing interface VLAN10 nexthop 9999::1, metric 1
```

例 3。次に、インターフェイス VLAN 1 を指定して入力した場合の **show ipv6 static** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 static interface vlan 1
IPv6 Static routes   Code: * - installed in Forwarding Information Base (FIB)
IPv6 Static routes distance is 1
* 5000::/16, via outgoing interface VLAN1 nexthop 4000::1, metric 1
```

例 4。次に、**detail** キーワードを指定した場合の **show ipv6 static** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 static detail
IPv6 Static routes   Code: * - installed in Forwarding Information Base (FIB)
IPv6 Static routes distance is 1
* 3000::/16, via outgoing interface tunnel1, metric 1
  5000::/16, via outgoing interface tunnel2, metric 1
  5000::/16, via outgoing interface VLAN2 nexthop 2003::1, metric 1
         Interface is down
* 5555::/16, via outgoing interface VLAN100 nexthop 4000::1, metric 1
  5555::/16, via outgoing interface VLAN10 nexthop 9999::1, metric 1
         Route does not fully resolve
* 5555::/16, via outgoing interface VLAN12 nexthop 4001:AF00::1, metric 1
* 6000::/16, via outgoing interface VLAN102 nexthop 2007::1, metric 1
```

IPv6 ファースト ホップ セキュリティ

この章は、次の項で構成されています。

- address-config （724 ページ）
- address-prefix-validation （726 ページ）
- clear ipv6 first hop security counters （727 ページ）
- clear ipv6 first hop security error counters （728 ページ）
- clear ipv6 neighbor binding prefix table （729 ページ）
- clear ipv6 neighbor binding table （730 ページ）
- device-role（IPv6 DHCP ガード） （731 ページ）
- device-role（ネイバー バインディング） （733 ページ）
- device-role（RA ガード ポリシー） （735 ページ）
- device-role（ND インスペクション ポリシー） （736 ページ）
- drop-unsecure （738 ページ）
- hop-limit （739 ページ）
- ipv6 dhcp guard （741 ページ）
- ipv6 dhcp guard attach-policy（ポート モード） （742 ページ）
- ipv6 dhcp guard attach-policy（VLAN モード） （744 ページ）
- ipv6 dhcp guard policy （745 ページ）
- ipv6 dhcp guard preference （747 ページ）
- ipv6 first hop security （749 ページ）
- ipv6 first hop security attach-policy（ポート モード） （750 ページ）
- ipv6 first hop security attach-policy（VLAN モード） （752 ページ）
- ipv6 first hop security logging packet drop （753 ページ）
- ipv6 first hop security policy （754 ページ）
- ipv6 nd inspection （756 ページ）
- ipv6 nd inspection attach-policy（ポート モード） （757 ページ）
- ipv6 nd inspection attach-policy（VLAN モード） （759 ページ）
- ipv6 nd inspection drop-unsecure （760 ページ）
- ipv6 nd inspection policy （761 ページ）
- ipv6 nd inspection sec-level minimum （763 ページ）

- ipv6 nd inspection validate source-mac （764 ページ）
- ipv6 nd raguard （765 ページ）
- ipv6 nd raguard attach-policy（ポート モード） （766 ページ）
- ipv6 nd raguard attach-policy（VLAN モード） （768 ページ）
- ipv6 nd raguard hop-limit （769 ページ）
- ipv6 nd raguard managed-config-flag （771 ページ）
- ipv6 nd raguard other-config-flag （772 ページ）
- ipv6 nd raguard policy （773 ページ）
- ipv6 nd raguard router-preference （775 ページ）
- ipv6 neighbor binding （777 ページ）
- ipv6 neighbor binding address-config （778 ページ）
- ipv6 neighbor binding address-prefix （780 ページ）
- ipv6 neighbor binding address-prefix-validation （782 ページ）
- ipv6 neighbor binding attach-policy（ポート モード） （783 ページ）
- ipv6 neighbor binding attach-policy（VLAN モード） （785 ページ）
- ipv6 neighbor binding lifetime （786 ページ）
- ipv6 neighbor binding max-entries （787 ページ）
- ipv6 neighbor binding policy （788 ページ）
- ipv6 neighbor binding static （790 ページ）
- ipv6 source guard （791 ページ）
- ipv6 source guard attach-policy（ポート モード） （792 ページ）
- ipv6 source guard policy （794 ページ）
- logging binding （796 ページ）
- logging packet drop （797 ページ）
- managed-config-flag （798 ページ）
- match ra address （799 ページ）
- match ra prefixes （800 ページ）
- match reply （802 ページ）
- match server address （804 ページ）
- max-entries （806 ページ）
- other-config-flag （808 ページ）
- preference （809 ページ）
- router-preference （810 ページ）
- sec-level minimum （811 ページ）
- show ipv6 dhcp guard （812 ページ）
- show ipv6 dhcp guard policy （813 ページ）
- show ipv6 first hop security （815 ページ）
- show ipv6 first hop security active policies （816 ページ）
- show ipv6 first hop security attached policies （818 ページ）
- show ipv6 first hop security counters （819 ページ）
- show ipv6 first hop security error counters （821 ページ）

- show ipv6 first hop security policy （822 ページ）
- show ipv6 nd inspection （824 ページ）
- show ipv6 nd inspection policy （825 ページ）
- show ipv6 nd raguard （827 ページ）
- show ipv6 nd raguard policy （828 ページ）
- show ipv6 neighbor binding （830 ページ）
- show ipv6 neighbor binding policy （831 ページ）
- show ipv6 neighbor binding prefix table （833 ページ）
- show ipv6 neighbor binding table （834 ページ）
- show ipv6 source guard （836 ページ）
- show ipv6 source guard policy （837 ページ）
- trusted-port（IPv6 Source Guard） （838 ページ）
- validate source-mac （839 ページ）

address-config

IPv6 ネイバー バインディング ポリシー内のグローバル IPv6 アドレスに許可された設定方法を指定するには、ネイバー バインディング ポリシーのコンフィギュレーション モードで address-config コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

address-config [stateless | any] [dhcp]

no address-config

パラメータ

- **stateless**：NDP メッセージからバインドされたグローバル IPv6 の自動設定のみが許可されます。
- **any**：NDP メッセージ（ステートレスおよび手動）からバインドされたグローバル IPv6 の設定方法のすべてが許可されます。キーワードが定義されていない場合は、キーワード **any** が適用されます。
- **dhcp**：DHCPv6 からのバインドが許可されます。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ネイバー バインディング ポリシー コンフィギュレーション モード。

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

キーワードが定義されていない場合は、**address-config any** コマンドが適用されます。

例

次の例では、DHCP アドレスの設定方法のみを許可するようにグローバル設定を変更する方法を示します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# address-config dhcp
switchxxxxxx(config-nbr-binding)# exit
```

address-prefix-validation

IPv6 ネイバー バインディング ポリシー内でバインドされたアドレス プレフィックス検証を定義するには、**address-prefix-validation** コマンドをネイバー バインディング ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

address-prefix-validation [enable | disable]

no address-prefix-validation

パラメータ

- **enable**：バインドされたアドレス プレフィックス検証を有効にします。キーワードが設定されていない場合、デフォルトでこのキーワードが適用されます。
- **disable**：バインドされたアドレス プレフィックス検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN に接続されているポリシー：グローバル設定された値。

コマンド モード

ネイバー バインディング ポリシー コンフィギュレーション モード。

使用上のガイドライン

このコマンドを含むポリシーがVLANに接続される場合、グローバル設定を上書きし、VLANのすべてのポートに適用されます。このコマンドをポートに接続されているポリシーで使用する場合、グローバル設定および VLAN 設定を上書きします。

例

次の例では、ネイバーバインディングでグローバルにバインドされたアドレスの検証を変更する policy1 を定義する方法を示します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# address-prefix-validation enable
switchxxxxxx(config-nbr-binding)# exit
```

clear ipv6 first hop security counters

IPv6 ファースト ホップ セキュリティ ポート カウンタをクリアするには、**clear ipv6 first hop security counters** コマンドを特権 EXEC モードで使用します。

構文

clear ipv6 first hop security counters [interface *interface-id*]

パラメータ

- **interface** *interface-id*：指定したイーサネット ポートまたはポート チャネルの IPv6 ファースト ホップ セキュリティ カウンタをクリアします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、IPv6 ファースト ホップ セキュリティによって処理されるパケットのポート カウンタをクリアします。

キーワード **interface** を使用すると、特定のポートのすべてのカウンタをクリアできます。

キーワードを指定せずにコマンドを使用すると、すべてのカウンタがクリアされます。

例

次に、ポート gi1/0/1 の IPv6 ファースト ホップ セキュリティ カウンタをクリアする例を示します。

```
switchxxxxxx# clear ipv6 first hop security counters interface gi1/0/1
```

clear ipv6 first hop security error counters

IPv6ファーストホップセキュリティ グローバルエラーカウンタをクリアするには、**clear ipv6 first hop security error counters** コマンドを特権 EXEC モードで使用します。

構文

clear ipv6 first hop security error counters

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドはグローバル エラー カウンタをクリアします。

例

次の例では、IPv6 ファースト ホップ セキュリティ エラー カウンタをクリアします。

```
switchxxxxxx# clear ipv6 first hop security error counters
```

clear ipv6 neighbor binding prefix table

ネイバー プレフィックス テーブルからダイナミック エントリを削除するには、**clear ipv6 neighbor binding prefix table** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

clear ipv6 neighbor binding prefix table [**vlan** *vlan-id*] [*prefix-address*/*prefix-length*]

パラメータ

- ***vlan-id***：指定した VLAN に一致するダイナミック プレフィックスをクリアします。
- ***prefix-address*/ *prefix-length***：特定のダイナミックプレフィックスをクリアします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドを使用すると、ネイバー プレフィックス テーブルのダイナミック エントリを削除できます。

clear ipv6 neighbor binding prefix table vlan *vlan-id prefix-address*/*prefix-length* コマンドを使用すると、特定の 1 つのエントリを削除できます。

clear ipv6 neighbor binding prefix table vlan *vlan-id* コマンドを使用すると、指定した VLAN に一致するダイナミック エントリを削除できます。

すべてのダイナミックエントリを削除するには、**clear ipv6 neighbor binding prefix table** コマンドを使用します。

例 1。次の例では、すべてのダイナミック エントリをクリアします。

```
switchxxxxxx# clear ipv6 neighbor binding prefix table
```

例 2。次の例では、VLAN 100 に一致するすべてのダイナミック プレフィックスをクリアします。

```
switchxxxxxx# clear ipv6 neighbor binding prefix table vlan 100
```

例 3。次の例では、特定の 1 つのプレフィックスをクリアします。

```
switchxxxxxx# clear ipv6 neighbor binding prefix table vlan 100 2002:11aa:0000:0001::/64
```

clear ipv6 neighbor binding table

ネイバー バインディング テーブルからダイナミック エントリを削除するには、**clear ipv6 neighbor binding table** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

clear ipv6 neighbor binding table [**vlan** *vlan-id*] [**interface** *interface-id*] [**ipv6** *ipv6-address*] [**mac** *mac-address*] [**ndp** | **dhcp**]

パラメータ

- **vlan** *vlan-id*：指定した VLAN に一致するダイナミック エントリをクリアします。
- **interface** *interface-id*：指定したポート（イーサネット ポートまたはポート チャネル）に一致するダイナミック エントリをクリアします。
- **ipv6** *ipv6-address*：指定した IPv6 アドレスに一致するダイナミック エントリをクリアします。
- **mac** *mac-address*：指定した MAC アドレスに一致するダイナミック エントリをクリアします。
- **ndp**：NDP メッセージからバインドされたダイナミック エントリをクリアします。
- **dhcp**：DHCPv6 メッセージからバインドされたダイナミック エントリをクリアします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドを使用すると、ネイバー バインディング テーブルのダイナミック エントリが削除されます。削除するダイナミック エントリは、引数 *vlan-id*、引数 *interface-id*、IPv6 アドレス、MAC アドレス、またはバインドされたダイナミック エントリのメッセージ タイプ別に指定できます。

キーワード **ndp** およびキーワード **dhcp** が定義されていない場合、エントリはその送信元に関係なく削除されます。キーワードまたは引数が入力されていない場合は、すべてのダイナミック エントリが削除されます。すべてのキーワードと引数の組み合わせを使用できます。

例

次に、VLAN 100 とポート gi1/0/1 上に存在するすべてのダイナミックエントリをクリアする例を示します。

```
switchxxxxxx# clear ipv6 neighbor binding table vlan 100 interface gi1/0/1
```

device-role（IPv6 DHCP ガード）

IPv6 DHCP ガード ポリシー内のポートに接続されたデバイスのロールを指定するには、**device-role** コマンドを IPv6 DHCPv6 ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

device-role {client | server}

no device-role

パラメータ

- **client**：デバイスのロールを DHCPv6 クライアントに設定します。
- **server**：デバイスのロールを DHCPv6 サーバに設定します。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN に接続されているポリシー：クライアント。

コマンド モード

DHCP ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

IPv6 DHCP ガードは、DHCPv6 サーバ/リレーで送信された、およびクライアントとして設定されているポートで受信した次の DHCPv6 メッセージを廃棄します。

- ADVERTISE
- REPLY
- RECONFIGURE
- RELAY-REPL
- LEASEQUERY-REPLY

例

次の例では、ポリシー 1 という名前の IPv6 DHCP ガード ポリシーを定義し、ポートのロールにサーバを設定します。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

device-role（ネイバー バインディング）

IPv6 ネイバー バインディング ポリシー内のポートに接続されたデバイスのロールを指定するには、**device-role** コマンドを IPv6 ネイバー バインディング ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

device-role {perimeter | internal}

no device-role

パラメータ

- **perimeter**：ポートが IPv6 ファースト ホップ セキュリティをサポートしていないデバイスに接続されるように指定します。
- **internal**：ポートが IPv6 ファースト ホップ セキュリティをサポートしているデバイスに接続されるように指定します。

デフォルト設定

ポートまたはポート チャネルに接続されたポリシー：VLAN に接続されたポリシーで設定された値。

VLAN に接続されているポリシー：境界。

コマンド モード

ネイバー バインディング ポリシー コンフィギュレーション モード。

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

NB 整合性は境界モードをサポートしています（RFC 6620 を参照）。

このモデルでは、次の 2 つのポート タイプを指定します。

- **Perimeter Port**：NB 整合性をサポートしていないデバイスに接続されたポートを指定します。NB 整合性により、このポートに接続されているネイバーのバインディングが確立されます。ソース ガードはこのポートでは機能しません。
- **Internal Port**：2 つ目のタイプでは、IPv6 ファースト ホップ セキュリティをサポートしているデバイスに接続されたポートを指定します。NB 整合性により、このポートに接続されているネイバーのバインディングは確立されませんが、境界ポートで確立されたバインディングは反映されます。

このロールが境界から内部に変更されると、ポートにバインドされたダイナミック IPv6 アドレスが削除されます。スタティック IPv6 アドレスが保持されます。

例

次の例では、ポリシー 1 という名前のネイバー バインディング ポリシーを定義し、ポートのロールに内部ポートを設定します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# exit
```

device-role（RA ガード ポリシー）

IPv6 RA ガード ポリシー内のポートに接続されたデバイスのロールを指定するには、**device-role** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

device-role {host | router}

no device-role

パラメータ

- **host**：デバイスの権限をホストに設定します。
- **router**：デバイスの権限をルータに設定します。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：ホスト。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

RA ガードは、ホストとして設定されているポートで受信された入力 RA、CPA、および ICMPv6 リダイレクト メッセージを廃棄します。

例

次の例では、ポリシー 1 という名前の RA ガード ポリシーを定義し、ポートのロールに **router** を設定します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

device-role（ND インスペクション ポリシー）

IPv6 ND インスペクション ポリシー内のポートに接続されたデバイスのロールを指定するには、**device-role** コマンドを ND インスペクション ポリシー コンフィギュレーション モードで使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

device-role {host | router}

no device-role

パラメータ

- **host**：デバイスの権限をホストに設定します。
- **router**：デバイスの権限をルータに設定します。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：ホスト。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

NDインスペクションは、ポートのロールに応じてNDPメッセージの出力フィルタリングを実行します。次の表では、フィルタリング ルールを指定します。

メッセージ	ホスト	ルータ
RA	許可	許可
RS	拒否	許可
CPA	許可	許可
CPS	拒否	許可
ICMP Redirect	許可	許可

例

次の例では、ポリシー1という名前のNDインスペクション ポリシーを定義し、ポートのロールにルータを設定します。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

drop-unsecure

IPv6 NDインスペクション ポリシー内のオプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップできるようにするには、drop-unsecure コマンドを ND インスペクション ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、no 形式のコマンドを使用します。

構文

drop-unsecure [enable | disable]

no drop-unsecure

パラメータ

- **enable**：オプションが指定されていないか無効なオプションが指定されているか、または署名が無効なメッセージのドロップを有効にします。キーワードが設定されていない場合、デフォルトでこのキーワードが適用されます。
- **disable**：オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップできません。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLANのポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

例

次の例では、policy1 という名前の ND インスペクション ポリシーを定義し、ND インスペクション ポリシー コンフィギュレーション モードでスイッチを配置して、オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをスイッチがドロップできるようにします。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure

switchxxxxxx(config-nd-inspection)# exit
```

hop-limit

IPv6 RA ガード ポリシー内の RA メッセージでアドバタイズされた Cur ホップ制限値の検証を有効にするには、**hop-limit** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

hop-limit {[maximum {*value* | disable}] [minimum {*value* | disable}]}

no hop-limit [maximum] [minimum]

パラメータ

- **maximum** *value*：ホップカウント制限が **value** 引数以下であることを確認します。範囲 1 ～ 255。高位境界の値は、低位境界の値以上でなければなりません。
- **maximum disable**：ホップカウント制限の高位境界の検証を無効にします。
- **minimum** *value*：ホップ数制限が **value** 引数以上であることを確認します。範囲 1 ～ 255。
- **minimum disable**：ホップカウント制限の下位境界の検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLANのポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

キーワード **disable** を使用すると、グローバル設定または VLAN 設定に関係なく検証を無効にできます。

例 1：次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード ポリシー コンフィギュレーション モードでスイッチを配置して、最小 Cur ホップ制限値を 5 に定義します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# hop-limit minimum 5
switchxxxxxx(config-ra-guard)# exit
```

例 2：次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード ポリシー コンフィギュレーション モードでスイッチを配置して、Cur ホップ制限の高位境界の検証を無効にします。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# hop-limit maximum disable
switchxxxxxx(config-ra-guard)# exit
```

ipv6 dhcp guard

VLAN 上の DHCPv6 ガード機能を有効にするには、**ipv6 dhcp guard** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 dhcp guard

no ipv6 dhcp guard

デフォルト設定

VLAN 上の DHCPv6 ガードは無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

DHCPv6 ガードは、DHCPv6 サーバ/リレーからクライアントに送信して DHCPv6 サーバとして設定されていないポートで受信したメッセージをブロックします。リレー エージェントによってクライアントからサーバに送信されるクライアント メッセージはブロックされません。

DHCPv6 ガードは、送信元ポートに接続されている DHCPv6 ガード ポリシーに基づいて受信した DHCPv6 メッセージを検証します。

例 1：次の例では、VLAN 100 上の DHCPv6 ガードを有効にします。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp guard
switchxxxxxx(config-if)# exit
```

例 2：次の例では、VLAN 100-107 上の DHCPv6 ガードを有効にします。

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 dhcp guard
switchxxxxxx(config-if-range)# exit
```

ipv6 dhcp guard attach-policy（ポート モード）

特定のポートに DHCPv6 ガード ポリシーを接続するには、**ipv6 dhcp guard attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 dhcp guard attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 dhcp guard attach-policy [*policy-name*]

パラメータ

- ***policy-name***：DHCPv6 ガード ポリシー名（最大 32 文字）。
- **vlan** *vlan-list*：DHCPv6 ガードポリシーを *vlan-list* 内の VLAN に接続するように指定します。キーワード **vlan** が設定されていない場合、ポリシーは DHCPv6 ガードが有効になっているデバイス上のすべての VLAN に適用されます。

デフォルト設定

DHCPv6 ガード デフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、DHCPv6 ガード ポリシーをポートに接続できます。

コマンドを使用するたびに、同じポリシー内の以前のコマンドが上書きされます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

vlan キーワードを使用した複数のポリシーは、共通の VLAN を持っていない場合は同じポートに接続できます。

入力パケットに適用されているルールのセットは次のように構築されます。

- パケットが到着した VLAN 上のインターフェイスに接続されたポートで設定されたルールがセットに追加されます。
- VLAN に接続されたポリシーで設定されたルールがセットに追加されます（追加されていない場合）。
- グローバル ルールがセットに追加されます（追加されていない場合）。

no ipv6 dhcp guard attach-policy を使用すると、ポートに接続されたすべてのユーザ定義済み DHCP ガード ポリシーを切り離すことができます。

ポートから特定のポリシーを切り離すには、**no ipv6 dhcp guard attach-policy** *policy-name* を使用します。

例 1：次に、DHCPv6 ガードポリシー policy1 を gi1/0/1 ポートに接続し、デフォルトのポリシー port_default を切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、DHCPv6 ガードポリシー policy1 を gi1/0/1 ポートに接続し、VLAN 1 ～ 10 と 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

例 3：次に、DHCPv6 ガードポリシー policy1 を gi1/0/1 ポートに接続して VLAN 1 ～ 10 に適用し、DHCPv6 ガードポリシー policy2 を gi1/0/1 ポートに接続して VLAN 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

例 4：次に、DHCPv6 ガードを gi1/0/1 ポートから policy1 を切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 dhcp guard attach-policy（VLAN モード）

指定した VLAN に DHCPv6 ガード ポリシーを接続するには、**ipv6 dhcp guard attach-policy** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 dhcp guard attach-policy *policy-name*

no ipv6 dhcp guard attach-policy

パラメータ

- ***policy-name***：DHCPv6 ガード ポリシー名（最大 32 文字）。

デフォルト設定

DHCPv6 ガード デフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、DHCPv6 ガード ポリシーを VLAN に接続できます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

コマンドの **no** 形式を使用すると、現在のポリシーを切り離してデフォルト ポリシーを再び接続できます。デフォルト ポリシーが接続されている場合、コマンドの **no** 形式は無効です。

例

次の例では、DHCPv6 ガード ポリシー policy1 は VLAN 100 に接続されています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 dhcp guard policy

DHCP ガード ポリシーを定義して DHCPv6 ガード ポリシー コンフィギュレーション モードでスイッチを配置するには、**ipv6 dhcp guard policy** コマンドをグローバル コンフィギュレーション モードで使用します。DHCPv6 ガード ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 dhcp guard policy *policy-name*

no ipv6 dhcp guard policy *policy-name*

パラメータ

- ***policy-name***：DHCPv6 ガード ポリシー名（最大 32 文字）。

デフォルト設定

DHCPv6 ガード ポリシーは設定されていません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、DHCPv6 ガードポリシー名を定義し、DHCPv6 ガードポリシー コンフィギュレーション モードでルータを配置します。

同じタイプの各ポリシー（たとえば、DHCPv6 ガードポリシーなど）には一意の名前が必要です。異なるタイプのポリシーには同じポリシー名を設定できます。

スイッチは、「vlan_default」と「port_default」という 2 つの定義済みのデフォルト DHCPv6 ガード ポリシーをサポートします。

```
ipv6 dhcp guard policy vlan_default
      exit
      ipv6 dhcp guard policy port_default
      exit
```

デフォルト ポリシーは空で削除できませんが、変更することはできます。**no ipv6 dhcp guard policy** はデフォルト ポリシーを削除せずに、ユーザが定義したポリシー設定のみを削除します。

ipv6 dhcp guard policy コマンドを複数回使用すると、ポリシーを定義できます。

接続したポリシーを削除する前に、次の例 3 が示すように確認要求がユーザに表示されます。

例 1：次の例では、policy1 という名前の DHCPv6 ガード ポリシーを定義して、DHCPv6 でガード ポリシー コンフィギュレーション モードでルータを配置し、ポートが保護

されていないメッセージをドロップするように設定して、デバイス ロールをルータに設定します。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address list1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

例 2：次の例では、policy1 という名前の DHCPv6 ガードを複数の手順で定義します。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

例 3：次の例では、接続している DHCPv6 ガード ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 dhcp guard policy policy1
Policy policy1 is applied on the following ports:
 gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 dhcp guard preference

DHCPv6 サーバから送信されたメッセージ内の環境設定の検証をグローバルに有効にするには、**ipv6 dhcp guard preference** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 dhcp guard preference {[**maximum** *value*] [**minimum** *value*]}

no ipv6 dhcp guard preference [maximum] [minimum]

パラメータ

- **maximum** *value*：アドバタイズされたプリファレンス値は、**value** 引数以下です。範囲 0 ～ 255。高境界の値は、低境界の値以上である必要があります。
- **minimum** *value*：アドバタイズ設定値は **value** 引数以上です。範囲 0 ～ 255。

デフォルト設定

検証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドにより、DHCPv6サーバから送信されたメッセージ内のプリファレンス値（RFC3315を参照）が *value* 引数を超えるまたは未満であることを検証できます。

注。DHCPv6 ガードが RELAY-REPL メッセージを受信する場合は、カプセル化されたメッセージから取得します。

minimum *value* キーワードと引数を設定すると、許容される最小値が指定されます。**value** 引数で指定した値未満のプリファレンス値を持つ受信済みDHCPv6返信メッセージはドロップされます。

maximum *value* キーワードと引数を設定すると、許容される最大値が指定されます。**value** 引数で指定した値を超えるプリファレンス値を持つ受信済みDHCPv6返信メッセージはドロップされます。

no ipv6 dhcp guard preference を使用すると、DHCPv6 返信メッセージ内でアドバタイズされたプリファレンス値の検証を無効にできます。

no ipv6 dhcp guard preference maximum を使用すると、DHCPv6 メッセージ内でアドバタイズされたプリファレンス値の最大境界の検証を無効にできます。

no ipv6 dhcp guard preference minimum コマンドを使用すると、DHCPv6 メッセージ内でアドバタイズされたプリファレンス値の最小境界の検証を無効にできます。

例 1：次の例では、2 つのコマンドを使用して、グローバル最小プリファレンス値に 10 を、グローバル最大プリファレンス値に 102 を定義します。

```
switchxxxxxx(config)# ipv6 dhcp guard preference minimum 10
switchxxxxxx(config)# ipv6 dhcp guard preference maximum 102
```

例 2：次の例では、1 つのコマンドを使用して、グローバル最小プリファレンス値に 10 を、グローバル最大プリファレンス値に 102 を定義します。

```
switchxxxxxx(config)# ipv6 dhcp guard preference minimum 10 maximum 102
```

ipv6 first hop security

VLAN 上で IPv6 ファースト ホップ セキュリティをグローバルに有効にするには、**ipv6 first hop security** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 first hop security

no ipv6 first hop security

デフォルト設定

VLAN 上で IPv6 ファースト ホップ セキュリティは無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

ipv6 first hop security コマンドを使用すると、VLAN 上で IPv6 ファースト ホップ セキュリティを有効にできます。

例 1：次の例では、VLAN 100 上の IPv6 ファースト ホップ セキュリティを有効にします。

switchxxxxxx(config)# **interface vlan** 100

switchxxxxxx(config-if)# **ipv6 first hop security**

switchxxxxxx(config-if)# **exit**

例 2：次の例では、VLAN 100-107 上の IPv6 ファースト ホップ セキュリティを有効にします。

switchxxxxxx(config)# **interface range vlan** 100-107

switchxxxxxx(config-if-range)# **ipv6 first hop security**

switchxxxxxx(config-if-range)# **exit**

ipv6 first hop security attach-policy（ポート モード）

特定のポートに IPv6 ファースト ホップ セキュリティ ポリシーを接続するには、**ipv6 first hop security attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 first hop security attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 first hop security attach-policy [*policy-name*]

パラメータ

- ***policy-name***：IPv6 ファーストホップ セキュリティ ポリシー名（最大 32 文字）。
- **vlan** *vlan-list*：IPv6 ファースト ホップ セキュリティ ポリシーが *vlan-list* で VLAN に接続されるように指定します。キーワード **vlan** が設定されていない場合、ポリシーは IPv6 ファースト ホップ セキュリティが有効になっているデバイス上のすべての VLAN に適用されます。

デフォルト設定

IPv6 ファーストホップ セキュリティのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、IPv6 ファースト ホップ セキュリティ ポリシーをポートに接続できます。

このコマンドの後続の各使用方法は、同じポリシーを使用したコマンドの以前の使用方法より優先されます。

コマンドを使用するたびに、同じポリシー内の以前のコマンドが上書きされます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

vlan キーワードを使用した複数のポリシーは、共通の VLAN を持っていない場合は同じポートに接続できます。

入力パケットに適用されているルールのセットは次のように構築されます。

- パケットが到着した VLAN 上のインターフェイスに接続されたポートで設定されたルールがセットに追加されます。
- VLAN に接続されたポリシーで設定されたルールがセットに追加されます（追加されていない場合）。

- グローバル ルールがセットに追加されます（追加されていない場合）。

no ipv6 first hop security attach-policy コマンドを使用すると、ポートに接続されたすべてのユーザ定義済みポリシーを切り離すことができます。デフォルトのポリシーがもう一度接続されます。

no ipv6 first hop security attach-policy *policy-name* コマンドを使用すると、ポートから特定のポリシーを切り離すことができます。

例 1：次に、IPv6 ファースト ホップ セキュリティ ポリシー policy1 を gi1/0/1 ポートに接続する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、IPv6 ファースト ホップ セキュリティ ポリシー policy1 をポート gi1/0/1 に接続し、VLAN 1 ～ 10 と 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

例 3：次に、IPv6 ファースト ホップ セキュリティ ポリシー policy1 をポート gi1/0/1 に接続して VLAN 1 ～ 10 に適用し、IPv6 ファースト ホップ セキュリティ ポリシー policy2 をポート gi1/0/1 に接続して VLAN 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

例 4：次に、IPv6 ファースト ホップ セキュリティ ポリシー policy1 を gi1/0/1 ポートから切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 first hop security attach-policy（VLAN モード）

特定の VLAN に IPv6 ファースト ホップ セキュリティ ポリシーを接続するには、**ipv6 first hop security attach-policy** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 first hop security attach-policy *policy-name*

no ipv6 first hop security attach-policy

パラメータ

- ***policy-name***：IPv6 ファーストホップ セキュリティ ポリシー名（最大 32 文字）。

デフォルト設定

IPv6 ファーストホップ セキュリティのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、IPv6 ファースト ホップ セキュリティ ポリシーを VLAN に接続できます。

policy-name 引数で指定されているポリシーが定義されていない場合、コマンドは拒否されます。

コマンドの **no** 形式を使用すると、現在のポリシーを切り離してデフォルト ポリシーを再び接続できます。デフォルト ポリシーが接続されている場合、コマンドの **no** 形式は無効です。

例

次の例では、IPv6 ファースト ホップ セキュリティ ポリシー policy1 は VLAN 100 に接続されています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 first hop security logging packet drop

IPv6ファーストホップセキュリティ機能によってドロップされたパケットのロギングをグローバルに有効にするには、**ipv6 first hop security logging packet drop** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 first hop security logging packet drop

no ipv6 first hop security logging packet drop

デフォルト設定

ロギングは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、ドロップされたパケットを記録できます。ロギングが有効になっている場合、スイッチはメッセージをドロップするたびにレート制限の SYSLOG メッセージを送信します。

例

次の例では、IPv6 ファースト ホップ セキュリティ機能によってドロップされたパケットのロギングを有効にする方法を示します。

```
switchxxxxxx(config)# ipv6 first hop security logging packet drop
```

ipv6 first hop security policy

IPv6 ファースト ホップ セキュリティを定義して IPv6 ファースト ホップ セキュリティ ポリシー コンフィギュレーション モードでスイッチを配置するには、**ipv6 first hop security policy** コマンドをグローバル コンフィギュレーション モードで使用します。IPv6 ファースト ホップ セキュリティ ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 first hop security policy *policy-name*

no ipv6 first hop security policy *policy-name*

パラメータ

- ***policy-name***：IPv6 ファーストホップ セキュリティ ポリシー名（最大 32 文字）。

デフォルト設定

IPv6 ファースト ホップ セキュリティ ポリシーは設定されていません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは IPv6 ファースト ホップ セキュリティ ポリシーを定義し、スイッチを IPv6 ファースト ホップ セキュリティ コンフィギュレーション モードにします。同じタイプの各ポリシー（たとえば、IPv6 ファースト ホップ セキュリティ ポリシーなど）には一意の名前が必要です。異なるタイプのポリシーには同じポリシー名を設定できます。スイッチは、「vlan_default」と「port_default」という 2 つの定義済みの空のデフォルト IPv6 ファースト ホップ セキュリティ ポリシーをサポートします。

```
ipv6 first hop security policy vlan_default
      exit
      ipv6 first hop security policy port_default
      exit
```

これらのポリシーは削除できませんが、変更することはできます。**no ipv6 first hop security policy** はこれらのポリシーを削除せずに、ユーザが定義したポリシー設定のみを削除します。

ipv6 first hop security policy コマンドを複数回使用すると、ポリシーを定義できます。

アタッチされているポリシーを削除すると、削除する前に自動的に切り離されます。

例

例 1：次の例では、policy1 という名前の IPv6 ファースト ホップ セキュリティ ポリシーを定義し、IPv6 ファースト ホップ セキュリティ ポリシー コンフィギュレーション モードでスイッチを配置し、ドロップされたパケットのロギングを有効にします。

```
switchxxxxxx(config)# ipv6 first hop security policy policy1
switchxxxxxx(config-ipv6-fhs)# logging packet drop
switchxxxxxx(config)# exit
```

例 2：次の例では、接続している IPv6 ファースト ホップ セキュリティ ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 first hop security policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy1 will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd inspection

VLAN 上で IPv6 ネイバー探索（ND）のインスペクション機能を有効にするには、**ipv6 nd inspection** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd inspection

no ipv6 nd inspection

デフォルト設定

VLAN 上の ND インスペクションは無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

コマンドを使用すると、VLAN 上で ND インスペクションを有効にできます。IPv6 ND インスペクションは、ND インスペクションポリシーおよびグローバル ND インスペクション設定を使用してネイバー探索プロトコル（NDP）メッセージを検証します。NDインスペクションは、次の例外を含む VLAN 内の送信元ポートを除いたすべてのポートに NDP メッセージをブリッジします。RS メッセージと CPS メッセージはホストとして設定されているポートにブリッジされません（**device-role** コマンドを参照）。ND インスペクションは RA ガード後に実行されます。

例 1：次の例では、VLAN 100 上の ND インスペクションを有効にします。

switchxxxxxx(config)# **interface vlan** 100

switchxxxxxx(config-if)# **ipv6 nd inspection**

switchxxxxxx(config-if)# **exit**

例 2：次の例では、VLAN 100-107 上の ND インスペクションを有効にします。

switchxxxxxx(config)# **interface range vlan** 100-107

switchxxxxxx(config-if-range)# **ipv6 nd inspection**

switchxxxxxx(config-if-range)# **exit**

ipv6 nd inspection attach-policy（ポートモード）

特定のポートにNDインスペクションポリシーを接続するには、**ipv6 nd inspection attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd inspection attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 nd inspection attach-policy [*policy-name*]

パラメータ

- ***policy-name***：ND インスペクション ポリシー名（最大 32 文字）。
- **vlan** *vlan-list*：ND インスペクション ポリシーが *vlan-list* で VLAN に接続されるように指定します。キーワード **vlan** が設定されていない場合、ポリシーは ND インスペクションが有効になっているデバイス上のすべての VLAN に適用されます。

デフォルト設定

ND インスペクションのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

ND インスペクションポリシーをポートに接続するには、**ipv6 nd inspection attach-policy** コマンドを使用します。

コマンドを使用するたびに、同じポリシー内の以前のコマンドが上書きされます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

vlan キーワードを使用した複数のポリシーは、共通の VLAN を持っていない場合は同じポートに接続できます。

入力パケットに適用されているルールのセットは次のように構築されます。

- パケットが到着した VLAN 上のインターフェイスに接続されたポートで設定されたルールがセットに追加されます。
- VLANに接続されたポリシーで設定されたルールがセットに追加されます（追加されていない場合）。
- グローバル ルールがセットに追加されます（追加されていない場合）。

ポートに接続されたユーザ定義済みのすべてのポリシーを切り離すには、**no ipv6 nd inspection attach-policy** を使用します。

no ipv6 nd inspection attach-policy *policy-name* コマンドを使用すると、ポートから特定のポリシーを切り離すことができます。

例 1：次に、ND インスペクションポリシー policy1 を gi1/0/1 ポートに接続する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、ND インスペクションポリシー policy1 をポート gi1/0/1 に接続して VLAN 1 ～ 10 と 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

例 3：次に、ND インスペクションポリシー policy1 を gi1/0/1 ポートに接続して VLAN 1 ～ 10 に適用し、ND インスペクションポリシー policy2 を gi1/0/1 ポートに接続して VLAN 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

例 4：次に、ND インスペクションがポート gi1/0/1 からポリシー policy1 を切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd inspection attach-policy（VLAN モード）

特定の VLAN に ND インスペクション ポリシーを接続するには、**ipv6 nd inspection attach-policy** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd inspection attach-policy *policy-name*

no ipv6 nd inspection attach-policy

パラメータ

- ***policy-name***：ND インスペクション ポリシー名（最大 32 文字）。

デフォルト設定

ND インスペクションのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用して、VLAN に ND インスペクション ポリシーを接続します。**policy-name** 引数で指定したポリシーが定義されていない場合、コマンドは拒否されます。コマンドの **no** 形式を使用すると、現在のポリシーを切り離してデフォルト ポリシーを再び接続できます。デフォルト ポリシーが接続されている場合、コマンドの **no** 形式は無効です。

例

次の例では、ND インスペクション ポリシー policy1 は VLAN 100 に接続されています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd inspection drop-unsecure

CGA と RSA シグネチャ オプションが指定されていないメッセージをグローバルにドロップするには、**ipv6 nd inspection drop-unsecure** コマンドをグローバル コンフィギュレーション モードで使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd inspection drop-unsecure

no ipv6 nd inspection drop-unsecure

デフォルト設定

すべてのメッセージがブリッジされます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

CGA および RSA シグネチャ オプションが含まれていない場合、**is** コマンドは NDP メッセージをドロップします。

このコマンドが設定されていない場合、**sec-level minimum** コマンドは無効です。

このコマンドが設定されている場合は、**sec-level minimum** コマンドのみが有効になり、設定された他のすべての ND インスペクション ポリシー コマンドは無視されます。

例

次の例では、オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをスイッチがドロップします。

```
switchxxxxxx(config)# ipv6 nd inspection drop-unsecure
```

ipv6 nd inspection policy

ND インスペクション ポリシーを定義して IPv6 ND インスペクション ポリシー コンフィギュレーション モードでスイッチを配置するには、**ipv6 nd inspection policy** コマンドをグローバル コンフィギュレーション モードで使用します。ND インスペクション ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd inspection policy *policy-name*

no ipv6 nd inspection policy *policy-name*

パラメータ

- ***policy-name***：ND インスペクション ポリシー名（最大 32 文字）。

デフォルト設定

ND インスペクション ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、ND インスペクション ポリシー名を定義し、ND インスペクション ポリシー コンフィギュレーション モードでルータを配置します。同じタイプの各ポリシー（たとえば、ND インスペクション ポリシーなど）には一意の名前が必要です。異なるタイプのポリシーには同じポリシー名を設定できます。

スイッチは、「vlan_default」と「port_default」という 2 つの定義済みの ND インスペクション ポリシーをサポートします。

```
ipv6 nd inspection policy vlan_default
      exit
      ipv6 nd inspection policy port_default
      exit
```

これらのポリシーは削除できませんが、変更することはできます。**no ipv6 nd inspection policy** はこれらのポリシーを削除せずに、ユーザが定義したポリシー設定のみを削除します。

ipv6 nd inspection policy コマンドを複数回使用すると、ポリシーを定義できます。

接続されているポリシーが削除される場合は、削除される前に自動的に切り離されます。

例 1。次の例では、policy1 という名前の ND インスペクション ポリシーを定義し、ND インスペクション ポリシー コンフィギュレーション モードでスイッチを配置して、ポートが保護されていないメッセージをドロップするように設定し、デバイス ロールをルータに設定します。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

例 2。次の例では、いくつかの手順を実行してNDインスペクション ポリシーをpolicy1に定義します。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure
switchxxxxxx(config-nd-inspection)# exit
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

例 3。次の例では、接続された ND インスペクション ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 nd inspection policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd inspection sec-level minimum

最小セキュリティ レベル値をグローバルに指定するには、**ipv6 nd inspection sec-level minimum** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd inspection sec-level minimum *value*

no ipv6 nd inspection sec-level minimum

パラメータ

- ***value***：最小セキュリティ レベルを設定します。範囲：0 ～ 7.

デフォルト設定

すべてのメッセージがブリッジされます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

drop-unsecured 機能が設定されると、is コマンドは最小セキュリティ レベル パラメータ値を指定します。

保護されていないメッセージが無効になると、このコマンドは無効になります。

例

次の例では、スイッチで最小 CGA セキュリティ レベルとして 2 を指定します。

```
switchxxxxxx(config)# ipv6 nd inspection sec-level minimum 2
```

ipv6 nd inspection validate source-mac

送信元/ターゲット リンク層オプションのリンク層アドレスに対して送信元 MAC アドレスをグローバルにチェックするには、**ipv6 nd inspection validate source-mac** コマンドをグローバル コンフィギュレーション モードで使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd inspection validate source-mac

no ipv6 nd inspection validate source-mac

パラメータ

該当なし

デフォルト設定

このコマンドは、デフォルトで無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

スイッチが NDP メッセージを受信し、送信元/ターゲット リンク層オプションにリンク層アドレスが含まれる場合、送信元 MAC アドレスはリンク層アドレスに対してチェックされます。リンク層アドレスと MAC アドレスが異なる場合、このコマンドを使用するとパケットをドロップできます。

例

次の例では、NDP メッセージの送信元/ターゲット リンク層オプションのリンク層アドレスが MAC アドレスと一致しない場合にスイッチがこのメッセージをドロップできます。

```
switchxxxxxx(config)# ipv6 nd inspection validate source-mac
```

ipv6 nd raguard

VLAN上でルータアドバタイズメント（RA）ガード機能をグローバルに有効にするには、**ipv6 nd raguard** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard

no ipv6 nd raguard

パラメータ

該当なし

デフォルト設定

VLAN 上の RA ガードは無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

ipv6 nd raguard コマンドを使用すると、VLAN 上で IPv6 RA ガードを有効にします。RA ガードは、ルータとして設定されていないポートで受信した RA、CPA、および ICMP リダイレクトメッセージを破棄します（**device-role** コマンドを参照）。RA ガードは、送信元ポートに接続されている RA ガードポリシーに基づいて受信した RA メッセージを検証します。

RA ガードは ND インスペクション前に実行されます。

例 1：次の例では、VLAN 100 上の RA ガードを有効にします。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd raguard
switchxxxxxx(config-if)# exit
```

例 2：次の例では、VLAN 100-107 上の RA ガードを有効にします。

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 nd raguard
switchxxxxxx(config-if-range)# exit
```

ipv6 nd raguard attach-policy（ポート モード）

特定のポートにRA ガード ポリシーを接続するには、**ipv6 nd raguard attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 nd raguard attach-policy [*policy-name*]

パラメータ

- ***policy-name***：RA ガード ポリシー名（最大 32 文字）。
- **vlan** *vlan-list*：RA ガード ポリシーが *vlan-list* で VLAN に接続されるように指定します。キーワード **vlan** が設定されていない場合、ポリシーは RA ガード ポリシーが有効になっているデバイス上のすべての VLAN に適用されます。

デフォルト設定

RA ガードのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、RA ガード ポリシーをポートに接続できます。コマンドを使用するたびに、同じポリシー内の以前のコマンドが上書きされます。*policy-name* 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

vlan キーワードを使用した複数のポリシーは、共通の VLAN を持っていない場合は同じポートに接続できます。

入力パケットに適用されているルールのセットは次のように構築されます。

- パケットが到着した VLAN 上のインターフェイスに接続されたポートで設定されたルールがセットに追加されます。
- VLANに接続されたポリシーで設定されたルールがセットに追加されます（追加されていない場合）。
- グローバル ルールがセットに追加されます（追加されていない場合）。

no ipv6 nd raguard attach-policy コマンドを使用すると、ポートに接続されたすべてのユーザ定義済みポリシーを切り離すことができます。

ipv6 nd raguard attach-policy *policy-name* コマンドを使用すると、ポートから特定のポリシーを切り離すことができます。

例 1：次に、RA ガードポリシー policy1 を gi1/0/1 ポートに接続する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、RA ガードポリシー policy1 を gi1/0/1 ポート に接続して VLAN 1 ～ 10 と 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

例 3：次に、RA ガードポリシー policy1 を gi1/0/1 ポートに接続して VLAN 1 ～ 10 に適用し、RA ガードポリシー policy2 を gi1/0/1 ポートに接続して VLAN 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

例 4：次に、RA ガードポリシー policy1 を gi1/0/1 ポートから切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd raguard attach-policy（VLAN モード）

指定した VLAN に RA ガード ポリシーを接続するには、**ipv6 nd raguard attach-policy** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard attach-policy *policy-name*

no ipv6 nd raguard attach-policy

パラメータ

- ***policy-name***：RA ガード ポリシー名（最大 32 文字）。

デフォルト設定

RA ガードのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、RA ガード ポリシーを VLAN に接続できます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

コマンドの **no** 形式を使用すると、現在のポリシーを切り離してデフォルト ポリシーを再び接続できます。コマンドの **No** 形式は、デフォルトのポリシーがアタッチされている場合は影響を与えません。

例

次の例では、RA ガード ポリシー policy1 は VLAN 100 に接続されています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd raguard hop-limit

RA メッセージのアドバタイズされた Cur ホップ制限値をグローバルに検証するには、**ipv6 nd raguard hop-limit** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard hop-limit {[maximum *value*] [minimum *value*]}

no ipv6 nd raguard hop-limit [maximum] [minimum]

パラメータ

- **maximum** *value*：ホップカウント制限が **value** 引数以下であることを確認します。範囲 1 ～ 255。高境界の値は、低境界の値以上である必要があります。
- **minimum** *value*：ホップ数制限が **value** 引数以上であることを確認します。範囲 1 ～ 255。

デフォルト設定

ホップカウント制限が検証されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドにより、RA メッセージのアドバタイズされた Cur ホップ制限値（RFC4861 を参照）が **value** 引数によって設定された値を超えている、または未満であることを検証できます。

minimum *value* のキーワードと引数を設定すると、攻撃者がホストで低 Cur ホップ制限値を設定するのを防ぎ、リモート宛先、つまり、デフォルトルータを超えてトラフィックを生成できないようにします。アドバタイズされる Cur ホップ制限値が指定されていない場合（これは 0 の値を設定するのと同じです）、パケットはドロップされます。

maximum *value* のキーワードと引数を設定すると、アドバタイズされた Cur ホップ制限値が **value** 引数によって設定された値以下であることを検証できます。アドバタイズされる Cur ホップ制限値が指定されていない場合（これは 0 の値を設定するのと同じです）、パケットはドロップされます。

no ipv6 nd raguard hop-limit maximum コマンドを使用すると、RA メッセージのアドバタイズされた Cur ホップ制限値の最大境界の検証を無効にできます。

no ipv6 nd raguard hop-limit minimum コマンドを使用すると、RA メッセージのアドバタイズされた Cur ホップ制限値の最小境界の検証を無効にできます。

例 1：次の例では、2 つのコマンドを使用して、最小 Cur ホップ制限値に 3 を、最大 Cur ホップ制限値に 100 を定義します。

```
switchxxxxxx(config)# ipv6 nd raguard hop-limit minimum 3
switchxxxxxx(config)# ipv6 nd raguard hop-limit maximum 100
```

例 2：次の例では、1 つのコマンドを使用して、最小 Cur ホップ制限値に 3 を、最大 Cur ホップ制限値に 100 を定義します。

```
switchxxxxxx(config)# ipv6 nd raguard hop-limit minimum 3 maximum 100
```

ipv6 nd raguard managed-config-flag

RA メッセージのアドバタイズされた管理対象アドレス設定フラグをグローバルに検証するには、**ipv6 nd raguard managed-config-flag** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard managed-config-flag {on | off}

no ipv6 nd raguard managed-config-flag

パラメータ

- **on**：フラグの値は 1 である必要があります。
- **off**：フラグの値は 0 である必要があります。

デフォルト設定

検証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドでは、RA メッセージのアドバタイズされた管理対象アドレス設定フラグ（または M フラグ）の検証を有効にできます（RFC4861 を参照）。このフラグは、ホストが信頼できない可能性のある DHCPv6 サーバを介してアドレスを強制的に取得するように、攻撃者によって設定される場合があります。

例

次の例では、フラグの値が 0 であるかどうかをチェックする M フラグ検証を有効にします。

```
switchxxxxxx(config)# ipv6 nd raguard managed-config-flag off
```

ipv6 nd raguard other-config-flag

RA メッセージのアドバタイズされた「その他の設定」フラグをグローバルに検証するには、**ipv6 nd raguard other-config-flag** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard other-config-flag {on | off}

no ipv6 nd raguard other-config-flag

パラメータ

- **on**：フラグの値は 1 である必要があります。
- **off**：フラグの値は 0 である必要があります。

デフォルト設定

検証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドでは、RA メッセージのアドバタイズされた「その他の設定」フラグ（または「O」フラグ）の検証を有効にできます（RFC4861 を参照）。このフラグは、ホストが信頼できない可能性のある DHCPv6 サーバを介して他の設定情報を強制的に取得するように、攻撃者によって設定される場合があります。

例

次の例では、フラグの値が 0 であるかどうかをチェックする O フラグ検証をコマンドが有効にする方法について示します。

```
switchxxxxxx(config)# ipv6 nd raguard other-config-flag off
```

ipv6 nd raguard policy

RA ガード ポリシー名を定義して IPv6 RA ガード ポリシー コンフィギュレーション モードでスイッチを配置するには、**ipv6 nd raguard policy** コマンドをグローバル コンフィギュレーション モードで使用します。RA ガード ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 nd raguard policy *policy-name*

no ipv6 nd raguard policy *policy-name*

パラメータ

- ***policy-name***：RA ガード ポリシー名（最大 32 文字）。

デフォルト設定

RA ガード ポリシーは設定されていません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、RA ガード ポリシー名を定義し、IPv6 RA ガード ポリシー コンフィギュレーション モードでスイッチを配置します。

同じタイプの各ポリシー（たとえば、RA ガード ポリシーなど）には一意の名前が必要です。異なるタイプのポリシーには同じポリシー名を設定できます。

スイッチは、「vlan_default」と「port_default」という 2 つの定義済みの RA ガード ポリシーをサポートします。

```
ipv6 nd raguard policy vlan_default
exit
ipv6 nd raguard policy port_default
exit
```

ポリシーは削除できませんが、変更することはできます。**no ipv6 nd raguard policy** はこれらのポリシーを削除せずに、ユーザが定義したポリシー設定のみを削除します。

VLAN に他のポリシーがアタッチされていない場合、デフォルトでは **vlan_default** ポリシーが VLAN にアタッチされています。ポートに他のポリシーがアタッチされていない場合、デフォルトでは **port_default** ポリシーがポートにアタッチされています。

ipv6 nd raguard policy コマンドを複数回使用すると、ポリシーを定義できます。アタッチされているポリシーを削除すると、削除する前に自動的に切り離されます。

例 1：次の例では、policy1 という名前の RA ガード ポリシーを定義して、RA ガード ポリシー コンフィギュレーション モードでルータを配置し、その他の設定フラグの検証を無効にして、デバイス ロールをルータに設定します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag disable
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

例 2：次の例では、policy1 という名前の RA ガードを複数の手順で定義します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag disable
switchxxxxxx(config-ra-guard)# exit
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

例 3：次の例では、接続している RA ガード ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 nd raguard policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd raguard router-preference

RA メッセージのアドバタイズされたデフォルト ルータ プリファレンス値の検証をグローバルに有効にするには、**ipv6 nd raguard router-preference** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 nd raguard router-preference {[**maximum** *value*] [**minimum** *value*]}

no ipv6 nd raguard router-preference [maximum] [minimum]

パラメータ

- **maximum** *value*：許可される最大のアドバタイズされるデフォルト ルータ設定値を指定します。次の値が許容されます：**low**、**medium** および **high**（RFC4191 を参照）。高境界の値は、低境界の値以上である必要があります。
- **minimum** *value*：許可される最小のアドバタイズされるデフォルト ルータ設定値を指定します。次の値が許容されます：**low**、**medium** および **high**（RFC4191 を参照）。

デフォルト設定

検証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドでは、RA メッセージのアドバタイズされたデフォルト ルータ プリファレンス値の検証を有効にします（RFC4191 を参照）。

minimum *value* キーワードと引数を設定すると、許容される最小値が指定されます。*value* 引数より小さいデフォルト ルータ プリファレンス値を持つ受信 RA メッセージはドロップされます。

maximum *value* キーワードと引数を設定すると、許容される最大値が指定されます。*value* 引数より大きいデフォルト ルータ プリファレンス値を持つ受信 RA メッセージはドロップされます。

no ipv6 nd raguard router-preference コマンドを使用すると、RA メッセージのアドバタイズされたデフォルト ルータ プリファレンス値の検証を無効にできます。

no ipv6 nd raguard router-preference maximum コマンドを使用すると、RA メッセージのアドバタイズされたデフォルト ルータ プリファレンス値の最大境界の検証を無効にできます。

no ipv6 nd raguard router-preference minimum コマンドを使用すると、RA メッセージのアドバタイズされたデフォルト ルータ プリファレンス値の検証を無効にできます。

例 1：次の例では、**medium** の値だけが 2 つのコマンドを使用して受け入れられるように定義します。

```
switchxxxxxx(config)# ipv6 nd raguard router-preference minimum medium
switchxxxxxx(config)# ipv6 nd raguard router-preference maximum medium
```

例 2：次の例では、**medium** の値だけが 1 つのコマンドを使用して受け入れられるように定義します。

```
switchxxxxxx(config)# ipv6 nd raguard router-preference minimum medium maximum medium
```

ipv6 neighbor binding

VLAN 上でネイバー バインディング（NB）整合性機能をグローバルに有効にするには、**ipv6 neighbor binding** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 neighbor binding

no ipv6 neighbor binding

パラメータ

該当なし

デフォルト設定

VLAN 上の NB 整合性は無効になっています。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

NB 完全性は、機能が有効になっている VLAN に属する境界ポートに接続されたネイバーのバインディングを確立します。

例 1：次の例では、VLAN 100 上の NB 整合性を有効にします。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 neighbor binding
switchxxxxxx(config-if)# exit
```

例 2：次の例では、VLAN 100-107 上の NB 整合性を有効にします。

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 neighbor binding
switchxxxxxx(config-if-range)# exit
```

ipv6 neighbor binding address-config

グローバル IPv6 アドレスで許可された設定方法を指定するには、**ipv6 neighbor binding address-config** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding address-config [stateless | any] [dhcp]

no ipv6 neighbor binding address-config

パラメータ

- **stateless**：NDP メッセージからバインドされたグローバル IPv6 で自動設定のみが許可されます。
- **any**：NDP メッセージ（ステートレスおよび手動）からバインドされたグローバル IPv6 の設定方法のすべてが許可されます。キーワードが定義されていない場合は、キーワード **any** が適用されます。
- **dhcp**：DHCPv6 からのバインディングが許可されます。

デフォルト設定

デフォルト パラメータは Any です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、グローバル IPv6 アドレスで許可されている IPv6 アドレス設定方法を定義します。

stateless および **any** キーワードで次のことを指定します。

- グローバル IPv6 アドレスが NDP メッセージからバインドされます。これらのキーワードを設定しない場合は、リンクローカル アドレスのみが NDP メッセージからバインドされます。
- プレフィックス検証が有効になっている場合、NDP メッセージからバインドされているグローバル IPv6 アドレスをネイバー プレフィックス テーブルと比較してチェックする方法。

  stateless：IPv6 アドレスは NDP メッセージからバインドされます。A フラグが設定された学習済みプレフィックスまたは **autoconfig** キーワードが手動で設定されたプレフィックスに属するグローバル アドレスのみが許可されます。

any：IPv6 アドレスは NDP メッセージからバインドされます。NPT のプレフィックスに属するグローバル アドレスのみが許可されます。

dhcp キーワードを使用すると、DHCPv6 メッセージからのバインディングが可能になります。DHCPv6 メッセージからバインドされた IPv6 アドレスは、ネイバー プレフィックス テーブルと比較して検証されることはありません。DHCPv6 メッセージからバインドされた IPv6 アドレスは、NDP メッセージからバインドされた IPv6 アドレスを上書きします。

注。dhcp キーワードが設定されていない場合、スイッチは NDP メッセージの DHCPv6 によって割り当てられた IPv6 アドレスをバインドします。これは、ホストがこのアドレスの DAD プロセスを実行する必要があるからです。

キーワードが定義されていない場合は、**ipv6 neighbor binding address-config any** コマンドが適用されます。

例 1。次の例では、グローバル IPv6 アドレスのあらゆる設定方法を適用し、DHCPv6 メッセージからバインドされないように指定します。

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config any
```

例 2。次の例では、NDP からバインドされたグローバル IPv6 アドレスおよび DHCPv6 メッセージからバインドされたグローバル IPv6 アドレスが許可されるように指定します。

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config any dhcp
```

例 3。次の例では、NDP からバインドされたステートレス グローバル IPv6 アドレスのみを適用できるように指定します

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config stateless
```

例 4。次の例では、DHCPv6 の設定方法でステートレス IPv6 アドレスのみを設定および割り当て、NDP メッセージからバインディングのみがサポートされるように指定します。

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config stateless dhcp
```

例 5。次の例では、グローバル IPv6 アドレスが DHCPv6 のみで割り当てられるように指定します。

```
switchxxxxxx(config)# ipv6 neighbor binding address-config dhcp
```

ipv6 neighbor binding address-prefix

NDP メッセージからバインドされたグローバル IPv6 アドレスのスタティック プレフィックスを定義するには、**ipv6 neighbor binding address-prefix** コマンドをグローバル コンフィギュレーション モードで使用します。プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding address-prefix vlan *vlan-id ipv6-prefix*/*prefix-length* [**autoconfig**]

no ipv6 neighbor binding address-prefix [vlan *vlan-id*] [*ipv6-prefix*/*prefix-length*]

パラメータ

- ***ipv6-prefix***/*prefix-length*：IPv6 prefix.
- **vlan** *vlan-id*：指定した VLAN の ID。
- **autoconfig**：プレフィックスをステートレス設定に使用できます。

デフォルト設定

スタティック プレフィックスなし

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ipv6 neighbor binding address-prefix コマンドを使用すると、ネイバー プレフィックス テーブルにスタティック プレフィックスを追加できます。

ネイバー プレフィックス テーブルから 1 つの静的エントリを削除するには、**no ipv6 neighbor binding address-prefix vlan** *vlan-id ipv6-prefix*/*prefix-length* コマンドを使用します。

特定の VLAN で定義されているネイバー プレフィックス テーブルからすべての静的エントリを削除するには、**no ipv6 neighbor binding address-prefix vlan** *vlan-id* コマンドを使用します。

no ipv6 neighbor binding address-prefix コマンドを使用すると、ネイバー プレフィックス テーブルからすべてのスタティック エントリを削除できます。

例 1。次の例では、2 つのスタティック エントリを追加します。2 つ目のエントリは、ステートレス設定に使用できます。

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:101::/64
switchxxxxxx(config)# ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:100::/64
autoconfig
```

例 2。次の例では、1 つのスタティック エントリを削除します。

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:101::/64
```

例 3。次の例では、指定された VLAN 上で定義されているすべてのスタティック エントリを削除します。

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix vlan 100
```

例 4。次の例では、すべてのスタティック エントリを削除します。

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix
```

ipv6 neighbor binding address-prefix-validation

ネイバー プレフィックス テーブルと比較してバインドされた IPv6 アドレスの検証をグローバルに有効にするには、**ipv6 neighbor binding address-prefix-validation** コマンドをグローバル コンフィギュレーション モードで使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding address-prefix-validation

no ipv6 neighbor binding address-prefix-validation

パラメータ

該当なし

デフォルト設定

機能は無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、バインドされたアドレス プレフィックス検証を有効にします。ネイバー バインディング機能が有効になっている場合、スイッチは ipv6 neighbor binding address-prefix コマンドをネイバー バインディング コンフィギュレーション モードを使用して、バインドされたアドレスがネイバー プレフィックス テーブルのプレフィックスのいずれか、または手動で設定したプレフィックス リストに属しているかどうかをチェックします。アドレスが属していない場合はバインドされません。

例

次の例では、ネイバー プレフィックス テーブルと比較してバインドされたアドレスの検証を有効にする方法を示します。

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
```

ipv6 neighbor binding attach-policy（ポート モード）

特定のポートにネイバー バインディング ポリシーを接続するには、**ipv6 neighbor binding attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 neighbor binding attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 neighbor binding attach-policy [*policy-name*]

パラメータ

- ***policy-name***：ネイバー バインディング ポリシー名（最大 32 文字）。
- **vlan** *vlan-list*：ネイバー バインディング ポリシーが *vlan-list* で VLAN に接続されるように指定します。キーワード **vlan** が設定されていない場合、ポリシーはネイバー バインディング ポリシーが有効になっているデバイス上のすべての VLAN に適用されます。

デフォルト設定

ネイバー バインディングのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、ネイバー バインディング ポリシーをポートに接続できます。

コマンドを使用するたびに、同じポリシー内の以前のコマンドが上書きされます。

policy-name 引数で指定されたポリシーが定義されていない場合、コマンドは拒否されます。

vlan キーワードを使用した複数のポリシーは、共通の VLAN を持っていない場合は同じポートに接続できます。

入力パケットに適用されているルールのセットは次のように構築されます。

- パケットが到着した VLAN 上のインターフェイスに接続されたポートで設定されたルールがセットに追加されます。
- VLANに接続されたポリシーで設定されたルールがセットに追加されます（追加されていない場合）。
- グローバル ルールがセットに追加されます（追加されていない場合）。

no ipv6 neighbor binding attach-policy コマンドを使用すると、ポートに接続されたすべてのユーザ定義済みポリシーを切り離すことができます。

no ipv6 neighbor binding attach-policy *policy-name* コマンドを使用すると、ポートから特定のポリシーを切り離すことができます。

例 1：次に、ネイバー バインディング ポリシー policy1 を gi1/0/1 ポートに接続する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、ネイバー バインディング ポリシー policy1 をポート gi1/0/1 に接続し、VLAN 1 ～ 10 と 12 ～ 20 に適用する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

例 3：次の例では、ネイバー バインディング ポリシー policy1 はポート gi1/0/1 に接続され、VLAN 1 ～ 10 に適用されます。ネイバー バインディング ポリシー policy2 はポート gi1/0/1 に接続され、VLAN 12～ 20 に適用されます。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

例 4：次の例では、ネイバー バインディング完全性が gi1/0/1 ポートに接続されたポリシー policy1 を切り離します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 neighbor binding attach-policy（VLAN モード）

特定の VLAN にネイバー バインディング ポリシーを接続するには、**ipv6 neighbor binding attach-policy** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 neighbor binding attach-policy *policy-name*

no ipv6 neighbor binding attach-policy

パラメータ

- ***policy-name***：ネイバー バインディング ポリシー名（最大 32 文字）。

デフォルト設定

ネイバー バインディングのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、ネイバー バインディング ポリシーを VLAN に接続できます。

policy-name 引数で指定されているポリシーが定義されていない場合、コマンドは拒否されます。

コマンドの **no** 形式を使用すると、現在のポリシーを切り離してデフォルト ポリシーを再び接続できます。コマンドの **No** 形式は、デフォルトのポリシーがアタッチされている場合は影響を与えません。

例

次の例では、ネイバー バインディング ポリシー policy1 は VLAN 100 に接続されています。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 neighbor binding lifetime

ネイバー バインディング テーブル エントリ有効期間のデフォルト値をグローバルに変更するには、**ipv6 neighbor binding lifetime** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding lifetime *value*

no ipv6 neighbor binding lifetime

パラメータ

- ***value***：有効期間（分単位）。指定できる範囲は 1 ～ 60 分です。

デフォルト設定

5 分

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ipv6 neighbor binding lifetime コマンドを使用すると、デフォルトの有効期間を変更できます。

例

次の例では、バインディング エントリの有効期間を 10 分に変更します。

```
switchxxxxxx(config)# ipv6 neighbor binding lifetime 10
```

ipv6 neighbor binding max-entries

バインディング テーブル キャッシュに挿入可能なダイナミック エントリの最大数をグローバルに指定するには、**ipv6 neighbor binding max-entries** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 neighbor binding max-entries {[**vlan-limit** *number*] [**interface-limit** *number*] [**mac-limit** *number*]}

no ipv6 neighbor binding max-entries [**vlan-limit**] [**interface-limit**] [**mac-limit**]

パラメータ

- **vlan-limit** *number*：VLAN の数ごとにネイバー バインディング制限を指定します。
- **interface-limit** *number*：ポートごとにネイバー バインディング制限を指定します。
- **mac-limit** *number*：MAC アドレスごとのネイバー バインディングの制限を指定します。

デフォルト設定

このコマンドは無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、バインディングテーブルのコンテンツを制限できます。このコマンドは、バインディング テーブル キャッシュに挿入可能なダイナミック エントリの最大数を指定します。この制限に達すると、新しいエントリは拒否され、新しいエントリを含むネイバー探索プロトコル（NDP）トラフィック送信元はドロップされます。

指定したエントリの最大数がデータベース内のエントリの現在の数より少ない場合は、エントリはクリアされず、通常のキャッシュ減少後に新しいしきい値に到達します。

例

次の例では、MAC ごとにキャッシュに挿入可能なエントリの最大数をグローバルに指定する方法を示します。

```
switchxxxxxx(config)# ipv6 neighbor binding max-entries mac-limit 2
```

ipv6 neighbor binding policy

ネイバーバインディングポリシーを定義してIPv6ネイバーバインディングポリシーコンフィギュレーション モードでスイッチを配置するには、**ipv6 neighbor binding policy** コマンドをグローバル コンフィギュレーション モードで使用します。ネイバー バインディング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding policy *policy-name*

no ipv6 neighbor binding policy *policy-name*

パラメータ

- ***policy-name***：ネイバー バインディング ポリシー名（最大 32 文字）。

デフォルト設定

ネイバー バインディング ポリシーが設定されていません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドはネイバー バインディング ポリシー名を定義し、追加のコマンドをポリシーに追加できるように、ネイバーバインディングポリシーのコンフィギュレーションモードでルータを配置します。

スイッチは、「vlan_default」と「port_default」という 2 つの定義済みのネイバー バインディング ポリシーをサポートします。

```
ipv6 neighbor binding policy vlan_default
      exit
      ipv6 neighbor binding policy port_default
      exit
```

ポリシーは削除できませんが、変更することはできます。**no ipv6 neighbor binding policy** はこれらのポリシーを削除せずに、ユーザが定義したポリシー設定のみを削除します。

ipv6 neighbor binding policy コマンドを複数回使用すると、ポリシーを定義できます。

アタッチされているポリシーを削除すると、削除する前に自動的に切り離されます。

例 1：次の例では、policy1 という名前のネイバー バインディング ポリシーを定義して、ネイバー バインディング ポリシー コンフィギュレーション モードでルータを配置し、ロギングを有効にして、内部としてポートを定義します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# logging binding
switchxxxxxx(config-nbr-binding)# exit
```

例 2：次の例では、policy1 という名前のネイバー バインディング ポリシーを複数の手順で定義します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# exit
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
logging binding
witchxxxxxx(config-nbr-binding)# exit
```

例 3：次の例では、接続しているネイバー バインディング ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 neighbor binding policy policy1
Policy policy1 is applied on the following ports:
 gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 neighbor binding static

ネイバー バインディング テーブルにスタティック エントリを追加するには、**ipv6 neighbor binding static** コマンドをグローバル コンフィギュレーション モードで使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 neighbor binding static ipv6 *ipv6-address* **vlan** *vlan-id* **interface** *interface-id* **mac** *mac-address*

no ipv6 neighbor binding static ipv6 *ipv6-address* **vlan** *vlan-id*

パラメータ

- **ipv6** *ipv6-address*：スタティック エントリの IPv6 アドレス。
- **vlan** *vlan-id*：指定した VLAN の ID。
- **interface** *interface-id*：指定したポートにスタティック エントリを追加します。
- **mac** *mac-address*：スタティック エントリの MAC アドレス。

デフォルト設定

スタティック エントリなし。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、スタティック エントリをネイバー バインディング テーブルに追加するために使用します。スタティック エントリは、ポートのロールに関係なく設定されます。

エントリ（ダイナミックまたはスタティック）がすでに存在する場合は、新しいスタティック エントリによって既存のエントリが上書きされます。

ネイバー バインディング テーブルがオーバーフローした場合は、スタティック エントリは追加されません。

例

次の例では、スタティック エントリを追加します。

```
switchxxxxxx(config)# ipv6 neighbor binding static ipv6 2001:600::1 vlan 100 interface
gi1/0/1 mac 00BB.CC01.F500
```

ipv6 source guard

VLAN 上で IPv6 ソース ガード機能を有効にするには、**ipv6 source guard** コマンドを VLAN コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 source guard

no ipv6 source guard

デフォルト設定

VLAN 上でソース ガードは無効です。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

ソース IPv6 アドレスが別のポートにバインドされている場合、または不明な場合、IPv6 ソース ガードはポートで受信した IPv6 データ メッセージをブロックします。

例 1：次の例では、VLAN 100 上の IPv6 ソース ガードを有効にします。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 source guard
switchxxxxxx(config-if)# exit
```

例 2：次の例では、VLAN 100-107 上の IPv6 ソース ガードを有効にします。

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 source guard
switchxxxxxx(config-if-range)# exit
```

ipv6 source guard attach-policy（ポート モード）

特定のポートで IPv6 ソース ガード ポリシーを接続するには、**ipv6 source guard attach-policy** コマンドをインターフェイス コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 source guard attach-policy *policy-name*

no ipv6 source guard attach-policy

パラメータ

- ***policy-name***：IPv6 ガード ポリシー名（最大 32 文字）。

デフォルト設定

IPv6 ソース ガードのデフォルト ポリシーが適用されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

is コマンドは IPv6 ソース ガード ポリシーをポートに接続します。

後続の各 **ipv6 source guard attach-policy** コマンドは、同じポートの前のポリシー アタッチメントを上書きします。

IPv6 ソース ガード ポリシーを使用すると、不明な送信元 IPv6 アドレスまたは入力ポートと異なるポートにバインドされた送信元 IPv6 アドレスが指定された転送 IPv6 データ メッセージをブロックできます。

policy-name 引数で指定されているポリシーが定義されていない場合、コマンドは拒否されます。

入力パケットに適用されているルールのセットは次のように構築されます。

- ポリシーで設定されたルールがポートに接続されています。
- グローバル ルールがセットに追加されます（追加されていない場合）。

no ipv6 source guard attach-policy コマンドを使用すると、ポートに接続されたユーザ定義ポリシーを切り離して、「port_default」という名前のデフォルト ポリシーを再接続します。

例 1：次に、IPv6 送信元ガードポリシー policy1 を gi1/0/1 ポートに接続する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 source guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

例 2：次に、IPv6 送信元ガードが policy1 を gi1/0/1 ポートから切り離す例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 source guard attach-policy
switchxxxxxx(config-if)# exit
```

ipv6 source guard policy

IPv6 ソース ガード ポリシー名を定義して IPv6 ソース ガード コンフィギュレーションでユーザを配置するには、**ipv6 source guard policy** コマンドをグローバル コンフィギュレーション モードで使用します。IPv6 ソース ガード ポリシー名を削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 source guard policy *policy-name*

no ipv6 source guard policy *policy-name*

パラメータ

- ***policy-name***：IPv6 ガード ポリシー名（最大 32 文字）。

デフォルト設定

IPv6 ソース ガード ポリシーが設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、IPv6 ソース ガード ポリシー名を定義し、IPv6 ソース ガード ポリシー コンフィギュレーション モードでルータを配置します。

同じタイプの各ポリシー（たとえば、IPv6 ソース ガード ポリシーなど）には一意の名前が必要です。異なるタイプのポリシーには同じポリシー名を設定できます。

スイッチは、「port_default」という名前の IPv6 ソース ガード ポリシーを 1 つサポートします。

```
ipv6 source guard policy port_default
      exit
```

ポリシーは削除できませんが、変更することはできます。**no ipv6 source guard policy** はポリシーを削除せずに、ユーザによって定義されたポリシー設定のみを削除します。

アタッチされているポリシーを削除すると、削除する前に自動的に切り離されます。

例 1：次の例では、policy1 という IPv6 ソース ガード ポリシーを定義し、IPv6 ソース ガード ポリシー コンフィギュレーション モードでルータを配置して、ポートを信頼済みとして設定します。

```
switchxxxxxx(config)# ipv6 source guard policy policy1
switchxxxxxx(config-ipv6-srcguard)# trusted-port
switchxxxxxx(config)# exit
```

例 2：次の例では、接続している IPv6 ソース ガード ポリシーを削除します。

```
switchxxxxxx(config)# no ipv6 source guard policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

logging binding

IPv6 ネイバー バインディング ポリシー内のバインディング テーブル メイン イベントのロギングを有効にするには、**logging binding** コマンドをネイバー バインディング ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

logging binding [enable | disable]

no logging binding

パラメータ

- **enable**：バインディング テーブル メイン イベントのロギングを有効にします。キーワードが設定されていない場合、デフォルトでこのキーワードが適用されます。
- **disable**：バインディング テーブル メイン イベントのロギングを無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ネイバー バインディング ポリシー コンフィギュレーション モード。

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

例

次の例では、policy1 という名前の IPv6 ネイバー バインディング ポリシー内でバインディング テーブル メイン イベントのロギングを有効にします。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# logging binding enable
switchxxxxxx(config-nbr-binding)# exit
```

logging packet drop

IPv6 ファースト ホップ セキュリティ ポリシー内でドロップされたパケットのロギングを有効にするには、**logging packet drop** コマンドを IPv6 ファースト ホップ セキュリティ ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

logging packet drop [enable | disable]

no logging packet drop

パラメータ

- **enable**：ドロップされたパケットのロギングを有効にします。キーワードが設定されていない場合、デフォルトでこのキーワードが適用されます。
- **disable**：ドロップされたパケットのロギングを無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

IPv6 ファースト ホップ セキュリティ ポリシーのコンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

例

次の例では、policy1 という名前の IPv6 ファースト ホップ セキュリティ ポリシーが指定されたドロップされたメッセージのロギングを有効にします。

```
switchxxxxxx(config)# ipv6 first hop security policy policy1
switchxxxxxx(config-ipv6-fhs)# logging packet drop
switchxxxxxx(config-ipv6-fhs)# exit
```

managed-config-flag

IPv6 RA ガード ポリシー内でアドバタイズされる管理対象のアドレス設定フラグの検証を有効にするには、**managed-config-flag** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

managed-config-flag {on | off | disable}

no managed-config-flag

パラメータ

- **on**：フラグの値は 1 である必要があります。
- **off**：フラグの値は 0 である必要があります。
- **disable**：フラグの値を検証されません。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

例

次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード ポリシー コンフィギュレーション モードでスイッチを配置して、フラグの値が 0 であるかどうかをチェックする M フラグの検証を有効にします。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# managed-config-flag off
switchxxxxxx(config-ra-guard)# exit
```

match ra address

IPv6 RA ガード ポリシー内で受信した RA メッセージでルータの IPv6 アドレスの検証を有効にするには、**match ra address** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

match ra address {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match ra address

パラメータ

- **prefix-list** *ipv6-prefix-list-name*：照合する IPv6 プレフィックス リストです。
- **disable**：ルータの IPv6 アドレスの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN に接続されているポリシー：ルータのアドレスは検証されません。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドは、設定済みプレフィックス リストを使用して受信した RA メッセージでルータの IPv6 アドレスの検証を有効にします。ルータの送信元 IPv6 アドレスがプレフィックス リストと一致しない場合、またはプレフィックス リストが設定されていない場合は、RA メッセージがドロップされます。

disable キーワードを使用すると、VLAN 設定に関係なく IPv6 アドレスのルータの検証を無効にします。

例

次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード ポリシー コンフィギュレーション モードでスイッチを配置して、list1 という名前のプレフィックス リストに対してルータ アドレスを照会し、リンクローカル アドレス FE80::A8BB:CCFF:FE01:F700 のみが指定されたルータを許可する list1 という名前のプレフィックス リストを定義します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# match ra address prefix-list list1
switchxxxxxx(config-ra-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 permit FE80::A8BB:CCFF:FE01:F700/128
```

match ra prefixes

IPv6 RA ガード ポリシー内で受信した RA メッセージでアドバタイズされたプレフィックスの検証を有効にするには、**match ra prefixes** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

match ra prefixes {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match ra prefixes

パラメータ

- **prefix-list** *ipv6-prefix-list-name*：照合する IPv6 プレフィックス リストです。
- **disable**：受信した RA メッセージ内のアドバタイズされたプレフィックスの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：アドバタイズされたプレフィックスは検証されません。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドは、設定済みプレフィックス リストを使用して受信した RA メッセージでアドバタイズされたプレフィックスの検証を有効にします。アドバタイズされたプレフィックスがプレフィックス リストと一致しない場合、またはプレフィックス リストが設定されていない場合は、RA メッセージがドロップされます。

disable キーワードを使用すると、グローバル設定と VLAN 設定の両方で受信した RA メッセージでアドバタイズされたプレフィックスの検証を無効にできます。

例

次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード コンフィギュレーション モードでスイッチを配置して、list1 という名前のプレフィックス リストに対して 2001:101::/64 プレフィックスを照会し、2001:100::/64 プレフィックスを拒否します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# match ra prefixes prefix-list list1
switchxxxxxx(config-ra-guard)# exit
```

```
switchxxxxxx(config)# ipv6 prefix-list list1 deny 2001:0DB8:101::/64
switchxxxxxx(config)# ipv6 prefix-list list1 permit 2001:0DB8:100::/64
```

match reply

DHCPv6 ガード ポリシー内で設定されたプレフィックス リストに DHCPv6 サーバ/リレーによって送信されたメッセージで割り当てられた IPv6 アドレスの検証を有効にするには、**match reply** コマンドを DHCPv6 ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

match reply {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match reply

パラメータ

- ***ipv6-prefix-list-name***：照合される IPv6 プレフィックス リスト。
- **disable**：応答にアドバタイズされたプレフィックスの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：アドバタイズされたプレフィックスは検証されません。

コマンド モード

DHCP ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

IPv6 DHCP ガードでは、割り当てられた IPv6 アドレスを検証して、DHCPv6 サーバ/リレーによって送信された次の DHCPv6 メッセージの IA_NA および IA_TA オプションで渡されたプレフィックス リストを設定できます。

- ADVERTISE
- REPLY
- RELAY-REPL

注 1：ステータス オプションの値（存在する場合）が次のオプションと異なる場合、割り当てられたアドレスは検証されません。

- Success
- UseMulticast

注 2：RELAY-REPL メッセージでは、DHCPv6 ガードは、DHCP-relay-message オプションでカプセル化されたメッセージを検証します。

disable キーワードを使用すると、応答で割り当てられた IPv6 アドレスの検証を無効にできます。

例

次の例では、policy1 という名前の DHCPv6 ガード ポリシーを定義し、DHCPv6 ガード ポリシー コンフィギュレーション モードでスイッチを配置して、list1 という名前のプレフィックス リストに対して割り当てられたアドレスを照会します。割り当てられたすべての IPv6 アドレスは 2001:0DB8:100:200/64 or to 2001:0DB8:100::/48 に属する必要があります。プレフィックス リストの各プレフィックスに対して、「**ge 128**」 パラメータを 128 未満のプレフィックス長で設定する必要があります。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match reply prefix-list list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 deny 2001:0DB8:100:200/64 ge 128
switchxxxxxx(config)# ipv6 prefix-list list1 permit 2001:0DB8:100::/48 ge 128
```

match server address

DHCPv6 ガードポリシー内で設定されたプレフィックス リストに DHCPv6 サーバまたは DHCPv6 リレーによって送信されたメッセージで送信元 IPv6 アドレスの検証を有効にするには、**match server address** コマンドを DHCPv6 ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

match server address {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match server address

パラメータ

- **prefix-list** *ipv6-prefix-list-name*：照合する IPv6 プレフィックス リストです。
- **disable**：DHCP サーバとリレーの IPv6 アドレスの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN に接続されているポリシー：サーバのアドレスは検証されません。

コマンド モード

DHCP ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドは、設定したプレフィックス リストに DHCPv6 サーバおよび DHCPv6 リレーによって送信されたメッセージで送信元 IPv6 アドレスの検証を有効にします。送信元 IPv6 アドレスが設定されているプレフィックス リストと一致しない場合、またはプレフィックス リストが設定されていない場合、DHCPv6 応答はドロップされます。

IPv6 DHCP ガードは、DHCPv6 サーバ/リレーによって送信された次の DHCPv6 メッセージで送信元 IPv6 アドレスを検証します。

- ADVERTISE
- REPLY
- RECONFIGURE
- RELAY-REPL
- LEASEQUERY-REPLY

disable キーワードを使用すると、DHCP サーバおよびリレーの IPv6 アドレスの検証を無効にします。

例

次の例では、policy1 という名前の DHCPv6 ガード ポリシーを定義し、DHCPv6 ガード ポリシー コンフィギュレーション モードでスイッチを配置して、list1 という名前のプレフィックス リストに対してサーバまたはリレー アドレスを照会し、リンクローカル アドレス FE80::A8BB:CCFF:FE01:F700 のみが指定されたサーバを許可する list1 という名前のプレフィックス リストを定義します。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address prefix-list list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 permit FE80::A8BB:CCFF:FE01:F700/128
```

max-entries

IPv6 ネイバー バインディング ポリシー内のバインディング テーブル キャッシュに挿入できるダイナミック エントリの最大数を定義するには、**max-entries** コマンドをネイバー バインディング ポリシー コンフィギュレーション モードで使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

max-entries {[**vlan-limit** {*number* | **disable**}] [**interface-limit** {*number* | **disable**}] [**mac-limit** {*number* | **disable**}]}

no max-entries [**vlan-limit**] [**interface-limit**] [**mac-limit**]

パラメータ

- **vlan-limit** *number*：VLAN の数ごとにネイバー バインディング制限を指定します。パラメータはポートに接続されたポリシーで無視されます。
- **vlan-limit disable**：VLAN の数ごとにネイバー バインディング制限を無効にします。
- **interface-limit** *number*：ポートごとにネイバー バインディング制限を指定します。
- **interface-limit disable**：ポートごとにネイバー バインディング制限を無効にします。
- **mac-limit** *number*：MAC アドレスごとのネイバー バインディングの制限を指定します。
- **mac-limit disable**：MAC アドレスごとにネイバー バインディング制限を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ネイバー バインディング ポリシー コンフィギュレーション モード。

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

例 1：次の例では、policy1 という名前のネイバー バインディング ポリシーを定義し、ネイバー バインディング ポリシー コンフィギュレーション モードでルータを配置して、ポートで許可される IPv6 アドレスの数を 25 に制限します。

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# max-entries interface-limit 25
switchxxxxxx(config)# exit
```

例 2：次の例では、policy1 という名前の RA ガード ポリシーを定義し、RA ガード ポリシー コンフィギュレーション モードでスイッチを配置して、MAC ごとに制限を無効にします。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# max-entries mac-limit disable

switchxxxxxx(config-ra-guard)# exit
```

other-config-flag

IPv6 RA ガード ポリシー内の RA メッセージでアドバタイズされたその他の設定フラグの検証を有効にするには、**other-config-flag** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

other-config-flag {on | off | disable}

no other-config-flag

パラメータ

- **on**：フラグの値は 1 である必要があります。
- **off**：フラグの値は 0 である必要があります。
- **disable**：フラグの値を検証されません。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

disable キーワードを使用すると、グローバル設定と VLAN 設定の両方でフラグの検証を無効にします。

例

次の例では、policy1 という名前の RA ガードポリシーを定義し、RA ガードポリシー コンフィギュレーション モードでスイッチを配置して、フラグの値が 0 であるかどうかをチェックする O フラグの検証を有効にします。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag off
switchxxxxxx(config-ra-guard)# exit
```

preference

DHCPv6 ガード ポリシー内で DHCPv6 サーバによって送信されたメッセージでプリファレンスの検証を有効にするには、**preference** コマンドを DHCPv6 ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

preference {[**maximum** {*value* | **disable**}] [**minimum** {*value* | **disable**}]}

no preference [maximum] [minimum]

パラメータ

- **maximum** *value*：アドバタイズされたプリファレンス値は value 引数以下です。範囲 0 ～ 255。高境界の値は、低境界の値以上である必要があります。
- **maximum disable**：アドバタイズされたプリファレンス値の高位境界の検証を無効にします。
- **minimum** *value*：アドバタイズ設定値は **value** 引数以上です。範囲 0 ～ 255。
- **minimum disable**：アドバタイズされたプリファレンス値の下位境界の検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

DHCP ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

disable キーワードを使用すると、グローバル設定と VLAN 設定の両方で検証を無効にします。

例

次の例では、policy1 という名前の DHCPv6 ガード ポリシーを定義し、DHCPv6 ガード ポリシー コンフィギュレーション モードでスイッチを配置して、最小プリファレンス値を 10 に定義します。

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# preference minimum 10
switchxxxxxx(config-dhcp-guard)# exit
```

router-preference

IPv6 RA ガード ポリシー内の RA メッセージでアドバタイズされたデフォルト ルータ プリファレンス値の検証を有効にするには、**router-preference** コマンドを RA ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

router-preference [**maximum** {*value* | **disable**}] [**minimum** {*value* | **disable**}]

no router-preference [maximum] [minimum]

パラメータ

- **maximum** *value*：許可される最大のアドバタイズされるデフォルト ルータ設定値を指定します。次の値が許容されます：**low**、**medium** および **high**（RFC4191 を参照）。高境界の値は、低境界の値以上である必要があります。
- **maximum disable**：アドバタイズされたデフォルト ルータ プリファレンスの高位境界の検証を無効にします。
- **minimum** *value*：許可される最小のアドバタイズされるデフォルト ルータ設定値を指定します。次の値が許容されます：**low**、**medium** および **high**（RFC4191 を参照）。
- **minimum disable**：アドバタイズされたデフォルト ルータ プリファレンスの下位境界の検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

RA ガード ポリシー コンフィギュレーション モード

例

次の例では、policy1 という名前の RA ガードポリシーを定義し、RA ガードポリシー コンフィギュレーション モードでスイッチを配置して、最小デフォルト ルータ プリファレンス値を 中に定義します。

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# router-preference minimum medium
switchxxxxxx(config-ra-guard)# exit
```

sec-level minimum

Ipv6 ND インスペクション ポリシー内で最小セキュリティ レベル値を指定するには、**sec-level minimum** コマンドを ND インスペクション ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

sec-level minimum *value* | disable

no sec-level minimum

パラメータ

- ***value***：最小セキュリティ レベルを設定します。値は 0 ～ 7 です。
- **disable**：セキュリティ レベル パラメータの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

保護されていないメッセージのドロップが無効になると、このコマンドは無効になります。

例

次の例では、policy1 という名前の NDP インスペクション ポリシーを定義し、ND インスペクション ポリシー コンフィギュレーション モードでスイッチを配置して、最小 CGA セキュリティ レベルに 2 を指定します。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# sec-level minimum 2
switchxxxxxx(config-nd-inspection)# exit
```

show ipv6 dhcp guard

DHCPv6 ガード グローバル コンフィギュレーションを表示するには、**show ipv6 dhcp guard** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 dhcp guard

コマンド モード

特権 EXEC モード

使用上のガイドライン

show ipv6 dhcp guard コマンドでは、DHCPv6 ガードのグローバル設定を表示します。

例

次に、**show ipv6 dhcp guard** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 dhcp guard
IPv6 DHCP Guard is enabled on VLANs:1-4,6,7,100-120
Default Preference
  minimum: 10
  maximum: 100
```

show ipv6 dhcp guard policy

DHCPv6 ガード機能を使用して設定されたすべてのポートで DHCPv6 ガード ポリシーを表示するには、**show ipv6 dhcp guard policy** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 dhcp guard policy [*policy-name* | **active**]

パラメータ

- ***policy-name***：任意の名前で DHCPv6 ガード ポリシーを表示します。
- **active**：接続されている DHCPv6 ガード ポリシーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、DHCPv6ガード機能を使用して設定されたすべてのポートでポリシー用に設定されたオプションを表示します。

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 dhcp guard policy policy1
DHCPv6 Guard Policy: policy1
  device-role: server
  preference
    minimum: 1
    maximum: 200
  server address prefix list: list1
  reply prefix list name: list10
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLAN
	gi1/0/1 ～ 2	1 ～ 58、68 ～ 4094
	gi1/0/3 ～ 4	1-4094
	Po1 ～ 4	1-4094

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 dhcp guard policy active
Attached to VLAN:
  Policy Name   VLANs
  policy2       200-300
  vlan-default  1-199,301-4094
Attached to ports:
```

	[Policy Name]	Ports	VLAN
	policy1	gi1/0/1 ～ 2	1-100
	port-default	gi1/0/1 ～ 2	101 ～ 4094
		gi1/0/3 ～ 4	1 ～ 1094

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 dhcp guard policy
policy1
policy2
```

show ipv6 first hop security

すべての IPv6 ファースト ホップ セキュリティ グローバル コンフィギュレーションを表示するには、**show ipv6 first hop security** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 first hop security

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、すべての IPv6 ファースト ホップ セキュリティ グローバル コンフィギュレーションを表示します。

例

次に、**show ipv6 first hop security** コマンドの例を示します。

```
switchxxxxxx# show ipv6 first hop security
IPv6 First Hop Security is enabled on VLANs:1-4,6,7,100-120
Logging Packet Drop: enabled
```

show ipv6 first hop security active policies

ポートおよびVLANに適用されたポリシーの情報を表示するには、**show ipv6 first hop security active policies** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 first hop security active policies interface *interface-id* vlan *vlan-id*

パラメータ

- **interface** *interface-id*：ポート識別子（イーサネット ポートまたはポート チャネル）。
- **vlan** *vlan-id*：VLAN ID。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、任意のポートで受信したフレームおよび任意の VLAN に属するフレームに適用されたポリシーを表示します。ポリシーは、ポート、VLAN、およびグローバル コンフィギュレーションに接続されているポリシーを使用して自動的に計算されます

例

次に、gi1/0/1 と VLAN 100 で接続されているアクティブなポリシーを表示する例を示します。

```
switchxxxxxx# show ipv6 first hop security active policies interface gi1/0/1 vlan 100
IPv6 First Hop Security is enabled on VLANs:1-4,6,7,100-120
IPv6 DHCP Guard is enabled on VLANs:1-4
IPv6 ND Inspection is enabled on VLANs:1-4,6,7,100-120
IPv6 Neighbor Binding Integrity is enabled on VLANs:1-4,6,7,100-120
IPv6 RA Guard is enabled on VLANs:1-4,6,7,100-120
IPv6 Source Guard is enabled on VLANs:1-3,7,100-112
gi1/0/1, VLAN 100
IPv6 First Hop Security Policy:
  logging packet drop: enabled (from global configuration)
DHCPv6 Guard Policy:
  device-role: server (from policy1 attached to the port)
  reply prefix list name: list10 (from policy2 attached to the VLAN)
  server address prefix list name: list22 (from policy2 attached to the VLAN)
  preference
    minimum: 1 (from policy2 attached to the VLAN)
    maximum: 200 (from policy2 attached to the VLAN)
ND Inspection Policy:
  device-role: host (default)
  drop-unsecure: enabled (from policy2 attached to the VLAN)
  sec-level minimum: 3 (from policy1 attached to the port)
  validate source-mac: enabled (from global configuration)
Neighbor Binding Policy: policy1
  device-role: perimiter (default)
  logging binding: enabled (from policy1 attached to the port)
  address-prefix-validation: enabled (from policy2 attached to the VLAN)
```

```
  address-config: any (default)
  maximum entries
   VLAN: unlimited (from global configuration)
   Port: 1 (from policy1 attached to the port)
   MAC: 2 (from policy2 attached to the VLAN)
RA Guard Policy:
  device-role: router (from policy1 attached to the port)
  hop-limit:
    minimum: 10 (from policy2 attached to the VLAN)
    maximum: 20 (from global configuration)
  manage-config-flag: on(from policy2 attached to the VLAN)
  ra address verification::  disabled(default)
  ra prefixes prefix list name: list1(from policy2 attached to the VLAN)
  other-flag: disabled (default)
  router-preference:
    minimum: medium (from policy2 attached to the VLAN)
    maximum: medium (from policy2 attached to the VLAN)
IPv6 Source Guard Policy:
  trusted port: enabled (from policy1 attached to the port)
```

show ipv6 first hop security attached policies

ポートおよびVLANに接続されたポリシーの情報を表示するには、**show ipv6 first hop security attached policies** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 first hop security attached policies interface *interface-id* vlan *vlan-id*

パラメータ

- **interface** *interface-id*：ポート識別子（イーサネット ポートまたはポート チャネル）。
- **vlan** *vlan-id*：VLAN ID。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、*vlan-id* 引数で指定された VLAN に接続されているすべての IPv6 ファースト ホップ セキュリティのポリシーと、*interface-id* 引数および *vlan-id* 引数で指定されたポートと VLAN に接続されているすべてのポリシーを表示します。

例

次に、gi1/0/1 と VLAN 100 に接続されているポリシーを表示する例を示します。

```
switchxxxxxx# show ipv6 first hop security attached policies interface gi1/0/1 vlan 100
Attached to VLAN 100
  RA Guard Policy: policy1
  Neighbor Bind Policy: policy2
Attached to port gi1/0/1 and VLAN 100
  IPv6 First Hop Security Policy: FHSpolicy
  ND Inspection Policy: policy1
  RA Guard Policy: policy3
  Neighbor Bind Policy: policy3
  IPv6 Source Guard Policy: policy4
```

show ipv6 first hop security counters

ポート カウンタでカウントされるパケットの情報を表示するには、**show ipv6 first hop security counters** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 first hop security counters interface *interface-id*

パラメータ

- **interface** *interface-id*：指定しているイーサネット ポートまたはポート チャネルのカウンタを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、ポート カウンタでカウントされているスイッチによって処理されたパケットを表示します。スイッチは、ポートごとにキャプチャされたパケットをカウントし、パケットの受信、ブリッジ、またはドロップが行われたかどうかを記録します。パケットがドロップされると、ドロップの理由とドロップの原因となった機能の両方が表示されます。

例

次に、ポート gi1/0/1 でカウントされたパケットに関する情報を表示する例を示します。

```
switchxxxxxx# show ipv6 first hop security counters interface gi1/0/1
Received messages on gi1/0/1:
  Protocol   Protocol message
  NDP        RA[63] RS[0] NA[13] NS[0] REDIR[0]
  DHCPv6     ADV[0] REP[20] REC[0] REL-REP[0] LEAS-REP[10] RLS[0] DEC[0]
Dropped messages on gi1/0/1:
  Protocol   Protocol message
  NDP        RA[2] RS[0] NA[0] NS[0] REDIR[0]
  DHCPv6     ADV[1] REP[2] REC[0] REL-REP[1] LEAS-REP[0] RLS[0] DEC[0]
Dropped reasons on gi1/0/1:
  Feature         Number Reason
  DHCP Guard           2  Server message on client port
  DHCP Guard           1  Unauthorized assigned address
  DHCP Guard           1  Unauthorized server source address
  DHCP Guard           0  Unauthorized server preference
  RA guard             1  Router message on host port
  RA guard             1  Unauthorized source address
  RA guard             0  Unauthorized advertise prefix
  RA guard             0  Unauthorized router preference
  RA guard             0  Unauthorized other config flag
  RA guard             0  Unauthorized managed config flag
  RA guard             0  Unauthorized cur hop limit
  ND Inspection        0  Invalid source MAC
  ND Inspection        0  Unsecure message
  ND Inspection        0  Unauthorized sec level
```

```
Source guard          0  NoBinding
NB Integrity          0  Illegal ICMPv6 message
NB Integrity          0  Illegal DHCPv6 message
```

show ipv6 first hop security error counters

グローバル エラー カウンタを表示するには、**show ipv6 first hop security error counters** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 first hop security error counters

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドはグローバル エラー カウンタを表示します。

例 1：次の例では、グローバル エラー カウンタを示します。

```
switchxxxxxx# show ipv6 first hop security error counters
Neighbor Binding Table Overflow counter: 0
Neighbor Prefix Table Overflow counter: 0
TCAM Overflow counter: 0
```

show ipv6 first hop security policy

IPv6 ファースト ホップ セキュリティ機能で設定したすべてのポートで IPv6 ファースト ホップ セキュリティ ポリシーを表示するには、**show ipv6 first hop security policy** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 first hop security policy [*policy-name* | **active**]

パラメータ

- ***policy-name***：任意の名前の IPv6 ファースト ホップ ポリシーを表示します。
- **active**：接続されている Ipv6 ファースト ホップ セキュリティ ポリシーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、IPv6 ファースト ホップ ガード機能を使用して設定されたすべてのポートでポリシー用に設定されたオプションを表示します。

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 first hop security policy policy1
IPv6D First Hop Security Policy: policy1
  logging packet drop: enabled
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLAN
	gi1/0/1 ～ 2	1 ～ 58、68 ～ 4094
	gi1/0/3 ～ 4	1-4094
	Po1 ～ 4	1-4094

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 first hop security policy active
Attached to VLAN:
  Policy Name   VLANs
  policy2       200-300
  vlan-default  1-199,301-4094
Attached to ports:
```

	[Policy Name]	Ports	VLAN
	policy1	gi1/0/1 ～ 2	1-100
	port-default	gi1/0/1 ～ 2	101 ～ 4094
		gi1/0/3 ～ 4	1 ～ 1094

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 first hop security policy
policy1
policy2
```

show ipv6 nd inspection

ND インスペクション グローバル コンフィギュレーションを表示するには、**show ipv6 nd inspection** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 nd inspection

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは ND インスペクション グローバル コンフィギュレーションを表示します。

例

次に、**show ipv6 nd snooping** コマンド出力の例を示します。

```
switchxxxxxx# show ipv6 nd snooping
IPv6 ND Inspection is enabled on VLANs:1-4,6,7,100-120
unsecure drop: enabled
sec-level minimum value: 2
source mac validation: disabled
```

show ipv6 nd inspection policy

ND インスペクション機能で設定したすべてのポートの IPv6 ND インスペクション ポリシーを表示するには、**show ipv6 nd inspection policy** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 nd inspection policy [*policy-name* | **active**]

パラメータ

- ***policy-name***：任意の名前の ND インスペクション ポリシーを表示します。
- **active**：接続されている ND インスペクション ポリシーを表示します。

コマンド モード

特権 EXEC モード

例

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 nd inspection policy policy1
ND Inspection Policy: policy1
  device-role: router
  drop-unsecure: enabled
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLAN
	gi1/0/1 ～ 2	1 ～ 58、68 ～ 4094
	gi1/0/3 ～ 4	1-4094
	Po1	1-4094

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 nd inspection policy active
Attached to VLANs:
  Policy Name   VLANs
  vlan-default  1-4094
Attached to ports:
```

	[Policy Name]	Ports	VLAN
	policy1	gi1/0/1 ～ 2	1-100
	port-default	gi1/0/1 ～ 2	101 ～ 4094
		gi1/0/3 ～ 4	1 ～ 1094

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 nd inspection policy
policy1
policy2
```

show ipv6 nd raguard

RA ガード グローバル コンフィギュレーションを表示するには、**show ipv6 nd raguard** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 nd raguard

コマンド モード

特権 EXEC モード

例

次に、**show ipv6 nd raguard** コマンド出力の例を示します。

```
switchxxxxxx# show ipv6 nd raguard
IPv6 RA Guard is enabled on VLANs:1-4,6,7,100-120
"Managed address configuration" flag (M-flag:) off
"Other configuration" flag (O-flag): disabled
Hop Limit:
  minimum: 10
  maximum: 100
Default Router Preference:
  minimum: 1
  maximum: 1
```

show ipv6 nd raguard policy

RA ガード機能で設定したすべてのポートでルータ アドバタイズメント（RA）ガード ポリシーを表示するには、**show ipv6 nd raguard policy** コマンドを特権 EXEC モードで使用します。

構文

show ipv6 nd raguard policy [*policy-name* | **active**]

パラメータ

- ***policy-name***：任意の名前で RA ガード ポリシーを表示します。
- **active**：接続されているユーザ定義 RA ガード ポリシーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、RA ガード機能を使用して設定されたすべてのポートでポリシー用に設定されたオプションを表示します。

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 nd raguard policy raguard1
RA Guard Policy: policy1
  device-role: router
  router address prefix list name: list1
  prefixes prefix list name: list2
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLAN
	gi1/0/1 ～ 2	1 ～ 58、68 ～ 4094
	gi1/0/3 ～ 4	1-4094
	Po1 ～ 4	1-4094

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 nd raguard policy active
Attached to VLANs:
  Policy Name   VLANs
  vlan-default  1-4094
Attached to ports:
```

	[Policy Name]	Ports	VLAN
	port-default	gi1/0/1 ～ 4	1-4094

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 nd raguard policy
policy1
policy2
```

show ipv6 neighbor binding

ネイバー バインディング グローバル コンフィギュレーションを表示するには、**show ipv6 neighbor binding** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 neighbor binding

コマンド モード

特権 EXEC モード

使用上のガイドライン

これにより、ネイバー バインディング グローバル コンフィギュレーションが表示されます。

例

次に、**show ipv6 neighbor binding** コマンド出力の例を示します。

```
switchxxxxxx# show ipv6 neighbor binding
Neighbor Binding Integrity is enabled on VLANs:1-4,6-7,100-120
Binding logging: disabled
Binding lifetime: 56 minutes
Address Configuration method: dhcp
Binding address prefix validation: disabled
Maximum entries
 VLAN: unlimited
 Port: 1
 MAC: 1
```

show ipv6 neighbor binding policy

ネイバー バインディング ポリシーを表示するには、**show ipv6 neighbor binding policy** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 neighbor binding policy [*policy-name* | active]

パラメータ

- ***policy-name***：ネイバー バインディング ポリシー名。
- **active**：接続されているネイバー バインディング ポリシーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、すべてのポリシーまたは特定の 1 つのポリシーのいずれかを表示します。

例

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 neighbor binding policy policy1
Neighbor Binding Policy: policy1
  address configuration method: dhcp
  binding address prefix validation: disabled
  device-role: perimiter
  binding logging: disabled
  max-entries
   VLAN: unlimited
   Port: 10
   MAC: 2
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLAN
	gi1/0/1 ～ 2	1 ～ 58、68 ～ 4094
	gi1/0/3 ～ 4	1-4094
	Po1 ～ 4	1-4094

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 neighbor binding policy active
Attached to VLAN:
  Policy Name     VLANs
  policy2         200-300
```

```
  vlan-default    1-199,301-4094
Attached to ports:
```

	[Policy Name]	Ports	VLAN
	policy1	gi1/0/1 ～ 4	1-100
	port-default	gi1/0/1 ～ 4	101 ～ 4094

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 neighbor binding policy
policy1
policy2
```

show ipv6 neighbor binding prefix table

ネイバー プレフィックス テーブルのコンテンツを表示するには、**show ipv6 neighbor binding prefix table** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 neighbor binding prefix table [**vlan** *vlan-id*]

パラメータ

- **vlan** *vlan-id*：指定した VLAN と一致するプレフィックスを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドはネイバー プレフィックス テーブルを表示します。表示する出力は指定した VLANに制限できます。VLANが設定されていない場合は、すべてのプレフィックスが表示されます。

例

次に、学習したプレフィックスを表示する例を示します。

```
switchxxxxxx# show ipv6 neighbor binding prefix table
Flags: A - the prefix can be used for autoconfig (stateless configuration)
Neighbor Prefix Table has 4 entries
VLAN  Prefix         Type    Flags   Remaining Lifetime
   7  2004:1::/64   static    A
   7  2006:1::/64   dynamic              1230
   7  2008:1::/64   static
1027  2002:1::/64   dynamic   A            230
```

show ipv6 neighbor binding table

バインディング テーブルのコンテンツを表示するには、**show ipv6 neighbor binding table** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 neighbor binding table [**vlan** *vlan-id*] [**interface** *interface-id*] [**ipv6** *ipv6-address*] [**mac** *mac-address*]

パラメータ

- **vlan** *vlan-id*：指定した VLAN に一致するバインディング テーブル エントリを表示します。
- **interface** *interface-id*：指定したポート（イーサネット ポートまたはポート チャネル）に一致するバインディング テーブル エントリを表示します。
- **ipv6** *ipv6-address*：指定した IPv6 アドレスに一致するバインディング テーブル エントリを表示します。
- **mac** *mac-address*：指定した MAC アドレスに一致するバインディング テーブル エントリを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

これにより、バインディングテーブルのコンテンツが表示されます。表示出力は、指定された VLAN、ポート、IPv6 アドレス、または MAC アドレスで指定できます。キーワードまたは引数が入力されていない場合は、すべてのバインディングテーブルコンテンツが表示されます。

すべてのキーワードと引数の組み合わせを使用できます。

例

次に、バインディング テーブルのコンテンツを表示する例を示します。

```
switchxxxxxx# show ipv6 neighbor binding table
Binding Table has 4 entries
```

VLAN	IPv6 address	Inter	MAC address	Origin	State	Expir	TCAM
-----	----------	-------	--------------	------	-----	Time	Ovrfl
100	2001:300::1	gi1/0/1	AABB.CC01.F500	NDP	VALID	------	-----
100	2001:600::1	gi1/0/1	AABB.CC01.F510	NDP	TENT	559	*
100	2001:100::2	gi1/0/2	AABB.CC01.F160	NDP	VALID	96	
200	2001:200::3	gi1/0/2			VALID	79	

Field Descriptions:

- **VLAN**：ホストが属する VLAN。
- **IPv6 address**：ホストの IPv6 アドレス。
- **Inter**：ホストが接続されているポート。
- **MAC address**：ホストの MAC アドレス。
- **Origin**：IPv6 アドレスが追加されたプロトコル。
- **Static**：**ipv6 neighbor binding static** コマンドで手動で定義された静的 IPv6 アドレス。
- **NDP**：NDP プロトコルメッセージから学習した IPv6 アドレス。
- **DHCP**：DHCPv6 プロトコルメッセージから学習した IPv6 アドレス。
- **State**：エントリの状態
- **TENT**：新しいホスト IPv6 アドレスは検証中です。有効期間が 1 秒未満のため、有効期間は表示されません。
- **VALID**：ホスト IPv6 アドレスがバインドされています。
- **Expir. Time**：確認されない場合、エントリが削除されるまでの残り時間（秒単位）。
- **TCAM Ovrflw**：TCAM がオーバーフローしているため、「*」がマークされたエントリは TCAM に追加されていません。

show ipv6 source guard

IPv6 ソース ガード グローバル コンフィギュレーションを表示するには、**show ipv6 source guard** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 source guard

パラメータ

該当なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

これにより、IPv6 ソース ガード グローバル コンフィギュレーションが表示されます。

例

次に、**show ipv6 source guard** コマンド出力の例を示します。

```
switchxxxxxx# show ipv6 source guard
IPv6 Source Guard is enabled on VLANs:1-4,6,7,100-120
```

show ipv6 source guard policy

IPv6 ソース ガード ポリシーを表示するには、**show ipv6 source guard policy** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

構文

show ipv6 source guard policy [*policy-name* | active]

パラメータ

- ***policy-name***：IPv6 ソース ガード ポリシー名。
- **active**：接続されている IPv6 ソース ガード ポリシーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、設定したすべての IPv6 ソース ガード ポリシー、接続している特定の 1 つまたはすべての IPv6 ソース ガード ポリシーを表示します。

例 1：次の例は、policy1 という名前のポリシーのポリシー設定を示します。

```
switchxxxxxx# show ipv6 source guard policy policy1
Neighbor Binding Policy: policy1
  trusted port: disabled
  Attached to ports:
   Ports
   gi1/0/1-2
   gi1/0/4
   Po1-4
```

例 2：次の例は、接続されているポリシーを示します。

```
switchxxxxxx# show ipv6 source guard policy active
Attached to VLAN:
Attached to ports:
```

	[Policy Name]	Ports
	policy1	gi1/0/1 ～ 2
	port-default	gi1/0/1 ～ 2
		gi1/0/3

例 3：次の例は、ユーザ定義ポリシーを示します。

```
switchxxxxxx# show ipv6 source guard policy
policy1
policy2
```

trusted-port（IPv6 Source Guard）

IPv6 ソース ガード ポリシー内の信頼されたポートとしてポートを設定するには、**trusted-port** コマンドを IPv6 ソース ガード ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

trusted-port

no trusted-port

デフォルト設定

信頼されていません。

コマンド モード

IPv6 ソース ガード ポリシー コンフィギュレーション モード

使用上のガイドライン

信頼できるポートからブリッジされた IPv6 データ メッセージは IPv6 ソース ガードによって検証されません。

例

次の例では、ポートを信頼済みに定義するポリシーを定義します。

```
switchxxxxxx(config)# ipv6 ipv6 source guard policy policy1
switchxxxxxx(config-ipv6-srcguard)# trusted-port
switchxxxxxx(config-ipv6-srcguard)# exit
```

validate source-mac

IPv6 ND インスペクション ポリシー内のリンク層アドレスに対する MAC アドレスのチェックを有効にするには、**validate source-mac** コマンドを ND インスペクション ポリシー コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

validate source-mac [enable | disable]

no validate source-mac

パラメータ

- **enable**：リンク層アドレスに対する MAC アドレスの検証を有効にします。キーワードが設定されていない場合、デフォルトでこのキーワードが適用されます。
- **disable**：リンク層アドレスに対する MAC アドレスの検証を無効にします。

デフォルト設定

ポートまたはポート チャネルにアタッチされているポリシー：VLAN にアタッチされているポリシーで設定されている値。

VLAN にアタッチされているポリシー：グローバル設定。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション モード

使用上のガイドライン

このコマンドが VLAN にアタッチされているポリシーの一部である場合、VLAN 内のすべてのポートに適用されます。VLAN のポートにアタッチされているポリシーで定義されている場合、この値が VLAN にアタッチされているポリシーの値をオーバーライドします。

例

次の例では、NDP メッセージのリンク層アドレスが MAC アドレスと一致しない場合にルータがこのメッセージをドロップできます。

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# validate source-mac
switchxxxxxx(config-nd-inspection)# exit
```

IPv6 IPM ルータ コマンド

この章は、次の項で構成されています。

- ipv6 multicast-routing （842 ページ）
- ipv6 multicast-routing （843 ページ）
- show ipv6 mroute （844 ページ）
- show ipv6 multicast （846 ページ）

ipv6 multicast-routing

ルータのすべての IPv6 が有効なインターフェイスで IPv6 マルチキャスト ルーティングを有効にし、マルチキャスト転送を有効にするには、**ipv6 multicast-routing** コマンドをグローバル コンフィギュレーション モードで使用します。マルチキャスト ルーティングおよび転送を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 multicast-routing mld-proxy

no ipv6 multicast-routing

パラメータ

- **mld-proxy**：MLD プロキシを使用してマルチキャスト ルーティングを有効にします。

デフォルト設定

マルチキャスト ルーティングが有効になっていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ipv6 multicast-routing コマンドを、必要な IPv6 マルチキャスト ルーティング プロトコルを指定するパラメータと使用します。

インターフェイスで IPv6 マルチキャスト パケットを転送するには、IPv6 マルチキャスト転送をグローバルに有効にし、IPMv6 ルーティング プロトコルをインターフェイスで有効にする必要があります。

例

次の例では、MLD プロキシを使用して IPv6 マルチキャスト ルーティングを有効にします。

```
switchxxxxxx(config)# ipv6 multicast-routing mld-proxy
```

ipv6 multicast-routing

ルータのすべての IPv6 が有効なインターフェイスで IPv6 マルチキャスト ルーティングを有効にし、マルチキャスト転送を有効にするには、**ipv6 multicast-routing** コマンドをグローバル コンフィギュレーション モードで使用します。マルチキャスト ルーティングおよび転送を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 multicast-routing mld-proxy

no ipv6 multicast-routing

パラメータ

- **mld-proxy**：MLD プロキシを使用してマルチキャスト ルーティングを有効にします。

デフォルト設定

マルチキャスト ルーティングが有効になっていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ipv6 multicast-routing コマンドを、必要な IPv6 マルチキャスト ルーティング プロトコルを指定するパラメータと使用します。

インターフェイスで IPv6 マルチキャスト パケットを転送するには、IPv6 マルチキャスト転送をグローバルに有効にし、IPMv6 ルーティング プロトコルをインターフェイスで有効にする必要があります。

例

次の例では、MLD プロキシを使用して IPv6 マルチキャスト ルーティングを有効にします。

```
switchxxxxxx(config)# ipv6 multicast-routing mld-proxy
```

show ipv6 mroute

マルチキャスト ルーティング（mroute）テーブルの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mroute** コマンドを使用します。

構文

show ipv6 mroute [*group-address* [*source-address*]] [**summary**]

パラメータ

- ***group-address***：宛先マルチキャスト IPv6 アドレス。
- ***source-address***：送信元 IPv6 アドレス。
- **summary**：出力をフィルタして、mroute テーブルの各エントリに対し、1 行の簡略サマリーを表示します。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

show ip mroute コマンドを使用して、mroute テーブルの Mroute エンティティに関する情報を表示します。スイッチは、(*,G) エントリから (S,G) エントリを作成することで、マルチキャスト ルーティング テーブルに値を代入します。アスタリスク（*）は、すべての送信元アドレスを示し、「S」は単一ソース アドレスを示し、「G」は宛先マルチキャスト グループ アドレスを示します。(S,G) エントリの作成時に、スイッチはユニキャスト ルーティング テーブルで見つかった（つまり、Reverse Path Forwarding（RPF）によって）、該当する宛先グループへの最適なパスを使用します。

例

次の例の重要なフィールドの説明

Timers:Uptime/Expires：「Uptime」は、エントリが IPv6 マルチキャスト ルーティング テーブルに格納されていた期間（時間、分、秒）をインターフェイスごとに示します。「Expires」は、IPv6 マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間（時間、分、秒）をインターフェイスごとに示します。

(*, FF07::1) および (FF07::1/128, FF07::1)：IPv6 マルチキャスト ルーティング テーブルのエントリ。エントリは、送信元ルータの IP アドレスと、それに続くマルチキャスト グループの IP アドレスで構成されます。送信元ルータの位置に置かれたアスタリスク（*）は、すべての送信元を意味します。

最初の形式のエントリは、(*,G) または「スター カンマ G」エントリと呼ばれます。2 番目の形式のエントリは、(S,G) または「S カンマ G」エントリと呼ばれます。(*,G) エントリは、(S,G) エントリを作成するために使用されます。

Incoming interface：送信元からのマルチキャスト パケットが着信する予定のインターフェイス。パケットがこのインターフェイスに着信しなかった場合、廃棄されます。

Outgoing Interface List (OIF):—Interfaces through which packets will be forwarded.

例 1。次に、**show ipv6 mroute** コマンドに summary キーワードを指定した場合の出力例を示します。

```
switchxxxxxx# show ip mroute summary
Timers: Uptime/Expires
IPv6 Multicast Routing Table
(2001:0DB8:999::99, FF07::5), 00:04:55/00:02:36, OIF count:1
(2001:0DB8:999::99, FF07::1), 00:02:46/00:00:12, OIF count:1
```

例 2。次に、**show ipv6 mroute** コマンドの出力例を示します。

```
switchxxxxxx# show ip mroute
Timers: Uptime/Expires
IPv6 Multicast Routing Table
(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6
  Incoming interface: vlan5
  Outgoing interface list:
    vlan40, 00:04:45/00:02:47
(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23
  Incoming interface: vlan5
  Outgoing interface list:
    vlan40, 00:02:06/00:03:27
```

show ipv6 multicast

IPv6 マルチキャスト構成に関する一般情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 multicast** コマンドを使用します。

構文

show ipv6 multicast [**interface** [*interface-id*]]

パラメータ

- **interface**：IPv6 マルチキャスト用に設定されたインターフェイスに関する、IPv6 マルチキャスト関連情報を表示します。
- ***interface-id***：IPv6 マルチキャスト情報を表示するインターフェイス識別子。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

show ipv6 multicast コマンドを **interface** キーワードを指定せずに使用して、ルータの IPv6 マルチキャストの状態に関する一般情報を表示します。

show ipv6 multicast コマンドを **interface** キーワードを指定して使用して、指定したインターフェイスに関する IPv6 マルチキャスト情報を表示します。

例 1。次に、IPv6 マルチキャスト ルーティング プロトコルが有効でないときに、**interface** キーワードなしでの **show ipv6 multicast** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 multicast
IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: No
```

例 2。次に、MLD プロキシが有効なときに、**interface** キーワードなしでの **show ipv6 multicast** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 multicast
IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: MLD Proxy
```

例 3。次に、指定したインターフェイスに関する **show ipv6 multicast** コマンドの出力例を示します。MLDプロキシがインターフェイスで有効になっており、そのインターフェイスは MLD プロキシ アップストリーム インターフェイスです。

```
switchxxxxxx# show ipv6 multicast interface vlan 200
IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: MLD Proxy
vlan 200
 IPv6 Status: enabled
```

```
 hop-threshold: 0
 MLD Protocol: MLDv2
 MLD Proxy: Upstream
```

例 4。次に、指定したインターフェイスに関する **show ipv6 multicast** コマンドの出力例を示します。MLDプロキシがインターフェイスで有効になっており、そのインターフェイスはMLDプロキシ ダウンリンク インターフェイスです。

```
switchxxxxxx# show ipv6 multicast interface vlan 100
IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: PIM
vlan 200
 IPv6 Status: enabled
 hop-threshold: 0
 MLD Protocol: MLDv2
 MLD Proxy: DownStream (Upstream: vlan 200)
```

例 5。次に、指定したインターフェイスに関する **show ipv6 multicast** コマンドの出力例を示します。MLDプロキシはインターフェイスで無効です。

```
switchxxxxxx# show ipv6 multicast interface vlan 100
IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: MLD Proxy
vlan 200
 IPv6 Status: enabled
 hop-threshold: 100
 MLD Protocol: MLDv2
 MLD Proxy: disabled
```

IPv6 プレフィックス リスト

この章は、次の項で構成されています。

- clear ipv6 prefix-list （850 ページ）
- ipv6 prefix-list （851 ページ）
- show ipv6 prefix-list （855 ページ）

clear ipv6 prefix-list

clear ipv6 prefix-list コマンドを特権 EXEC モードで使用すると、IPv6 プレフィックス リスト エントリのヒット カウントをリセットできます。

構文

clear ipv6 prefix-list [*prefix-list-name* [*ipv6-prefix*/*prefix-length*]]

パラメータ

- ***prefix-list-name***：ヒット カウントをクリアするプレフィックス リストの名前。
- ***ipv6-prefix***：ヒット カウントをクリアする IPv6 ネットワーク。この引数は、RFC 4293 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
- ***prefix-length***：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。

デフォルト設定

すべての IPv6 プレフィックス リストのヒット カウントは自動的にクリアされます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

ヒット カウントは、特定のプレフィックス リスト エントリに一致する数を示す値です。

例

次の例では、ネットワーク マスク 2001:0DB8::/35 と一致する、first_list という名前のプレフィックス リストのプレフィックス リスト エントリからヒット カウントをクリアします。

```
switchxxxxxx# clear ipv6 prefix-list first_list 2001:0DB8::/35
```

ipv6 prefix-list

ipv6 prefix-list コマンドをグローバル コンフィギュレーション モードで使用すると、IPv6 プレフィックス リストでエントリを作成できます。エントリを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 prefix-list *list-name* [**seq** *number*] {{**deny**|**permit**} *ipv6-prefix*/*prefix-length* [**ge** *ge-length*] [**le** *le-length*]} | **description** *text*

no ipv6 prefix-list *list-name* [**seq** *number*]

パラメータ

- ***list-name***：プレフィックス リストの名前。名前には最大 32 文字を使用できます。
- **seq** *seq-number*：設定しているプレフィックス リスト エントリのシーケンス番号。これは、1 ～ 4294967294 の整数値です。
- **deny**：条件に一致するネットワークを拒否します。
- **permit**：条件に一致するネットワークを許可します。
- ***ipv6-prefix***：指定したプレフィックス リストに割り当てられている IPv6 ネットワーク。この引数は、RFC 4293 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
- ***prefix-length***：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。0 ～ 128 の 10 進数の値の前にはスラッシュ記号が必要です。*ipv6-prefix* (::) がゼロの場合のみ、*prefix-length* をゼロにすることができます。
- **description** *text*：テキストの長さは最大 80 文字です。
- **ge** *ge-value*：*prefix-length* 引数以上のプレフィックス長を指定します。これは length の範囲の最小値です（長さ範囲の「下限」に該当する値）。
- **le** *le-value*：*prefix-length* 引数以下のプレフィックス長を指定します。これは length の範囲の最大値です（長さの範囲の「まで」の部分）。

デフォルト設定

プレフィックス リストは作成されません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

seq キーワードを指定せずにこのコマンドを使用すると、最後のシーケンス番号に 5 を足した番号のプレフィックスリストの最後のエントリの後に新しいエントリが追加されます。たとえば、最後に設定されているシーケンス番号が 43 の場合、新しいエントリのシーケンス番号は 48 になります。リストが空の場合は、最初のプレフィックスリスト エントリには番号 5 が割り当てられ、後続のプレフィックス リスト エントリは 5 ずつ増分します。

seq キーワードを指定してこのコマンドを使用すると、パラメータで指定された場所に新しいエントリが配置されます。シーケンス番号が指定されたエントリが存在する場合、新しいエントリで置き換えられます。

seq キーワードを指定してこのコマンドを使用すると、プレフィックス リストが削除されます。

seq キーワードを指定したこのコマンドの **no** バージョンを使用すると、指定したエントリが削除されます。

プレフィックス リスト エントリのシーケンス番号によって、リスト中のエントリの順番が決まります。ルータは、ネットワーク アドレスとプレフィックスリストエントリを比較します。ルータは、プレフィックス リストの先頭（最も小さいシーケンス番号）から比較を開始します。

プレフィックスリストの複数のエントリがプレフィックスに一致する場合、シーケンス番号が最も小さいエントリが実際の一致と見なされます。一致または拒否が発生すると、プレフィックスリストの残りのエントリは処理されません。効率を求めるために、シーケンス番号の引数を使用してリスト上位付近に最も一般的な許可または拒否を配置することもできます。

IPv6 プレフィックス リストは、permit 文または deny 文を適用する前に照合が必要な特定のプレフィックスまたはプレフィックスの範囲を指定するために使用されます。2 つのオペランドキーワードを使用して、照合するプレフィックス長の範囲を指定できます。ある値以下のプレフィックス長は、**le** キーワードで設定します。ある値以上のプレフィックス長は、**ge** キーワードを使用して指定します。**ge** および **le** キーワードを使用すると、通常の *ipv6-prefix*/*prefix-length* 引数よりも詳細に、照合するプレフィックス長の範囲を指定できます。

プレフィックスリストのエントリと照合される候補プレフィックスに対して、次の条件が存在している必要があります。

- 候補プレフィックスは、指定したプレフィックスリストおよびプレフィックス長エントリと一致している必要があります
- 省略可能な **le** キーワードの値によって、許可されるプレフィックス長が、0 から *le-length* 引数の値（この値を含む）までの範囲で指定されます。

  省略可能な **ge** キーワードの値によって、許可されるプレフィックス長が、*ge-length* キーワードの値から 128（この値を含む）までの範囲で指定されます。

最初の条件は、他の条件が有効になる前に一致している必要があることに**注意**してください。

ge または **le** キーワードを指定しなかった場合は、完全一致であると想定されます。1 つのキーワードオペランドだけを指定した場合、そのキーワードの条件が適用され、もう 1 つの条件は

適用されません。*prefix-length* 値は、**ge** 値よりも小さい必要があります。**ge** 値は、**le** 値以下である必要があります。**le** 値は、128 以下である必要があります。

すべての IPv6 プレフィックス リスト（許可および拒否の条件文が含まれていないプレフィックス リストを含む）には、最後の一致条件として暗黙的な **deny any any** 文が含まれています。

公式指定

選択したプレフィックスは **cP**、選択したプレフィックス長は **cL** です。

関数 **PrefixIsEqual**(P1, P2, L) は、2 つのアドレス P1 と P2 の最初の L ビットを比較し、等しい場合は true を返します。

ケース 1. プレフィックス リストのエントリは次のとおりです。

- **P**：プレフィックス アドレス
- **L**：プレフィックス長
- **ge**：未定義
- **le**：未定義

PrefixIsEqual(cP,P,L) && **cL** == **L** の場合、プレフィックス cP/cL はプレフィックス リストのエントリと一致します

ケース 2。プレフィックス リスト エントリは次のとおりです。

- **P**：プレフィックス アドレス
- **L**：プレフィックス長
- **ge**：定義済み

  le：未定義

PrefixIsEqual(cP,P,L) && **cL** >= **ge** の場合、プレフィックス cP/cL はプレフィックス リストのエントリと一致します

ケース 3。プレフィックス リスト エントリは次のとおりです。

- **P**：プレフィックス アドレス
- **L**：プレフィックス長
- **ge**：未定義

  le：定義済み

PrefixIsEqual(cP,P,L) && **cL** <= **le** の場合、プレフィックス cP/cL はプレフィックス リストのエントリと一致します

ケース 4。プレフィックス リスト エントリは次のとおりです。

- **P**：プレフィックス アドレス
- **L**：プレフィックス長

- **ge**：定義済み

  le：定義済み

PrefixIsEqual(cP,P,L) && **ge** <= **cL** <= **le** の場合、プレフィックス cP/cL はプレフィックス リストのエントリと一致します

例 1。次の例では、プレフィックス ::/0 を指定したすべてのルートが拒否されます。

```
switchxxxxxx(config)# ipv6 prefix-list abc deny ::/0
```

例 2。次に、プレフィックス 2002::/16 を許可する例を示します。

```
switchxxxxxx(config)# ipv6 prefix-list abc permit 2002::/16
```

例 3。次の例では、プレフィックス 5F00::/48 からプレフィックス 5F00::/64（この値を含む）までのプレフィックスを許可するプレフィックス グループを指定する方法を示します。

```
switchxxxxxx(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

例 4。次の例では、プレフィックス 2001:0DB8::/64 を指定したルートで 64 ビットよりも大きなプレフィックス長が拒否されます。

```
switchxxxxxx(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

例 5。次の例では、すべてのアドレス空間で 32 から 64 ビットのマスク長が許可されます。

```
switchxxxxxx(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

例 6。次の例では、すべてのアドレス空間で 32 ビットを超えるマスク長が拒否されます。

```
switchxxxxxx(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

例 7。次の例では、プレフィックス 2002::/128 を指定したすべてのルートが拒否されます。

```
switchxxxxxx(config)# ipv6 prefix-list abc deny 2002::/128
```

例 8。次の例では、プレフィックス ::/0 を指定したすべてのルートが許可されます。

```
switchxxxxxx(config)# ipv6 prefix-list abc permit ::/0
```

show ipv6 prefix-list

show ipv6 prefix-list コマンドをユーザ EXEC または特権 EXEC モードで使用すると、IPv6 プレフィックス リストまたは IPv6 プレフィックス リストのエントリに関する情報を表示できます。

構文

show ipv6 prefix-list [**detail** [*list-name*] | **summary** [*list-name*]]

show ipv6 prefix-list *list-name ipv6-prefix*/*prefix-length* [**longer** | f**irst-match**]

show ipv6 prefix-list *list-name* **seq** *seq-num*

パラメータ

- **detail | summary**：すべての IPv6 プレフィックス リストの詳細情報または要約情報を表示します。
- ***list-name***：特定の IPv6 プレフィックス リストの名前。
- ***ipv6-prefix***：指定した IPv6 ネットワークのすべてのプレフィックスリストのエントリ。この引数は、RFC 4293 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
- ***prefix-length***：IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
- **longer**：任意の ipv6-prefix/prefix-length 値よりも大きな IPv6 プレフィックス リストのすべてのエントリを表示します。
- **first-match**：任意の ipv6-prefix/prefix-length 値に一致する IPv6 プレフィックス リストのエントリを表示します。
- **seq** *seq-num*：IPv6 プレフィックス リストのエントリのシーケンス番号。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

detail および **summary** キーワードを省略すると、**detail** オプションが適用されます。

longer および **first-match** キーワードを省略すると、任意のネットワーク/長さと一致する指定されたプレフィックス リストのすべてのエントリが表示されます。

例 1。次の例は、**detail** キーワードを指定したこのコマンドの出力を示します。

```
switchxxxxxx# ipv6 prefix-list detail
ipv6 prefix-list 6to4:
  count: 1, range entries: 0
  seq 5 permit 2002::/16 (hit count: 313)
ipv6 prefix-list aggregate:
  count: 3, range entries: 2
  seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568)
  seq 10 description The Default Action
  seq 15 permit ::/0 le 48 (hit count: 31310)
```

フィールドの説明

- **count**：リスト内のエントリ数。
- **range entries**：一致範囲内のエントリ数。
- **seq**：リスト内のエントリ番号。
- **permit, deny**：付与ステータス。
- **description**：コメント。
- **hit count**：プレフィックス エントリの一致の数。

Example 2. The following example shows the output of the **show ipv6 prefix-list** command with the **summary** keyword:

```
switchxxxxxx# show ipv6 prefix-list summary
ipv6 prefix-list 6to4:
  count: 1, range entries: 0
ipv6 prefix-list aggregate:
  count: 2, range entries: 2
```

Example 3. The following example shows the output of the **show ipv6 prefix-list** command with the **seq** keyword:

```
switchxxxxxx# show ipv6 prefix-list bgp-in seq 15
  seq 15 deny ::/1 (hit count: 0)
```

iSCI QoS コマンド

この章は、次の項で構成されています。

- iscsi enable （858 ページ）
- iscsi flow （859 ページ）
- iscsi qos （861 ページ）
- show iscsi （862 ページ）

iscsi enable

サービス品質プロファイルを Internet Small Computer System Interface（iSCSI）フローに適用できるようにするには、グローバル コンフィギュレーション モードで **iscsi enable** コマンドを使用します。デフォルト設定を復元するには、コマンドの **no** 形式を使用します。

構文

iscsi enable

no iscsi enable

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

iSCSI QoS を有効にするには、**iscsi enable** コマンドを使用します。

ACL がインターフェイスにバインドされ、フレームが iSCLI ルールと ACL ルールの両方に一致する場合、iSCSI ルールのみがこのフレームに適用されます。

例

次に、iSCSI QoS をグローバルに有効にする例を示します。

```
switchxxxxxx(config)# iscsi enable
```

iscsi flow

iSCSI フローを定義するには、グローバル コンフィギュレーション モードで **iscsi flow** コマンドを使用します。iSCSI フローを削除するには、このコマンドの **no** 形式を使用します。

構文

iscsi flow default | {*tcp-port* [*ip-address*]}

no iscsi flow [default | {*tcp-port* [*ip-address*]}]

パラメータ

- **default**：デフォルトの IPv4 フローを復元します。
- ***tcp-port***：iSCSI ターゲットが要求をリッスンする TCP ポート番号を指定します。（範囲：1 ～ 65535）
- ***ip-address***：iSCSI が要求をリッスンする IPv4 アドレスを指定します。

デフォルト設定

既知の TCP ポート 3260 と 860 の 2 つの iSCSI IPv4 フロー。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

各 **iscsi flow**コマンドで、次の 2 つのサブフローを含めて iSCSI フローを定義します。

- イニシエータからターゲットサブフローへ：このサブフローは、*tcp-port* 引数で指定した宛先 TCP ポートと、*ip-address* 引数を設定した場合は、設定した宛先 IP アドレスで分類されます。
- ターゲットからイニシエータのサブフローへ：このサブフローは、tcp-port 引数で定義した送信元 TCP ポートと、*ip-address* を設定した場合は、設定した送信元 IP アドレスによって分類されます。

最大 8 つの iSCSIフ ローがサポートされます。

iSCSI のデフォルト設定を復元するには、**iscsi flow default** コマンドを使用します。

同じ TCP ポートの場合は、**iscsi flow** *tcp-port* コマンドを使用するか、またはいくつかの **iscsi flow** *tcp-port ip-address* コマンドを異なる IPアドレスで使用できます。

iscsi target port *tcp-port ip-address* コマンドで定義した iSCSI フローを削除するには、**no iscsi flow** *tcp-port ip-address* コマンドを使用します。

iscsi flow *tcp-port* コマンドで定義した iSCSI フローを削除するには、**no iscsi flow** *tcp-port* コマンドを使用します。

デフォルトの iSCSI フローを削除するには、**no iscsi flow** *tcp-port* コマンドを使用します。

デフォルトのすべての iSCSI フローを削除するには、**no iscsi flow default** コマンドを使用します。

すべての iSCSIフ ロー（デフォルトのフローを含む）を削除するには、**no iscsi flow** コマンドを使用します。

例

次に、iSCSI フローの 4 つのペアを定義する例を示します。

```
switchxxxxxx(config)# no iscsi flow default
switchxxxxxx(config)# iscsi flow 1200
switchxxxxxx(config)# iscsi flow 1201 1.1.1.1
switchxxxxxx(config)# iscsi flow 1201 1.1.1.10
switchxxxxxx(config)# iscsi flow 1201 101.12.21.410
```

iscsi qos

iSCSI フローに適用するサービス品質プロファイルを定義するには、グローバル コンフィギュレーション モードで **iscsi qos** コマンドを使用します。デフォルト設定を復元するには、コマンドの **no** 形式を使用します。

構文

iscsi qos {[**vpt** *vpt*] [**dscp** *dscp*] [**queue** *queue*]}

no iscsi qos

パラメータ

- **vpt** *vpt*：iSCSI タグ付きフレームが割り当てられる VLAN 優先順位タグ（VPT）の値を指定します（範囲：0 ～ 7）
- **dscp** *dscp*：iSCSI フレームが割り当てられる DiffServ コードポイント（DSCP）を指定します（範囲：0 ～ 63）。
- **queue** *queue*：iSCSI フレームが送信される発信キューを指定します（範囲：1 ～ 8）。

デフォルト設定

- VPT は変更されません。
- DSCP は変更されません。
- キュー：7

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

iSCSI フローに適用するデフォルトのサービス品質プロファイルを変更するには、**iscsi qos** コマンドを使用します。

注。1 つ以上のパラメータが必須です。

例

次に、iSCSI フローに適用するデフォルトのサービス品質プロファイルを設定する例を示します。

```
switchxxxxxx(config)# iscsi qos vpt 6 queue 8
```

show iscsi

iSCSI 設定を表示するには、ユーザ EXEC モードで **show iscsi** コマンドを使用します。

構文

show iscsi

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

このコマンドには、デフォルト設定がありません。

コマンド モード

ユーザ EXEC モード

例

次に、iSCSI 設定を表示する例を示します。

```
switchxxxxxx> show iscsi
iSCSI is enabled
iSCSI vpt is not changed
iSCSI DSCP is 18
iSCSI Queue is 7 (default)
iSCSI Flows:
  TCP         Target IP
  Port        Address
---------  ---------------
   860     0.0.0.0            default
  3260     0.0.0.0            default
  9876     0.0.0.0
  20002    192.111.220.110
  20002    192.1.3.230
  25555    0.0.0.0
```

IPv6 トンネル コマンド

この章は、次の項で構成されています。

- interface tunnel （864 ページ）
- tunnel destination （865 ページ）
- tunnel isatap solicitation-interval （866 ページ）
- tunnel isatap robustness （867 ページ）
- show ipv6 tunnel （868 ページ）

interface tunnel

インターフェイス コンフィギュレーション（トンネル）モードを開始するには、グローバル コンフィギュレーション モードで **interface tunnel** コマンドを使用します。

構文

interface tunnel *number*

パラメータ

- ***number***：トンネル番号を指定します。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、インターフェイス コンフィギュレーション（トンネル）モードを開始しています。

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# tunnel source auto
switchxxxxxx(config-if)# exit
```

tunnel destination

手動のトンネルインターフェイスの宛先IPv4アドレスを指定するには、インターフェイス（トンネル）コンフィギュレーション モードで**tunnel destination** コマンドを使用します。宛先 IPv4 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。

構文

tunnel destination {*host-name* | *ip-address*}

no tunnel destination

パラメータ

- ***host-name***：リモート ホストの DNS 名。
- ***ip-address***：リモート ホストの IPv4 アドレス。

デフォルト設定

トンネル インターフェイス宛先は指定されていません。

コマンド モード

インターフェイス（トンネル）コンフィギュレーション モード

使用上のガイドライン

2 つのトンネルに、発信元アドレスと宛先アドレスが正確に同一である同一カプセル化モードを使用するように設定することはできません。

例

次の例では、手動IPv6トンネルのトンネル宛先アドレスを設定する方法について説明します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 10.0.0.1 255.255.255.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface tunnel1
switchxxxxxx(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
switchxxxxxx(config-if)# tunnel source vlan1
switchxxxxxx(config-if)# tunnel destination 192.168.30.1
switchxxxxxx(config-if)# tunnel mode ipv6ip
switchxxxxxx(config-if)# exit
```

tunnel isatap solicitation-interval

非要請ルータ要請メッセージ間の時間間隔を設定するには、グローバル コンフィギュレーション モードで **tunnel isatap solicitation-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

tunnel isatap solicitation-interval *seconds*

no tunnel isatap solicitation-interval

パラメータ

- ***seconds***：ISATAP ルータ要請メッセージ間の時間間隔を秒単位で指定します。（範囲：10 ～ 3600）。

デフォルト設定

ISATAP ルータ要請メッセージ間のデフォルトの時間間隔は 10 秒です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、ISATAP ルータを検出するために送信する非要請ルータ要請メッセージ間の間隔を決定します。

例

次の例では、ISATAP ルータ要請メッセージ間の時間間隔を 30 秒に設定しています。

```
switchxxxxxx(config)# tunnel isatap solicitation-interval 30
```

tunnel isatap robustness

デバイスが送信するルータ要請更新メッセージの数を設定するには、グローバル コンフィギュレーション モードで **tunnel isatap robustness** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

tunnel isatap robustness *number*

no tunnel isatap robustness

パラメータ

- ***number***：デバイスが送信するルータ要請更新メッセージの数を指定します。（範囲：1 ～ 20）。

デフォルト設定

デバイスが送信するルータ要請更新メッセージのデフォルトの数は 3 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ルータ要請間隔（アクティブな ISATAP ルータがある場合）は、ISATAP ルータから受信した最小ルータ有効期間を（堅牢性 + 1）で除算した値です。

例

次の例では、デバイスが送信するルータ要請更新メッセージの数を 5 に設定しています。

```
switchxxxxxx(config)# tunnel isatap robustness 5
```

show ipv6 tunnel

IPv6 トンネルに関する情報を表示するには、ユーザ EXEC モードで **show ipv6 tunnel** コマンドを使用します。

構文

show ipv6 tunnel [**all**]

パラメータ

- **all**：（オプション）スイッチは、トンネルのすべてのパラメータを表示します。このキーワードを設定しない場合、そのタイプに対応するトンネル パラメータのみが表示されます。

コマンド モード

ユーザ EXEC モード

例 1。次に、all キーワードを設定していない場合に、ISATAP トンネルに関する情報を表示する例を示します。

```
switchxxxxxx# show ipv6 tunnel
Tunnel 1
  Tunnel type                     : Manual
  Tunnel status                   : UP
  Tunnel Local address type       : VLAN 100
  Tunnel Local Ipv4 address       : 192.1.3.4
  Tunnel Remote Ipv4 address      : 192.3.4.5
Tunnel 2
  Tunnel type                     : ISATAP
  Tunnel status                   : UP
  Tunnel Local address type       : auto
  Tunnel Local Ipv4 address       : 192.1.3.4
  Router DNS name                 : ISATAP
  Router IPv4 addresses
    1.1.1.1          Detected
    100.1.1.1        Detected
    14.1.100.1       Not Detected
  Router Solicitation interval    : 10 seconds
Robustness : 2

Tunnel 3
  Tunnel type                     : 6to4
  Tunnel status                   : UP
  Tunnel Local address type       : auto
  Tunnel Local Ipv4 address       : 192.1.3.4
```

例 2。次の例では、**all** キーワードが設定されている場合の情報を表示します。

```
switchxxxxxx# show ipv6 tunnel all
Tunnel 1
  Tunnel type                     : Manual
  Tunnel status                   : UP
  Tunnel Local address type       : VLAN 100
  Tunnel Local Ipv4 address       : 192.1.3.4
```

```
  Manual parameters
    Tunnel Remote Ipv4 address     : 192.3.4.5
  ISATAP Parameters
    Router DNS name                : ISATAP
    Router Solicitation interval   : 10 seconds
 Robustness : 2

Tunnel 2
  Tunnel type                      : Manual
  Tunnel status                    : DOWN
  Tunnel Local address type        : auto
  Manual parameters
    Tunnel Remote Ipv4 address     : 0.0.0.0
  ISATAP Parameters
    Tunnel Local Ipv4 address      : 0.0.0.0
    Router DNS name                : ISATAP
    Router Solicitation interval   : 10 seconds
Robustness : 2

Tunnel 3
  Tunnel type                      : ISATAP
  Tunnel status                    : UP
  Tunnel Local address type        : auto
  Manual parameters
    Tunnel Remote Ipv4 address     : 0.0.0.0
  ISATAP Parameters
    Tunnel Local Ipv4 address      : 192.1.3.4
    Router DNS name                : ISATAP
    Router IPv4 addresses
      1.1.1.1          Detected
      100.1.1.1        Detected
      14.1.100.1       Not Detected
    Router Solicitation interval   : 10 seconds
 Robustness : 2
```

ライン コマンド

この章は、次の項で構成されています。

- autobaud （872 ページ）
- exec-timeout （873 ページ）
- line （874 ページ）
- speed （875 ページ）
- show line （876 ページ）

autobaud

自動ボー レート検出（自動ボー）の回線を設定するには、**autobaud** コマンドを回線設定モードで使用します。

自動ボー レート検出を無効にするには、このコマンドの **no** 形式を使用します。

構文

autobaud

no autobaud

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

自動ボー レート検出を有効にします。

コマンド モード

ライン コンフィギュレーション モード

使用上のガイドライン

このコマンドを有効にすると、次のようにアクティブ化されます。コンソールをデバイスに接続し、Enter キーを 2 回押します。デバイスは、ボー レートを自動的に検出します。

Enter 以外の文字が入力された場合、誤った速度が認識される可能性があることに注意してください。

例

次の例では、自動ボーを有効にします。

```
switchxxxxxx(config)#  line console
switchxxxxxx(config-line)# autobaud
```

exec-timeout

セッションアイドル間隔を設定するには、自動的にログオフされるまでシステムがユーザ入力を待機する間、**exec-timeout** 回線設定モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

exec-timeout *minutes* [*seconds*]

no exec-timeout

パラメータ

- **minutes**：分数を指定します。（範囲：0 ～ 65535）
- **seconds**：（オプション）秒数を指定します。（範囲：0 ～ 59）

デフォルト設定

デフォルトのアイドル間隔は 10 分です。

コマンド モード

ライン コンフィギュレーション モード

例

次の例では、自動的にログオフされるまでの telnet セッション アイドル間隔を 20 分と 10 秒に設定します。

```
switchxxxxxx(config)#  line telnet
switchxxxxxx(config-line)# exec-timeout 20 10
```

line

設定の特定の回線を特定し、回線設定コマンド モードを入力するには、**line** グローバル コンフィギュレーション モード コマンドを使用します。

構文

line *{***console** | **telnet** | **ssh***}*

パラメータ

- **console**：端末回線モードを入力します。
- **telnet**：リモート アクセス（Telnet）の仮想端末としてデバイスを設定します。
- **ssh**：保護されたリモート アクセス（SSH）の仮想端末としてデバイスを設定します。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、リモート アクセス（Telnet）の仮想端末としてデバイスを設定します。

```
switchxxxxxx(config)#  line telnet
switchxxxxxx(config-line)#
```

speed

回線ボー レートを設定するには、**speed** コマンドを回線設定モードで使用します。

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

speed *bps*

no speed

パラメータ

bps：1秒あたりのビット数（bps）でボー レートを指定します。使用可能な値は、9600、19200、38400、57600、および 115200 です。

デフォルト設定

デフォルトの速度は 115200 bps です。

コマンド モード

ライン コンフィギュレーション モード

使用上のガイドライン

設定した速度は、**autobaud** が無効になっている場合のみ適用されます。この設定は、現在のセッションのみに適用されます。

例

次の例では、1 秒あたり 9600 ビット数として回線ボー レートを設定します。

```
switchxxxxxx(config-line)# speed 9600
```

show line

回線パラメータを表示するには、**show line** 特権 EXEC モード コマンドを使用します。

構文

show line *[***console** | **telnet** | **ssh***]*

パラメータ

- **console**：（オプション）コンソール設定を表示します。
- **telnet**：（オプション）Telnet 設定を表示します。
- **ssh**：（オプション）SSH 設定を表示します。

デフォルト設定

回線が指定されていない場合は、すべての回線設定パラメータが表示されます。

コマンド モード

特権 EXEC モード

例

次に、回線設定を表示する例を示します。

```
switchxxxxxx#  show line
Console configuration:
Interactive timeout: Disabled
History: 10
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1
Telnet configuration:
Telnet is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10
SSH configuration:
SSH is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10
```

LACP コマンド

この章は、次の項で構成されています。

- lacp port-priority （878 ページ）
- lacp system-priority （879 ページ）
- lacp timeout （880 ページ）
- show lacp （881 ページ）
- show lacp port-channel （883 ページ）

lacp port-priority

物理ポートの優先度を設定するには、**lacp port-priority** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lacp port-priority *value*

no lacp port-priority

パラメータ

value：ポートの優先順位を指定します。（範囲：1 ～ 65535）

デフォルト設定

デフォルトのポートの優先順位は 1 です。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、gi1/0/6 の優先順位を設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/6
switchxxxxxx(config-if)#  lacp port-priority 247
```

lacp system-priority

システム優先度を設定するには、**lacp system-priority** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lacp system-priority *value*

no lacp system-priority

パラメータ

value：システムの優先順位値を指定します。（範囲：1 ～ 65535）

デフォルト設定

デフォルトのシステム優先度は 1 です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、システム優先度を 120 に設定します。

```
switchxxxxxx(config)#  lacp system-priority 120
```

lacp timeout

管理 LACP タイムアウトをインターフェイスに割り当てるには、**lacp timeout** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lacp timeout *{***long** | **short***}*

no lacp timeout

パラメータ

- **long**：長いタイムアウト値を指定します。
- **short**：短いタイムアウト値を指定します。

デフォルト設定

デフォルトのポート タイムアウトは Long です。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、長い管理 LACP タイムアウトを gi1/0/6 に割り当てる例を示します。

```
switchxxxxxx(config)#  interface gi1/0/6
switchxxxxxx(config-if)#  lacp timeout long
```

show lacp

すべてのイーサネット ポートまたは特定のイーサネット ポートの LACP 情報を表示するには、**show lacp** 特権 EXEC モード コマンドを使用します。

構文

show lacp *interface-id [***parameters** | **statistics** | **protocol-state**]

パラメータ

- **interface-id**：インターフェイス ID を指定します。インターフェイス ID にはイーサネット ポートを指定する必要があります
- **parameters**：（オプション）パラメータのみを表示します。
- **statistics**：（オプション）統計情報のみを表示します。
- **protocol-state**：（オプション）プロトコルの状態のみを表示します。

コマンド モード

特権 EXEC モード

例

次に、gi1/0/1 の LACP 情報を表示する例を示します。

```
switchxxxxxx#  show lacp ethernet gi1/0/1
Port gi1/0/1 LACP parameters:
    Actor
        system priority:            1
        system mac addr:            00:00:12:34:56:78
        port Admin key:             30
        port Oper key:              30
        port Oper number:           21
        port Admin priority:        1
        port Oper priority:         1
        port Admin timeout:         LONG
        port Oper timeout:          LONG
        LACP Activity:              ACTIVE
        Aggregation:                AGGREGATABLE
        synchronization:            FALSE
        collecting:                 FALSE
        distributing:               FALSE
        expired:                    FALSE
    Partner
```

		system priority: system mac addr: port Admin key: port Oper key: port Oper number: port Admin priority: port Oper priority: port Admin timeout: port Oper timeout: LACP Activity: Aggregation: synchronization: collecting: distributing: expired:	0 00:00:00:00:00:00 0 0 0 0 0 LONG LONG PASSIVE AGGREGATABLE FALSE FALSE FALSE FALSE
Port gi1/0/1 LACP Statistics: LACP PDUs sent: LACP PDUs received:			2 2
Port gi1/0/1 LACP Protocol State:			
	LACP State Machines:		
		Receive FSM: Mux FSM:	Port Disabled State Detached State
	Control Variables:		
		BEGIN: LACP_Enabled: Ready_N: Selected: Port_moved: NNT: Port_enabled:	FALSE TRUE FALSE UNSELECTED FALSE FALSE FALSE
	Timer counters:		
		periodic tx timer: current while timer: wait while timer:	0 0 0

show lacp port-channel

ポート チャネルの LACP 情報を表示するには、**show lacp port-channel** 特権 EXEC モード コマンドを使用します。

構文

show lacp port-channel *[port_channel_number]*

パラメータ

port_channel_number：（オプション）ポート チャネル番号を指定します。

コマンド モード

特権 EXEC モード

例

次の例では、ポート チャネル 1 の LACP 情報を表示します。

```
switchxxxxxx#  show lacp port-channel 1

Port-Channel 1:Port Type 1000 Ethernet

      Actor
            System Priority:    1
            MAC Address:        000285:0E1C00
            Admin Key:          29
            Oper Key:           29

      Partner
            System Priority:    0
            MAC Address:        00:00:00:00:00:00
            Oper Key:           14
```

LLDP コマンド

この章は、次の項で構成されています。

- clear lldp statistics （887 ページ）
- clear lldp table （888 ページ）
- lldp chassis-id （889 ページ）
- lldp hold-multiplier （890 ページ）
- lldp lldpdu （891 ページ）
- lldp management-address （893 ページ）
- lldp med （895 ページ）
- lldp med notifications topology-change （896 ページ）
- lldp med fast-start repeat-count （897 ページ）
- lldp med location （898 ページ）
- lldp med network-policy（グローバル） （899 ページ）
- lldp med network-policy（インターフェイス） （901 ページ）
- lldp med network-policy voice auto （902 ページ）
- lldp notifications （903 ページ）
- lldp notifications interval （904 ページ）
- lldp optional-tlv （905 ページ）
- lldp optional-tlv 802.1 （906 ページ）
- lldp run （908 ページ）
- lldp receive （909 ページ）
- lldp reinit （910 ページ）
- lldp timer （911 ページ）
- lldp transmit （912 ページ）
- lldp tx-delay （913 ページ）
- show lldp configuration （914 ページ）
- show lldp local （916 ページ）
- show lldp local tlvs-overloading （918 ページ）
- show lldp med configuration （919 ページ）
- show lldp neighbors （920 ページ）

- show lldp statistics （925 ページ）

clear lldp statistics

デバイスの LLDP 統計情報をクリアするには、特権 EXEC モードで **clear lldp statistics** コマンドを使用します。

構文

clear lldp statistics [**global** | *interface-id*]

パラメータ

- **global**：（オプション）グローバル LLDP テーブル統計情報のみをクリアします。
- ***interface-id***：（オプション）指定したポート ID のカウンタのみをクリアします。

デフォルト設定

すべての LLDP 統計情報（グローバル統計情報とすべてのインターフェイスカウンタ）をクリアします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

デバイスのすべての LLDP 統計情報をクリアするには、パラメータを指定せずに **clear lldp statistics** コマンドを使用します。これにより、グローバル LLDP テーブルの統計情報とすべてのインターフェイスカウンタの両方がクリアされます。

グローバル LLDP テーブルの統計情報のみをクリアするには、**clear lldp statistics global** を使用します。

特定のインターフェイスのカウンタをクリアするには、**clear lldp statistics** *interface-id* コマンドを使用します。

例

次に、インターフェイス gi1/0/1 から lldp カウンタをクリアする例を示します。

```
switchxxxxxx#  clear lldp statistics gi1/0/1
```

clear lldp table

すべてのポートまたは特定のポートのネイバー テーブルをクリアするには、**clear lldp table** コマンドを特権 EXEC モードで使用します。

構文

clear lldp table *[interface-id]*

パラメータ

interface-id：（オプション）ポート ID を指定します。

デフォルト設定

インターフェイスが指定されていない場合、デフォルトではすべてのポートのLLDPテーブルがクリアされます。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx#  clear lldp table gi1/0/1
```

lldp chassis-id

ポートのシャーシ ID のソースを設定するには、**lldp chassis-id** グローバル コンフィギュレーション モード コマンドを使用します。シャーシ ID ソースをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

lldp chassis-id *{***mac-address** | **host-name***}*

no lldp chassis-id

パラメータ

- **mac-address**：デバイスの MAC アドレスを使用するシャーシ ID を指定します。
- **host-name**：デバイスで設定したホスト名を使用するシャーシ ID を指定します。

デフォルト設定

MAC アドレス。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ホスト名には、一意の値を設定する必要があります。

LLDP パケットで使用するために設定されたシャーシ ID が空の場合、LLDP はデフォルト シャーシ ID（上記で指定）を使用します。

例

次の例では、シャーシ ID を MAC アドレスに設定します。

```
switchxxxxxx(config)#  lldp chassis-id mac-address
```

lldp hold-multiplier

受信側デバイスが LLDP パケットを破棄するまで保持する期間を指定するには、**lldp hold-multiplier** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lldp hold-multiplier *number*

no lldp hold-multiplier

パラメータ

hold-multiplier *number*：LLDP パケット保持期間を LLDP タイマー値の倍数に指定します（範囲：2 ～ 10）。

デフォルト設定

デフォルト LLDP 保持係数は 4 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

LLDP フレームの実際の存続可能時間（TTL）値は、次の式で計算されます。

TTL = min(65535, LLDP-Timer * LLDP-hold-multiplier)

たとえば、LLDP タイマーの値が 30 秒で、LLDP 保持係数の値が 4 の場合、LLDP ヘッダーの TTL フィールドで値 120 がエンコードされます。

例

次の例では、LLDP パケット保持間隔を 90 秒に設定します。

```
switchxxxxxx(config)#  lldp timer 30
switchxxxxxx(config)#  lldp hold-multiplier 3
```

lldp lldpdu

LLDP がグローバルに無効になっている場合に LLDP パケット処理を定義するには、**lldp lldpdu** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lldp lldpdu {***filtering*** | ***flooding***}

no lldp lldpdu

パラメータ

- **filtering**：LLDP がグローバルに無効になっている場合、LLDP パケットがフィルタリング（削除）されるように指定します。
- **flooding**：LLDP がグローバルに無効になっている場合、LLDP パケットがあふれるように（すべてのインターフェイスに転送されるように）指定します。

デフォルト設定

LLDP がグローバルに無効になっている場合、LLDP パケットがフィルタリングされます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

STP モードが MSTP の場合は、LLDP パケット処理モードを **flooding** に設定したり、その逆を行うことはできません。

LLDP がグローバルに無効になり、LLDP パケット処理モードが **flooding** の場合、LLDP パケットは、次の例外を除いてデータ パケットとして処理されます。

- VLAN 入力ルールは LLDP パケットに適用されません。LLDP パケットは、STP の状態が Forwarding の場合にすべてのポートで捕捉されます。
- デフォルトの **deny-all** ルールは LLDP パケットに適用されません。
- VLAN 出力ルールは LLDP パケットに適用されません。LLDP パケットは、STP の状態が Forwarding の場合にすべてのポートにあふれます。
- LLDP パケットはタグなしで送信されます。

例

次の例では、LLDP がグローバルに無効になっている場合に LLDP パケット処理モードを Flooding に設定します。

```
switchxxxxxx(config)#  lldp lldpdu flooding
```

lldp management-address

インターフェイスにアドバタイズされる管理アドレスを指定するには、**lldp management-address** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。管理アドレス情報のアドバタイズを停止するには、このコマンドの **no** 形式を使用します。

構文

lldp management-address *{ip-address* | **none** | **automatic** *[interface-id]}*

no lldp management-address

パラメータ

- **ip-address**：アドバタイズするスタティック管理アドレスを指定します。
- **none**：アドレスがアドバタイズされないように指定します。
- **automatic**：ソフトウェアが製品のすべての IP アドレスからアドバタイズする管理アドレスを選択するように指定します。複数の IP アドレスの場合、ソフトウェアはダイナミック IP アドレスの中で最小の IP アドレスを選択します。ダイナミック アドレスがない場合、ソフトウェアはスタティック IP アドレスの中で最小の IP アドレスを選択します。
- **automatic** *interface-id*：ソフトウェアがインターフェイス ID に設定されている IP アドレスからアドバタイズする管理アドレスを自動的に選択することを指定します。複数の IP アドレスの場合、ソフトウェアはインターフェイスのダイナミック IP アドレスの中で最小の IP アドレスを選択します。ダイナミック アドレスがない場合、ソフトウェアはインターフェイスのスタティック IP アドレスの中で最小の IP アドレスを選択します。インターフェイス ID は次のタイプのいずれかです。イーサネット ポート、ポート チャネルまたは VLAN。ポートまたはポート チャネルが IP アドレスを持つ VLAN のメンバーである場合、このアドレスは VLAN に関連付けられているため含まれません。

デフォルト設定

IP アドレスはアドバタイズされません。

デフォルトのアドバタイズメントは **automatic** です。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

各ポートで 1 つの IP アドレスをアドバタイズできます。

例

次に、gi1/0/2 で LLDP 管理アドレスアドバタイズモードを **automatic** に設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/2
switchxxxxxx(config-if)#  lldp management-address automatic
```

lldp med

ポートで LLDP Media Endpoint Discovery（MED）を有効または無効にするには、**lldp med** インターフェイス（イーサネット）コンフィギュレーションモードコマンドを使用します。デフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

構文

lldp med {*enable* [*tlv … tlv4*] | ***disable***}

no lldp med

パラメータ

- **enable**：LLDP MED を有効にします。
- **tlv**：追加する TLV を指定します。利用可能な TLV は、Network-Policy、Location、POE-PSE、Inventory です。LLDP-MED が有効になっている場合、機能 TLV は常に含まれます。
- **disable**：ポートの LLDP MED を無効にします。

デフォルト設定

network-policy TLV で有効

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、gi1/0/3 で **location** TLV が指定された LLDP MED を有効にします。

```
switchxxxxxx(config)#  interface gi1/0/3
switchxxxxxx(config-if)#  lldp med enable location
```

lldp med notifications topology-change

ポートで LLDP MED トポロジ変更通知の送信を有効にするには、**lldp med notifications topology-change** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lldp med notifications topology-change {**enable** | **disable**}

no lldp med notifications topology-change

パラメータ

- **enable**：LLDP MED トポロジ変更通知の送信を有効にします。
- **disable**：LLDP MED トポロジ変更通知の送信を無効にします。

デフォルト設定

デフォルトは disable です。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、gi1/0/2 で LLDP MED トポロジ変更通知を送信できるようにする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/2
switchxxxxxx(config-if)#  lldp med notifications topology-change enable
```

lldp med fast-start repeat-count

ポートが起動すると、LLDPは自身の高速起動メカニズムを使用して通常よりもすばやくパケットを送信することができます。

高速起動メカニズムが有効な間に送信されるパケットの数を設定するには、**lldp med fast-start repeat-count** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

lldp med fast-start repeat-count *number*

no lldp med fast-start repeat-count

パラメータ

repeat-count *number*：高速起動メカニズムが有効な間に高速起動LLDPDUが送信される回数を指定します。指定できる範囲は、1 ～ 10 です。

デフォルト設定

3

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)#  lldp med fast-start repeat-count 4
```

lldp med location

ポートの LLDP Media Endpoint Discovery（MED）のロケーション情報を設定するには、**lldp med location** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。ポートのロケーション情報を削除するには、このコマンドの **no** 形式を使用します。

構文

lldp med location *{{***coordinate** *data}* | *{***civic-address** *data}* | *{***ecs-elin** *data}}*

no lldp med location *{***coordinate** | **civic-address** | **ecs-elin***}*

パラメータ

- **coordinate** *data*：ロケーション データを 16 進表記の座標として指定します。
- **civic-address** *data*：ロケーション データを 16 進表記の住所として指定します。
- **ecs-elin** *data*：ロケーション データを緊急電話サービスの緊急位置識別番号として 16 進表記で指定します。
- **data**：ANSI/TIA 1057 で定義された形式でロケーション データを指定します（ドット付き 16 進数データ）。16 進数文字列の各バイトは 2 つの 16 進数桁です。バイトは、ピリオドまたはコロンで区切られます。（長さ：coordinate：16 バイト。Civic-address：6 ～ 160 バイト。Ecs-elin：10 ～ 25 バイト）

デフォルト設定

ロケーションは設定されていません。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、gi1/0/2 で LLDP MED の位置情報を住所として設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/2
switchxxxxxx(config-if)#  lldp med location civic-address 616263646566
```

lldp med network-policy（グローバル）

LLDP MED ネットワークポリシーを定義するには、**lldp med network-policy** グローバル コンフィギュレーション モード コマンドを使用します。音声アプリケーションの場合は、lldp med network-policy voice auto （902 ページ） を使用する方が簡単です。

lldp med network-policy コマンドはネットワーク ポリシーを作成し、lldp med network-policy（インターフェイス） （901 ページ） によってポートに接続されます。

ネットワーク ポリシーは、LLDP パケットを構築する方法を定義します。

LLDP MED ネットワーク ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

lldp med network-policy *number application [***vlan** *vlan-id] [***vlan-type** *{***tagged** | **untagged***}] [***up** *priority] [***dscp** *value]*

no lldp med network-policy *number*

パラメータ

- **number**：ネットワーク ポリシーのシーケンス番号。有効な範囲は 1 ～ 32 です。
- **application**：このネットワーク ポリシーで定義されたアプリケーションの主な機能の名前または番号。使用可能なアプリケーション名は次のとおりです。
  - voice
  - voice-signaling
  - guest-voice
  - guest-voice-signaling
  - softphone-voice
  - video-conferencing
  - streaming-video
  - video-signaling
- **vlan** *vlan-id*：（オプション）アプリケーションの VLAN 識別子。
- **vlan-type**：アプリケーションがタグ付き VLAN とタグなし VLAN のどちらを使用するかを指定します。
- **up** *priority*：（オプション）指定されたアプリケーションで使用するユーザ優先度（レイヤ 2 優先度）。
- **dscp** *value*：（オプション）指定されたアプリケーションで使用する DSCP 値。

デフォルト設定

ネットワーク ポリシーは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

lldp med network-policy インターフェイス コンフィギュレーション コマンドを使用すると、ポートにネットワーク ポリシーを接続できます。

最大で 32 個のネットワーク ポリシーまで定義できます。

例

次の例では、音声信号アプリケーション用のネットワーク ポリシーを作成し、ポート 1 に接続します。ポート 1 で送信された LLDP パケットには、ネットワーク ポリシーで定義された情報が含まれます。

```
switchxxxxxx(config)#  lldp med network-policy 1 voice-signaling vlan 1 vlan-type untagged
 up 1 dscp 2
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  lldp med network-policy add 1
```

lldp med network-policy（インターフェイス）

ポートでLLDP MEDネットワーク ポリシーを接続または削除するには、**lldp med network-policy** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。ネットワーク ポリシーは lldp med network-policy（グローバル） （899 ページ） で作成されます。

ポートからすべての LLDP MED ネットワーク ポリシーを削除するには、このコマンドの **no** 形式を使用します。

構文

lldp med network-policy *{***add** | **remove***}* *number*

no lldp med network-policy *number*

パラメータ

- **add/remove** *number*：指定されたネットワーク ポリシーをインターフェイスに接続または削除します。
- **number**：ネットワーク ポリシーのシーケンス番号を指定します。範囲は 1 ～ 32 です

デフォルト設定

ネットワーク ポリシーはインターフェイスに接続されていません。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

各ポートの場合、1 つのアプリケーション（音声、音声信号など）に対して 1 つのネットワーク ポリシーのみを定義できます。

例

この例では、音声信号アプリケーションのネットワーク ポリシーを作成し、ポート 1 にアタッチします。ポート 1 で送信された LLDP パケットには、ネットワーク ポリシーで定義された情報が含まれます。

```
switchxxxxxx(config)#  lldp med network-policy 1 voice-signaling vlan 1 vlan-type untagged
 up 1 dscp 2
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  lldp med network-policy add 1
```

lldp med network-policy voice auto

lldp med network-policy（グローバル） （899 ページ） を使用すると、音声 LLDP パケットのネットワーク ポリシーを作成できます。**lldp med network-policy voice auto** グローバル コンフィギュレーション モードでは、ユーザが手動で設定する代わりに、音声アプリケーションの設定をしてネットワーク ポリシーを簡単に作成します。

音声 VLAN 動作モードが **auto voice VLAN** の場合、このコマンドは音声の LLDP MED ネットワーク ポリシーを生成します。音声 VLAN, 802.1p 優先度および音声 VLAN の DSCP がポリシーで使用されます。

このモードを無効にするには、このコマンドの **no** 形式を使用します。

ネットワーク ポリシーは音声 VLAN に自動的に接続されます。

構文

lldp med network-policy voice auto

no lldp med network-policy voice auto

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

自動モードの音声 VLAN 機能では、アプリケーション タイプ **voice** が指定されたネットワーク ポリシー TLV をアドバタイズするインターフェイスを特定し、この TLV のパラメータを制御します。

自動音声 VLAN に基づいてネットワーク ポリシーの自動生成を有効にするには、音声アプリケーションのネットワーク ポリシーを手動で設定してはいけません

自動モードでは、lldp med network-policy（グローバル） （899 ページ） コマンドを使用して音声アプリケーションのネットワーク ポリシーを手動で定義することはできません。

例

```
switchxxxxxx(config)#  lldp med network-policy voice auto
```

lldp notifications

インターフェイスで LLDP 通知の送信を有効/無効にするには、**lldp notifications** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lldp notifications *{***enable** | **disable***}*

no lldp notifications

パラメータ

- **enable**：LLDP 通知の送信を有効にします。
- **disable**：LLDP 通知の送信を無効にします。

デフォルト設定

無効

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、gi1/0/1 で LLDP 通知の送信を有効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  lldp notifications enable
```

lldp notifications interval

LLDP 通知の最大転送速度を設定するには、**lldp notifications interval** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

lldp notifications interval *seconds*

no lldp notifications interval

パラメータ

interval *seconds*：デバイスは指定期間（範囲：5 ～ .3600）に通知を複数回送信しません。

デフォルト設定

5 秒

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)#  lldp notifications interval 10
```

lldp optional-tlv

転送されるオプション TLV を指定するには、**lldp optional-tlv** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lldp optional-tlv *tlv* [*tlv2 … tlv5* | ***none***]

パラメータ

- **tlv**：追加する TLV を指定します。使用可能なオプションの TLV は、port-desc、sys-name、sys-desc、sys-cap、802.3-mac-phy、802.3-lag、802.3-max-frame-size、Power-via-MDI、4-wirePower-via-MDI です。

  none：（オプション）オプションのすべての TLV をインターフェイスからクリアします。

802.1 プロトコルが選択されている場合は、次のコマンドを参照してください。

デフォルト設定

次の TLV が転送されます。

- sys-name
- sys-cap

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、ポート説明 TLV を gi1/0/2 で送信するように指定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/2
switchxxxxxx(config-if)#  lldp optional-tlv port-desc
```

lldp optional-tlv 802.1

802.1 TLV を転送するかどうかを指定するには、**lldp optional-tlv 802.1** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lldp optional-tlv 802.1 pvid ***{enable*** | ***disable}*** ：PVID がアドバタイズされるかされないかを指定します。

no lldp optional-tlv 802.1 pvid：PVID のアドバタイズの状態をデフォルトに戻します。

lldp optional-tlv 802.1 ppvid *add ppvid*：プロトコル ポート VLAN ID（PPVID）がアドバタイズされます。PPVID は、パケットのプロトコルに応じて使用される PVID です。

lldp optional-tlv 802.1 ppvid *remove ppvid*：PPVID はアドバタイズされません。

lldp optional-tlv 802.1 vlan *add vlan-id*：この *vlan-id* はアドバタイズされます。

lldp optional-tlv 802.1 vlan *remove vlan-id*：この *vlan-id* はアドバタイズされません。

lldp optional-tlv 802.1 protocol *add {**stp*** | ***rstp*** | ***mstp*** | ***pause*** | ***802.1x*** | ***lacp*** | ***gvrp}***：選択したプロトコルをアドバタイズします。

lldp optional-tlv 802.1 protocol *remove {***stp** | **rstp** | **mstp** | **pause** | **802.1x** | **lacp** | **gvrp***}*：選択したプロトコルがアドバタイズされません。

パラメータ

- **lldp optional-tlv 802.1 pvid** ***{enable*** | ***disable}***：ポートの PVID のアドバタイズまたはアドバタイズ停止を行います。
- **lldp optional-tlv 802.1 ppvid add/remove** *ppvid*：アドバタイジング用に PPVID を追加/削除します。（範囲：0 ～ 4094）。PPVID = 0 は、ポートがポートとプロトコル VLAN をサポートできないこと、およびポートがプロトコル VLAN を使用して有効にされていないことを示します。
- **add/remove** *vlan-id*：アドバタイズする VLAN を追加/削除します。（範囲：1 ～ 4094）
- **add/remove** ***{stp*** | ***rstp*** | ***mstp*** | ***pause*** | ***802.1x*** | ***lacp*** | ***gvrp}***：add は指定したプロトコルをアドバタイズするように指定し、removeは指定したプロトコルをアドバタイズしないように指定します。

デフォルト設定

次の 802.1 TLV が転送されます。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

```
switchxxxxxx(config)#  lldp optional-tlv 802.1 protocol add stp
```

lldp run

LLDP を有効にするには、**lldp run** グローバル コンフィギュレーション モード コードを使用します。LLDP を無効にするには、このコマンドの **no** 形式を使用します。

構文

lldp run

no lldp run

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)#  lldp run
```

lldp receive

インターフェイス上でLLDPの受信を有効にするには、**lldp receive**インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。インターフェイス（イーサネット）コンフィギュレーションモードインターフェイス上でLLDPの受信を停止するには、このコマンドの **no** 形式を使用します。

構文

lldp receive

no lldp receive

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

有効

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

LLDP は LAG ポートを個別に管理します。LAG ポートを介して受信した LLDP データはポートごと格納されます。

ポートの LLDP 動作は、ポートの STP の状態に依存しません。つまり、LLDP フレームはブロックされたポートで受信されます。

ポートが802.1xによって制御されている場合、ポートが承認された場合にのみLLDPが動作します。

例

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  lldp receive
```

lldp reinit

LLDP転送を再初期化するまでLLDPポートが待機する最小時間を指定するには、**lldp reinit** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lldp reinit *seconds*

no lldp reinit

パラメータ

reinit *seconds*：LLDP 転送を再初期化するまで LLDP ポートが待機する最小時間を秒単位で指定します（範囲：1 ～ 10）。

デフォルト設定

2 秒

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)#  lldp reinit 4
```

lldp timer

ソフトウェアがLLDP更新を送信する頻度を指定するには、**lldp timer** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lldp timer *seconds*

no lldp timer

パラメータ

timer *seconds*：ソフトウェアが LLDP 更新を送信する頻度を秒単位で指定します（範囲：5 ～ 32768 秒）。

デフォルト設定

30 秒

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、LLDP 更新の送信間隔を 60 秒に設定します。

```
switchxxxxxx(config)#  lldp timer 60
```

lldp transmit

インターフェイスでの LLDP の伝送を有効にするには、**lldp transmit** インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。インターフェイスでの LLDP の伝送を停止するには、このコマンドの **no** 形式を使用します。

構文

lldp transmit

no lldp transmit

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

有効

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

switchxxxxxx(config-if)#

使用上のガイドライン

LLDP は LAG ポートを個別に管理します。LLDP は、LAG 内の各ポートで個別のアドバタイズメントを送信します。

ポートの LLDP 動作は、ポートの STP の状態に依存しません。つまり、LLDP フレームはブロックされたポートで送信されます。

ポートが 802.1x によって制御されている場合、ポートが承認された場合にのみ LLDP が動作します。

例

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  lldp transmit
```

lldp tx-delay

LLDP ローカル システム MIB の値/ステータス変更によって開始される LLDP フレーム連続転送間の遅延を設定するには、**lldp tx-delay** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

lldp tx-delay *seconds*

no lldp tx-delay

パラメータ

tx-delay *seconds*：LLDP ローカルシステム MIB で 値/ステータスの変更で開始される LLDP フレームの連続転送間の遅延を秒単位で指定します（範囲：1 ～ 8192 秒）

デフォルト設定

デフォルトの LLDP フレーム転送遅延は 2 秒です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

tx-delay は LLDP タイマー間隔の 25% 未満であることをお勧めします。

例

次に、LLDP 転送遅延を 10 秒に設定する例を示します。

```
switchxxxxxx(config)#  lldp tx-delay 10
```

show lldp configuration

すべてのポートまたは特定のポートの LLDP 設定を表示するには、**show lldp configuration** 特権 EXEC モード コマンドを使用します。

構文

show lldp configuration *[interface-id* | **detailed**]

パラメータ

- **interface-id**：（オプション）ポート ID を指定します。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのポートについて表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

例 1：すべてのポートの LLDP 設定を表示します。

```
switchxxxxxx#  show lldp configuration
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering
Port      State  Optional TLVs      Address       Notifications
--------  -----  --------------     -----------   ------------
gi1/0/1       RX,TX  PD, SN, SD, SC , 4W      172.16.1.1    Disabled
gi1/0/2       TX     PD, SN              172.16.1.1    Disabled
gi1/0/3       RX,TX  PD, SN, SD, SC      None          Disabled
gi1/0/4       RX,TX  D,  SN, SD, SC      automatic     Disabled
```

例 2：ポート 1 の LLDP 設定を表示します。

```
switchxxxxxx#  show lldp configuration gi1/0/1
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering
Chassis ID: mac-address
Port State      Optional TLVs     Address      Notifications
---- ---------- --------------    -----------  -----------
```

```
gi1/0/1  RX, TX     PD, SN, SD, SC, 4W    72.16.1.1    Disabled
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size
802.1 optional TLVs
PVID: Enabled
PPVIDs: 0, 1, 92
VLANs: 1, 92
Protocols: 802.1x
```

次の表に、この出力で表示される重要なフィールドについて説明します。

フィールド	説明
Timer	LLDP 更新間の間隔。
Hold multiplier	受信側デバイスが LLDP パケットを破棄するまで保持する合計時間（タイマー間隔の倍数）。
Reinit timer	LLDP 転送を再初期化するまで LLDP ポートが待機する最小間隔。
Tx delay	LLDP ローカル システム MIB の値/ステータス変更によって開始される LLDP フレーム連続転送間の遅延。
Port	ポート番号
State	ポートの LLDP 状態。
Optional TLVs	アドバタイズされるオプション TLV。値は次のとおりです。 PD：ポートの説明 SN：システム名 SD：システムの説明 SC：システム機能 4 W：4 線式スペアペア機能
Address	アドバタイズされる管理アドレス。
Notifications	LLDP 通知が有効か無効かどうかを示します。
PVID	アドバタイズされるポート VLAN ID。
PPVID	アドバタイズされたプロトコル ポート VLAN ID。
Protocols	アドバタイズされたプロトコル。

show lldp local

特定のポートからアドバタイズされる LLDP 情報を表示するには、**show lldp local** 特権 EXEC モード コマンドを使用します。

構文

show lldp local *interface-id*

パラメータ

Interface-id：ポート ID を指定します。

デフォルト設定

該当なし。

コマンド モード

特権 EXEC モード

例

次に、gi1/0/1 と 2 からアドバタイズされる LLDP 情報を表示する例を示します。

```
switchxxxxxx#  show lldp local gi1/0/1
Device ID: 0060.704C.73FF
Port ID: gi1/0/1
Capabilities: Bridge
System Name: ts-7800-1
System description:
Port description:
Management address: 172.16.1.8
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex, 1000BASE-T full duplex
Operational MAU type: 1000BaseTFD
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522
Power Type: Type 1 PSE
Power Source: Primary Power Source
Power Priority: Unknown
PSE Allocated Power Value: 30
4-Pair POE supported: Yes
Spare Pair Detection/Classification required: Yes
PD Spare Pair Desired State: Enabled
802.3 EEE
Local Tx: 30 usec
Local Rx: 25 usec
Remote Tx Echo: 30 usec
Remote Rx Echo: 25 usec
802.1 PVID: 1
```

```
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2 (VLAN2)
802.1 Protocol: 88 08 00 01 (PAUSE)
LLDP-MED capabilities: Network Policy, Location Identification
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice
Flags: Tagged VLAN
VLAN ID: 2
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Sourcing Entity
Power source: Primary Power Source
Power priority: High
Power value: 9.6 Watts
LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
Hardware Revision: B1
Firmware Revision: A1
Software Revision: 3.8
Serial number: 7978399
Manufacturer name: Manufacturer
Model name: Model 1
Asset ID: Asset 123
switchxxxxxx#  show lldp local gi1/0/2
LLDP is disabled.
```

show lldp local tlvs-overloading

LLDP パケットに含まれる 1 つのパケットの情報が多すぎる場合、これはオーバーロードと呼ばれます。すべてのポートまたは特定のポートで LLDP の TLV オーバーロードのステータスを表示するには、**show lldp local tlvs-overloading** EXEC モード コマンドを使用します。

構文

show lldp local tlvs-overloading *[interface-id]*

パラメータ

interface-id：（オプション）ポート ID を指定します。

デフォルト設定

ポート ID が入力されていない場合、コマンドはすべてのポートの情報を表示します。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

このコマンドは、送信された最後の LLDP パケットではなく、現在の LLDP 設定のオーバーロード ステータスを計算します。

例

```
switchxxxxxx#  show lldp local tlvs-overloading gi1/0/1
TLVs Group             Bytes       Status
------------           ------      --------------
Mandatory               31         Transmitted
LLDP-MED Capabilities   9          Transmitted
LLDP-MED Location       200        Transmitted
802.1                   1360       Overloading
Total: 1600 bytes
Left: 100 bytes
```

show lldp med configuration

すべてのポートまたは特定のポートの LLDP Media Endpoint Discovery（MED）設定を表示するには、**show lldp med configuration** 特権 EXEC モード コマンドを使用します。

構文

show lldp med configuration *[interface-id* | **detailed**]

パラメータ

- **interface-id**：（オプション）ポート ID を指定します。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

ポート ID が入力されていない場合、コマンドはすべてのポートの情報を表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

例 1：次の例では、すべてのインターフェイスの LLDP MED 設定を表示します。

```
switchxxxxxx#  show lldp med configuration
Fast Start Repeat Count: 4.
lldp med network-policy voice: manual
Network policy 1
-------------------
Application type: voiceSignaling
VLAN ID: 1  untagged
Layer 2 priority: 0
DSCP: 0
Port    Capabilities   Network Policy Location  Notifications  Inventory
------ -------------- -------------- ---------- -------------   --------
gi1/0/1    Yes             Yes            Yes         Enabled        Yes
gi1/0/2    Yes             Yes            No          Enabled        No
gi1/0/3    No              No             No          Enabled        No
```

例 2：次に、gi1/0/1 で LLDP MED 設定を表示する例を示します。

```
switchxxxxxx#  show lldp med configuration gi1/0/1
Port    Capabilities   Network Policy   Location  Notifications Inventory
------- -------------- ---------------- --------- ----------    --------
gi1/0/1     Yes             Yes             Yes       Enabled        Yes
Network policies:
Location:
Civic-address: 61:62:63:64:65:66
```

show lldp neighbors

LLDP を使用して検出されたネイバー デバイスの情報を表示するには、**show lldp neighbors** 特権 EXEC モード コマンドを使用します。情報はすべてのポートまたは特定のポートで表示できます。

構文

show lldp neighbors *[interface-id]*

パラメータ

interface-id：（オプション）ポート ID を指定します。

デフォルト設定

ポート ID が入力されていない場合、コマンドはすべてのポートの情報を表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

ASCII 文字列として表示できない TLV 値は 16 進数の文字列として表示されます。

例 1：次の例では、LLDP が有効にされているすべてのポートで LLDP を使用して検出されたネイバー デバイスの情報および有効なユーザを表示します。

また、ロケーション情報が存在する場合は表示されます。

```
switchxxxxxx#  show lldp neighbors
System capability legend:
B - Bridge; R - Router; W - Wlan Access Point; T - telephone;
D - DOCSIS Cable Device; H - Host; r - Repeater;
TP - Two Ports MAC Relay; S - S-VLAN; C - C-VLAN; O - Other
Port  Device ID         Port ID  System Name Capabilities TTL
----- ---------------   -------- ----------  -----------  ----
gi1/0/1 00:00:00:11:11:11 gi1/0/1 ts-7800-2 B 90
gi1/0/1 00:00:00:11:11:11 gi1/0/1 ts-7800-2 B 90
gi1/0/2 00:00:26:08:13:24 gi1/0/3 ts-7900-1 B,R 90
gi1/0/3 00:00:26:08:13:24 gi1/0/2 ts-7900-2 W 90
```

例 2：次に、ポート 1 の LLDP を使用して検出されたネイバーデバイスに関する情報を表示する例を示します。

```
switchxxxxxx#  show lldp neighbors gi1/0/1
Device ID: 00:00:00:11:11:11
Port ID: gi1/0/1
System Name: ts-7800-2
Capabilities: B
System description:
Port description:
Management address: 172.16.1.1
Time To Live: 90 seconds
```

```
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported.
Auto-negotiation status: Enabled.
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex, 1000BASE-T full duplex.
Operational MAU type: 1000BaseTFD
802.3 Power via MDI
MDI Power support Port Class: PD
PSE MDI Power Support: Not Supported
PSE MDI Power State: Not Enabled
PSE power pair control ability: Not supported.
PSE Power Pair: Signal
PSE Power class: 1
Power Type: Type 1 PSE
Power Source: Primary Power Source
Power Priority: Unknown
PD Requested Power Value: 30
4-Pair POE supported: Yes
Spare Pair Detection/Classification required: Yes
PD Spare Pair Desired State: Enabled
PD Spare Pair Operational State: Enabled
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522
802.3 EEE
Remote Tx: 25 usec
Remote Rx: 30 usec
Local Tx Echo: 30 usec
Local Rx Echo: 25 usec
802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2(VLAN2)
802.1 Protocol: 88 8E 01
LLDP-MED capabilities: Network Policy.
LLDP-MED Device type: Endpoint class 2.
LLDP-MED Network policy
Application type: Voice
Flags: Unknown policy
VLAN ID: 0
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Device
Power source: Primary power
Power priority: High
Power value: 9.6 Watts
Hardware revision: 2.1
Firmware revision: 2.3
Software revision: 2.7.1
Serial number: LM759846587
Manufacturer name: VP
Model name: TR12
Asset ID: 9
LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
```

次の表では、この出力で表示される重要な LLDP フィールドについて説明します。

フィールド	説明
LLDP MED	

フィールド	説明
LLDP MED - ネットワーク ポリシー	
LLDP MED - Power Over Ethernet	
LLDP MED - Location	
Port	ポート番号
Device ID	ネイバー デバイスの設定されている ID（名前）または MAC アドレス。
Port ID	ネイバー デバイスのポート ID。
System name	ネイバー デバイスの管理用に割り当てられた名前。
Capabilities	ネイバー デバイスで検出される機能。値は次のとおりです。 • B：ブリッジ • R：ルータ • W：WLAN アクセス ポイント • T：電話 • D：DOCSIS ケーブル デバイス • H：ホスト • r：リピータ • O：その他
System description	ネイバー デバイスのシステムの説明。
Port description	ネイバー デバイスのポートの説明。
Management address	ネイバー デバイスの管理アドレス。
Auto-negotiation support	ポートの自動ネゴシエーション サポートのステータス。（サポート対象またはサポート非対象）
Auto-negotiation status	ポートの自動ネゴシエーションのアクティブ ステータス。（有効または無効）
Auto-negotiation Advertised Capabilities	自動ネゴシエーションによってアドバタイズされたポートの速度/デュプレックス/フロー制御機能。
Operational MAU type	ポートの MAU タイプ。

フィールド	説明
Power Source	PSE または PD デバイスによって使用される電源です。PSE デバイスは、その電力能力をアドバタイズします。使用可能な値は、Primary power source と Backup power source です。Unknown Power source、PSE and local power source、Local Only power source and PSE only power source。
Capabilities	送信者の LLDP MED 機能。
Device type	デバイスのタイプ。送信者がネットワーク接続デバイスかエンドポイント デバイスかを示します。エンドポイントの場合は属するエンドポイント クラスです。
Application type	このネットワーク ポリシーに定義されているアプリケーションの主な機能です。
Flags	フラグ. 次の値が可能です。 Unknown policy：デバイスにポリシーが必要ですが、現在は不明です。 Tagged VLAN：指定されたアプリケーション タイプがタグ付き VLAN を使用しています。 Untagged VLAN：指定されたアプリケーション タイプはタグなしの VLAN を使用しています。
VLAN ID	アプリケーションの VLAN ID。
Layer 2 priority	指定されたアプリケーションに使用しているレイヤ2の優先順位。
DSCP	指定されたアプリケーションに使用している DSCP 値。
Power type	デバイスの電源のタイプ。可能な値は、Power Sourcing Entity（PSE）または Power Device（PD）です。
Power Source	PSE または PD デバイスによって使用される電源です。PSE デバイスは、その電力能力をアドバタイズします。可能な値は、Primary power source および Backup power source です。PD デバイスは、その電源をアドバタイズします。可能な値は、Primary power、Local power、Primary and Local power です。

フィールド	説明
Power priority	PD デバイスの優先順位です。PSE デバイスは、ポートの設定されている電源優先順位をアドバタイズします。PD デバイスは、デバイスの設定されている電源優先順位をアドバタイズします。可能な値は、Critical、High および Low です。
Power value	PSE デバイスから PD デバイスに必要なワット単位の総電力、または PSE デバイスが現在の構成に基づいて最大長のケーブルを介して供給できる総電力です。
Coordinates, Civic address, ECS ELIN.	ロケーション情報の raw データ。

show lldp statistics

すべてのポートまたは特定のポートでLLDP統計情報を表示するには、**lldp statistics** EXECモード コマンドを使用します。

構文

show lldp statistics *[interface-id* | **detailed**]

パラメータ

- **interface-id**：（オプション）ポート ID を指定します。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

ポート ID が入力されていない場合、コマンドはすべてのポートの情報を表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

ユーザ EXEC モード

例

```
switchxxxxxx#  show lldp statistics
Tables Last Change Time: 14-Oct-2010 32:08:18
Tables Inserts: 26
Tables Deletes: 2
Tables Dropped: 0
Tables Ageouts: 1
       TX Frames      RX Frame                RX  TLVs         RX Ageouts
Port  Total Total Discarded Errors   Discarded   Unrecognized  Total
----- ---- ----- --------- --------- ---------   ---------     ------------
gi1/0/1   730   850    0       0         0             0          0
gi1/0/2   0       0    0       0         0              0          0
gi1/0/3   730     0    0       0         0              0          0
gi1/0/4   0       0    0       0         0              0          0
```

次の表では、この出力で表示される重要なLLDPフィールドについて説明します。

フィールド	説明
LLDP MED	
LLDP MED - Power Over Ethernet	
LLDP MED - Location	
Port	ポート番号

フィールド	説明
Device ID	ネイバー デバイスの設定されている ID（名前）または MAC アドレス。
Port ID	ネイバー デバイスのポート ID。
System name	ネイバー デバイスの管理用に割り当てられた名前。
Capabilities	ネイバー デバイスで検出される機能。値は次のとおりです。 • B：ブリッジ • R：ルータ • W：WLAN アクセス ポイント • T：電話 • D：DOCSIS ケーブル デバイス • H：ホスト • r：リピータ • O：その他
System description	ネイバー デバイスのシステムの説明。
Port description	ネイバー デバイスのポートの説明。
Management address	ネイバー デバイスの管理アドレス。
Auto-negotiation support	ポートの自動ネゴシエーション サポートのステータス。（サポート対象またはサポート非対象）
Auto-negotiation status	ポートの自動ネゴシエーションのアクティブ ステータス。（有効または無効）
Auto-negotiation Advertised Capabilities	自動ネゴシエーションによってアドバタイズされたポートの速度/デュプレックス/フロー制御機能。
Operational MAU type	ポートの MAU タイプ。
Capabilities	送信者の LLDP MED 機能。
Device type	デバイスのタイプ。送信者がネットワーク接続デバイスかエンドポイント デバイスかを示します。エンドポイントの場合は属するエンドポイント クラスです。
`LLDP MED - Network Policy`	

フィールド	説明
Application type	このネットワーク ポリシーに定義されているアプリケーションの主な機能です。
Flags	フラグ. 次の値が可能です。 Unknown policy：デバイスにポリシーが必要ですが、現在は不明です。 Tagged VLAN：指定されたアプリケーション タイプがタグ付き VLAN を使用しています。 Untagged VLAN：指定されたアプリケーション タイプはタグなしの VLAN を使用しています。
VLAN ID	アプリケーションの VLAN ID。
Layer 2 priority	指定されたアプリケーションに使用しているレイヤ 2 の優先順位。
DSCP	指定されたアプリケーションに使用している DSCP 値。
Power type	デバイスの電源のタイプ。可能な値は、Power Sourcing Entity（PSE）または Power Device（PD）です。
Power Source	PSE または PD デバイスによって使用される電源です。PSE デバイスは、その電力能力をアドバタイズします。可能な値は、Primary power source および Backup power source です。PD デバイスは、その電源をアドバタイズします。可能な値は、Primary power、Local power、Primary and Local power です。
Power priority	PD デバイスの優先順位です。PSE デバイスは、ポートの設定されている電源優先順位をアドバタイズします。PD デバイスは、デバイスの設定されている電源優先順位をアドバタイズします。可能な値は、Critical、High および Low です。
Power value	PSE デバイスから PD デバイスに必要なワット単位の総電力、または PSE デバイスが現在の構成に基づいて最大長のケーブルを介して供給できる総電力です。
Coordinates, Civic address, ECS ELIN.	ロケーション情報の raw データ。

ループバック検出コマンド

この章は、次の項で構成されています。

- loopback-detection enable（グローバル） （930 ページ）
- loopback-detection enable（インターフェイス） （931 ページ）
- loopback-detection interval （932 ページ）
- show loopback-detection （933 ページ）

loopback-detection enable（グローバル）

ループバック検出（LBD）機能をグローバルに有効にするには、**loopback-detection enable** グローバル コンフィギュレーション モード コマンドを使用します。ループバック検出機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

loopback-detection enable

no loopback-detection enable

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

ループバック検出は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、ループバック検出機能をグローバルに有効にします。**loopback-detection enable** インターフェイス コンフィギュレーション モード コマンドを使用すると、インターフェイスでループバック検出を有効にできます。

例

次の例では、デバイスでループバック検出機能を有効にします。

```
switchxxxxxx(config)#  loopback-detection enable
```

loopback-detection enable（インターフェイス）

インターフェイスでループバック検出（LBD）機能を有効にするには、**loopback-detection enable** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。インターフェイスでループバック検出機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

loopback-detection enable

no loopback-detection enable

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

ループバック検出はインターフェイスで有効になっています。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドは、インターフェイスでループバック検出を有効にします。**loopback-detection enable** 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、ループバック検出をグローバルに有効にします。

例

次に、ポート gi1/0/4 でループバック検出機能を有効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  loopback-detection enable
```

loopback-detection interval

LBD パケット間の間隔を設定するには、**loopback-detection interval** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

loopback-detection interval *seconds*

no loopback-detection interval

パラメータ

seconds：LBD パケット間の間隔を秒単位で指定します。（範囲：10 ～ 60 秒）

デフォルト設定

LBD パケット間のデフォルトの間隔は 30 秒です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、LBD パケット間の間隔を 45 秒に設定します。

```
switchxxxxxx(config)#  loopback-detection interval 45
```

show loopback-detection

ループバック検出の情報を表示するには、**show loopback-detection** 特権 EXEC モード コマンドを使用します。

構文

show loopback-detection [*interface-id* | **detailed**]

パラメータ

- **interface-id**：（オプション）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。これが設定されていない場合、デフォルトでは、存在するすべてのポートが表示されます。

デフォルト設定

すべてのポートが表示されます。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

動作ステータス Active は、次の条件を満たしていることを確認します。

- ループバックはグローバルに有効になっています。
- ループバックはインターフェイスで有効になっています。
- インターフェイスの動作状態は up です。
- インターフェイスの STP の状態が Forwarding または STP の状態が無効になっています。

LoopDetected の動作ステータスは、インターフェイスが errDisabled 状態になったことを示します。

動作ステータス Inactive は、ループバック検出がループを積極的に検出しないことを示します。つまり、Active ステータス条件が満たされていません。

例

次の例では、ループバック検出のステータスの情報を示します。

```
Console# show loopback-detection
Loopback detection: Enabled
LBD packets interval: 30 Seconds
```

Interface	Loopback Detection Admin State	Loopback Detection Operational State
gi1/0/1	Enabled	Active
gi1/0/2	Enabled	LoopDetected
gi1/0/3	Enabled	Inactive
gi1/0/4	Disabled	Inactive

マクロ コマンド

この章は、次の項で構成されています。

- macro name （936 ページ）
- macro （939 ページ）
- macro description （941 ページ）
- macro global （943 ページ）
- macro global description （945 ページ）
- show parser macro （946 ページ）

macro name

macro name グローバル コンフィギュレーション モード コマンドを使用すると、マクロを定義できます。定義できるマクロの種類は 2 つです。

- グローバル マクロは、常時実行可能な CLI コマンドのグループを定義します。

  Smartport マクロは Smartport タイプに関連付けられています。各 Smartport マクロの場合、アンチマクロにする必要があります（**no_** と連結した名前のマクロ）。アンチマクロはマクロのアクションを元に戻します。

この名前のマクロがすでに存在している場合、事前定義済みのマクロが上書きされます。

マクロ定義を削除するには、このコマンドの **no** 形式を使用します。

構文

macro name *macro-name*

no macro name [*macro-name*]

パラメータ

- ***macro-name***：マクロの名前。マクロ名では、大文字と小文字が区別されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

マクロは、CLI コマンドを含み、ユーザによって名前が割り当てられているスクリプトです。最大 3000 文字、200 行の文字を含めることができます。

キーワード

マクロにはキーワード（パラメータ）を含められます。キーワードの説明は次のとおりです。

- マクロには、最大 3 つのキーワードを含めることができます。
- キーワードに一致したすべての値が、**macro** コマンドで指定された対応する値に置き換えられます。
- キーワードの一致では、大文字と小文字が区別されます

  キーワードを使用してマクロを適用しても、元のマクロ定義の状態は変更されません。

  ### ユーザ フィードバック

ユーザ フィードバックを求めるマクロ コマンドの動作は、コマンドを端末から開始した場合と同じです。端末にプロンプトを表示し、ユーザの応答を受け入れます。

マクロの作成

マクロを作成する場合は、次のガイドラインを順守します。

- 名前を指定してマクロを作成するには、**macro name** を使用します。
- 1 行に 1 つのマクロ コマンドを入力します。
- マクロを終了するには、**@** 文字を使用します。
- マクロにコメントを入力する場合は、行頭に **#** 文字を指定します。

  さらに、マクロ内でのみ使用できる特定のプリプロセッサ コマンドを特定する場合も # を使用します。利用可能なプリプロセッサ コマンドは 2 つあります。

  #macro key description：マクロごとに最大 3 つのキーワードと説明のペアを使用して設定できます。キーワードおよび説明は、マクロが表示されている場合、GUI ページに表示されます。

  このプリプロセッサ コマンドのシンタックスは次のとおりです。

  #macro key description $*keyword1 description1 $keyword2 description2 $keyword3 description3*

  キーワードの先頭には「$」を指定する必要があります。

  #**macro keywords**：この指示により、デバイスで CLI ヘルプの一部としてキーワードを表示できます。最大 3 つのキーワードを受け入れます。コマンドは、マクロでキーワードを指定して CLI ヘルプ文字列を作成します。ヘルプ文字列は、**macro** および **macro global** コマンドからマクロのヘルプが要求された場合に表示されます。また、GUI は、コマンドで指定されたキーワードをマクロのパラメータ名としても使用します。CLI でのこのコマンドの使用方法については、例 2 および 例 3 を参照してください。

  このプリプロセッサ コマンドのシンタックスは次のとおりです。

  #macro keywords $*keyword1* $*keyword2* $*keyword3*

  keywordn はキーワードの名前です。

  ### マクロの編集

マクロは編集できません。既存のマクロと同じ名前の新しいマクロを作成して、マクロを変更します。新しいマクロにより、既存のマクロが上書きされます。

この例外には、Smartport 機能に組み込まれたマクロと対応するアンチマクロがあります。Smartport マクロを上書きすることはできません。

マクロの範囲

任意のユーザ定義マクロの範囲を考慮することが重要です。予期しない設定が適用される潜在的な危険があるため、**exit**、**end**、または **interface** *interface-id* などのコマンドを使用してマクロ内でコンフィギュレーション モードを変更しないでください。いくつかの例外を除き、さまざまなコンフィギュレーション モードでマクロを実行する他の方法があります。マクロは、特権 Exec モード、グローバル コンフィギュレーション モード、インターフェイス コンフィギュレーション モードでも実行できます（インターフェイスが VLAN 以外の場合）。

例 1：次の例では、ポートのデュプレックス モードを設定するマクロを作成する方法を示します。

```
switchxxxxxx(config)# macro name dup
Enter macro commands one per line. End with the character '@'.
#macro description dup
duplex full
negotiation
@
```

例 2：次の例では、DUPLEX と SPEED パラメータを使用してマクロを作成する方法を示します。マクロを実行する場合、ユーザは DUPLEX と SPEED を指定する必要があります。**#macro keywords** コマンドにより、ユーザは例 3 のようにマクロのヘルプを受信できるようになります。

```
switchxxxxxx(config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex $DUPLEX
no negotiation
speed $SPEED
#macro keywords $DUPLEX $SPEED
@
```

例 3：次の例では、（上記の **#macro keywords** コマンドで定義したように）ヘルプ文字 **?** を使用してキーワードを表示する方法を示し、ポートでマクロを実行します。マクロ定義で入力された **#macro keywords** コマンドにより、ユーザは、以下の e.g. の後に示すようにマクロのヘルプを受信できるようになります。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# macro apply duplex ?
    WORD <1-32>   Keyword to replace with value e.g. $DUPLEX, $SPEED
    <cr>
switchxxxxxx(config-if)# macro apply duplex $DUPLEX ?
    WORD<1-32>   First parameter value
    <cr>
switchxxxxxx(config-if)# macro apply duplex $DUPLEX full $SPEED ?
    WORD<1-32>   Second parameter value
switchxxxxxx(config-if)# macro apply duplex $DUPLEX full $SPEED 100
```

macro

macro apply/trace インターフェイス コンフィギュレーション コマンドを使用すると、いずれかのことを実行できます。

- 実行されるアクションを表示せずにマクロをインターフェイスに適用します
- 実行されるアクションを表示しながらマクロをインターフェイスに適用します

構文

macro {**apply** | **trace**} *macro-name* [*parameter-name1 value*] [*parameter-name2 value*] [*parameter-name3 value*]

パラメータ

- **apply**：特定のインターフェイスにマクロを適用します。
- **trace**：特定のインターフェイスにマクロを追加およびトレースします。
- ***macro-name***：マクロの名前。
- ***parameter-name value***：マクロで定義された各パラメータに対してその名前と値を指定します。最高3つのパラメータ値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。マクロのパラメータ名で一致が見られると、すべて対応する値に置き換えられます。

デフォルト設定

このコマンドには、デフォルト設定はありません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

macro apply コマンドにより、実行中はマクロのコマンドが非表示になります。**macro trace** コマンドにより、コマンドの実行中はコマンドによって生成されるエラーとコマンドが一緒に表示されます。これを使用すると、マクロをデバッグし、構文または設定のエラーを検出できます。

マクロを実行した場合、構文または設定のエラーが原因で失敗しても、マクロはインターフェイスに残りのコマンドを適用し続けます。

コマンド内にパラメータが含まれるマクロを適用する場合、このパラメータの値を指定しないと、コマンドは失敗します。**macro apply** macro-name で「**?**」を使用すると、マクロキーワードのヘルプ文字列を表示できます（**#macro keywords** プロセッサコマンドを使用してキーワードを定義している場合）。

パラメータ（キーワード）の照合では、大文字と小文字が区別されます。パラメータで一致が見られると、指定したすべての値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。

マクロをインターフェイスに適用すると、スイッチはマクロ名を付けたマクロ説明コマンドを自動的に生成します。その結果、マクロ名はインターフェイスのマクロ履歴に追加されます。**show parser macro** コマンドはインターフェイスのマクロ履歴を表示します。

インターフェイスの範囲に適用されたマクロは、単一インターフェイスに適用されたマクロと同じ動作をします。マクロがインターフェイス範囲に適用される場合、範囲内の各インターフェイスに連続して適用されます。マクロ コマンドが 1 つのインターフェイスで失敗すると、残りのインターフェイスに適用しようとしたかどうかに関係なく、失敗または成功することがあります。

例 1：次に、トレース オプションを指定してインターフェイスに適用するマクロの例を示します。

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# macro trace dup $DUPLEX full $SPEED 100
  Applying command…  'duplex full'
  Applying command…  'speed 100'
switchxxxxxx(config-if)#
```

例 2：次に、トレース オプションを指定せずに適用するマクロの例を示します。

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# macro apply dup $DUPLEX full $SPEED 100
switchxxxxxx(config-if)#
```

例 3：次に、正しくないマクロを適用している例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# macro trace dup
Applying command...'duplex full'
Applying command...'speed auto'
% bad parameter value
switchxxxxxx(config-if)#
```

macro description

macro description インターフェイス コンフィギュレーション モード コマンドを使用すると、マクロ名などの説明をインターフェイスのマクロ履歴に追加できます。インターフェイスのマクロ履歴をクリアするには、このコマンドの **no** 形式を使用します。マクロがインターフェイスに適用されると、スイッチはマクロ名を付けたマクロ説明コマンドを自動的に生成します。その結果、マクロ名はインターフェイスのマクロ履歴に追加されます。

構文

macro description text

no macro description

パラメータ

- ***text***：説明テキスト。このテキストには、最大 160 文字を含めることができます。テキストに複数の単語が含まれる場合、テキストを二重引用符で囲む必要があります。

デフォルト設定

このコマンドには、デフォルト設定はありません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

複数のマクロが 1 つのインターフェイスに適用されると、説明テキストは以前に適用したマクロの番号のテキストと連結されます。

例

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# macro apply dup
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface gi1/0/3
switchxxxxxx(config-if)# macro apply duplex $DUPLEX full $SPEED 100
switchxxxxxx(config-if)# macro description dup
switchxxxxxx(config-if)# macro description duplex
switchxxxxxx(config-if)# end
switchxxxxxx(config)# exit
switchxxxxxx# show parser macro description
Global Macro(s):
Interface      Macro Description(s)
------------   -------------------------------------------------
gi1/0/2             dup
gi1/0/3             duplex | dup | duplex
-----------------------------------------------------------------
switchxxxxxx# configure
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# no macro description
```

```
switchxxxxxx(config-if)# end
switchxxxxxx(config)# exit
switchxxxxxx# show parser macro description
Global Macro(s):
Interface      Macro Description(s)
---------      -------------------------------------------------------
gi1/0/3            duplex | dup | duplex
------------------------------------------------------------------
```

macro global

macro global 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、マクロをスイッチ（トレース オプションに関係なく）に適用できます。

構文

macro global {**apply** | **trace**} *macro-name* [*parameter-name1 value*] [*parameter-name2 value*] *[parameter -name3 value*]

パラメータ

- **apply**：スイッチにマクロを適用します。
- **trace**：スイッチにマクロを追加およびトレースします。
- ***macro-name***：マクロの名前を指定します。
- ***parameter-name*** value：スイッチに必要なパラメータ値を指定します。最高 3 つのパラメータ値の組み合わせを入力できます。パラメータ キーワードの照合では、大文字と小文字が区別されます。パラメータで一致が見られると、対応する値にすべて置き換えられます。

デフォルト設定

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション モード。

使用上のガイドライン

マクロを適用したとき、構文エラーまたは設定エラーのためにコマンドが失敗した場合、マクロは引き続き残りのコマンドをスイッチに適用します。

キーワードの照合では、大文字と小文字が区別されます。キーワードで一致が見られると、すべて対応する値に置き換えられます。キーワードが完全に一致すると、それが長い文字列の一部であったとしても一致と見なされて、対応する値に置き換えられます。

コマンド内にキーワードが含まれるマクロを適用する場合、このマクロを適用するときにキーワードに適切な値を指定しないと、コマンドは失敗します。このコマンドで「?」を使用すると、マクロ キーワードのヘルプ文字列を表示できます。マクロを定義する場合は、**#macro keywords** プロセッサ コマンドを使用してヘルプ文字列でキーワードを定義します。

マクロをグローバル コンフィギュレーション モードで適用すると、スイッチはマクロ名を付けたグローバルマクロ説明コマンドを自動的に生成します。その結果、マクロ名はグローバルマクロ履歴に追加されます。

例

次の例では、マクロを定義して、トレース オプションが指定されたスイッチに適用されています。

```
switchxxxxxx(config)# macro name console-timeout
Enter macro commands one per line. End with the character '@'.
line console
exec-timeout $timeout-interval
@
switchxxxxxx(config)# macro global trace console-timeout $timeout-interval 100
  Applying command…  'line console'
  Applying command…  'exec-timeout 100'
```

macro global description

macro global description 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、スイッチに適用されているマクロを示すために使用される説明を入力できます。説明を削除するには、このコマンドの **no** 形式を使用します。

構文

macro global description text

no macro global description

パラメータ

- ***text***：説明テキスト。このテキストには、最大 160 文字を含めることができます。

デフォルト設定

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

複数のグローバルマクロがスイッチに適用されると、グローバル説明テキストは以前に適用したマクロの番号のテキストと連結されます。

例

```
switchxxxxxx(config)# macro global description "set console timeout interval"
```

show parser macro

設定されているすべてのマクロ、またはスイッチ上の1つのマクロのパラメータを表示するには、**show parser macro** ユーザ EXEC モードコマンドを使用します。

構文

show parser macro [{**brief** | **description** [**interface** interface-id **| detailed**] | **name** macro-name}]

パラメータ

- **brief**：すべてのマクロの名前を表示します。
- **description** [**interface** interface-id]：すべてのインターフェイスのマクロの説明を表示するか、またはインターフェイスを指定した場合は、そのインターフェイスのマクロの説明を表示します。
- **name** macro-name：マクロ名で識別される 1 つのマクロに関する情報を表示します。
- **detailed**：現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

現在のポートですべてのマクロの説明を表示します。

detailed キーワードを使用しないと、現在のポートだけが表示されます。

コマンド モード

ユーザ EXEC モード

例 1：次の例では、**show parser macro** コマンドの出力を示します。

```
switchxxxxxx# show parser macro
Total number of macros = 6
------------------------------------------------------------------
Macro name : company-global
Macro type : default global
# Enable dynamic port error recovery for link state
# failures
------------------------------------------------------------------
Macro name : company-desktop
Macro type : default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access
```

例 2：次の例では、**show parser macro name** コマンドの出力を示します。

```
switchxxxxxx# show parser macro standard-switch10
Macro name : standard-switch10
Macro type : customizable
macro description standard-switch10
```

```
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp
```

例 3：次の例では、**show parser macro brief** コマンドの出力を示します。

```
switchxxxxxx# show parser macro brief
default global : company-global
default interface: company-desktop
default interface: company-phone
default interface: company-switch
default interface: company-router
customizable : snmp
```

例 4：次の例では、**show parser macro description** コマンドの出力を示します。

```
switchxxxxxx# show parser macro description
Global Macro(s): company-global
```

例 5：次の例では、**show parser macro description interface** コマンドの出力を示します。

```
switchxxxxxx# show parser macro description interface gi1/0/2
Interface Macro Description
---------------------------------------------------------------
gi1/0/2 this is test macro
---------------------------------------------------------------
```

管理 ACL コマンド

この章は、次の項で構成されています。

- deny（管理） （950 ページ）
- permit（管理） （952 ページ）
- management access-list （954 ページ）
- management access-class （956 ページ）
- show management access-list （957 ページ）
- show management access-class （958 ページ）

deny（管理）

管理アクセス リスト（ACL）の permit ルール（ACE）を設定するには、**deny** 管理アクセス リスト コンフィギュレーション モード コマンドを使用します。

構文

deny [*interface-id*] [**service** *service*]

deny ip-source {*ipv4-address* | i*pv6-address*/ipv6-prefix-length} [**mask** {*mask* | *prefix-length*}] [*interface-id*] [**service** *service*]

パラメータ

- **interface-id**：（オプション）インターフェイス ID を指定します。インターフェイス ID には次のタイプのいずれかを指定できます：イーサネット ポート、ポート チャネルまたは VLAN
- **service** *service*：（オプション）サービス タイプを指定します。使用可能な値は、Telnet、SSH、HTTP、HTTPS、および SNMP です。
- ***ipv4-address***：送信元 IPv4 アドレスを指定します。
- ***ipv6-address***/*ipv6-prefix-length*：送信元 IPv6 アドレスと送信元 IPv6 アドレスのプレフィックス長を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。パラメータは、省略可能です。
- **mask** *mask*：送信元 IPv4 アドレス ネットワーク マスクを指定します。パラメータは、IPv4 アドレスにのみ関連します。
- **mask** *prefix-length*：送信元 IPv4 アドレス プレフィックスを構成するビット数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。パラメータは、IPv4 アドレスにのみ関連します。（範囲：0 ～ 32）

デフォルト設定

ルールは設定されていません。

コマンド モード

管理アクセスリスト コンフィギュレーション モード

使用上のガイドライン

IP アドレスが適切なインターフェイスで定義されている場合は、イーサネット、VLAN、ポート チャネル パラメータのルールが有効です。

例

次の例では、**mlist** と呼ばれる ACL のすべてのポートを拒否します。

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny
```

permit（管理）

管理アクセス リスト（ACL）の permit ルール（ACE）を設定するには、**permit** 管理アクセス リスト コンフィギュレーション モード コマンドを使用します。

構文

permit *[interface-id] [service service]*

permit ip-source {*ipv4-address* | *ipv6-address*/ipv6-prefix-length} *[***mask** {mask | prefix-length}] [interface-id] [**service** service]

パラメータ

- **interface-id**：（オプション）インターフェイス ID を指定します。インターフェイス ID には次のタイプのいずれかを指定できます：イーサネット ポート、ポート チャネルまたは VLAN
- **service** *service*：（オプション）サービス タイプを指定します。使用可能な値は、Telnet、SSH、HTTP、HTTPS、および SNMP です。
- **ipv4-address**：送信元 IPv4 アドレスを指定します。
- **ipv6-address/ipv6-prefix-length**：送信元 IPv6 アドレスおよび送信元 IPv6 アドレスのプレフィックス長を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。パラメータは、省略可能です。
- **mask** *mask*：送信元 IPv4 アドレス ネットワーク マスクを指定します。このパラメータは、IPv4 アドレスにのみ関連します。
- **mask** *prefix-length*：送信元 IPv4 アドレス プレフィックスを構成するビット数を指定します。プレフィックス長は、スラッシュ（/）で開始する必要があります。このパラメータは、IPv4 アドレスにのみ関連します。（範囲：0 ～ 32）

デフォルト設定

ルールは設定されていません。

コマンド モード

管理アクセスリスト コンフィギュレーション モード

使用上のガイドライン

IP アドレスが適切なインターフェイスで定義されている場合は、イーサネット、VLAN、ポート チャネル パラメータのルールが有効です。

例

次の例では、**mlist** と呼ばれる ACL のすべてのポートを許可します

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit
```

management access-list

管理アクセス リスト（ACL）を設定して、管理アクセスリスト コンフィギュレーション モードを開始するには、**management access-list** グローバル コンフィギュレーション モード コマンドを使用します。ACL を削除するには、このコマンドの **no** 形式を使用します。

構文

management access-list *name*

no management access-list *name*

パラメータ

name：ACL 名を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

該当なし

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、管理アクセス リストを設定できます。このコマンドは、管理アクセスリスト コンフィギュレーション モードを開始します。ここでは、拒否アクセス条件または許可アクセス条件が **deny** と **permit** コマンドを使用して定義されています。

一致条件が定義されていない場合、デフォルト値は **deny** です。

アクセス リスト コンテキストを再入力すると、新しいルールがアクセス リストの最後に入力されます。

management access-class （956 ページ） コマンドを使用すると、アクティブなアクセス リストを選択できます。

アクティブな管理リストは更新または削除することはできません。

静音モード期間のアクセスクラスとして設定された管理アクセスリスト（AAA コマンドセクションのコマンド login quiet-mode access-class）は、変更または削除することはできません。

IPv4 パケットでトンネル化されている IPv6 管理トラフィックの場合、管理 ACL が外部 IPv4 ヘッダーに最初に適用され（サービス フィールドのルールは無視され）、次に内部 IPv6 ヘッダーに適用されます。

例 1：次に、**mlist** という管理アクセスリストを作成し、管理 gi1/0/1 と gi1/0/9 を設定し、新しいアクセスリストをアクティブリストにする例を示します。

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit gi1/0/1
```

```
switchxxxxxx(config-macl)# permit gi1/0/9
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

例 2：次に、「mlist」という管理アクセスリストを作成し、gi1/0/1 と gi1/0/9 を除くすべてのインターフェイスを管理インターフェイスに設定し、新しいアクセスリストをアクティブリストにする例を示します。

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny gi1/0/1
switchxxxxxx(config-macl)# deny gi1/0/9
switchxxxxxx(config-macl)# permit
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

management access-class

アクティブな管理アクセス リスト（ACL）を定義して管理接続を制限するには、**management access-class** グローバル コンフィギュレーション モード コマンドを使用します。管理接続制限を無効にするには、このコマンドの **no** 形式を使用します。

構文

management access-class {**console-only** | *name*}

no management access-class

パラメータ

- **console-only**：デバイスをコンソールのみから管理できるように指定します。
- **name**：使用する ACL 名を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

デフォルト設定では、管理接続が制限されていません。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、**mlist** と呼ばれるアクセス リストをアクティブな管理アクセス リストとして定義します。

```
switchxxxxxx(config)# management access-class mlist
```

show management access-list

管理アクセス リスト（ACL）を表示するには、**show management access-list** 特権 EXEC モード コマンドを使用します。

構文

show management access-list [*name*]

パラメータ

name：（オプション）表示する管理アクセス リストの名前を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

すべての管理 ACL が表示されます。

コマンド モード

特権 EXEC モード

例

次の例では、**mlist** 管理 ACL を表示します。

```
switchxxxxxx# show management access-list mlist
m1
--
deny service telnet
permit gi1/0/1 service telnet
! (Note: all other access implicitly denied)
console(config-macl)#
```

show management access-class

アクティブな管理アクセス リスト（ACL）の情報を表示するには、**show management access-class** 特権 EXEC モード コマンドを使用します。

構文

show management access-class

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

例 1：次の例では、アクティブな管理 ACL 情報を表示します。

```
switchxxxxxx# show management access-class
Management access-class is enabled, using access list mlist
```

例 2：次の例では、デバイスで管理アクセスクラスが有効になっており、デバイスが静音モード期間である場合に、アクティブな管理 ACL 情報を表示します（「AAA コマンド」セクションの login block-for および login quiet-mode access-class コマンドを参照）。

```
switchxxxxxx# show management access-class
Management access-class is enabled, using login quiet-mode period
access-class quiet-ACL(mlist access-list will be active when login quiet-mode
period ends
```

MLD コマンド

この章は、次の項で構成されています。

- clear ipv6 mld counters （960 ページ）
- ipv6 mld last-member-query-count （961 ページ）
- ipv6 mld last-member-query-interval （962 ページ）
- ipv6 mld query-interval （963 ページ）
- ipv6 mld query-max-response-time （964 ページ）
- ipv6 mld robustness （965 ページ）
- ipv6 mld version （966 ページ）
- show ipv6 mld counters （967 ページ）
- show ipv6 mld groups （968 ページ）
- show ipv6 mld groups summary （970 ページ）
- show ipv6 mld interface （971 ページ）

clear ipv6 mld counters

マルチキャスト リスナー検出（MLD）のインターフェイス カウンタをクリアするには、特権 EXEC モードで **clear ipv6 mld counters** コマンドを使用します。

構文

clear ipv6 mld counters [interface-id]

パラメータ

- ***interface-id***：（オプション）インターフェイス識別子。

コマンド モード

特権 EXEC モード

使用上のガイドライン

受信した参加および脱退の数を追跡する MLD カウンタをクリアするには、**clear ipv6 mld counters** コマンドを使用します。オプションの *interface-id* 引数を省略した場合、**clear ipv6 mld counters** コマンドはすべてのインターフェイスのカウンタをクリアします。

例

次の例では、VLAN 100 のカウンタをクリアします。

```
switchxxxxxx# clear ipv6 mld counters vlan 100
```

ipv6 mld last-member-query-count

マルチキャストリスナー検出（MLD）のラストメンバークエリーカウンタを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 mld last-member-query-count** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld last-member-query-count count

no ipv6 mld last-member-query-count

パラメータ

count：脱退を示すメッセージの受信時にグループまたはグループ送信元固有のクエリーを送信した回数。（範囲：1 ～ 7）

デフォルト設定

MLD 堅牢性変数の値。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

MLD ラスト メンバー クエリーカウンタを変更するには、**ipv6 mld robustness** コマンドを使用します。

例

次の例では、MLD の最後のメンバーのクエリー カウンタの値を 3 に変更します。

```
switchxxxxxx(config)# interface vlan 1
ipv6 mld last-member-query-count 3
exit
```

ipv6 mld last-member-query-interval

マルチキャスト リスナー検出（MLD）のラスト メンバー クエリー間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 mld last-member-query-interval** コマンドを使用します。デフォルトの MLD クエリー間隔に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld last-member-query-interval *milliseconds*

no ipv6 mld last-member-query-interval

パラメータ

- ***milliseconds***：インターフェイスで MLD グループ固有のホスト クエリー メッセージが送信されたミリ秒単位の間隔。（範囲：100 ～ 25500）。

デフォルト設定

MLD の最後のメンバーのデフォルトのクエリー間隔は 1000 ミリ秒です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

インターフェイスで MLD ラスト メンバー クエリー間隔を設定するには、**ipv6 mld last-member-query-interval** コマンドを使用します。

例

次に、MLD ラスト メンバー クエリー間隔を 1500 ミリ秒に増加する例を示します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld last-member-query-interval 1500
switchxxxxxx(config-if)# exit
```

ipv6 mld query-interval

スイッチがマルチキャスト リスナー検出（MLD）ホストクエリー メッセージを送信する頻度を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 mld query-interval** コマンドを使用します。デフォルトの頻度に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld query-interval *seconds*

no ipv6 mld query-interval

パラメータ

- ***seconds***：スイッチがインターフェイスからMLDクエリーメッセージを送信する頻度（秒単位）。範囲は 30 ～ 18000 です。

デフォルト設定

デフォルトの MLD クエリー間隔は 125 秒です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

インターフェイスから MLD クエリアが MLD ホストクエリー メッセージを送信する頻度を設定するには、**ipv6 mld query-interval** コマンドを使用します。ルータの接続されたネットワーク上にメンバーがいるマルチキャスト グループを検出するために、MLD クエリアはクエリー ホスト メッセージを送信します。

クエリー間隔は、クエリーの最大応答時間よりも長い必要があります。

例

次に、MLD クエリアが MLD ホスト クエリー メッセージを送信する頻度を 180 秒に増加する例を示します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld query-interval 180
switchxxxxxx(config-if)# exit
```

ipv6 mld query-max-response-time

マルチキャスト リスナー検出（MLD）クエリーでアドバタイズされる最大応答所要時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 mld query-max-response-time** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld query-max-response-time *seconds*

no ipv6 mld query-max-response-time

パラメータ

- ***seconds***：MLD クエリーでアドバタイズされる最大応答時間（秒単位）。（範囲：5～20）

デフォルト設定

10 秒。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

このコマンドは、応答側が MLD クエリー メッセージに応答できる期間を制御します。この期間を過ぎると、ルータはグループを削除します。

このコマンドは、ルータがグループを削除する前に、どれくらいの時間でホストが MLD クエリー メッセージに応答する必要があるかを制御します。10 秒未満の値を設定すると、ルータはグループをすばやくプルーニングすることができます。

クエリーの最大応答時間はクエリー間隔よりも短い必要があります。

注。ホストが十分な速さで応答しない場合、誤ってプルーニングされる可能性があります。したがって、ホストは10秒（または設定した値）よりも早く、応答を認識する必要があります。

例

次に、最大応答時間を 8 秒に設定する例を示します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld query-max-response-time 8
switchxxxxxx(config-if)# exit
```

ipv6 mld robustness

マルチキャスト リスナー検出（MLD）の堅牢性変数を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 mld robustness** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld robustness count

no ipv6 mld robustness

パラメータ

- ***count***：リンク上で予期されるパケット損失の数。パラメータの範囲。（範囲：1 ～ 7）。

デフォルト設定

デフォルト値は 2 です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

MLD の堅牢性変数を変更するには、**ipv6 mld robustness** コマンドを使用します。

例

次の例では、MLD の堅牢性変数の値を 3 に変更します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld robustness 3
switchxxxxxx(config-if)# exit
```

ipv6 mld version

ルータが使用するマルチキャスト リスナー検出プロトコル（MLD）のバージョンを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 mld version** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld version {**1** | **2**}

no ipv6 mld version

パラメータ

- **1**：MLD バージョン 1。
- **2**：MLD バージョン 2。

デフォルト設定

1

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

MLD のデフォルト バージョンを変更するにはこのコマンドを使用します。

例

次の例では、MLD バージョン 1 を使用するようにルータを設定します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld version 1
switchxxxxxx(config-if)# exit
```

show ipv6 mld counters

マルチキャストリスナー検出（MLD）のトラフィックカウンタを表示するには、ユーザEXECモードで **show ipv6 mld counters** コマンドを使用します。

構文

show ipv6 mld counters [*interface-id*]

パラメータ

- ***interface-id***：（オプション）インターフェイス識別子。

コマンドモード

ユーザ EXEC モード

使用上のガイドライン

予期される数の MLD メッセージが受信および送信されたかどうかをチェックするには、**show ipv6 mld counters** コマンドを使用します。

オプションの *interface-id* 引数を省略した場合、**show ipv6 mld counters** コマンドはすべてのインターフェイスのカウンタを表示します。

例

次に、送受信された MLD プロトコル メッセージを表示する例を示します。

```
switchxxxxxx# show ipv6 mld counters vlan 100
VLAN 100
Elapsed time since counters cleared:00:00:21
 Failed received Joins: 0
 Total MLDv1 received messages: 10
 Total MLDv2 received messages: 0
 Total invalid received messages: 0
 General Sent Queries: 0
 Specific Sent Queries: 0
```

show ipv6 mld groups

ルータに直接接続されマルチキャスト リスナー検出（MLD）を通じて学習されたマルチキャスト グループを表示するには、ユーザ EXEC モードで **show ipv6 mld groups** コマンドを使用します。

構文

show ipv6 mld groups [**link-local** | *group-name* | *group-address* | *interface-id*] [**detail**]

パラメータ

- **link-local**：（オプション）リンクローカル グループを表示します。
- ***group-name* | *group-address***：（オプション）：マルチキャスト グループの IPv6 アドレスまたは名前。
- ***interface-id***：（オプション）インターフェイス識別子。
- **detail**：（オプション）個々のソースに関する詳細情報が表示されます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

直接接続しているすべてのグループを表示するには、**show ipv6 mld groups** [**detail**] コマンドを使用します。

直接接続しているすべてのリンクローカルグループを表示するには、**show ipv6 mld groups link-local** [**detail**] コマンドを使用します。

直接接続している指定した 1 グループを表示するには、**show ipv6 mld groups** [*group-name* | *group-address*] [**detail**] コマンドを使用します。

指定したインターフェイスに直接接続しているすべてのグループを表示するには、**show ipv6 mld groups** *interface-id* [**detail**] コマンドを使用します。

例 1。次に、**show ipv6 mld groups** コマンドの出力例を示します。VLAN 100 により参加しているすべてのグループが表示されます。

```
switchxxxxxx# show ipv6 mld groups vlan 100
```

MLD Connected Group Membership

```
Expires: never - switch itself has joined the group
Group Address Interface Expires
FF02::2 VLAN 100 never
FF02::1:FF00:1 VLAN 00:10:27
FF02::1:FFAF:2C39 VLAN 100 00:09:11
FF06:7777::1 VLAN 100 00:00:26
```

例 2。次に、**show ipv6 mld groups** コマンドで **detail** キーワードを指定した場合の出力例を示します。

```
switchxxxxxx# show ipv6 mld groups detail
Expires: zero value - INCLUDE state; non-zero value - EXCLUDE state
Interface: VLAN 100
 Group: FF33::1:1:1
 Router mode: INCLUDE
 Last reporter: 2009:5::12:1
 Group Timer Expires: 00:20:11
 Group source list:
 Source Address Expires
 2004:4::6 00:00:11
 2004:4::16 00:08:11
 Group: FF33::1:1:2
 Router mode: EXCLUDE
 Last reporter: 2008:5::2A:10
 Group Timer Expires: 00:20:11
 Exclude Mode Expiry (Filter) Timer: 00:10:11
 Group source list:
 Source Address Expires
 2004:5::1 00:04:08
 2004:3::1 00:04:08
 2004:7::10 00:00:00
 2004:50::1 00:00:00
```

show ipv6 mld groups summary

マルチキャスト リスナー検出（MLD）キャッシュ内に存在する (*,G) および (S,G) メンバーシップ レポートの数を表示するには、ユーザ EXEC モードで **show ipv6 mld groups summary** コマンドを使用します。

構文

show ipv6 mld groups summary

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

show ipv6 mld groups summary コマンドは、直接接続しているマルチキャスト グループ（リンクローカル グループを含む）の数を表示します。

例

次に、**show ipv6 mld groups summary** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 mld groups summary
MLD Route Summary
 No. of (*,G) routes = 5
 No. of (S,G) routes = 0
```

```
Field Descriptions:
No. of (*,G) routes = 5—Displays the number of groups present in the MLD cache.
No. of (S,G) routes = 0—Displays the number of include and exclude mode sources present
 in the MLD cache.
```

show ipv6 mld interface

インターフェイスのマルチキャスト関連情報を表示するには、ユーザ EXEC モードで **show ipv6 mld interface** コマンドを使用します。

構文

show ipv6 mld interface [*interface-id*]

パラメータ

- ***interface-id***：インターフェイス識別子。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

オプションの *interface-id* 引数を省略した場合、**show ipv6 mld interface** コマンドはすべてのインターフェイスの情報を表示します。

例

次に、イーサネット インターフェイス 2/1/1 に対する **show ipv6 mld interface** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 mld interface vlan 100
VLAN 100 is up
 Administrative MLD Querier IPv6 address is FE80::260:3EFF:FE86:5649
 Operational MLD Querier IPv6 address is FE80::260:3EFF:FE86:5649
 Current MLD version is 3
 Administrative MLD robustness variable is 2 seconds
 Operational MLD robustness variable is 2 seconds
 Administrative MLD query interval is 125 seconds
 Operational MLD query interval is 125 seconds
 Administrative MLD max query response time is 10 seconds
 Operational MLD max query response time is 10 seconds
 Administrative Last member query response interval is 1000 milliseconds
 Operational Last member query response interval is 1000 milliseconds
```

MLD プロキシ

この章は、次の項で構成されています。

- ipv6 mld-proxy ssm （974 ページ）
- ipv6 mld-proxy （975 ページ）
- ipv6 mld-proxy downstream protected （976 ページ）
- ipv6 mld-proxy downstream protected interface （977 ページ）
- show ipv6 mld-proxy interface （978 ページ）

ipv6 mld-proxy ssm

IP マルチキャスト アドレスの Source Specific Multicast（SSM）範囲を定義するには、グローバル コンフィギュレーション モードで **ipv6 mld-proxy ssm** コマンドを使用します。SSM 範囲を無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld-proxy ssm {**default** | **range** *access-list*}

no ipv6 mld-proxy ssm

パラメータ

default：FF3x::/32 への SSM 範囲のアクセス リストを定義します（rfc4607 を参照してください）。

range *access-list*：SSM 範囲を定義する標準の IPv6 アクセス リスト名を指定します。

デフォルト設定

このコマンドは無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

新しい **ipv6 mld-proxyssm** コマンドは、以前の **ipv6 mld-proxy ssm** コマンドをオーバーライドします。

定義されているすべての範囲を削除するには、**no ipv6 mld-proxy ssm** コマンドを使用します。

例

次の例は、デフォルトの IPv6 アドレス範囲とアクセス リスト **list1** によって定義された IPv6 アドレス範囲の SSM サービスを設定する方法を示します。

```
switchxxxxxx(config)# ipv6 access-list list1 permit FF7E:1220:2001:DB8::/64
switchxxxxxx(config)# ipv6 access-list list1 deny FF7E:1220:2001:DB1::1
switchxxxxxx(config)# ipv6 access-list list1 permit FF7E:1220:2001:DB1::/64
switchxxxxxx(config)# ipv6 pim mld-proxy range list1
```

ipv6 mld-proxy

MLD プロキシ ツリーにダウンストリーム インターフェイスを追加するには、インターフェイス コンフィギュレーション モードで **ip mld-proxy** コマンドを使用します。インターフェイスから MLD プロキシ ツリーへのダウンストリームを削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld-proxy *upstream-interface-id*

no ipv6 mld-proxy

パラメータ

- ***upstream-interface-id***：アップストリーム インターフェイス識別子。

デフォルト設定

プロトコルはインターフェイスで無効です。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

MLD プロキシ ツリーにダウンストリーム インターフェイスを追加するには、**ipv6 mld-proxy** コマンドを使用します。プロキシ ツリーが存在しない場合は、作成されます。

ダウンストリーム インターフェイスを削除するには、このコマンドの **no** 形式を使用します。最後のダウン ストリーム インターフェイスがプロキシ ツリーから削除されると、プロキシ ツリーも削除されます。

例 1。次の例では、そのアップストリーム インターフェイスとして vlan 200 を持つ MLD プロキシ プロセスに、ダウンストリーム インターフェイスを追加します。

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld-proxy vlan 200
switchxxxxxx(config-if)# exit
```

例 2。次の例では、vlan 200 をアップストリーム インターフェイスとする、IGMP プロキシ プロセスに、ダウンストリーム インターフェイスの範囲を追加します。

```
switchxxxxxx(config)# interface range vlan 100-105
switchxxxxxx(config-if)# ipv6 mld-proxy vlan 200
switchxxxxxx(config-if)# exit
```

ipv6 mld-proxy downstream protected

ダウンストリーム インターフェイスからの IPv6 マルチキャスト トラフィックの転送を無効にするには、グローバル コンフィギュレーション モードで **ipv6 mld-proxy downstream protected** コマンドを使用します。ダウンストリームインターフェイスからの転送を許可するには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld-proxy downstream protected

no ipv6 mld-proxy downstream protected

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

ダウンストリーム インターフェイスからの転送を許可します。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ダウンストリームインターフェイスからの転送をブロックするには、**pv6 mld-proxy downstream protected** コマンドを使用します。

例

次の例では、ダウンストリーム インターフェイスからの転送を禁止します。

```
switchxxxxxx(config)# ipv6 mld-proxy downstream protected
```

ipv6 mld-proxy downstream protected interface

特定のダウンストリーム インターフェイスからの IPv6 マルチキャスト トラフィックの転送を無効または有効にするには、インターフェイス コンフィギュレーション モードで**ipv6 mld-proxy downstream protected interface** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld-proxy downstream protected interface {enabled | disabled}

no ipv6 mld-proxy downstream protected interface

パラメータ

- **enabled**：インターフェイスでのダウンストリーム インターフェイスの保護が有効です。インターフェイスに到着した IPv6 マルチキャスト トラフィックは転送されません。
- **disabled**：インターフェイスでのダウンストリーム インターフェイスの保護が無効です。インターフェイスに到着した IPv6 マルチキャスト トラフィックは転送されます。

デフォルト設定

グローバル ダウンストリーム保護の設定（**ipv6 mld-proxy downstream protected** コマンドを参照してください）

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

特定のダウンストリーム インターフェイスからの転送をブロックするには、**ipv6 mld-proxy downstream protected interface disabled** コマンドを使用します。

特定のダウンストリーム インターフェイスからの転送を許可するには、**ipv6 mld-proxy downstream protected interface enabled** コマンドを使用します。

このコマンドは、ダウンストリームインターフェイスに対してのみ設定できます。ダウンストリーム インターフェイスが MLD プロキシ ツリーから削除されると、設定も削除されます。

例

次の例では、ダウンストリーム インターフェイス vlan 100 からの転送を禁止します。

```
switchxxxxxx(config)# interface vlan100
switchxxxxxx(config-if)# ipv6 mld-proxy downstream protected interface enabled
switchxxxxxx(config-if)# exit
```

show ipv6 mld-proxy interface

MLDプロキシに設定されたインターフェイスに関する情報を表示するには、ユーザEXECモードまたは特権 EXEC モードで **show ipv6 mld-proxy interface** コマンドを使用します。

構文

show ipv6 mld-proxy interface [*interface-id*]

パラメータ

- ***interface-id***：（オプション）インターフェイスに関するMLDプロキシ情報を表示します。

コマンド モード

ユーザ EXEC モード

特権 EXEC モード

使用上のガイドライン

MLD プロキシが有効になっているすべてのインターフェイスを表示する、または特定のインターフェイスの MLD プロキシ設定を表示するには、**show ipv6 mld-proxy interface** コマンドを使用します。

例 1。次の例では、MLD プロキシが有効になっているすべてのインターフェイスの MLD プロキシ ステータスを表示します。

```
switchxxxxxx# show ip mld-proxy interface
```

* - the switch is the Querier on the interface

```
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
Global Downdtream interfaces protection is disabled
SSM Access List Name: list1
Interface  Type         Dicarding IPv6 Multicast
 vlan 100  upstream
*vlan 102  downstream   enabled
*vlan 110  downstream   default
 vlan 113  downstream   disabled
```

例 2。次に、指定したアップストリーム インターフェイスに対する **show ipv6 mld-proxy interface** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 mld-proxy interface vlan 100
```

* - the switch is the Querier on the interface

```
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
Global Downdtream interfaces protection is disabled
SSM Access List Name:
```

```
vlan 100 is a Upstream interface
Downstream interfaces:
 *vlan 102, *vlan 110, vlan 113
```

例 3。次に、指定したダウンストリームインターフェイスに対する **show ipv6 mld-proxy interface** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 mld-proxy interface vlan 102
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
Global Downdtream interfaces protection is disabled
SSM Access List Name: default
vlan 102 is a Downstream interface
The switch is the Querier on vlan 102
Upstream interface: vlan 100
```

例 4。次に、IGMP プロキシが無効になっているインターフェイスに対する **show ipv6 mld-proxy interface** コマンドの出力例を示します。

```
switchxxxxxx# show ipv6 mld-proxy interface vlan 1
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is disabled
```

MLD スヌーピング コマンド

この章は、次の項で構成されています。

- ipv6 mld snooping（グローバル） （982 ページ）
- ipv6 mld snooping vlan （983 ページ）
- ipv6 mld snooping querier （984 ページ）
- ipv6 mld snooping vlan querier （985 ページ）
- ipv6 mld snooping vlan querier election （986 ページ）
- ipv6 mld snooping vlan querier version （987 ページ）
- ipv6 mld snooping vlan mrouter （988 ページ）
- ipv6 mld snooping vlan mrouter interface （989 ページ）
- ipv6 mld snooping vlan forbidden mrouter （990 ページ）
- ipv6 mld snooping vlan static （991 ページ）
- ipv6 mld snooping vlan immediate-leave （992 ページ）
- show ipv6 mld snooping groups （993 ページ）
- show ipv6 mld snooping interface （995 ページ）
- show ipv6 mld snooping mrouter （996 ページ）

ipv6 mld snooping（グローバル）

IPv6 マルチキャスト リスナー検出（MLD）スヌーピングを有効にするには、**ipv6 mld snooping** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 mld snooping

no ipv6 mld snooping

デフォルト設定

IPv6 MLD スヌーピングは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、IPv6 MLD スヌーピングを有効にします。

```
switchxxxxxx(config)# ipv6 mld snooping
```

ipv6 mld snooping vlan

特定の VLAN で MLD スヌーピングを有効にするには、**ipv6 mld snooping vlan** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 mld snooping vlan *vlan-id*

no ipv6 mld snooping vlan *vlan-id*

パラメータ

- ***vlan-id***：VLAN を指定します。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

MLD スヌーピングは、スタティック VLAN のみで有効にできます。

MLDv1 および MLDv2 はサポートされています。

例

```
switchxxxxxx(config)# ipv6 mld snooping vlan 2
```

ipv6 mld snooping querier

MLD スヌーピング クエリアをグローバルに有効にするには、**ipv6 mld snooping querier** コマンドをグローバル コンフィギュレーション モードで使用します。MLD スヌーピング クエリアをグローバルに無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld snooping querier

no ipv6 mld snooping querier

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

VLAN で MLD スヌーピング クエリアを実行するには、VLAN 上でグローバルに有効にします。

例

次の例では、MLD スヌーピング クエリアをグローバルに無効にしています。

```
switchxxxxxx(config)# no ipv6 mld snooping querier
```

ipv6 mld snooping vlan querier

特定の VLAN 上でインターネット MLD スヌーピング クエリアを有効にするには、**ipv6 mld snooping vlan querier** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 mld snooping vlan *vlan-id* **querier**

no ipv6 mld snooping vlan *vlan-id* **querier**

パラメータ

- ***vlan-id***：VLAN を指定します。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

MLD スヌーピング クエリアは、その VLAN に MLD スヌーピングが有効になっている場合にのみ、VLAN 上で有効にできます。

例

次の例では、VLAN 1 上で MLD スヌーピング クエリアを有効にしています。

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 querier
```

ipv6 mld snooping vlan querier election

特定の VLAN 上で MLD スヌーピング クエリアの MLD クエリア選択メカニズムを有効にするには、**ipv6 mld snooping vlan querier election** コマンドをグローバル コンフィギュレーション モードで使用します。クエリア選択メカニズムを無効にするには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld snooping vlan *vlan-id* **querier election**

no ipv6 mld snooping vlan *vlan-id* **querier election**

パラメータ

- ***vlan-id***：VLAN を指定します。

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ipv6 mld snooping vlan querier election コマンドの **no** 形式を使用すると、VLAN で MLD クエリア選択メカニズムを無効にできます。

MLD クエリア選定メカニズムが有効の場合、MLD スヌーピング クエリアは RFC2710 と RFC3810 で指定された標準的な MLD クエリア選定メカニズムをサポートします。

MLD クエリア選定メカニズムが無効の場合、MLD スヌーピング クエリアは有効になってから 60 秒間、一般的なクエリー メッセージの送信を遅らせます。このときにスイッチが別クエリアから IGMP クエリーを受信しなかった場合は、一般的なクエリー メッセージの送信を開始します。スイッチがクエリアとして動作する場合、VLAN で別のクエリアが検出されると、一般的なクエリー メッセージの送信を停止します。この場合、スイッチが次の式に等しいクエリー パッシブ間隔で別のクエリアを受信すると、一般的なクエリー メッセージの送信を再開します

<堅牢性>*<クエリー間隔> + 0.5*<クエリー応答間隔>。

VLAN に IPMv6 マルチキャスト ルータがある場合は、MLD クエリア選定メカニズムを無効にすることをお勧めします。

例

次の例では、VLAN 1 で MLD スヌーピング クエリア選定を無効にしています。

```
switchxxxxxx(config)# no ipv6 mld snooping vlan 1 querier election
```

ipv6 mld snooping vlan querier version

特定の VLAN で IGMP クエリアの IGMP バージョンを設定するには、**ipv6 mld snooping vlan querier version** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 mld snooping vlan *vlan-id* **querier version** {**1** | **2**}

no ipv6 mld snooping vlan *vlan-id* **querier version**

パラメータ

- ***vlan-id***：VLAN を指定します。
- **querier version** {**1** | **2**}：MLD のバージョンを指定します。

デフォルト設定

MLDv1。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、MLD スヌーピング クエリア VLAN 1 のバージョンを 2 に設定します。

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 querier version 2
```

ipv6 mld snooping vlan mrouter

マルチキャスト ルータ ポートの自動学習を有効にするには、**ipv6 mld snooping vlan mrouter** コマンドをグローバル コンフィギュレーション モードで使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

構文

ipv6 mld snooping vlan *vlan-id* **mrouter learn pim-dvmrp**

no ipv6 mld snooping vlan *vlan-id* **mrouter learn pim-dvmrp**

パラメータ

- ***vlan-id***：VLAN を指定します。
- **pim-dvmrp**：PIM, DVMRP および MLD メッセージでマルチキャスト ルータ ポートを学習します。

デフォルト設定

pim-dvmrp の学習が有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

VLAN を作成する前に、このコマンドを実行できます。

例

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter learn pim-dvmrp
```

ipv6 mld snooping vlan mrouter interface

マルチキャスト ルータ ポートに接続されたポートを定義するには、**ipv6 mld snooping mrouter interface** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 mld snooping vlan *vlan-id* **mrouter interface** *interface-list*

no ipv6 mld snooping vlan *vlan-id* **mrouter interface** *interface-list*

パラメータ

- ***vlan-id***：VLAN を指定します。
- ***interface-list***：インターフェイスのリストを指定します。インターフェイスは、ポートまたはポートチャネルのいずれかのタイプから指定できます。

デフォルト設定

ポートは定義されません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

マルチキャスト ルータ ポートとして定義されているポートは、すべての MLD パケット（レポートとクエリー）とすべてのマルチキャスト データを受信します。

VLAN の作成前に、例で示すようにポートの範囲として実行することができます。

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 mld snooping vlan 1 mrouter interface gi1/0/1-4
```

ipv6 mld snooping vlan forbidden mrouter

スタティック設定または自動学習でポートがマルチキャスト ルータ ポートとして定義されないようにするには、**ipv6 mld snooping vlan forbidden mrouter** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 mld snooping *vlan vlan-id* **forbidden mrouter** *interface interface-list*

no ipv6 mld snooping *vlan vlan-id* **forbidden mrouter** *interface interface-list*

パラメータ

- ***vlan-id***：VLAN を指定します。
- ***interface-list***：インターフェイスのリストを指定します。インターフェイスには、イーサネット ポートまたはポートチャネルのいずれかを指定できます。

デフォルト設定

デフォルトでは禁止ポートがありません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

マルチキャスト ルータ ポート（mrouter ポート）としての定義が禁止されているポートは、動的に学習したり、静的に割り当てたりすることはできません。

VLAN を作成する前に、このコマンドを実行できます。

例

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forbidden mrouter interface gi1/0/1
```

ipv6 mld snooping vlan static

ブリッジ テーブルに IPv6 層マルチキャスト アドレスを登録して、グループにポートを静的に追加するには、**ipv6 mld snooping vlan static** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 mld snooping vlan *vlan-id* **static** *ipv6-address* [**interface** *interface-list*]

no ipv6 mld snooping vlan *vlan-id* **static** *ipv6-address* [**interface** *interface-list*]

パラメータ

- ***vlan-id***：VLAN を指定します。
- ***ipv6-address***：IP マルチキャスト アドレスを指定します。
- **interface** *interface-list*：（オプション）インターフェイスのリストを指定します。インターフェイスの種類は、イーサネット ポートまたはポートチャネルのいずれかにできます。

デフォルト設定

マルチキャスト アドレスは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

スタティック マルチキャスト アドレスは、スタティック VLAN 上でのみ定義できます。

VLAN を作成する前に、このコマンドを実行できます。

インターフェイスを指定せずにエントリを登録できます。

ポートリストを指定せずに **no** コマンドを使用すると、エントリが削除されます。

例

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 static FF12::3 gi1/0/1
```

ipv6 mld snooping vlan immediate-leave

VLAN で MLD スヌーピング即時脱退処理を有効にするには、**ipv6 mld snooping vlan immediate-leave** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

ipv6 mld snooping vlan *vlan-id* **immediate-leave**

no ipv6 mld snooping vlan *vlan-id* **immediate-leave**

パラメータ

vlan-id：VLAN ID 値を指定します。（範囲：1 ～ 4094）

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

MLD 脱退グループ メッセージをホストから受信すると、システムはテーブル エントリからホスト ポートを削除します。マルチキャスト ルータからの IGMP クエリーを中継後は、マルチキャスト クライアントから MLD メンバーシップ レポートを受信しない限り、定期的にエントリを削除します。

MLD スヌーピング即時脱退処理では、スイッチは脱退メッセージを送信したインターフェイスに対して MAC ベースの一般クエリーを送信せずに、転送テーブルからそのインターフェイスを削除できます。

VLAN を作成する前に、このコマンドを実行できます。

例

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 immediate-leave
```

show ipv6 mld snooping groups

MLD スヌーピングで学習したマルチキャスト グループを表示するには、**show ipv6 mld snooping groups** EXEC モード コマンドをユーザ EXEC モードで使用します。

構文

show ipv6 mld snooping groups [**vlan** *vlan-id*] [**address** *ipv6-multicast-address*] [**source** *ipv6-address*]

パラメータ

- **vlan** *vlan-id*：（オプション）VLAN ID を指定します。
- **address** *ipv6-multicast-address*：（オプション）IPv6 マルチキャストアドレスを指定します。
- **source** *ipv6-address*：（オプション）IPv6 送信元アドレスを指定します。

コマンド モード

ユーザ EXEC モード

デフォルト設定

定義したすべての VLAN とアドレスの情報を表示します。

使用上のガイドライン

Include リストには、スヌーピング データベースに応じてこのグループでフォワーディング ステートにあるポートが含まれます。一般に、Exclude リストには、マルチキャスト グループでその特定の送信元に対して明示的な除外を発行したポートが含まれます。

Reporters That Are Forbidden Statically リストには、マルチキャスト フローを受信するよう求められたけども、マルチキャストブリッジのそのマルチキャストグループで禁止されているポートのリストが含まれます。

注：特定の状況では、Exclude リストに正確な情報が含まれない場合があります。たとえば、2 つの Exclude レポートを同じグループの同じポートで受信したけども、送信元が異なる場合、このポートは、Exclude リストではなく、Include リストに含まれます

例

次に、show ipv6 mld snooping groups の出力例を示します。

```
switchxxxxxx# show ipv6 mld snooping groups
```

VLAN	Group Address	Source Address	Include Ports	Exclude Ports	Compatibility Mode
1	FF12::3	FE80::201:C9FF:FE40:8001	gi1/0/1	gi1/0/2	1
1	FF12::3	FE80::201:C9FF:FE40:8002	gi1/0/2	gi1/0/3	1
19	FF12::8	FE80::201:C9FF:FE40:8003	gi1/0/4		2
19	FF12::8	FE80::201:C9FF:FE40:8004	gi1/0/1		2
19	FF12::8	FE80::201:C9FF:FE40:8005	gi1/0/10-11		2

MLD Reporters that are forbidden statically:

VLAN	Group Address	Source Address	Ports
1	FF12::3	FE80::201:C9FF:FE40:8001	gi1/0/3
19	FF12::8	FE80::201:C9FF:FE40:8001	gi1/0/4

show ipv6 mld snooping interface

特定の VLAN で IPv6 MLD スヌーピング設定を表示するには、**show ipv6 mld snooping interface** EXEC モード コマンドをユーザ EXEC モードで使用します。

構文

show ipv6 mld snooping interface *vlan-id*

パラメータ

- ***vlan-id***：VLAN ID を指定します。

デフォルト設定

すべての VLAN の情報を表示します。

コマンド モード

ユーザ EXEC モード

例

次の例では、VLAN 1000 上の MLD スヌーピング設定を示します。

```
switchxxxxxx# show ipv6 mld snooping interface 1000
MLD Snooping is globally enabled
MLD Snooping Querier is globally enabled
VLAN 1000
  MLD Snooping is enabled
  MLD snooping last immediate leave: enable
  Automatic learning of multicast router ports is enabled
  MLD Snooping Querier is enabled
  MLD Snooping Querier operation state: is running
  MLD Snooping Querier version: 2
  MLD Snooping Querier election is enabled
  MLD snooping robustness: admin 2  oper 2
  MLD snooping query interval: admin 125 sec oper 125 sec
  MLD snooping query maximum response: admin 10 sec oper 10 sec
  MLD snooping last member query counter: admin 2 oper 2
  MLD snooping last member query interval: admin 1000 msec oper 500 msec
  Groups that are in MLD version 1 compatibility mode:
    FF12::3, FF12::8
```

show ipv6 mld snooping mrouter

すべての VLAN または特定の VLAN で動的に学習したマルチキャスト ルータ インターフェイスの情報を表示するには、**show ipv6 mld snooping mrouter** EXEC モード コマンドをユーザ EXEC モードで使用します。

構文

show ipv6 mld snooping mrouter [**interface** *vlan-id*]

パラメータ

- **interface** *vlan-id*：（オプション）VLAN ID を指定します。

デフォルト設定

すべての VLAN の情報を表示します。

コマンド モード

ユーザ EXEC モード

例

次の例では、VLAN 1000 で動的に学習したマルチキャスト ルータ インターフェイスの情報を表示します。

```
switchxxxxxx# show ipv6 mld snooping mrouter interface 1000
```

VLAN	Dynamic	Static	Forbidden
----	---------	---------	----------
1000	gi1/0/1	gi1/0/2	gi1/0/3 ～ 4

SNMP コマンド

この章は、次の項で構成されています。

- snmp-server community （998 ページ）
- snmp-server community-group （1000 ページ）
- snmp-server server （1002 ページ）
- snmp-server source-interface （1003 ページ）
- snmp-server source-interface-ipv6 （1005 ページ）
- snmp-server view （1007 ページ）
- snmp-server group （1009 ページ）
- show snmp views （1011 ページ）
- show snmp groups （1012 ページ）
- snmp-server user （1014 ページ）
- show snmp users （1016 ページ）
- snmp-server filter （1018 ページ）
- show snmp filters （1019 ページ）
- snmp-server host （1020 ページ）
- snmp-server engineID local （1022 ページ）
- snmp-server engineID remote （1024 ページ）
- show snmp engineID （1025 ページ）
- snmp-server enable traps （1026 ページ）
- snmp-server trap authentication （1027 ページ）
- snmp-server contact （1028 ページ）
- snmp-server location （1029 ページ）
- snmp-server set （1030 ページ）
- snmp trap link-status （1031 ページ）
- show snmp （1032 ページ）

snmp-server community

SNMP コマンド（v1 および v2）へのアクセスを許可するコミュニティ アクセス ストリング（パスワード）を設定するには、**snmp-server community** グローバル コンフィギュレーション モード コマンドを使用します。これは、GET や SET などの SNMP コマンドに使用されます。

このコマンドは、SNMP v1 および v2 の両方を設定します。

指定したコミュニティ ストリングを削除するには、このコマンドの **no** 形式を使用します。

構文

snmp-server community *community-string [***ro** | **rw** | **su***]* [*ip-address* | *ipv6-address*] *[***mask** *mask* | **prefix** *prefix-length] [***view** *view-name]* [**type** {**router** | **oob**}]

no snmp-server community *community-string [ip-address]* [**type** {**router** | **oob**}]

パラメータ

- **community-string**：SNMP プロトコルへのアクセスを許可するパスワードを定義します。（範囲：1 ～ 20 文字）。
- **ro**：（オプション）読み取り専用アクセスを指定します（デフォルト）。
- **rw**：（オプション）読み取りと書き込みアクセスを指定します。
- **su**：（オプション）SNMP 管理者アクセス権を指定します。
- **ip-address**：（オプション）管理ステーション IP アドレス。デフォルトは、すべての IP アドレスです。IPv4、IPv6 または IPv6z アドレスを使用できます。
- **mask**：（オプション）IPv4 アドレスのマスクを指定します。これはネットワーク マスクではありませんが、設定されている IP アドレスと比較するパケットの発信元アドレスのビットを定義するマスクです。指定しない場合、デフォルトで 255.255.255.255 に設定されます。IPv4 アドレスなしでマスクを指定した場合、コマンドはエラーを返します。
- **prefix-length**：（オプション）IPv4 アドレス プレフィックスを構成するビット数を指定します。指定しない場合、デフォルトで 32 になります。IPv4 アドレスなしでプレフィックス長を指定した場合、コマンドはエラーを返します。
- **view** *view-name*：（オプション）snmp-server view （1007 ページ） コマンドを使用して設定されたビューの名前を指定します（コマンド設定において特定の順序をユーザが意識する必要はありません）。ビューには、コミュニティで使用できるオブジェクトが定義されています。これは **su** には該当しません。MIB 全体にアクセスできるからです。指定しないと、コミュニティ テーブル、SNMPv3 ユーザ テーブル、アクセス テーブルを除き、すべてのオブジェクトを使用できます。（範囲：1 ～ 30 文字）
- **type** *router*：（オプション）IP アドレスがアウトオブバンド ネットワーク上にあるかインバンド ネットワーク上にあるかを示します。

デフォルト設定

コミュニティは定義されていません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

コマンドの論理キーはペア（community, ip-address）です。ip-address を省略した場合、キーは（community, All-IPs）です。つまり、2 つのコマンドに同じ community, ip-address ペアを指定することはできません。

view-name は、コミュニティ ストリングのアクセス権を制限するために使用します。view-name を指定すると、ソフトウェアは次のことを行います。

- 内部セキュリティ名を生成します。
- SNMPv1 および SNMPv2 セキュリティ モデルの内部セキュリティ名を内部グループ名にマップします。
- SNMPv1 および SNMPv2 セキュリティ モデルの内部グループ名を view-name にマップします（読み取りビューと通知ビューには常にマップし、rw を指定している場合は書き込みビューにもマップします）。

例

IP アドレス 1.1.1.121 およびマスク 255.0.0.0 にある管理ステーションへの管理者アクセス権のパスワードを定義します。

```
switchxxxxxx(config)# snmp-server community abcd su 1.1.1.121 mask 255.0.0.0
```

snmp-server community-group

ユーザ グループにアクセス権を設定するには、**snmp-server community-group** を使用します。アクセス権を指定するためには、グループが存在している必要があります。このコマンドは、SNMP v1 および v2 の両方を設定します。

構文

snmp-server community-group *community-string group-name [ip-address | ipv6-address]* **[mask** *mask* | **prefix** *prefix-length]* [**type** {**router** | **oob**}]

パラメータ

- **community-string**：SNMP プロトコルへのアクセスを許可するパスワードを定義します。（範囲：1 ～ 20 文字）。
- **group-name**：これは、snmp-server group （1009 ページ） に v1 または v2 を指定して設定したグループの名前です（2 つのコマンド設定において特定の順序をユーザが意識する必要はありません）。グループには、コミュニティで使用できるオブジェクトが定義されています。（範囲：1 ～ 30 文字）
- **ip-address**：（オプション）管理ステーション IP アドレス。デフォルトは、すべての IP アドレスです。IPv4、IPv6 または IPv6z アドレスを使用できます。
- **mask**：（オプション）IPv4 アドレスのマスクを指定します。これはネットワーク マスクではありませんが、設定されている IP アドレスと比較するパケットの発信元アドレスのビットを定義するマスクです。指定しない場合、デフォルトで 255.255.255.255 に設定されます。IPv4 アドレスなしでマスクを指定した場合、コマンドはエラーを返します。
- **prefix-length**：（オプション）IPv4 アドレス プレフィックスを構成するビット数を指定します。指定しない場合、デフォルトで 32 になります。IPv4 アドレスなしでプレフィックス長を指定した場合、コマンドはエラーを返します。
- **type** *router*：（オプション）IP アドレスがアウトオブバンド ネットワーク上にあるかインバンド ネットワーク上にあるかを示します。

デフォルト設定

コミュニティは定義されていません

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

group-name は、コミュニティ ストリングのアクセス権を制限するために使用します。group-name を指定すると、ソフトウェアは次のことを行います。

- 内部セキュリティ名を生成します。
- SNMPv1 および SNMPv2 セキュリティ モデルの内部セキュリティ名をグループ名にマップします。

例

グループ *abcd* に対してパスワード *tom* を定義して、このグループがプレフィックス 8 の管理ステーション 1.1.1.121 にアクセスできるようにします。

```
switchxxxxxx(config)# snmp-server community-group tom abcd 1.1.1.122 prefix 8
```

snmp-server server

SNMP プロトコルでデバイスを設定できるようにするには、**snmp-server server** グローバル コンフィギュレーション モード コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

snmp-server server

no snmp-server server

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# snmp-server server
```

snmp-server source-interface

簡易ネットワーク管理プロトコル（SNMP）トラップがインフォームやトラップの送信元とするインターフェイスを指定するには、グローバル コンフィギュレーション モードで **snmp-server source-interface** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

snmp-server source-interface {**traps** | **informs**} *interface-id*

no snmp-server source-interface [**traps** | **informs**]

パラメータ

- **traps**：SNMP トラップ インターフェイスを指定します。
- **informs**：SNMP インフォームを指定します。
- **interface-id**：送信元インターフェイスを指定します。

デフォルト設定

送信元 IPv4 アドレスは、発信インターフェイスで定義され、ネクスト ホップ IPv4 サブネットに属する IPv4 アドレスです。

no snmp-server source-interface でパラメータが指定されていない場合、デフォルトは両方 traps、および informs です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスの場合は、ネクスト ホップ IPv4 サブネットに属するインターフェイス IP アドレスが適用されます。

送信元インターフェイスが発信インターフェイスでない場合は、送信元インターフェイスで定義された最小 IPv4 アドレスが適用されます。

使用できる IPv4 送信元アドレスがない場合は、SNMP トラップまたは SNMP インフォームを送信しようとすると、Syslog メッセージが発行されます。

SNMP トラップの送信元インターフェイスを削除するには、**no snmp-server source-interface traps** コマンドを使用します。

SNMP インフォームの送信元インターフェイスを削除するには、**no snmp-server source-interface informs** コマンドを使用します。

SNMP トラップおよび SNMP インフォームの送信元インターフェイスを削除するには、**no snmp-server source-interface** コマンドを使用します。

例

次に、VLAN 10 をトラップの送信元インターフェイスとして設定する例を示します。

```
switchxxxxxx(config)# snmp-server source-interface traps vlan 100
```

snmp-server source-interface-ipv6

簡易ネットワーク管理プロトコル（SNMP）トラップがインフォームやトラップの送信元とするインターフェイスを指定するには、グローバル コンフィギュレーション モードで **snmp-server source-interface** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

snmp-server source-interface-ipv6 {**traps** | **informs**} *interface-id*

no snmp-server source-interface-ipv6 [**traps** | **informs**]

パラメータ

- **traps**：SNMP トラップ インターフェイスを指定します。
- **informs**：SNMP トラップ インフォームを指定します。
- **interface-id**：送信元インターフェイスを指定します。

デフォルト設定

IPv6 送信元アドレスは、発信インターフェイスの IPv6 アドレスであり、RFC6724 に従って選択されます。

no snmp-server source-interface でパラメータが指定されていない場合、デフォルトは両方 traps、および informs です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスである場合は、インターフェイスで定義され、RFC 6724 に従って選択された IPv6 アドレスです。

送信元インターフェイスが発信インターフェイスでない場合は、送信元インターフェイス上で宛先 IPv6 アドレスの範囲で定義された最小 IPv6 アドレスが適用されます。

使用できる IPv6 送信元アドレスがない場合は、SNMP トラップまたは SNMP インフォームを送信しようとすると、Syslog メッセージが発行されます。

SNMP トラップの送信元 IPv6 インターフェイスを削除するには、**no snmp-server source-interface-ipv6 traps** コマンドを使用します。

SNMP インフォームの送信元 IPv6 インターフェイスを削除するには、**no snmp-server source-interface-ipv6 informs** コマンドを使用します。

SNMP トラップおよび SNMP インフォームの送信元 IPv6 インターフェイスを削除するには、**no snmp-server source-interface-ipv6** コマンドを使用します。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# snmp-server source-interface-ipv6 traps vlan 100
```

snmp-server view

SNMP ビューを作成または更新するには、**snmp-server view** グローバル コンフィギュレーション モード コマンドを使用します。SNMP ビューを削除するには、このコマンドの **no** 形式を使用します。

構文

snmp-server view *view-name oid-tree {***included** | **excluded***}*

no snmp-server view *view-name* [*oid-tree*]

パラメータ

- **view-name**：作成または更新しているビューの名前を指定します。（長さ：1 ～ 30 文字）
- **included**：ビュー タイプが含まれることを指定します。
- **excluded**：ビュー タイプが除外されることを指定します。
- **oid-tree**：（オプション）ビューに含める、またはビューから除外する ASN.1 サブツリー オブジェクト識別子を指定します。サブツリーを識別するには、数字（1.3.6.2.4 など）や単語（Systemなど）や一連の番号（任意）で構成されるテキスト文字列を指定します。サブツリー ファミリを指定するには、サブ ID の 1 文字をアスタリスク（*）ワイルドカードに変えます。たとえば、1.3.*.4 です。このパラメータは、指定している MIB によって異なります。

デフォルト設定

次のビューがデフォルトで作成されます。

- **Default**：SNMP パラメータ自体を設定するものを除きすべての MIB を含みます。
- **DefaultSuper**：すべての MIB を含みます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、同じビューに対して複数回入力できます。

コマンドの論理キーはペア（view-name, oid-tree）です。このため、2 つのコマンドに同じ view-name と oid-tree を指定することはできません。

ビューの数は 64 に制限されています。

Default ビューおよびDefaultSuper ビューは、内部ソフトウェア用に予約されており、削除も変更もできません。

例

次の例では、sysServices（システム 7）を除くすべてのオブジェクトが MIB-II システム グループに含まれ、インターフェイス 1 のすべてのオブジェクトが MIB-II インターフェイス グループに含まれているビューを作成しています（この形式は、ifEntryに指定されているパラメータで指定します）。

```
switchxxxxxx(config)# snmp-server view user-view system included
switchxxxxxx(config)# snmp-server view user-view system.7 excluded
switchxxxxxx(config)# snmp-server view user-view ifEntry.*.1 included
```

snmp-server group

SNMP グループを設定するには、**snmp-server group** グローバル コンフィギュレーション モード コマンドを使用します。グループは、SNMP ユーザを SNMP ビューにマップするために使用します。SNMP 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。

構文

snmp-server group *groupname* {***v1*** | **v2** | **v3** {**noauth** | **auth** | **priv**} [**notify** *notifyview*]} [**read** *readview*] [**write** *writeview*]

no snmp-server group *groupname* {**v1** | **v2** | **v3** [**noauth** | **auth** | **priv**]}

パラメータ

- **group** *groupname*：グループ名を指定します。（長さ：1 ～ 30 文字）
- **v1**：SNMP バージョン 1 のセキュリティ モデルを指定します。
- **v2**：SNMP バージョン 2 のセキュリティ モデルを指定します。
- **v3**：SNMP バージョン 3 のセキュリティ モデルを指定します。
- **noauth**：パケット認証が実行されないことを指定します。SNMP バージョン 3 のセキュリティ モデルにのみ適用されます。
- **auth**：パケット認証が暗号化なしで実行されることを指定します。SNMP バージョン 3 のセキュリティ モデルにのみ適用されます。
- **priv**：パケット認証が暗号化ありで実行されることを指定します。SNMP バージョン 3 のセキュリティ モデルにのみ適用されます。認証とプライバシーの両方による SNMPv3 ユーザの作成は、GUI で行う必要があることに注意してください。他のすべてのユーザは、CLI で作成できます。
- **notify** *notifyview*：（オプション）インフォームまたはトラップを生成できるビュー名を指定します。inform は確認が必要なトラップです。SNMP バージョン 3 のセキュリティ モデルにのみ適用されます。（長さ：1 ～ 32 文字）
- **read** *readview*：（オプション）表示のみできるビュー名を指定します。（長さ：1 ～ 32 文字）
- **write** *writeview*：（オプション）エージェントを設定できるビュー名を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

グループ エントリは存在しません。

notifyview を指定しないと、通知ビューは定義されません。

readview を指定しないと、コミュニティ テーブル、SNMPv3 ユーザ テーブル、アクセス テーブルを除き、すべてのオブジェクトを取得できます。

writeview を指定しないと、書き込みビューは定義されません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドに定義されているグループは、ユーザをグループにマップするために snmp-server user （1014 ページ） コマンドで使用します。これらのユーザは、このコマンドに定義されているビューに自動的にマップされます。

コマンドの論理キーは（**groupname, snmp-version, security-level**）です。snmp-version v1/v2 の場合、security-level は常に **noauth** です。

例

次の例では、*user-group* というグループを SNMPv3 にアタッチし、暗号化されたセキュリティ レベルをグループに割り当て、*user-view* というビューのアクセス権を読み取り専用に制限しています。次に、*user-group* にユーザ *tom* を割り当てています。そのため、ユーザ *tom* には *user-view* で権利が割り当てられます。

```
switchxxxxxx(config)# snmp-server group user-group v3 priv read user-view
switchxxxxxx(config)# snmp-server user tom user-group v3
```

show snmp views

SNMP ビューを表示するには、**show snmp views** 特権 EXEC モード コマンドを使用します。

構文

show snmp views [*viewname*]

パラメータ

viewname：（オプション）ビュー名を指定します。（長さ：1 ～ 30 文字）

デフォルト設定

viewname を指定しないと、すべてのビューが表示されます。

コマンド モード

特権 EXEC モード

例

次に、設定した SNMP ビューを表示する例を示します。

```
switchxxxxxx# show snmp views

Name                OID Tree                Type
----------------    ----------------------  ----------
Default             iso                     Included
Default             snmpNotificationMIB     Excluded
DefaultSuper        iso                     Included
```

show snmp groups

設定した SNMP グループを表示するには、**show snmp groups** 特権 EXEC モード コマンドを使用します。

構文

show snmp groups [*groupname*]

パラメータ

groupname：（オプション）グループ名を指定します。（長さ：1 ～ 30 文字）

デフォルト設定

すべてのグループを表示します。

コマンド モード

特権 EXEC モード

例

次に、設定した SNMP グループを表示する例を示します。

switchxxxxxx# **show snmp groups**							
Name		Security				Views	
------------- user-group managers-group	Model ----- V2 V2		Level ---- no_auth no_auth		Read ------- Default Default	Write ------- "" Default	Notify ------- "" ""

次の表では、上記の重要なフィールドについて説明します。

フィールド		説明
名前（Name）		**グループ名。**
Security	Model	使用中の SNMP モデル（v1、v2 または v3）。
Security	Level	パケット セキュリティ。SNMP v3 セキュリティにのみ適用できます。 .

フィールド		説明
Views	Read	エージェントの内容を表示できるビュー名。指定しないと、コミュニティ テーブル、SNMPv3 ユーザ テーブル、アクセス テーブルを除き、すべてのオブジェクトを使用できます。
	Write	データを入力し、エージェントの内容を管理できるビュー名。
	Notify	インフォームまたはトラップを指定できるビュー名。

snmp-server user

新しい SNMP ユーザを設定するには、**snmp-server user** グローバル コンフィギュレーション モード コマンドを使用します。ユーザを削除するには、このコマンドの **no** 形式を使用します。認証およびプライバシー パスワードを暗号化形式（SSD を参照）で入力するには、このコマンドの**暗号化**形式を使用します。

構文

snmp-server user *username groupname* {**v1** | **v2c** | [**remote** *host*] **v3**[**auth** { **sha** | **sha224**| **sha256**| **sha384**| **sha512**} *auth-password* [***priv*** *priv-password*]]}

encrypted snmp-server user *username groupname* {**v1** | **v2c** | [**remote** *host]* **v3**[**auth** { **sha** | **sha224**| **sha256**| **sha384**| **sha512**} *encrypted-auth-password* [**priv** *encrypted-priv-password*]]}

no snmp-server user *username* {**v1** | **v2c** | [**remote** *host*] ***v3***}

パラメータ

- **username**：エージェントに接続するホストのユーザ名を定義します。（範囲：最大 20 文字）。
- **groupname**：ユーザが属すグループの名前。グループは、snmp-server group （1009 ページ）コマンドに v1 または v2c パラメータを指定して設定する必要があります（2 つのコマンド設定において特定の順序をユーザが意識する必要はありません）。（範囲：最大 30 文字）
- **v1**：ユーザが v1 ユーザであることを指定します。
- **v2c**：ユーザが v2c ユーザであることを指定します。
- **v3**：ユーザが v3 ユーザであることを指定します。
- **remote** *host*：（オプション）リモート SNMP ホストの IP アドレス（IPv4、IPv6 または IPv6z）またはホスト名。
- **auth**：（オプション）どの認証レベルを使用するかを指定します。

  Sha：（オプション）HMAC-SHA-96 認証レベルを指定します。

  Sha224：（オプション）HMAC-SHA-224-128 認証レベルを指定します。

  Sha256：（オプション）HMAC-SHA-256-192 認証レベルを指定します。

  Sha384：（オプション）HMAC-SHA-384-256 認証レベルを指定します。

  Sha512：（オプション）HMAC-SHA-512-384 認証レベルを指定します。
- ***auth-password***：（オプション）認証パスワードを指定します。範囲：32 文字以内。
- ***encrypted-auth-password***：（オプション）認証パスワードを暗号化形式で指定します。
- **priv** *priv-password*：（オプション）プライベート（priv）暗号化とプライバシーパスワードを指定します（範囲：最大 32 文字）。使用する暗号化アルゴリズムは、128 ビットの暗

号キーを使用する暗号フィードバックモード（CFB：Cipher Feedback Mode）の高度暗号化規格（AES）アルゴリズムです。

- ***encrypted-priv-password***：（オプション）プライバシー パスワードを暗号化形式で指定します。

デフォルト設定

グループ エントリは存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

SNMP v1 および v2 に対して、このコマンドは snmp-server community-group と同じ操作を実行します。ただし、snmp-server community-group は v1 と v2 の両方を同時に設定する点が異なります。このコマンドでは、v1 と v2 に対して 1 回ずつ実行する必要があります。

デバイスに SNMPv3 ユーザを追加するには、ローカル SNMP エンジン ID を定義する必要があります。リモートホストユーザの場合、リモート SNMP エンジン ID も必要です。

snmpEngineID の値を変更または削除すると、SNMPv3 ユーザのデータベースが削除されます。

このコマンドの論理キーは username です。

インフォームは確認応答を必要とするトラップです。そのため、リモートホストにインフォームを送信するには、そのリモートホストを設定する必要があります。設定したリモートホストは（インフォームの取得以外に）デバイスを管理することもできます。

リモート ユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応する IP アドレスを指定します。また、特定のエージェントにリモート ユーザを設定する前に、snmp-server engineID remote （1024 ページ） コマンドを使用して SNMP エンジン ID を設定します。リモート エージェントの SNMP エンジン ID は、パスワードから認証とプライバシー ダイジェストを計算する際に必要です。最初にリモート エンジン ID が設定されていない場合、コンフィギュレーション コマンドは失敗します。

異なるバージョンやアクセス レベル（noauth、auth または auth & priv）のたびに、同じグループを複数回定義できるため、ユーザを定義するときにグループ名を指定するだけでは不十分です。そうではなく、このユーザからのパケットを処理する方法を完全に決定するためには、グループ名、バージョンおよびアクセス レベルを指定する必要があります。

例

この例では、SNMP v1 および v2c を使用して、ユーザ *tom* をグループ *abcd* に割り当てています。. ユーザ *jerry* が SNMP v3 を使用してグループ *efgh* に割り当てられます。

```
switchxxxxxx(config)# snmp-server user tom acbd v1
switchxxxxxx(config)# snmp-server user tom acbd v2c
switchxxxxxx(config)# snmp-server user jerry efgh v3 auth sha pass1234
```

show snmp users

設定した SNMP ユーザを表示するには、**show snmp users** 特権 EXEC モード コマンドを使用します。

構文

show snmp users [*username*]

パラメータ

username：（オプション）ユーザ名を指定します。（長さ：1 ～ 30 文字）

デフォルト設定

すべてのユーザを表示します。

コマンド モード

特権 EXEC モード

例

次に、設定した SNMP ユーザを表示する例を示します。

```
switchxxxxxx# show snmp users
User name                          :u1rem
  Group name                       :group1
  Authentication Method      : None
  Privacy Method             : None
  Remote                           :11223344556677
  Auth Password                    :
  Priv Password                    :
User name                          : qqq
  Group name                       : www
  Authentication Method      : SHA256
  Privacy Method             : None
  Remote                           :
  Auth Password                    : helloworld1234567890987665
  Priv Password                    :
User name                          : hello
  Group name                       : world
  Authentication Method      :  SHA256
  Privacy Method             :  AES-128
  Remote                           :
  Auth Password (encrypted): Z/tC3UF5j0pYfmXm8xeMvcIOQ6LQ4GOACCGYLRdAgOE6XQKTC
                             qMlrnpWuHraRlZj
  Priv Password (encrypted) : kN1ZHzSLo6WWxlkuZVzhLOo1gI5waaNf7Vq6yLBpJdS4N68tL
                             1tbTRSz2H4c4Q4o
User name                          : u1noAuth
  Group name                       : group1
  Authentication Method            : None
  Privacy Method                   : None
  Remote                             :
  Auth Password (encrypted)        :
  Priv Password (encrypted)        :
```

```
User name                          : u1OnlyAuth
  Group name                       : group1
  Authentication Method      : SHA1
  Privacy Method               : None
  Remote                           :
  Auth Password (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
  Priv Password (encrypted) :
```

snmp-server filter

SNMP サーバ通知フィルタを作成または更新するには、**snmp-server filter** グローバル コンフィギュレーション モード コマンドを使用します。通知フィルタを削除するには、このコマンドの **no** 形式を使用します。

構文

snmp-server filter *filter-name oid-tree {***included** | **excluded***}*

no snmp-server filter *filter-name* [*oid-tree*]

パラメータ

- **filter-name**：更新または作成しているフィルタ レコードのラベルを指定します。名前は、他のコマンドでそのフィルタを参照するために使用します。（長さ：1 ～ 30 文字）
- **oid-tree**：ビューに含めるまたはビューから除外する ASN.1 サブツリーのオブジェクト識別子を指定します。サブツリーを識別するために、1.3.6.2.4 などの数字や system などの単語で構成されるテキスト文字列を指定します。サブツリー ファミリを指定するには、サブ ID の 1 文字をアスタリスク（*）ワイルドカードに変えます。たとえば、1.3.*.4 です。
- **included**：フィルタ タイプが含まれることを指定します。
- **excluded**：フィルタ タイプが除外されることを指定します。

デフォルト設定

ビュー エントリは存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、同じフィルタに対して複数回入力できます。オブジェクト識別子が複数の行に含まれている場合、後の行が優先されます。コマンドの論理キーはペア（filter-name, oid-tree）です。

例

次に、sysServices（System 7）と MIB-II インターフェイス グループ内のインターフェイス 1 のすべてのオブジェクトを除く、MIB-II システム グループのすべてのオブジェクトを含むフィルタを作成する例を示します（この形式は ifEntry で指定したパラメータによって異なります）。

```
switchxxxxxx(config)# snmp-server filter f1 system included
switchxxxxxx(config)# snmp-server filter f2 system.7 excluded
switchxxxxxx(config)# snmp-server filter f3 ifEntry.*.1 included
```

show snmp filters

定義した SNMP フィルタを表示するには、**show snmp filters** 特権 EXEC モード コマンドを使用します。

構文

show snmp filters [*filtername*]

パラメータ

filtername：フィルタ名を指定します。（長さ：1 ～ 30 文字）

デフォルト設定

フィルタ名を定義しないと、すべてのフィルタが表示されます。

コマンド モード

特権 EXEC モード

例

次に、設定した SNMP フィルタを表示する例を示します。

```
switchxxxxxx# show snmp filters user-filter

Name                 OID Tree                  Type
-------------        ----------------------    ---------
user-filter          1.3.6.1.2.1.1             Included
user-filter          1.3.6.1.2.1.1.7           Excluded
user-filter          1.3.6.1.2.1.2.2.1.*.1     Included
```

snmp-server host

SNMP 通知（トラップ/インフォーム）用にホストを設定するには、**snmp-server host** グローバル コンフィギュレーション モード コマンドを使用します。このコマンドの **no** 形式を使用すると、指定したホストを削除します。

構文

snmp-server host *{host-ip | hostname} [***traps** | **informs***] [***version** *{1 | 2c | 3 [***auth** | **noauth** | **priv***]}] community-string [***udp-port** *port] [***filter** *filtername] [***timeout** *seconds] [***retries** *retries]*

no snmp-server host *{ip-address | hostname} [***traps** | **informs***] [***version** *{***1** | **2c** | **3***}]*

パラメータ

- **host-ip**：ホスト（ターゲットとなる受信側）の IP アドレス。デフォルトは、すべての IP アドレスです。IPv4、IPv6 または IPv6z アドレスを使用できます。
- **hostname**：ホスト（ターゲットとなる受信側）のホスト名。（範囲：1 ～ 158 文字。ホスト名の各部分の最大ラベル サイズ：63）。
- **trap**：（オプション）このホストに SNMP トラップを送信します（デフォルト）。
- **informs**：（オプション）このホストに SNMP インフォームを送信します。伝達は、確認応答を必要とするトラップです。SNMPv1 には適用できません。
- ***version* 1**：（オプション）SNMPv1 トラップが使用されます。
- ***version* 2c**：（オプション）SNMPv2 トラップまたはインフォームが使用されます。
- ***version* 3**：（オプション）SNMPv2 トラップまたはインフォームが使用されます。
- 認証オプションは、SNMP v3 のみに使用できます。次のオプションを使用できます。

  noauth：（オプション）パケットを認証しないことを指定します。

  auth：（オプション）暗号化なしでパケットを認証することを指定します。

  priv：（オプション）暗号化ありでパケットを認証することを指定します。
- **community-string**：通知操作により送信されるパスワードのようなコミュニティ ストリング。（範囲：1 ～ 20 文字）。v1 および v2 の場合、コミュニティ ストリングをここに入力できます。v3 の場合、コミュニティ ストリングは v3 の snmp-server user（ISCLI）コマンドに定義されているユーザ名に一致する必要があります。
- **udp-port** *port*：（オプション）使用するホストの UDP ポート。デフォルトは 162 です。（範囲：1 ～ 65535）
- **filter** *filtername*：（オプション）このホストのフィルタ。指定しないと、何もフィルタ処理されません。フィルタを定義するには、**snmp-server filter** を使用します（コマンドの特定の順序をユーザが意識する必要はありません）。（範囲：最大 30 文字）

- **timeout** *seconds*：（オプション）（インフォームのみ）インフォームを再送信するまでに確認応答を待機する秒数。デフォルトは 15 秒です。（範囲：1 ～ 300）
- **retries** *retries*：（オプション）（インフォームのみ）生成したメッセージに対する応答を受信しない場合に、インフォーム要求を再送信する最大回数。デフォルトは3 です。（範囲：0 ～ 255）

デフォルト設定

バージョン：SNMP V1

通知のタイプ：トラップ

udp-port：162

インフォームを指定した場合、デフォルトの再試行回数は 3 です。

タイムアウト：15

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドの論理キーは一覧（ip-address/hostname, traps/informs, version）です。

SNMP v1 または v2 通知の受信者を設定すると、すべての MIB に対してその受信者の通知ビューが自動的に生成されます。

SNMPv3 の場合、ユーザまたは通知ビューは自動的に作成されません。

ユーザまたはグループを作成するには、snmp-server user（ISCLI）および snmp-server group コマンドを使用します。

例

次に、表示された IP アドレスでホストを定義する例を示します。

switchxxxxxx(config)# *snmp-server host 1.1.1.121 abc*

snmp-server engineID local

SNMP v3 のローカル デバイスで SNMP engineID を指定するには、**snmp-server engineID local** グローバル コンフィギュレーション モード コマンドを使用します。このエンジン ID を削除するには、このコマンドの **no** 形式を使用します。

構文

snmp-server engineID local {*engineid-string* | ***default***}

no snmp-server engineID local

パラメータ

- **engineid-string**：エンジン ID を識別する連結 16 進数文字を指定します。16 進数文字列の各バイトは、2 桁の 16 進数です。バイトは、ピリオドまたはコロンで区切られます。16 進数の奇数を入力すると、その文字列にプレフィックスとして数字 0 が自動的に付与されます。（長さ：5 ～ 32 文字、9 ～ 64 16 進数）
- **default**：デバイスの MAC アドレスに基づいてエンジン ID が自動的に作成されることを指定します。

デフォルト設定

デフォルトのエンジン ID は、規格に従って次のように定義されています。

- 最初の 4 オクテット：最初のビット = 1、残りの部分は割り当てられた IANA エンタープライズ番号。
- 5 番目のオクテット：後に MAC アドレスが続くことを示すために 3 に設定されます。
- 最後 6 番目のオクテット：デバイスの MAC アドレス。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

SNMPv3 を使用するには、デバイスにエンジン ID を指定する必要があります。任意の ID を指定したり、デフォルトの文字列（デバイスの MAC アドレスを使用して生成されたもの）を使用したりできます。

エンジン ID は管理ドメイン内で一意である必要があるため、次のガイドラインが推奨されます。

- デフォルト以外の EngineID を設定し、管理ドメイン内で一意であることを確認します。
- **snmpEngineID** の値を変更または削除すると、SNMPv3 ユーザ データベースが削除されます。

• SNMP エンジン ID は、すべて 0x0 やすべて 0xF や 0x000000001 にすることはできません。

例

次の例では、デバイスで SNMPv3 を有効にし、デバイスのローカル エンジン ID をデフォルト値に設定しています。

```
switchxxxxxx(config)# snmp-server engineid local default
The engine-id must be unique within your administrative domain.
Do you wish to continue? [Y/N]Y
The SNMPv3 database will be erased. Do you wish to continue? [Y/N]Y
```

snmp-server engineID remote

リモート SNMP デバイスの SNMP エンジン ID を指定するには、**snmp-server engineID remote** グローバル コンフィギュレーション モード コマンドを使用します。設定したエンジン ID を削除するには、このコマンドの **no** 形式を使用します。

構文

snmp-server engineID remote *ip-address engineid-string*

no snmp-server engineID remote *ip-address*

パラメータ

- **ip-address**：リモート デバイスの IPv4、IPv6 または IPv6z アドレス。
- **engineid-string**：エンジン ID を識別する文字列。エンジン ID は、連結した 16 進文字列です。16 進数文字列の各バイトは、2 桁の 16 進数です。各バイトは、ピリオドまたはコロンで区切ることができます。ユーザが 16 進数の奇数を入力すると、16 進文字列に自動的にプレフィックスとして 0 が付与されます。（範囲：engineid-string：5 ～ 32 文字。9 ～ 64 16 進数）

デフォルト設定

リモート エンジン ID は、デフォルトでは設定されません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

リモート エンジン ID は、SNMP バージョン 3 インフォームが設定されている場合に必要です。リモート エンジン ID は、リモート ホスト上のユーザに送信されるパケットを認証して暗号化するためのセキュリティ ダイジェストを計算する場合に使用します。

例

```
switchxxxxxx(config)# snmp-server engineID remote 1.1.1.1 11:AB:01:CD:23:44
```

show snmp engineID

ローカル SNMP エンジン ID を表示するには、**show snmp engineID** 特権 EXEC モード コマンドを使用します。

構文

show snmp engineID

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

次に、SNMP エンジン ID を表示する例を示します。

```
switchxxxxxx# show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
IP address Remote SNMP engineID
---------- --------------------------------
172.16.1.1 08009009020C0B099C075879
```

snmp-server enable traps

デバイスが SNMP トラップを送信できるようにするには、**snmp-server enable traps** グローバル コンフィギュレーション モード コマンドを使用します。すべての SNMP トラップを無効にするには、このコマンドの **no** 形式を使用します。

構文

snmp-server enable traps

no snmp-server enable traps

デフォルト設定

SNMP トラップは有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

no snmp-server enable traps を入力した場合、例に示すように、snmp-server trap authentication（1027 ページ） を使用して失敗トラップを有効にすることができます。

例

次の例では、SNMP 失敗トラップを除き、SNMP トラップを有効にしています。

```
switchxxxxxx(config)# snmp-server enable traps
switchxxxxxx(config)# no snmp-server trap authentication
```

snmp-server trap authentication

認証が失敗したときにデバイスが SNMP トラップを送信できるようにするには、**snmp-server trap authentication** グローバル コンフィギュレーション モード コマンドを使用します。SNMP 失敗認証トラップを無効にするには、このコマンドの **no** 形式を使用します。

構文

snmp-server trap authentication

no snmp-server trap authentication

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

SNMP 失敗認証トラップは有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、すべての SNMP トラップを無効にし、失敗認証トラップのみを有効にしています。

```
switchxxxxxx(config)# no snmp-server enable traps
switchxxxxxx(config)# snmp-server trap authentication
```

snmp-server contact

システム接点（sysContact）文字列の値を設定するには、**snmp-server contact** グローバル コンフィギュレーション モード コマンドを使用します。システム接点情報を削除するには、このコマンドの **no** 形式を使用します。

構文

snmp-server contact *text*

no snmp-server contact

パラメータ

text：システム接点情報を指定します。（長さ：1 ～ 160 文字）

デフォルト設定

なし

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、システム接点情報を Technical_Support に設定しています。

```
switchxxxxxx(config)# snmp-server contact Technical_Support
```

snmp-server location

システム ロケーション ストリングの値を設定するには、**snmp-server location** グローバル コンフィギュレーション モード コマンドを使用します。位置のストリングを削除するには、このコマンドの **no** 形式を使用します。

構文

snmp-server location *text*

no snmp-server location

パラメータ

text：システムのロケーション情報を指定します。（長さ：1 ～ 160 文字）

デフォルト設定

なし

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、デバイス ロケーションを New_York に設定しています。

```
switchxxxxxx(config)# snmp-server location New_York
```

snmp-server set

対応するCLIコマンドがないアクションをMIBが実行する場合にコンフィギュレーション ファイルにSNMP MIBコマンドを定義するには、**snmp-server set** グローバル コンフィギュレーション モード コマンドを使用します。

構文

snmp-server set *variable-name name value* [*name2 value2...*]

パラメータ

- **variable-name**：SNMP MIB 変数名を指定します。これは、有効な文字列である必要があります。
- **name** *value*：名前と値のペアの一覧を指定します。それぞれの名前と値は、有効な文字列である必要があります。スカラーMIBの場合、単一の名前と値のペアのみが存在します。テーブルのエントリの場合、名前と値のペアが1つ以上あり、その後に1つ以上のフィールドが続きます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

CLI では必要に応じてどのような設定でも設定できますが、同等の CLI コマンドがない MIB 変数を SNMP ユーザが設定するという場合もあります。

例

次の例では、スカラー MIB sysName を値 TechSupp で設定しています。

```
switchxxxxxx(config)# snmp-server set sysName sysname TechSupp
```

snmp trap link-status

SNMP トラップのリンク ステータス生成を有効にするには、**snmp trap link-status** インターフェイス コンフィギュレーション モード コマンドを使用します。SNMP トラップのリンク ステータス生成を無効にするには、このコマンドの **no** 形式を使用します。

構文

snmp trap link-status

no snmp trap link-status

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

SNMP リンク ステータス トラップの生成は有効になっています。

コマンド モード

インターフェイス コンフィギュレーション モード

例

次の例では、SNMP リンク ステータス トラップの生成を無効にしています。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# # no snmp trap link-status
```

show snmp

SNMP ステータスを表示するには、**show snmp** 特権 EXEC モード コマンドを使用します。

構文

show snmp

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

特権 EXEC モード

例

次に、SNMP 通信ステータスを表示する例を示します。

```
switchxxxxxx# show snmp
SNMP is enabled
SNMP traps Source IPv4 interface: vlan 1
SNMP informs Source IPv4 interface: vlan 11
SNMP traps Source IPv6 interface: vlan 10
SNMP informs Source IPv6 interface:
```

Community-String	Community-Access	View name	IP Address	Mask
public	read only	user-view	All	
private	read write	Default	172.16.1.1/10	
private	su	DefaultSuper	172.16.1.1	

Community-string	Group name	IP Address	Mask	Type	
public	user-group	All		Router	

```
Traps are enabled.
Authentication trap is enabled.
Version 1,2 notifications
```

Target Address	Type	Community	Version	UDP Port	Filter Name	TO Sec	Retries
192.122.173.42	Trap	public	2	162		15	3
192.122.173.42	Inform	public	2	162		15	3

```
Version 3 notifications
```

Target Address ---------- 192.122.173.42	Type ---- Inform	Username -------- Bob	Security Level ------- Priv	UDP Port ---- 162	Filter name ----- 	TO Sec --- 15	Retries ------- 3
System Contact: Robert System Location: Marketing							

次の表に、この出力で表示される重要なフィールドの説明を示します。

フィールド	説明
Community-string	SNMP へのアクセスを許可するコミュニティ アクセス ストリング。
Community-access	許可されているアクセス タイプ：読み取り専用、読み取り/書き込み、スーパー アクセス。
IP Address	管理ステーション IP アドレス。
Target Address	ターゲットとなる受信側の IP アドレス。
Version	送信されたトラップの SNMP バージョン。

PHY コマンド

この章は、次の項で構成されています。

- test cable-diagnostics tdr （1036 ページ）
- show cable-diagnostics tdr （1037 ページ）
- show cable-diagnostics cable-length （1038 ページ）
- show fiber-ports optical-transceiver （1039 ページ）

test cable-diagnostics tdr

タイムドメイン反射率計（TDR）技術を使用してポートに接続された銅線ケーブルの品質と特性を診断するには、**test cable-diagnostics tdr** 特権 EXEC モードコマンドを使用します。

構文

test cable-diagnostics tdr interface *interface-id*

パラメータ

interface-id：（オプション）イーサネット ポート ID を指定します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドはファイバポートでは機能しません（デバイス上に存在する場合）。テスト対象のポートをファイバポートと組み合わせていない限り、テスト中はシャットダウンする必要があります。この場合、テストはファイバポートでは機能しないため、シャットダウンする必要がありません。

TDR テストのケーブルの最大長は 120 メートルです。

例 1：ポート gi1/0/1（銅線ポート）に接続された銅線ケーブルをテストします。

```
switchxxxxxx#  test cable-diagnostics tdr interface gi1/0/1
Cable is open at 64 meters
```

例 2：ポート 2（ポートとファイバの組み合わせ）に接続した銅ケーブルをテストします。

```
switchxxxxxx#  test cable-diagnostics tdr interface gi1/0/2
Fiber ports are not supported
```

show cable-diagnostics tdr

すべての銅線ポートまたは特定の銅線ポートで最後に実行したタイムドメイン反射率計（TDR）テストの情報を表示するには、**show cable-diagnostics tdr** 特権 EXEC モード コマンドを使用します。

構文

show cable-diagnostics tdr *[***interface** *interface-id*]

パラメータ

- **interface-id**：（オプション）イーサネット ポート ID を指定します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

TDR テストのケーブルの最大長は 120 メートルです。

例

次の例では、すべての銅線ポートで最後に実行した TDR テストの情報を示します。

```
switchxxxxxx#  show cable-diagnostics tdr
```

Port	Result	Length [meters]	Date
gi1/0/1	OK		
gi1/0/2	Short	50	13:32:00 23 July 2010
gi1/0/3	Test has not been performed		
gi1/0/4	Open	64	13:32:00 23 July 2010

show cable-diagnostics cable-length

すべてのポートまたは特定のポートに接続されている銅ケーブルの予想長さを表示するには、**show cable-diagnostics cable-length** 特権 EXEC モード コマンドを使用します。

構文

show cable-diagnostics cable-length *[***interface** *interface-id*]

パラメータ

- **interface-id**：（オプション）イーサネット ポート ID を指定します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

ポートはアクティブである必要があります。リンクが 100 Mbps で動作している場合、ケーブル長の結果は使用できません。インターフェイスでグリーン イーサネット ショート リーチ機能が有効になっている場合、このコマンドで提供されるケーブル長の結果が影響を受けることがあります。

例

次の例では、すべてのポートに接続されている銅ケーブルの予想長さを示します。

```
switchxxxxxx#  show cable-diagnostics cable-length
```

Port	Length [meters]
----	-----------------
gi1/0/1	< 50
gi1/0/2	Copper not active
gi1/0/3	110-140

show fiber-ports optical-transceiver

光学トランシーバ診断を表示するには、**show fiber-ports optical-transceiver** 特権 EXEC モードコマンドを使用します。

構文

show fiber-ports optical-transceiver *[***interface** *interface-id*]

パラメータ

- **interface-id**：（オプション）イーサネット ポート ID を指定します。

デフォルト設定

すべてのポートが表示されます。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx#  show fiber-ports optical-transceiver
   Port       Temp  Voltage Current Output  Input   LOS
              [C]   [Volt]  [mA]    Power   Power
                                    [mWatt] [mWatt]
----------- ------ ------- ------- ------- ------- ---
  gi1/0/1     Copper
  gi1/0/2     Copper
  gi1/0/3      28    3.32    7.26    3.53    3.68   No
  gi1/0/4      29    3.33    6.50    3.53    3.71   No
 Temp         - Internally measured transceiver temperature
 Voltage      - Internally measured supply voltage
 Current      - Measured TX bias current
 Output Power - Measured TX output power in milliWatts
 Input Power  - Measured RX received power in milliWatts
 LOS          - Loss of signal
 N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

PnP コマンド

この章は、次の項で構成されています。

- pnp device （1042 ページ）
- pnp discovery timeout （1043 ページ）
- pnp enable （1044 ページ）
- pnp reconnect interval （1045 ページ）
- pnp resume （1046 ページ）
- pnp transport （1047 ページ）
- pnp watchdog timeout （1049 ページ）
- show pnp （1050 ページ）

pnp device

デバイスのユーザ名とパスワードを定義するには、グローバル コンフィギュレーション モードで **pnp device** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

pnp device username *username* **password** *password*

encrypted pnp device username *username* **password** encrypted-*password*

no pnp device

パラメータ

- ***username***：デバイスのユーザ名を指定します（範囲：1 ～ 64 文字）。
- ***password***：デバイスのパスワードを指定します（範囲：1 ～ 64 文字）。
- ***encrypted-password***：暗号化されたデバイスパスワードを指定します。

デフォルト設定

該当なし

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

PnP エージェントによって PnP サーバに送信される各 PnP メッセージに使用するユーザ名とパスワードを設定するには、**pnp device** コマンドを使用します。

例

次に、デバイス名とパスワードを設定する例を示します。

```
switchxxxxxx(config)# pnp device username sjohn password Tan123
```

pnp discovery timeout

PnP エージェント検出タイムアウト（秒単位）と指数係数を定義するには、グローバル コンフィギュレーション モードで **pnp discovery timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

pnp discovery timeout *timeout exponential-factor max-timeout*

no pnp discovery timeout

パラメータ

- *timeout*：検出が失敗した後で検出を再試行するまで待機する時間を指定します（秒単位）。範囲は 1 ～ 2000000 です。
- *exponential-factor*：指数係数値は、検出試行を指数的にトリガーする値です。指定できる範囲は 1 ～ 9 です。
- *max-timeout*：タイムアウトの最大値を指定します。範囲は 1 ～ 2000000 です。

デフォルト設定

timeout：60 秒

exponential-factor：3

max-timeout：540 秒

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

検出タイムアウト（秒単位）と指数係数を設定するには、**pnp discovery timeout** コマンドを使用します。次の式は、前のタイムアウトを使用して次のタイムアウトを計算するために使用します。

next-timeout = (*previous-timeout***exponential-factor* < *max-timeout*) ?

*previous-timeout***exponential-factor* : *max-timeout*;

例

次に、検出タイムアウトと係数を設定する例を示します。

```
switchxxxxxx(config)# pnp discovery timeout 100 2 800
```

pnp enable

PnP エージェントを有効にするには、グローバル コンフィギュレーション モードで **pnp enable** コマンドを使用します。PnP エージェントを無効にするには、このコマンドの **no** 形式を使用します。

構文

pnp enable

no pnp enable

デフォルト設定

PnP エージェントが有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

PnP エージェントを有効にするには、このコマンドを使用します。

例

次に、PnP エージェントを無効にする例を示します。

```
switchxxxxxx(config)# no pnp enable
```

pnp reconnect interval

連続PnPセッション間のPnPエージェント間隔を定義するには、グローバル コンフィギュレーション モードで **pnp reconnect interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

pnp reconnect interval *timeout*

no pnp reconnect interval

パラメータ

- ***timeout***：接続が失われた後にセッションの再接続を試行するまでの間隔を指定します（秒単位）。範囲は 1 ～ 2000000 で、デフォルトは 30 です。

デフォルト設定

30 秒

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

PnP セッションの間隔を設定するには、**pnp reconnect interval** コマンドを使用します。

例

次に、PnP セッション間隔を設定する例を示します。

```
switchxxxxxx(config)# pnp interval reconnect interval 100
```

pnp resume

PnP エージェントを再開するには、グローバル コンフィギュレーション モードで **pnp resume** コマンドを使用します。

構文

pnp resume

デフォルト設定

PnP エージェントが有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

PnP エージェントをただちに待機状態から解除するには、**pnp resume** コマンドを使用します。

- 検出待機状態から検出状態へ、または
- PnP セッション待機状態から PnP セッション状態へ

例

次に、PnP サーバ検出を再開する例を示します。

```
switchxxxxxx(config)# pnp resume
```

pnp transport

PnP トランスポートを定義するには、グローバル コンフィギュレーション モードで **pnp transport** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

pnp transport {**http** | **https**} *ip-address* [**port** *port-number*]

no pnp transport

パラメータ

- **http** | **https**：トランスポートプロトコルを指定します。
- ***ip-address***：PnP サーバの IPv4 アドレスまたは IPv6 アドレス、あるいは DNS 名を指定します。
- ***port-number***：PnP サーバの TCP ポートを指定します。パラメータを指定しない場合は、次のデフォルト値が適用されます。
  - **HTTP**：80
  - **HTTPS**：443

デフォルト設定

- DHCP オプション 43
- DNS：

  PnP サーバの IP アドレス：pnpserver

  プロトコル：HTTP

  ポート：80
- Cisco Cloud（デフォルト）：

  PnP サーバの IP アドレス：devicehelper.cisco.com

  プロトコル：HTTPS

  ポート：443

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

PnP プロトコルが実行されるトランスポートプロトコルを設定するには、**pnp transport** コマンドを使用します。

例

次に、PnP トランスポートを設定する例を示します。

```
switchxxxxxx(config)# pnp transport http 145.1.3.4
```

pnp watchdog timeout

PnPエージェント ウォッチドッグ タイムアウトを定義するには、グローバル コンフィギュレーション モードで **pnp watchdog timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

pnp watchdog timeout *timeout*

no pnp watchdog timeout

パラメータ

- ***timeout***：PnPサーバまたはファイルサーバからの応答を待機する時間を指定します。指定できる範囲は 1 ～ 180 です。

デフォルト設定

60 秒

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ウォッチドッグタイムアウトを秒単位で設定するには、**pnp watchdog timeout** コマンドを使用します。

例

次に、ウォッチドッグタイムアウトを設定する例を示します。

```
switchxxxxxx(config)# pnp watchdog timeout 120
```

show pnp

PnPエージェント情報を表示するには、特権EXECモードで**showpnp**コマンドを使用します。

構文

show pnp

コマンド モード

特権 EXEC モード

使用上のガイドライン

PnP エージェントの情報を表示するには、このコマンドを使用します。

例 1。次に、PnP エージェントが無効になっている場合に PnP エージェント情報を表示する例を示します。

```
switchxxxxxx# show pnp
Administrative status: disabled
Operational status:
PnP Agent state:
Transport protocol: HTTP
Source Ip address:
TCP port: 80 (default)
Username:
Password's MD5 digest:
Discovery
  Timeout: 60 seconds (default)
  Exponential Factor: 3 (default)
  Maximum Timeout: 540 seconds
PnP Session Reconnection Interval:
  Current:
 >Default: 60 sec
  Manual Configuration:
  PnP:
PnP Watchdog Timeout: 60 seconds
```

例 2。次に、PnP エージェントの準備ができていない場合に PnP エージェント情報を表示する例を示します。

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: notReady (No PnP Server IP Address)
PnP Agent state:
Transport protocol: HTTP (from DHCP Option 43)
Server IP address:
Source Ip address:
TCP port: 80 (default)
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery
  Timeout: 60 seconds (default)
  Exponential Factor: 3 (default)
  Maximum Timeout: 540 seconds
PnP Session Reconnection Interval:
```

```
  Current:
 >Default: 60 sec
  Manual Configuration:
  PnP:
PnP Watchdog Timeout: 60 seconds
```

例 3。次に、PnP セッション状態で PnP エージェントが有効になっている場合に PnP エージェント情報を表示する例を示します。

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: PnP Session
Transport protocol: HTTP (from DHCP Option 43)
Server IP address: 176.1.1.1 (from DHCP Option 43)
Source Ip address:
TCP port: 80 (default)
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery Timeout: 60 seconds (default)
Discovery Exponential Factor: 3 (default)
Discovery Maximum Timeout: 540 seconds
PnP Session Interval Timeout: 60 (default)
PnP Watchdog Timeout: 60 seconds
```

例 4。次に、PnP セッション状態で PnP エージェントが有効になっており、PnP サーバが変更された場合に PnP エージェント情報を表示する例を示します。

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: PnP Session
Transport protocol: HTTP (from DHCP Option 43
Server IP address: 176.1.1.1 (from DHCP Option 43);
     Next session: 167.21.3.4 (from DHCP Option 43)
Source Ip address:
TCP port: 80 (default)
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery Timeout: 60 seconds (default)
Discovery Exponential Factor: 3 (default)
Discovery Maximum Timeout: 540 seconds
PnP Session Interval Timeout: 60 (default)
PnP Watchdog Timeout: 60 seconds
```

例 5。次に、PnP セッション待機状態で PnP エージェントが有効になっている場合に PnP エージェント情報を表示する例を示します。

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: PnP Session Waiting
Transport protocol: HTTPS
Server IP address: 176.1.1.1
Source Ip address: 120.10.10.10
TCP port: 180
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery Timeout: 60 seconds (default)
Discovery Exponential Factor: 3 (default)
Discovery Maximum Timeout: 540 seconds
PnP Session Interval Timeout: 180 seconds (from PnP Backoff message)
Timer Remainder: 150 seconds
PnP Watchdog Timeout: 60 seconds
```

例 6。次に、PnP エージェントが検出状態の場合に PnP エージェント情報を表示する例を示します。

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: PnP Session
Transport protocol: HTTP (from DHCP Option 43
Server IP address: 176.1.1.1 (from DHCP Option 43);
     Next session: 167.21.3.4 (from DHCP Option 43)
Source Ip address:
TCP port: 80 (default)
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery Timeout: 60 seconds (default)
Discovery Exponential Factor: 3 (default)
Discovery Maximum Timeout: 540 seconds
PnP Session Interval Timeout: 60 (default)
PnP Watchdog Timeout: 60 seconds
```

例 7。次に、PnP エージェントが検出待機中状態の場合に PnP エージェント情報を表示する例を示します。

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: PnP Session
Transport protocol: HTTP (from DHCP Option 43
Server IP address: 176.1.1.1 (from DHCP Option 43);
     Next session: 167.21.3.4 (from DHCP Option 43)
Source Ip address:
TCP port: 80 (default)
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery Timeout: 60 seconds (default)
Discovery Exponential Factor: 3 (default)
Discovery Maximum Timeout: 540 seconds
PnP Session Interval Timeout: 60 (default)
PnP Watchdog Timeout: 60 seconds
```

PoE コマンド

この章は、次の項で構成されています。

- power inline （1054 ページ）
- power inline inrush test disable （1055 ページ）
- power inline legacy support disable （1056 ページ）
- power inline powered-device （1057 ページ）
- power inline priority （1058 ページ）
- power inline usage-threshold （1059 ページ）
- power inline traps enable （1060 ページ）
- power inline limit （1061 ページ）
- power inline limit-mode （1062 ページ）
- power inline four-pair forced （1063 ページ）
- power inline negotiation （1064 ページ）
- show power inline （1065 ページ）
- show power inline savings （1071 ページ）
- clear power inline counters （1072 ページ）
- clear power inline monitor consumption （1073 ページ）
- show power inline monitor consumption （1074 ページ）

power inline

インターフェイスでインライン電源管理モードを設定するには、**power inline** インターフェイス コンフィギュレーション モード コマンドを使用します。

構文

power inline auto *[***time-range** *time-range-name]*

power inline never

パラメータ

- **auto**：デバイス検出プロトコルをオンにして、デバイスに電力を供給します。
- **never**：デバイス検出プロトコルをオフにして、デバイスへの電力供給を停止します。
- **time-range-name**：時間範囲を指定します。時間範囲が有効でない場合、電力は接続デバイスに供給されません。時間範囲が指定されていない場合、ポートに限定される時間範囲はありません。（範囲：1 ～ 32 文字）

デフォルト設定

デフォルトは auto に設定されています。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

never パラメータを時間範囲で使用することはできません。

例

次の例では、ポート 4 でデバイス検出プロトコルをオンにします。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# power inline auto
```

power inline inrush test disable

突入電流テスト（PoEデバイスの入力サージ電流をチェックするハードウェア テスト）を無効にするには、**power inline inrush test disable** グローバル コンフィギュレーション モード コマンドを使用します。突入電流テストを有効にするには、このコマンドのno形式を使用します。

構文

power inline inrush test disable

no power inline inrush test disable

デフォルト設定

突入電流テストは有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、突入電流テストを無効にします。

```
switchxxxxxx(config)# power inline inrush test disable
```

power inline legacy support disable

To disable the legacy PDs support, use the **power inline legacy support disable** Global Configuration mode command. To enable the legacy support, use the no form of this command.

構文

power inline legacy support disable

no power inline legacy support disable

デフォルト設定

レガシー サポートは有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、レガシー PD サポートを無効にします。

```
switchxxxxxx(config)# power legacy support disable
```

power inline powered-device

デバイスタイプの説明を追加するには、**power inline powered-device** インターフェイス コンフィギュレーション モード コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

構文

power inline powered-device *pd-type*

no power inline powered-device

パラメータ

pd-type：このインターフェイスに接続されているデバイスのタイプを認識できるようにコメントまたは説明を入力します。（長さ：1 ～ 24 文字）

デフォルト設定

説明はありません。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、ポート 4 に接続されているデバイスに「ip phone」という説明を追加する例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# power inline powered-device ip_phone
```

power inline priority

インターフェイス インライン電源管理優先度を設定するには、**power inline priority** インターフェイス コンフィギュレーション（イーサネット）モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

power inline priority *{***critical** | **high** | **low***}*

no power inline priority

パラメータ

- **critical**：デバイス動作がクリティカルであることを指定します。
- **high**：デバイスの動作の優先順位が高いことを指定します。
- **low**：デバイスの動作の優先順位が低いことを指定します。

デフォルト設定

デフォルトの優先度は low に設定されています。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

例

次に、ポート gi1/0/4 のインラインパワー管理の優先順位を High に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# power inline priority high
```

power inline usage-threshold

送信側インライン電力使用アラームのしきい値を設定するには、**power inline usage-threshold** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

power inline usage-threshold *percent*

no power inline usage-threshold

パラメータ

percent：測定された電源を比較するしきい値をパーセントで指定します。（範囲：1 ～ 99）

デフォルト設定

デフォルトのしきい値は 95% です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、送信側インライン電力使用アラームのしきい値を 90 パーセントに設定します。

```
switchxxxxxx(config)# power inline usage-threshold 90
```

power inline traps enable

インライン電力トラップを有効にするには、**power inline traps enable** グローバル コンフィギュレーション モード コマンドを使用します。トラップを無効にするには、このコマンドの **no** 形式を使用します。

構文

power inline traps enable

no power inline traps enable

デフォルト設定

インライン電力トラップは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、インライン電力トラップを有効にします。

```
switchxxxxxx(config)# power inline traps enable
```

power inline limit

インターフェイスのポートごとに電力制限を設定するには、**power inline limit** インターフェイス コンフィギュレーション モード コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

power inline limit *power*

no power inline limit

パラメータ

power：ポートの電力消費制限を指定します（ミリワット単位）。（範囲：0 ～ 60000）

デフォルト設定

デフォルト値は 30 W です。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

ユーザ ガイドライン

動作電力制限は、ポートで設定された電力の最小制限値および最大電力機能です。たとえば、PoE ポートで設定した値が 15.4W より大きい場合、動作電力制限は 15.4W です。

例

次の例では、ポートでインライン電力を設定します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# power inline limit 2222
```

power inline limit-mode

システムの電力制限モードを設定するには、**power inline limit-mode** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

power inline limit-mode {***class*** | ***port***}

no power inline limit-mode

パラメータ

- **class**：ポートの電力制限は、分類処理中に検出した PD（電力デバイス）のクラスに基づいています
- **port**：ポートの電力制限は、検出した PD のクラスに関係なく固定されます。

デフォルト設定

デフォルト値は class です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

システムの PoE 制限モードを変更すると、すべての PoE ポートの電源のオンとオフが切り替わります。

例

次の例では、電源制限を class に設定します。

```
switchxxxxxx(config)# power inline limit-mode class
"Changing the PoE limit mode of the system will turn the power OFF and ON for all PoE
ports. Are you sure? [y/n]"
```

power inline four-pair forced

インラインパワーを設定してスペアペアを有効にするには、**power inline four-wire forced** インターフェイス コンフィギュレーション モード コマンドを使用します。

構文

power inline four-pair forced

no power inline four-pair forced

パラメータ

デフォルト設定

デフォルト設定は、no four-pair forced に設定されています。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

このコマンドは、CDP/LLDP プロトコルまたは MDI TLV 経由の新しい 4 線式電源（UPOE スプリッタなど）をサポートしていないデバイスに接続されているポートにのみ使用してください。

このコマンドは、スペアペアに電力を供給するように強制します。これによって、60 ワットの PoE を使用できます。

CDP/LLDP は、要求された電力に関係なく、割り当てられた 60 W の電力を反映します。

この force コマンドは、ポートモードまたはポート制限の設定をオーバーライドします。

例

次に、ポート 4 のスペアペアに強制する例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# power inline four-pair forced
```

power inline negotiation

power inline negotiate インターフェイス コンフィギュレーション モード コマンドは、インターフェイスで許可されるネゴシエーションタイプを選択するために使用されます。インターフェイスをデフォルトでサポートされているネゴシエーションタイプに戻すには、このコマンドの no 形式を使用します。

構文

power inline negotiation {none | all}

no power inline negotiation

パラメータ

none：ポートでネゴシエーションが許可されないことを示します。

all：サポートされているすべてのネゴシエーションメソッドがポートで許可されることを示します。

デフォルト設定

サポートされているすべてのネゴシエーションメソッドがポートで許可されます。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

none オプションを選択すると、すべてのネゴシエーションパケットが無視されます。

次の例では、ポートでネゴシエーションが無効になります。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# power inline negotiation none
```

show power inline

すべてのインターフェイスまたは特定のインターフェイスのインライン電力に関する情報を表示するには、**show power inline** 特権 EXEC モード コマンドを使用します。

構文

show power inline [*interface-id* | ***module*** *unit-id*]

パラメータ

- **interface-id**：インターフェイス ID を指定します。インターフェイス ID はイーサネットポートである必要があります。
- **module** *unit-id*：スタックメンバーのユニット ID を指定します。

デフォルト設定

すべてのポートの情報を表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

スタックでは、PoE をサポートするデバイスのみが表示されます。

例 1：次の例では、すべてのポート（ポートの電源ベース）のインライン電力に関する情報を表示します。

```
switchxxxxxx(config)# show power inline
Port limit mode: Enabled
Usage threshold: 95%
Trap: Enabled
Legacy Mode: Disabled
Inrush test: Enabled
Class Error Detection: Enabled
'
```

Unit	Module	Nominal Power（w）	割り当て済み電力 (w)	Temp（c）	SW Version	PSE チップセット Revision
------	----------	----------	----------	----------	----------	----------
1	48P	320	120（37.5%）	30	1.222.3	PD69208 - 0x4BC2 PD69204 - 0x4AC
2	24P	240	0（0%）	50	1.222.3	PD69208* - 0x4A
3	24P	120	0（0%）	50	4.0.10.0	TPS3288 - 0x40c4

Interface	Admin	Oper	Power	Class	Device	Priority
--------	----------	------------	---------	-------	-------------------	-----------
gi1/0/1	Auto	On	15.4（30）	3	IP フォンモデル A	Critical
gi1/0/2	Auto	Searching	0	0		High
gi1/0/3	Never	Off	0	0		Low

例 2：次の例では、特定のポートのインライン電力に関する情報を表示します。

```
switchxxxxxx(config)# show power inline gi1/0/1
```

Interface	Admin	Oper	Power	Class	Device	Priority
--------	----------	------------	---------	-------	-------------------	-----------
gi1/0/1	Auto	On		3	IP フォンモデル A	Critical

```
Port status: Port is on - Valid PD resistor signature detected
Port standard: 802.3AT
Admin power limit: 30.0 watts
Time range:
Link partner standard: 802.3AF
Operational power limit: 30 watts
Negiotiated power: 18 watts (LLDP)
```

#EDITOR：電力ネゴシエーションは CDP/LLDP を介して行われます。PD との電力ネゴシエーションが行われなかった場合、プロトコルタイプの表示は（none）になります。電力ネゴシエーションは行われたものの PSE による電力の割り当てにつながらなかった場合、表示は「0 watts (LLDP)」になります（電力は引き続きハードウェアによって割り当てられる可能性があります）。ネゴシエーションが期限切れになった場合は、ネゴシエートされた最新の値とともに「Expired」という単語が追加されます（例：「20Watts（LLDP - Expired）」）。

```
Allocated power: 16 watts
Current (mA): 81
Voltage(V): 50.8
Overload Counter: 5
Denied Counter: 2
Absent Counter: 0
Invalid Signature Counter: 0
```

次の表に、この出力で表示されるフィールドについて説明します。

フィールド	説明
Power	インライン電力供給機器の動作ステータス。
Nominal Power	インライン電力供給機器の公称電力（ワット単位）。
割り当て済み電力	現在の電力割り当ての合計（ワット単位）。

フィールド	説明
Usage Threshold	測定した電力を比較して、しきい値を超えている場合はアラームを作動するための使用率のしきい値をパーセントで表示します。
Traps	インライン電力トラップが有効になっているかどうかを示します。
Port	イーサネット ポート番号。
device	デバイスタイプの説明。
State	電源供給のためにポートが有効になっているかどうかを示します。有効な値は Auto または Never です。
Priority	ポート インライン電源管理の優先度。有効な値は、Critical、High、または Low です。
Status	電源動作の状態。有効な値は、On、Off、Test-Fail、Testing、Searching、または Fault です。
Class	デバイスの電力消費分類。
Overload Counter	検出したオーバーロード条件の数をカウントします。
Short Counter	検出したショート条件の数をカウントします。
Denied Counter	電源が拒否された回数をカウントします。
Absent Counter	デバイスのドロップアウトが検出されたため電力が切断された回数をカウントします。
Invalid Signature Counter	デバイスの無効な署名が検出された回数をカウントします。
Inrush Test	突入電流テストが有効になっているか、無効になっているかを表示します。

フィールド	説明
Port limit mode	ポート制限では Enabled、クラス制限では Disable。
Legacy Mode	レガシーデバイスのサポートを無効化または有効化。
Inrush Test	突入電流テストが有効になっているか、無効になっているかを表示します。
SW version	POE ファームウェアのバージョン。

フィールド	説明
HW Version	POE ハードウェアのバージョン。
Usage Threshold	測定した電力を比較して、しきい値を超えている場合はアラームを作動するための使用率のしきい値をパーセントで表示します。
Traps	インライン電力トラップが有効になっているかどうかを示します。
Module	モジュール名。
Available Power	インライン電力供給機器の公称電力（ワット単位）。
割り当て済み電力	現在の電力割り当ての合計（ワット単位）。
Temp	POE デバイスの温度を表示します。
Interface	イーサネット ポート番号。
Admin	電源供給のためにポートが有効になっているかどうかを示します。有効な値は Auto または Never です。
Oper	電源動作の状態。有効な値は、On、Off、Test-Fail、Testing、Searching、または Fault です。
Power	消費された電力（ワット単位）、割り当てられた電力は括弧（）内に表示されます。
Class	デバイスの電力消費分類（0 ～ 4）。
Device	ユーザが設定したデバイスタイプの説明。
Priority	ポート インライン電源管理の優先度。有効な値は、Critical、High、または Low です。
Port status	詳細な理由によるポートステータスのオン/オフ（詳細については、以下を参照）。
Port standard	802.3AF /802.3AT /60W POE。
Admin power limit	**ポート制限モード**が有効になっている場合に使用するポート制限（ワット単位）。
Time Range	インターフェイスに関連付けられている時間範囲の名前。
Link partner standard	802.3AF/802.3AT/60W POE。

フィールド	説明
Operational Power Limit	ポートの実際の電力制限（ワット単位）。
Current (mA)	ポート電流（ミリアンペア単位）。
Voltage (V)	ポート電圧（ボルト単位）。
Overload Counter	検出したオーバーロード条件の数をカウントします。
Short Counter	検出したショート条件の数をカウントします。
Denied Counter	電源が拒否された回数をカウントします。
Absent Counter	デバイスのドロップアウトが検出されたため電力が切断された回数をカウントします。
Invalid Signature Counter	デバイスの無効な署名が検出された回数をカウントします。

```
Following is a list of port status values:
Port is on - Valid capacitor/resistor detected.
Port is on - Valid resistor/capacitor detected.
Port is on - 4 pairs.
Port is on - Forced 4 pairs.
Port is off - Main supply voltage is high.
Port is off - Main supply voltage is low.
Port is off - Hardware pin disables all ports.
Port is off - Non-existing port number.
Port is yet undefined.
Port is off - Internal hardware fault.
Port is off - User setting.
Port is off - Detection is in process.
Port is off - Non-802 - 3af powered device.
Port is off - Overload & Underload states.
Port is off - Underload state.
Port is off - Overload state.
Port is off - Power budget exceeded.
Port is off - Internal hardware fault.
Port is off - Voltage injection into the port.
Port is off - Improper Capacitor Detection results.
Port is off - Discharged load.
Port is on - Detection regardless (Force On).
Undefined error during Force On.
Supply voltage higher than settings.
Supply voltage lower than settings.
Disable_PDU flag raised during Force On.
Port is forced on, then disabled.
Port is off - Forced power error due to Overload.
Port is off - Out of power budget while in Force On.
Communication error with PoE devices after Force On.
Port is off - Short condition.
Port is off - Over temperature at the port.
Port is off - Device is too hot.
Unknown device port status.
ForcePowerErrorShortCircuit.
ForcePowerErrorChannelOverTemperature.
ForcePowerErrorChipOverTemperature .
```

```
PowerManagment - Static Calculated power is bigger than power limit.
PowerManagment - Static OVL PD class report (user predefined power value).
Static Calculated power (power limit during Force On).
Static OVL PD class report (user predefined power value during Force On).
High power port is ON - High power device was detected.
Chip Over Power - Sum of square currents exceeded SumPowerLimit.
Force Power Error Chip Over Power, during Force On.
Port is off - Class Error - Illegal class.
```

show power inline savings

デバイスのインラインパワーの節減に関する情報を表示するには、**show power inline savings** 特権 EXEC モードコマンドを使用します。

構文

show power inline savings

コマンド モード

特権 EXEC モード

使用上のガイドライン

特定の時間にポートへの PoE をシャットダウンする PoE 時間範囲機能を使用することによって節約された総電力を表示するには、**show power inline savings** コマンドを使用します。

例 1：次に、デバイスの PoE 省電力を示します。

```
switchxxxxxx(config)# show power inline savings
Current Power Savings: 45W
Cumulative Energy Saved: 180 [Watt*Hour]
* Estimated Annual Power saving: 1800 [Watt*Hour]
* Annual estimate is based on the saving during the previous week
NA – information for previous week is not available
```

clear power inline counters

電源インラインインターフェイスのカウンタをクリアするには、**clear power inline counters** 特権 EXEC モードコマンドを使用します。

構文

clear power inline counters [*interface-id*]

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID はイーサネットポートタイプにする必要があります。インターフェイス ID を指定しない場合は、すべてのインターフェイスのカウンタがクリアされます。

デフォルト設定

すべてのインターフェイスカウンタがクリアされます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

電源インライン インターフェイス カウンタ（Overload、Short、Denied、Absent、Invalid Signature）をリセットするには、**clear power inline counters** コマンドを使用します。

次に、gi1/0/2 の電源インラインカウンタをクリアする例を示します。

```
switchxxxxxx#  clear power inline counters gi1/0/2
```

clear power inline monitor consumption

すべてのインターフェイスまたは特定のインターフェイス、あるいはインターフェイスリストの電力インライン消費量のモニタ情報をクリアするには、**clear power inline monitor consumption** 特権 EXEC モードコマンドを使用します。

構文

clear power inline monitor consumption *[interface-id-list]*

パラメータ

interface-id-list：（オプション）インターフェイス ID のリストを指定します。インターフェイス ID はイーサネットポートタイプにする必要があります。インターフェイス ID を指定しない場合：すべてのインターフェイスの消費情報がクリアされます。

デフォルト設定

すべてのモニタ対象のインターフェイスの情報がクリアされます。

コマンド モード

特権 EXEC モード

例

次に、gi1/0/1 のモニタ対象の統計情報をクリアする例を示します。

```
switchxxxxxx#  clear power inline monitor consumption gi1/0/1
```

show power inline monitor consumption

モニタ対象の平均電力消費量の情報を表示するには、**show power inline monitor consumption** 特権 EXEC モードコマンドを使用します。

構文

show power inline monitor consumption {**interface** *interface-id* | **Unit** *unit-id***}** {**minutes**|**hours | days |weeks**}

パラメータ

- **interface** *interface-id*：インターフェイス ID を指定します。インターフェイス ID はイーサネット ポートである必要があります。
- **Unit** *unit-id*：指定したユニット ID の合計 PoE 消費量情報を表示します。
- **minutes**：1 分あたりの平均消費量。60 秒ごと（システム時刻に基づく 1 分ごと）にサンプリングされた最新の 60 個のサンプルを表示します。
- **hours**：平均時間消費量。60 分ごと（システム時刻に基づく 1 時間ごと）にサンプリングされた最新の 24 個のサンプルを表示します。
- **days**：1 日の平均消費量。24 時間ごとにサンプリングされた最新の 7 つのサンプルを表示します（システム時刻に従って午前 0 時から午前 0 時まで）。
- **weeks**：1 週間の平均消費量。7 日ごと（システム時刻に基づく土曜日の午前 0 時から土曜日の午前 0 時まで）にサンプリングされた最新の 52 個のサンプルを表示します。

デフォルト設定

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

指定した時間枠の平均電力消費量を表示するには、**show power inline monitor** を使用します。

注：リロード後に保持されるのは、**days** と **weeks** のサンプルのみです。

例 1:

次に、インターフェイス gi1/0/1 について収集された過去 1 日の 1 時間あたりの平均電力消費量を表示する例を示します。

```
switchxxxxxx#  show power inline monitor consumption gi1/0/1 hours
```

Sample Time	Consumption (W)
03:00:00	7.1
02:00:00	7.1
01:00:00(~)	8.5
00:00:00	9.0

（ー）すべてのサンプルが使用できるわけではありません。

* タイムスタンプはサンプリング期間の終了を表します。

例 2：

次に、ユニット 1 について収集した過去 52 週間の 1 週間あたりの平均電力消費量を表示する例を示します。

```
switchxxxxxx#  show power inline monitor  consumption  unit 1  weeks
```

Sample Time	Consumption (W)
Sun 15/11/2015 00:00:00	55.1
Sun 22/11/2015 00:00:00	75.2
Sun 29/11/2015 00:00:00(~)	45.3

```
unit 1
```

（ー）すべてのサンプルが使用できるわけではありません。

* タイムスタンプはサンプリング期間の終了を表します。

ポート チャネル コマンド

この章は、次の項で構成されています。

- channel-group （1078 ページ）
- port-channel load-balance （1079 ページ）
- show interfaces port-channel （1080 ページ）

channel-group

ポートとポートチャネルを関連付けるには、**channel-group**インターフェイス（イーサネット）コンフィギュレーション モード コマンドを使用します。ポート チャネルからポートを削除するには、このコマンドの **no** 形式を使用します。

構文

channel-group *port-channel* **mode** {**on** | **auto**}

no channel-group

パラメータ

- ***port-channel***：参加する現在のポートのポート チャネル数を指定します。
- **mode**：ポートチャネルに参加するモードを指定します。次の値が可能です。

  on：LACP 操作をせずにチャネルにポートを強制的に参加させます。

  auto：LACP の操作結果としてポートをチャネルに強制的に参加します。

デフォルト設定

ポートはポートチャネルに割り当てられていません。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

デフォルトのモードは **on** です。

使用上のガイドライン

LACP はポート参加の管理を開始します。

auto モードが設定されていて、すべてのポート候補で受信済みの LACP メッセージがない場合、候補のいずれかが参加しています。最初のLACPメッセージを受信すると、ポートが参加解除され、LACP がポート参加の管理を開始します。

例

次に、LACP 操作をせずにポートチャネル 1 にポート gi1/0/1 を強制的に参加させる例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  channel-group 1 mode on
```

port-channel load-balance

ポート チャネリングのロードバランシング ポリシーを設定するには、**port-channel load-balance** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトにリセットするには、このコマンドの **no** 形式を使用します。

構文

port-channel load-balance *{***src-dst-mac** | **src-dst-mac-ip***}*

no port-channel load-balance

パラメータ

- **src-dst-mac**：ポート チャネル ロード バランシングは送信元と宛先 MAC アドレスに基づいています。
- **src-dst-mac-ip**：ポート チャネル ロード バランシングは、送信元と宛先の MAC および IP アドレスに基づいています。

デフォルト設定

src-dst-mac

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)#  port-channel load-balance src-dst-mac
```

show interfaces port-channel

すべてのポートチャネルまたは特定のポートチャネルのポートチャネル情報を表示するには、**show interfaces port-channel** 特権 EXEC モード コマンドを使用します。

構文

show interfaces port-channel *[interface-id]*

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID はポート チャネルにする必要があります。

コマンド モード

特権 EXEC モード

例

次の例では、すべてのポート チャネルの情報を表示します。

```
switchxxxxxx#  show interfaces port-channel
Load balancing: src-dst-mac.
Gathering information...
Channel  Ports
-------  -----
Po1      Active: 1,Inactive: gi1/0/2-3
Po2      Active: 5 Inactive: gi1/0/4
```

QoS コマンド

この章は、次の項で構成されています。

- qos （1083 ページ）
- qos advanced-mode trust （1084 ページ）
- show qos （1085 ページ）
- class-map （1086 ページ）
- show class-map （1088 ページ）
- match （1089 ページ）
- policy-map （1090 ページ）
- class （1091 ページ）
- show policy-map （1092 ページ）
- trust （1093 ページ）
- set （1094 ページ）
- redirect （1095 ページ）
- mirror （1096 ページ）
- police （1097 ページ）
- service-policy （1099 ページ）
- qos aggregate-policer （1101 ページ）
- show qos aggregate-policer （1103 ページ）
- police aggregate （1104 ページ）
- wrr-queue cos-map （1105 ページ）
- wrr-queue bandwidth （1106 ページ）
- priority-queue out num-of-queues （1107 ページ）
- traffic-shape （1108 ページ）
- traffic-shape queue （1109 ページ）
- qos wrr-queue wrtd （1110 ページ）
- show qos wrr-queue wrtd （1111 ページ）
- show qos interface （1112 ページ）
- qos map policed-dscp （1115 ページ）
- qos map dscp-queue （1116 ページ）

- qos trust（グローバル） （1117 ページ）
- qos trust（インターフェイス） （1119 ページ）
- qos cos （1120 ページ）
- qos dscp-mutation （1121 ページ）
- show qos map （1122 ページ）
- clear qos statistics （1124 ページ）
- qos statistics policer （1125 ページ）
- qos statistics aggregate-policer （1126 ページ）
- clear queue statistics （1127 ページ）
- show queue statistics （1128 ページ）
- show qos statistics （1130 ページ）

qos

デバイスでQoSを有効にしてモードを設定するには、**qos** グローバル コンフィギュレーション モード コマンドを使用します。デバイス上の QoS を無効にするには、このコマンドの **no** 形式を使用します。

構文

qos [**basic** | {**advanced** [**ports-not-trusted** | **ports-trusted**]}]

no qos

パラメータ

- **basic**：QoS の基本モード。オプションが指定されていない場合は、QoS モードが基本モードにデフォルト設定されます。
- **advanced**：QoS 拡張モードを指定します。QoS 設定のすべての範囲を有効にします。
- **ports-not-trusted**：拡張モードのみに関連します。ポリシー マップ ルールによって QoS アクションに分類されるパケットが、出力キュー 0 にマッピングされていることを示します。これは、拡張モードのデフォルト設定です。
- **ports-trusted**：拡張モードにのみ関連します。ポリシー マップ ルールによって QoS アクションに分類されるパケットが、パケットのフィールドに基づいて出力キューにマッピングされていることを示します。信頼モードを指定するには、qos advanced-mode trust （1084 ページ） コマンドを使用します。

デフォルト設定

QoS 基本モード

コマンド モード

グローバル コンフィギュレーション モード

例 1：次の例では、デバイスの QoS を無効にします。

```
switchxxxxxx(config)#  no qos
```

例 2：次の例では、**ports-not-trusted** オプションを使用してデバイスの QoS 拡張モードを有効にします。

```
switchxxxxxx(config)# qos advanced
```

qos advanced-mode trust

qos advanced-mode trust グローバル コンフィギュレーション モード コマンドを使用すると、拡張モードで信頼モードを設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

qos advanced-mode trust {**cos** | **dscp** | **cos-dscp**}

no qos advanced-mode trust

パラメータ

- **cos**：パケットの CoS 値で入力パケットを分類します。タグなしパケットの場合、ポートのデフォルト CoS が使用されます。
- **dscp**：パケットの DSCP 値で入力パケットを分類します。
- **cos-dscp**：IP パケットのパケット DSCP 値で入力パケットを分類します。その他のパケット タイプの場合は、パケット CoS 値を使用します。

デフォルト設定

cos-dscp

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

設定は、次の場合に拡張モードに関係します。

- **ports-not-trusted mode**：QoS アクション信頼に分類されるパケットの場合。
- **ports-trusted mode**：QoS アクションに分類されないパケット、または QoS アクション信頼に分類されるパケットの場合。

例

次の例では、デバイス上の QoS の信頼モードとして **cos** を設定します。

```
switchxxxxxx(config)# qos advanced-mode trust cos
```

show qos

show qos 特権 EXEC モード コマンドを使用すると、デバイスの QoS 情報を表示できます。信頼モードは QoS 基本モードで表示されます。

構文

show qos

デフォルト設定

コマンド モードは無効です

コマンド モード

特権 EXEC モード

使用上のガイドライン

信頼モードは、QoS が基本モードで有効になっている場合に表示されます。

例

```
switchxxxxxx(config)# show qos
Qos: Disabled
switchxxxxxx(config)# show qos
Qos: Basic mode
Basic trust: dscp
switchxxxxxx(config)# show qos
Qos: Advanced mode
Advanced mode trust type: cos
Advanced mode ports state: Trusted
```

class-map

class-map グローバル コンフィギュレーション モード コマンドを使用すると、クラス マップを作成または変更し、クラスマップ コンフィギュレーション モードを開始できます（QoS が拡張モードの場合にのみ利用可能）。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

構文

class-map *class-map-name* [**match-all** | **match-any**]

no class-map *class-map-name*

パラメータ

- ***class-map-name***：クラス マップ名を指定します。（長さ：1 ～ 32 文字）
- **match-all**：このクラス マップに属する ACL のすべての基準の論理 AND 演算を実行します。このクラス マップ内のすべての一致基準と一致する必要があります。**match-all** と **match-any** のどちらも指定されていない場合は、**match-all** パラメータがデフォルトで選択されます。
- **match-any**：このクラス マップに属する ACL の基準の論理 OR 演算を実行します。このクラス マップ内の 1 つの一致基準とだけ一致する必要があります。

デフォルト設定

クラス マップはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

インターフェイスごとに適用される、グローバルに名前が付けられたサービス ポリシーの一部として、パケットの分類、マーキング、および集約ポリシングを定義する場合は、**class-map** コマンドおよびそのサブコマンドを使用します。

クラス マップは 1 つまたは複数の ACL から構成されます。ACL で指定した一部またはすべての基準と一致するパケットを特定して、トラフィック フローを定義します。

すべてのクラス マップ コマンドは、QoS が拡張モードの場合にのみ利用可能です。

class-map はクラスマップ コンフィギュレーション モードを開始します。このモードでは、最大 2 つの **match** コマンドを開始して、このクラスの基準を設定できます。**match** ごとに ACL を指定します。

いくつかの **match** コマンドを使用する場合、各コマンドで、1 つの IP ACL、1 つの IPv6 ACL、1 つの MAC ACL など、さまざまなタイプの ACL を指定する必要があります。分類は最初の一致で決まるため、ACL の順序が重要です。

次の場合には、エラー メッセージが生成されます。

- **match-all** クラス マップに複数の match （1089 ページ） クラス マップが存在する場合

  参加している ACL 内で分類フィールドが繰り返されている場合。

クラスマップ コンフィギュレーション モードの開始後、次のコンフィギュレーション コマンドが利用可能になります。

- **exit**：クラスマップ コンフィギュレーション モードを終了します。
- match （1089 ページ）：分類基準を設定します。
- **no**：クラス マップから一致ステートメントを削除します。

例

次の例では、Class1 と呼ばれるクラス マップを作成し、パケットが指定した ACL 内のすべての分類基準と一致することを確認するように設定します。

```
switchxxxxxx(config)# class-map class1 match-all
switchxxxxxx(config-cmap)# match access-group acl-name
```

show class-map

show class-map 特権 EXEC モード コマンドは、QoS が拡張モードの場合にすべてのクラス マップを表示します。

構文

show class-map [*class-map-name*]

パラメータ

class-map-name：表示されるクラス マップの名前を指定します。（長さ：1 ～ 32 文字）

コマンド モード

特権 EXEC モード

例

次の例では、Class1 のクラス マップを表示します。

```
switchxxxxxx(config)# show class-map
Class Map matchAny class1
   Match access-group mac
```

match

match クラスマップ コンフィギュレーション モード コマンドを使用すると、設定しているクラスマップに属する ACL をバインディングできます。ACL を削除するには、このコマンドの **no** 形式を使用します。

構文

match access-group *acl-name*

no match access-group *acl-name*

パラメータ

acl-name：MAC、IP ACL 名、または IPv6 ACL 名を指定します（長さ：1 ～ 32 文字）

デフォルト設定

一致基準はサポートされていません。

使用上のガイドライン

このコマンドは、デバイスが QoS 拡張モードの場合のみ利用可能です。

コマンド モード

クラスマップ コンフィギュレーション モード。

例

次の例では、Class1 と呼ばれるクラス マップを定義します。Class1 には **enterprise** と呼ばれる ACL が含まれます。**enterprise** のすべての基準と一致するトラフィックのみがクラス マップに属します。

```
switchxxxxxx(config)#  class-map class1
switchxxxxxx(config-cmap)#  match access-group enterprise
```

policy-map

policy-map グローバル コンフィギュレーション モード コマンドを使用すると、ポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始できます。ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

構文

policy-map *policy-map-name*

no policy-map *policy-map-name*

パラメータ

policy-map-name：ポリシー マップ名を指定します。（長さ：1 ～ 32 文字）

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは QoS が拡張モードのときにのみ使用できます。

policy-map グローバル コンフィギュレーション モード コマンドを使用すると、一致基準がクラスマップで定義されているクラスのポリシーを設定する前に、作成、追加、または変更するポリシー マップの名前を指定できます。ポリシー マップには、1 つまたは複数のクラス マップ、およびパケットがクラスマップと一致する場合に実行するアクションが含まれます。ポリシー マップは、ポート/ポートチャネルにバインディングできます。ポリシー マップは入力パスに対して適用されます。

一致基準はクラス マップ用です。サポートされるポリシー マップは、インターフェイスごとに 1 つだけです。同じポリシーマップを複数のインターフェイスおよび方向に適用できます。

例

次の例では、Policy1 と呼ばれるポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。

```
switchxxxxxx(config)#  policy-map policy1
switchxxxxxx(config-pmap)#
```

class

policy-map （1090 ページ） コマンドの後に **class** ポリシーマップ コンフィギュレーション モード コマンドを使用すると、ACL を policy-map に接続できます。ポリシー マップからクラス マップを切り離すには、このコマンドの **no** 形式を使用します。

構文

class *class-map-name* [**access-group** *acl-name*]

no class *class-map-name*

パラメータ

- **class-map-name**：既存のクラス マップの名前を指定します。クラス マップが存在しない場合、新しいクラス マップは指定した名前の下に作成されます。（長さ：1 ～ 32 文字）
- **access-group** *acl-name*：IP、IPv6、または MAC アクセス コントロール リスト（ACL）の名前を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

ポリシー マップのクラス マップが定義されていません。

コマンド モード

ポリシーマップ コンフィギュレーション モード。

使用上のガイドライン

このコマンドは QoS が拡張モードのときにのみ使用できます。

これは、クラス マップを作成し、ポリシー マップにバインドする作業と同じです。

このコマンドの既存クラス マップを指定するか、**access-group** パラメータを使用して新しいクラス マップを作成できます。

ポリシーマップを定義すると、service-policy （1099 ページ） コマンドを使用してポート/ポート チャネルに接続します。

例

次の例では、**enterprise** と呼ばれる ACL を含む、**class1** と呼ばれるトラフィック分類（クラス マップ）を定義します。クラスは、**policy1** と呼ばれるポリシーマップ内にあります。ポリシーマップ **policy1** に ACL **enterprise** が含まれるようになりました。

```
switchxxxxxx(config)#  policy-map policy1
switchxxxxxx(config-pmap)#  class class1 access-group enterprise
```

show policy-map

show policy-map 特権 EXEC モード コマンドを使用すると、すべてのポリシー マップまたは特定のポリシー マップを表示できます。

このコマンドは QoS が拡張モードのときにのみ使用できます。

構文

show policy-map [*policy-map-name*]

パラメータ

policy-map-name：ポリシー マップ名を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

すべてのポリシーマップが表示されます。

コマンド モード

特権 EXEC モード

例

次に、すべてのポリシー マップを表示する例を示します。

```
switchxxxxxx(config)#   show policy-map
Policy Map policy1
class class1
set dscp 7
Policy Map policy2
class class 2
police 96000 4800 exceed-action drop
class class2
redirect gi1/0/2
class class 3
police 96000 4800 exceed-action policed-dscp-transmit peak 128000 9600 violate-action
policed-dscp-transmit
```

trust

trust ポリシーマップ クラス コンフィギュレーション モード コマンドを使用すると、信頼状態を設定できます。デフォルトの信頼状態に戻すには、このコマンドの**no**形式を使用します。

構文

trust

no trust

デフォルト設定

デフォルトの状態は、qos コマンドで選択されたモード（拡張モード）に従います。信頼のタイプは qos advanced-mode trust で決定されます。

コマンド モード

ポリシーマップ クラス コンフィギュレーション モード。

使用上のガイドライン

このコマンドは、QoS が ports-not-trusted 拡張モードの場合にのみ関連します。trust は、トラフィックがパケットの QoS パラメータ（UP または DSCP）に応じてキューに送信されることを示します。

特定のトラフィックの QoS の trust 動作を他のトラフィックと区別するために、このコマンドを使用します。たとえば、特定の DSCP 値を持つ着信トラフィックが信頼されます。クラスマップは、着信トラフィックの DSCP 値と一致して信頼するように設定できます。

例

次に、ACL を作成してクラスマップに配置し、そのクラスマップをポリシーマップに配置して信頼状態を設定する例を示します。

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)#  permit ip any any
switchxxxxxx(config-ip-al)#  exit
switchxxxxxx(config)#  class-map c1
switchxxxxxx(config-cmap)#  match access-group ip1
switchxxxxxx(config-cmap)#  exit
switchxxxxxx(config)#  policy-map p1
switchxxxxxx(config-pmap)#  class c1
switchxxxxxx(config-pmap-c)#  trust
```

set

set ポリシーマップ クラス コンフィギュレーション モード コマンドを使用すると、QoS が DSCP 値として使用する値や出力キューを選択したり、ユーザ プライオリティ値を設定したりできます。

構文

set {**dscp** *new-dscp* | **queue** *queue-id* | **cos** *new-cos*}

no set

パラメータ

- **dscp** new-dscp：分類したトラフィックの新しい DSCP 値を指定します。(範囲：0 ～ 63)
- **queue** *queue-id*：出力キューを指定します。（範囲：1 ～ 8）
- **cos** new-cos：パケット内でマークする新しいユーザ優先順位を指定します。（範囲：0 ～ 7）

コマンド モード

ポリシーマップ クラス コンフィギュレーション モード。

使用上のガイドライン

このコマンドは QoS が拡張モードのときにのみ使用できます。

set （1094 ページ） および trust （1093 ページ） コマンドは、同じポリシーマップ内で相互排他的です。

コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

イーグレス ポリシーでは **queue** キーワードはサポートされていません。

例

次の例では、ACL を作成し、クラス マップに配置して、このクラス マップをポリシー マップに配置し、p1 と呼ばれるポリシー マップ内のクラスに対して、パケットの DSCP 値を 56 に設定します。

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# set dscp 56
```

redirect

特定のイーサネット ポートまたはポート チャネルにトラフィック フローをリダイレクトするには、**redirect** ポリシーマップ クラス コンフィギュレーション モード コマンドを使用します。

構文

redirect *interface-id*

no redirect

パラメータ

- ***interface-id***：フローをリダイレクトする先のイーサネット ポートまたはポート チャネルを指定します。

コマンド モード

ポリシーマップ クラス コンフィギュレーション モード。

使用上のガイドライン

フレームが割り当てられている VLAN にフレームをリダイレクトするには、**redirect** コマンドを使用します。

このコマンドは QoS が拡張モードのときにのみ使用できます。

例

次に、ACL を作成してそれをクラスマップに配置し、クラスマップをポリシーマップに配置し、フローをイーサネット ポート gi1/0/2 にリダイレクトする例を示します。

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# redirect gi1/0/2
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
switchxxxxxx(config)#
```

mirror

アナライザ イーサネット ポートへのトラフィックフローをミラーリングするには、**mirror** ポリシーマップ クラス コンフィギュレーション モード コマンドを使用します。

構文

mirror *session_number*

no mirror

パラメータ

- *session_number*：SPAN セッションまたは RSPAN セッションで識別したセッション番号を指定します。使用できる値は 1 のみです。

コマンド モード

ポリシーマップ クラス コンフィギュレーション モード。

使用上のガイドライン

このコマンドは QoS が拡張モードのときにのみ使用できます。

この ACL のコマンド（permit または deny）に関係なく、フレームがクラスの ACL のいずれかに一致する場合、そのフレームは同じ形式でミラーリングされます。

VLAN と フローミラーリングからの 1 つの送信元セッションのみがサポートされます。

例

次に、ACL を作成してクラスマップに配置し、そのクラスマップをポリシーマップに配置して、セッション 2 で定義されたアナライザ イーサネット ポートへのフローをミラーリングする例を示します。

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# mirror 2
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
switchxxxxxx(config)#
```

police

police ポリシーマップ クラス コンフィギュレーション モード コマンドを使用すると、分類したトラフィックのポリサーを定義できます。ここでは、ポリシーマップ（クラスマップごと）にアクションの別のグループを定義します。ポリサーを削除するには、このコマンドの **no** 形式を使用します。

構文

police *committed-rate-kbps committed-burst-byte* [**exceed-action** *action*] [**peak** *peak-rate-kbps peak-burst-byte* [**violate-action** *action*]]

no police

パラメータ

- ***committed-rate-kbps***：平均トラフィックレート（CIR）を kbit/秒（bps）で指定します。（範囲：3 ～ 最大ポート速度）
- ***committed-burst-byte***：通常のバースト サイズ（CBS）をバイト単位で指定します。（範囲：3000 ～ 19173960）
- **exceed-action**：認定レートを超過し、ピーク レートの超過がない場合に実行するアクションを指定します。キーワードが設定されていない場合は、次のアクションが適用されます。

  drop（**peak** キーワードが設定されていない場合）。

  policed-dscp-transmit（**peak** キーワードが設定されている場合）。
- **peak**：2 レート 3 色のポリサーを指定します。ピーク レートを超過している場合、パケットはドロップされます。
- ***peak-rate-kbps***：平均トラフィックレート（CIR）を kbit/秒（bps）で指定します。（範囲：3 ～ 最大ポート速度）
- ***peak-burst-byte***：ピーク バースト サイズ（PBS）をバイト単位で指定します。（範囲：3000 ～ 19173960）
- **violate-action**：ピーク レートを超過した場合に実行するアクションを指定します。キーワードが設定されていない場合、**drop** アクションが適用されます。
- *action*：トークンアクションを指定します。次の値が可能です。

  drop：パケットをドロップします。

  policed-dscp-transmit：IP トラフィックのパケット DSCP にコメントを付けます。DSCP へのコメント付けは、**qos map policed-dscp** コマンドを使用して、違反アクションには **violation** キーワードを使用し、超過アクションにはこのキーワードを使用せずに設定します。DSCP へのコメント付けは、モードが信頼できる DSCP の場合にのみ有効です。

デフォルトの使用

ポリサーなし

コマンド モード

ポリシーマップ クラス コンフィギュレーション モード。

使用上のガイドライン

このコマンドは、policy-map（1090ページ）と class（1091ページ）コマンドの後に使用します。

このコマンドは QoS が拡張モードのときにのみ使用できます。

ポリシングは、トークン バケット アルゴリズムを使用します。

例 1。次の例では、分類されたトラフィックのポリサーを定義します。トラフィック レートが 124,000 kbps を超え、通常のバースト サイズが 9600 バイトを超えると、パケットはドロップされます。クラスは class1 と呼ばれ、policy1 と呼ばれるポリシー マップ内にあります。

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class cls1
switchxxxxxx(config-pmap-c)# police 124000 9600 exceed-action drop
```

例 2。次の例では、分類されたトラフィックの 2 レート 3 色のポリサーを定義します。認定トラフィック レートが 124,000 kbps を超え、認定バースト サイズが 9600 バイトを超えると、パケットはマークされます。ピークトラフィックレートが 200,000 kbps を超えており、ピークバーストサイズが 19200 バイトを超えている場合にパケットがマークされます。クラスは class1 と呼ばれ、policy1 と呼ばれるポリシー マップ内にあります。

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class cls1
switchxxxxxx(config-pmap-c)# police 124000 9600 exceed-action policed-dscp-transmit peak
 200000 19200 violate-action policed-dscp-transmi
```

service-policy

service-policy インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用すると、ポリシー マップをインターフェイスにバインディングできます。インターフェイスからポリシー マップを切り離すには、このコマンドの **no** 形式を使用します。

構文

service-policy {**input** | **output**} *policy-map-name* [**default-action** {**permit-any** | **deny-any**}]

no service-policy input | **output**

service-policy {**input** | **output**} *policy-map-name*

パラメータ

- **input**：入力ポリシーを指定します。
- **output**：イーグレス ポリシーを指定します。
- ***policy-map-name***：入力インターフェイスに適用するポリシーマップ名を指定します。（長さ：1 ～ 32 文字）
- **default-action**：デフォルト アクションを指定します。キーワードが設定されていない場合は、**deny-any** デフォルト アクションが適用されます。
- **deny-any**：ポリシー内のルールに一致しない（ポートの入力である）すべてのパケットを拒否します。
- **permit-any**：ポリシー内のルールに一致しない（ポートの入力である）すべてのパケットを送信します。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

デフォルト

ポリシー マップはバインドされていません。

使用上のガイドライン

このコマンドは QoS 拡張モードでのみ使用できます。

方向ごとのインターフェイスごとに適用できるポリシー マップは 1 つだけです。

バインドポリシーにイーグレスポリシーでサポートされていないアクションが含まれている場合、**service-policy output** コマンドは失敗します。

ポリシーマップを入力および出力として同時にバインドすることはできません。

例

次の例では、Policy1 というポリシー マップを入力インターフェイスにアタッチします。

```
switchxxxxxx(config-if)# service-policy input policy1
```

次の例では、Policy1 というポリシー マップを入力インターフェイスにアタッチし、ポリシーのルールを満たしていないすべてのパケットを転送します。

```
switchxxxxxx(config-if)# service-policy input policy1 permit-any
```

次の例では、Policy2 というポリシー マップを出力インターフェイスにアタッチします。

```
switchxxxxxx(config-if)# service-policy output policy2
```

qos aggregate-policer

qos aggregate-policer グローバル コンフィギュレーション モード コマンドを使用すると、複数のトラフィック クラスに適用できるポリサー パラメータを定義できます。既存の集約ポリサーを削除するには、このコマンドの **no** 形式を使用します。

構文

qos aggregate-policer *aggregate-policer-name committed-rate-kbps committed-burst-byte* [**exceed-action** *action*] [**peak** *peak-rate-kbps peak-burst-byte* [**violate-action** *action*]]

no qos aggregate-policer *aggregate-policer-name*

パラメータ

- ***aggregate-policer-name***：集約ポリサー名を指定します。（長さ：1 ～ 32 文字）
- ***committed-rate-kbps***：平均トラフィック レート（CIR）をキロビット/秒（bps）で指定します。（範囲：3 ～ 57982058）
- ***committed-burst-byte***：通常のバースト サイズ（CBS）をバイト単位で指定します。（範囲：3000 ～ 19173960）
- **exceed-action**：認定レートを超過し、ピーク レートの超過がない場合に実行するアクションを指定します。キーワードが設定されていない場合は、次のアクションが適用されます。

  drop（**peak** キーワードが設定されていない場合）。

  policed-dscp-transmit（**peak** キーワードが設定されている場合）。
- **peak**：2 レート 3 色のポリサーを指定します。ピーク レートを超過している場合、パケットはドロップされます。
- ***peak-rate-kbps***：平均トラフィック レート（CIR）をキロビット/秒（bps）で指定します。（範囲：3 ～ 57982058）
- ***peak-burst-byte***：ピーク バースト サイズ（PBS）をバイト単位で指定します。（範囲：3000 ～ 19173960）
- **violate-action**：ピーク レートを超過した場合に実行するアクションを指定します。キーワードが設定されていない場合、**drop** アクションが適用されます。
- ***action***：トークン アクションを指定します。次の値が可能です。
  - **drop**：パケットをドロップします。
  - **policed-dscp-transmit**：IP トラフィックのパケット DSCP にコメントを付けます。DSCP へのコメント付けは、**qos map policed-dscp** コマンドを使用して、違反アクションには **violation** キーワードを使用し、超過アクションにはこのキーワードを使用せずに設

定します。DSCP へのコメント付けは、モードが信頼できる DSCP の場合にのみ有効です。

デフォルト設定

集約ポリサーは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは QoS が拡張モードのときにのみ使用できます。

qos aggregate-policer コマンドを使用すると、複数のクラス マップからトラフィックを集約するポリサーを定義できます。

集約ポリサーは複数のデバイスからをトラフィックを集約できません。集約ポリサーを複数のデバイスに適用する場合、各デバイスのトラフィックは個別にカウントされ、デバイスごとに制限されます。

同じデバイス上で異なる2つのポートのトラフィックは、ポリシングのために集約できます。

集約ポリサーは、同一ポリシー マップ内の複数のクラスに適用できます。

集約ポリサーがポリシー マップで使用されている場合は削除することはできません。**no qos aggregate-policer** コマンドを使用する前に、**no police aggregate** ポリシーマップ コンフィギュレーション モード コマンドは、すべてのポリシー マップから集約ポリサーを削除するために使用する必要があります。

ポリシングは、トークン バケット アルゴリズムを使用します。CIR は、トークンをバケットに追加する速度を表します。CBS は、バケットの深さを表します。

例 1。次の例では、同じポリシー マップ内で複数のクラスに適用できる policer1 と呼ばれるポリサーのパラメータを定義します。平均トラフィック レートが 124,000 kbps を超えたり、通常のバースト サイズが 9600 バイトを超えたりする場合、パケットはドロップされます。

```
switchxxxxxx(config)# qos aggregate-policer policer1 124000 9600 exceed-action drop
```

例 2。次の例では、同じポリシー マップ内の複数のクラスに適用できる policer2 という2レート3色ポリサーのパラメータを定義します。平均トラフィック レートが 124,000 kbps を超えるか、または通常バースト サイズが 9600 バイトを超えると、パケットは再マークされます。平均トラフィック レートが 200,000 kbps を超えるか、または通常バースト サイズが 9600 バイトを超えると、パケットはドロップされます。

```
switchxxxxxx(config)# qos aggregate-policer policer2 124000 9600 exceed-action
policed-dscp-transmit peak 200000 19200 violate-action policed-dscp-transmit
```

show qos aggregate-policer

show qos aggregate-policer 特権 EXEC モード コマンドを使用すると、集約ポリサーを表示できます

このコマンドは QoS 拡張モードでのみ使用できます。

構文

show qos aggregate-policer [*aggregate-policer-name*]

パラメータ

aggregate-policer-name：集約ポリサー名を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

すべてのポリサーが表示されます。

コマンド モード

特権 EXEC モード

例 1。次の例では、Policer1 という集約ポリサーのパラメータを表示します。

```
switchxxxxxx# show qos aggregate-policer policer1
aggregate-policer policer1 96000 4800 exceed-action drop
```

not used by any policy map.

例 2。次の例では、Policer1 という集約 2 レート 3 色ポリサーのパラメータを表示します。

```
switchxxxxxx# show qos aggregate-policer policer1
aggregate-policer policer1 124000 9600 exceed-action policed-dscp-transmit peak 200000
19200 violate-action policed-dscp-transmit
```

not used by any policy map.

police aggregate

police aggregate ポリシーマップ クラス コンフィギュレーション モード コマンドを使用すると、同じポリシー マップ内の複数のクラス マップに集約ポリサーを適用できます。ポリシー マップから既存の集約ポリサーを削除するには、このコマンドの **no** 形式を使用します。

このコマンドは QoS 拡張モードでのみ使用できます。

構文

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

パラメータ

aggregate-policer-name：集約ポリサー名を指定します。（長さ：1 ～ 32 文字）

コマンド モード

ポリシーマップ クラス コンフィギュレーション モード。

使用上のガイドライン

集約ポリサーは、同一ポリシーマップ内の複数のクラスに適用できます。複数のポリシーマップまたはインターフェイス全体に集約ポリサーを適用することはできません。

コンフィギュレーションモードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

例

次の例では、Policer1 と呼ばれる集約ポリサーを、ポリシー マップ policy1 で class1 と呼ばれるクラスおよびポリシー マップ policy2 で class2 と呼ばれるクラスに適用します。

```
switchxxxxxx(config)# qos aggregate-policer policer1 124000 9600 exceed-action drop
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1
switchxxxxxx(config-pmap-c)# police aggregate policer1
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
switchxxxxxx(config)# policy-map policy2
switchxxxxxx(config-pmap)# class class2
switchxxxxxx(config-pmap-c)# police aggregate policer1
```

wrr-queue cos-map

wrr-queue cos-map グローバル コンフィギュレーション モード コマンドを使用すると、サービス クラス（CoS）値を特定の出力キューにマップできます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

wrr-queue cos-map *queue-id cos0... cos7*

no wrr-queue cos-map [*queue-id*]

パラメータ

- **queue-id**：CoS 値のマップ先のキュー番号を指定します。
- **cos0... cos7**：指定したキュー番号にマップする最大 8 個の CoS 値を指定します。（範囲：0 ～ 7）

デフォルト設定

8 個のキューにマップするデフォルトの CoS 値は次のとおりです。

CoS 値 0 はキュー 1 へマッピングされます。

CoS 値 1 はキュー 2 へマッピングされます。

CoS 値 2 はキュー 3 へマッピングされます。

CoS 値 3 はキュー 6 へマッピングされます。

CoS 値 4 はキュー 5 へマッピングされます。

CoS 値 5 はキュー 8 へマッピングされます。

CoS 値 6 はキュー 8 にマッピングされます。

CoS 値 7 はキュー 7 へマッピングされます

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、異なるキューにトラフィックを配布できます。

例

次の例では、CoS 値 4 と 6 をキュー 2 にマップします。

```
switchxxxxxx(config)# wrr-queue cos-map 2 4 6
```

wrr-queue bandwidth

wrr-queue bandwidth グローバル コンフィギュレーション モード コマンドを使用すると、加重ラウンド ロビン（WRR）の加重を出力キューに割り当てることができます。重み比率により、パケット スケジューラは各キューからパケットを削除する頻度が決定されます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

wrr-queue bandwidth *weight1 weight2... weighting*

no wrr-queue bandwidth

パラメータ

weight1 weight1... weighting：WRR パケット スケジューラによってパケット キューに割り当てられた帯域幅の比率です。ユーザ ガイドラインの説明を参照してください。各値はスペースで区切ります。(各ウェイトの範囲：0 ～ 255）

デフォルト設定

wrr はデフォルトでは無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

各キューの比率は、すべてのキューの重みの合計（正規化された重み）で割られたキューのウェイトとして定義されます。これにより、各キューの帯域幅割り当てが設定されます。

緊急キューを除いたすべてのキューが WRR に参加します。これに対応する重みは比率計算に使用しません。

緊急キューは優先キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。緊急キューは、priority-queue out num-of-queues （1107 ページ） コマンドによって指定されます。

例

次は、WRR 値をキューに割り当てます。

```
switchxxxxxx(config)# priority-queue out num-of-queues 0
switchxxxxxx(config)# wrr-queue bandwidth 6 6 6 6 6 6 6 6
```

priority-queue out num-of-queues

priority-queue out num-of-queues グローバル コンフィギュレーション モード コマンドを使用すると、緊急キューの数を設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

priority-queue out num-of-queues *number-of-queues*

no priority-queue out num-of-queues

パラメータ

- **number-of-queues**：緊急（絶対優先）キューの数を指定します。緊急キューは、インデックス数の高いキューに割り当てられます。（範囲：0 ～ 8。wrr キューの数は 0 または複数にする必要があります。

  number-of-queues = 0 の場合はすべてのキューが相対的優先転送（wrr の重みに従う）、**number-of-queues** = 8 の場合がすべてのキューが完全優先（絶対優先キュー）になります。

デフォルト設定

すべてのキューが緊急キューです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

緊急キューは絶対優先キューであり、優先度の低い他のキューのサービスが提供される前に空になるまでサービスを提供します。

加重ラウンドロビン（WRR）の重み比率は、WRR に参加するキューが少ないため、緊急キューの数に影響を受けます。これは、**wrr-queue bandwidth** インターフェイス コンフィギュレーション モード コマンドで対応する重みが（比率計算で使用されずに）無視されていることを示します。

例

次の例では、緊急キューの数を 2 に設定しています。

```
switchxxxxxx(config)#  priority-queue out num-of-queues 2
```

traffic-shape

出力ポート シェーパーを設定するには、**traffic-shape** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。シェーパーを無効にするには、このコマンドの **no** 形式を使用します。

構文

traffic-shape *committed-rate* [*committed-burst*]

no traffic-shape

パラメータ

- **committed-rate**：最大平均トラフィック レート（CIR）を kbit/秒（kbps）単位で指定します。（範囲：GE：64 kbps ～ 最大ポート速度、10 GE：64 Kbps ～ 最大ポート速度）
- **committed-burst**：最大許容超過バースト サイズ（CBS）をバイト単位で指定します。（範囲：4096 ～ 16670940 バイト）

デフォルト設定

シェーパーは無効です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

出力ポート シェーパーは、ポートのトラフィック送信レート（Tx レート）を制御します。

例

次に、平均トラフィック レートが 64 kbps を超えた場合、または通常のバースト サイズが 4096 バイトを超えた場合に、gi1/0/1 のトラフィック シェーパーを設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)#  traffic-shape 64 4096
```

traffic-shape queue

出力キュー シェーパーを設定するには、**traffic-shape queue** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。シェーパーを無効にするには、このコマンドの **no** 形式を使用します。

構文

traffic-shape queue *queue-id committed-rate* [*committed-burst*]

no traffic-shape queue *queue-id*

パラメータ

queue-id：シェーパーの割り当て先のキュー番号を指定します。（範囲：1 ～ 8）。

- **committed-rate**：平均トラフィック レート（CIR）を kbits/秒（kbps）で指定します。（範囲：64 kbps - 最大ポート速度）
- **committed-burst**：超過バースト サイズ（CBS）をバイト単位で指定します。（範囲：4096 ～ 16670940 バイト）

デフォルト設定

シェーパーは無効です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

出力ポート シェーパーは、ポートのキューのトラフィック送信レート（Tx レート）を制御します。

例

次に、平均トラフィック レートが 124000 kbps を超えるか、または通常のバースト サイズが 9600 バイトを超える場合に gi1/0/1 のキュー 1 のシェイパーを設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)#  traffic-shape queue 1 64 4096
```

qos wrr-queue wrtd

qos wrr-queue wrtd グローバル コンフィギュレーション モード コマンドを使用すると、重み付けランダム テール ドロップを有効にできます。WRTD を無効にするには、このコマンドの **no** 形式を使用します。

構文

qos wrr-queue wrtd

no qos wrr-queue wrtd

デフォルト

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

コマンドはリセット後に有効になります。

例

```
switchxxxxxx(config)# qos wrr-queue wrtd
This setting will take effect only after copying running configuration to startu
p configuration and resetting the device
switchxxxxxx(config)#
```

show qos wrr-queue wrtd

重み付けランダムテールドロップ（WRTD）設定を表示するには、**show qos wrr-queue wrtd** 特権 EXEC モードコマンドを使用します。

構文

show qos wrr-queue wrtd

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx(config)# show qos wrr-queue wrtd
 Weighted Random Tail Drop is disabled
 Weighted Random Tail Drop will be enabled after reset
```

show qos interface

show qos interface 特権 EXEC モード コマンドを使用すると、インターフェイスに Quality of Service（QoS）情報を表示できます。

構文

show qos interface [**buffers** | **queueing** | **policers** | **shapers**] [*interface-id*]

パラメータ

- **buffers**：インターフェイスのキューのバッファ設定を表示します。GE ポートの場合、各キューの深さを表示します。
- **queueing**：キューの戦略（WRR または EF）、WRR キューの重み付け、CoS/キュー マップ、EF 優先度を表示します。
- **policers**：このインターフェイスで設定されたすべてのポリサー、その設定、現在未使用のポリサーの数（VLAN 上）を表示します。
- **shapers**：指定したインターフェイスのシェーパーと、指定したインターフェイス上のキューのシェーパーを表示します。
- ***interface-id***：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポートチャネルのいずれかのタイプを指定できます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

show qos interface コマンドでパラメータを指定していない場合は、ポート QoS モード（信頼済み DSCP、信頼済み CoS、非信頼など）、デフォルトの CoS 値、ポートに接続されている DSCP/DSCP 変換マップ（存在する場合）、インターフェイスに接続されているポリシー マップ（存在する場合）が表示されます。特定のインターフェイスが指定されていない場合は、すべてのインターフェイスの情報が表示されます。

ポリサー、シェーパー、レート制限の場合、デフォルト設定に含まれないポートのみが表示されます。

例 1：次に、**show qos interface** コマンドの出力例を示します。

```
switchxxxxxx(config)# show qos interface gi1/0/1
Ethernet gi1/0/0/1
Default CoS: 0
Trust mode: disabled
Ingress Policy applied: AV1
Egress Policy applied: AV2
Default ACE ingress action: deny-all
Default ACE egress action: deny-all
```

例 2：次に、4 つのキューに対する **show qos interface queueing** コマンドの出力例を示します。

```
switchxxxxxx(config)# show qos interface queueing gi1/0/1
Ethernet gi1/0/0/1
wrr bandwidth weights and EF priority:
qid-weights      Ef - Priority
1 - N/A          ena- 1
2 - N/A          ena- 2
3 - N/A          ena- 3
4 - N/A          ena- 4
Cos-queue map:
cos-qid
0 - 1
1 - 1
2 - 2
3 - 3
4 - 3
5 - 4
6 - 4
7 - 4
```

例 3：次に、8 つのキューに対する **show qos interface buffers** コマンドの出力例を示します。

```
switchxxxxxx(config)# show qos interface buffers gi1/0/1
gi1/0/1
Notify Q depth:
buffers gi1/0/1
Ethernet gi1/0/1
qid  thresh0  thresh1  thresh2
1    100      100      80
2    100      100      80
3    100      100      80
4    100      100      80
5    100      100      80
6    100      100      80
7    100      100      80
8    100      100      80
```

例 4：次に、**show qos interface shapers** コマンドの出力例を示します。

```
switchxxxxxx(config)# show qos interface shapers gi1/0/1
gi1/0/1
Port shaper: enable
Committed rate: 64 kbps
Committed burst: 9600 bytes
```

QID	Status	Target Committed Rate [kbps]	Target Committed Burst [bytes]
1	Enable	64	17000
2	Disable	N/A	N/A
3	Enable	N/A	N/A
4	Disable	N/A	N/A
5	Disable	N/A	N/A
6	Disable	N/A	N/A
7	Enable	N/A	N/A
8	Enable	N/A	N/A
		N/A	N/A
		N/A	N/A

例 5：次に、**show qos interface policer** の出力例を示します

```
switchxxxxxx(config)#   show qos interface policer gi1/0/1
Ethernet gi1/0/1
Ingress Policers:
Class map: A
Policer type: aggregate
Commited rate: 19 kbps
Commited burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Class map: B
Policer type: single
Commited rate: 19 kbps
Commited burst: 9600 bytes
Peak rate: 26 kbps
Peak burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Violate-action: drop
Class map: C
Policer type: none
Egress Policers:
Class map: D
```

qos map policed-dscp

qos map policed-dscp グローバル コンフィギュレーション モード コマンドを使用すると、コメントを追加できるようにポリシングした DSCP マップを設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

qos map policed-dscp [**violation**] *dscp-list* **to** *dscp-mark-down*

no qos map policed-dscp [**violation**] [*dscp-list*]

パラメータ

- **violation**：違反アクションでの DSCP 再マッピングを指定します。キーワードが設定されていない場合、このコマンドは超過アクションにおける DSCP 再マッピングを指定します。
- ***dscp-list***：最大 8 つの DSCP 値をスペースで区切って指定します。（範囲：0 ～ 63）
- ***dscp-mark-down***：マークダウンする DSCP 値を指定します。(範囲：0 ～ 63)

デフォルト設定

デフォルトのマップは、各着信の DSCP 値が同じ DSCP 値にマッピングされていることを意味する Null マップです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

元の DSCP 値とポリシングした DSCP 値は、並べ替えを回避するために同じキューにマップする必要があります。

例

次の例では、ポリシングした DSCP マップで着信 DSCP 値 3 を DSCP 値 5 としてマークしています。

```
switchxxxxxx(config)# qos map policed-dscp 3 to 5
```

qos map dscp-queue

qos map dscp-queue グローバル コンフィギュレーション モード コマンドを使用すると、DSCP/キュー マップを設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

qos map dscp-queue *dscp-list* to *queue-id*

no qos map dscp-queue [*dscp-list*]

パラメータ

- **dscp-list**：最大 8 つの DSCP 値をスペースで区切って指定します。（範囲：0 ～ 63）
- **queue-id**：DSCP 値のマップ先のキュー番号を指定します。

デフォルト設定

8 つのキューのデフォルト マップを以下に示します。

DSCP の値	9 ～ 15	0-8	17 ～ 23	32、41 ～ 47	25 ～ 31	33 ～ 39	16、24、40、48 ～ 63	なし
キュー ID	2	1	3	7	4	5	6	8

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、DSCP 値 33、40、および 41 をキュー 1 にマップします。

```
switchxxxxxx(config)# qos map dscp-queue 33 40 41 to 1
```

qos trust（グローバル）

qos trust グローバル コンフィギュレーション モード コマンドを使用すると、システムを基本モードおよび trust 状態に設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

qos trust {cos | **dscp**| **cos-dscp**}

no qos trust

パラメータ

- **cos**：入力パケットがパケット CoS 値で分類されるように指定します。タグなしのパケットはデフォルト ポートの CoS 値で分類されます。
- **dscp**：入力パケットがパケット DSCP 値で分類されるように指定します。
- **cos-dscp**：入力パケットが IP パケットの場合はパケット DSCP 値、IP パケットではない場合は CoS 値で分類するように指定します。

デフォルト設定

dscp

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、QoS の基本モードでのみ使用できます。

QoS ドメインに入るパケットは、そのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチ ポートはいずれか 1 つの trust 状態に設定できます。

ポートが信頼されているかどうか、またどのパケットのフィールドがトラフィックの分類に使用されるのかを指定する場合に、このコマンドを使用します。

システムが trust DSCP で設定されている場合、トラフィックは DSCP キュー マップによってキューにマップされます。

システムが trust CoS で設定されている場合、トラフィックは CoS キューマップによってキューにマップされます。

QoS ドメイン間境界の場合は、ポートを DSCP trust 状態に設定し、DSCP 値が QoS ドメインで異なる場合は DSCP/DSCP 変換マップを適用します。

例

次に、システムを DSCP trust 状態に設定する例を示します。

```
switchxxxxxx(config)# qos trust dscp
```

qos trust（インターフェイス）

qos trust インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用すると、システムが QoS 基本モードの場合にポートの trust 状態を有効にできます。各ポートの trust 状態を無効にするには、このコマンドの **no** 形式を使用します。

構文

qos trust

no qos trust

デフォルト設定

システムが基本モードの場合に各ポートが有効になっています。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、gi1/0/1 をデフォルトの trust 状態に設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)# qos trust
```

qos cos

qos cos インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用すると、ポートのデフォルトのCoS値を定義できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

qos cos *default-cos*

no qos cos

パラメータ

default-cos：ポートのデフォルトの CoS 値（VPT 値）を指定します。ポートが信頼され、パケットのタグが解除されると、デフォルトの CoS 値が CoS 値になります。（範囲：0 ～ 7）

デフォルト設定

ポートのデフォルトの CoS 値は 0 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

デフォルトのCoS値を使用すると、インターフェイスに入力されるすべてのタグなしパケットに CoS 値を割り当てることができます。

例

次に、ポート gi1/0/1 のデフォルトの CoS 値を 3 に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)#  qos cos 3
```

qos dscp-mutation

qos dscp-mutation グローバル コンフィギュレーション モード コマンドを使用すると、DSCP 変換マップをシステム DSCP 信頼済みポートに適用できます。DSCP 変換を使用せずに信頼済みポートに戻すには、このコマンドの **no** 形式を使用します。

構文

qos dscp-mutation

no qos dscp-mutation

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

DSCP/DSCP 変換マップは、Quality of Service（QoS）管理ドメインの境界にあるポートに適用します。2 つの QoS ドメインで異なる DSCP 定義が使用されている場合は、一方のドメインの一連の DSCP 値を変換して、もう一方のドメインの定義に一致させる DSCP/DSCP 変換マップを使用します。マップは入力ポートおよびDSCP信頼済みポートにのみ適用します。このマップをポートに適用すると、IPパケットが入力ポートに新しくマップされたDSCP値で書き換えられます。信頼できないポート、サービス クラス（CoS）、または IP 優先信頼済みポートに DSCP 変換マップを適用する場合。

グローバル信頼モードは、DSCP または CoS-DSCP にする必要があります。CoS 拡張モードの場合、ポートは信頼できる必要があります。

例

次の例では、DSCP 変換マップをシステムの DSCP トラステッド ポートに適用します。

```
switchxxxxxx(config)# qos dscp-mutation
```

show qos map

show qos map 特権 EXEC モード コマンドを使用すると、QoS マッピングのさまざまなタイプを表示できます。

構文

show qos map [dscp-queue | **dscp-dp| dscp-mutation** | policed-dscp | policed-cos]

パラメータ

- **dscp-queue**：DSCP/キュー マップを表示します。
- **dscp-dp**：DSCP/ドロップ優先マップを表示します。
- **policed-dscp**：DSCP/DSCP コメント テーブルを表示します。
- **dscp-mutation**：DSCP/DSCP 変換テーブルを表示します。

デフォルト設定

すべてのマップを表示します。

コマンド モード

特権 EXEC モード

例 1。次に、QoS マッピング情報の表示例を示します。

```
switchxxxxxx(config)# show qos map dscp-queue
Dscp-queue map:
     d1 : d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :   01 01 01 01 01 01 01 01 01 01
      1 :   01 01 01 01 01 01 02 02 02 02
      2 :   02 02 02 02 02 02 02 02 02 02
      3 :   02 02 03 03 03 03 03 03 03 03
      4 :   03 03 03 03 03 03 03 03 04 04
      5 :   04 04 04 04 04 04 04 04 04 04
      6 :   04 04 04 04
```

例 2。次に、dscp 再マッピング情報の表示例を示します。

```
switchxxxxxx(config)# show qos map policed-dscp
Policed-dscp map (exceed):
     d1 : d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :   00 01 02 03 04 05 06 07 08 09
      1 :   10 11 12 13 14 15 16 17 18 19
      2 :   20 21 22 23 24 25 26 27 28 29
      3 :   30 31 32 33 34 35 36 37 38 39
      4 :   40 41 42 43 44 45 46 47 48 49
      5 :   50 51 52 53 54 55 56 57 58 59
      6 :   21  21 21
Policed-dscp map (violate):
     d1 : d2 0  1  2  3  4  5  6  7  8  9
```

```
-----------------------------------
 0 :   00 01 02 03 04 05 06 07 08 09
 1 :   10 11 12 13 14 15 16 17 18 19
 2 :   20 21 22 23 24 25 26 27 28 29
 3 :   30 31 32 33 34 35 36 37 38 39
 4 :   40 41 42 43 44 45 46 47 48 49
 5 :   50 51 52 53 54 55 56 57 58 59
 6 :   11  11 11
```

clear qos statistics

clear qos statistics 特権 EXEC モード コマンドを使用すると、QoS 統計情報カウンタをクリアできます。

構文

clear qos statistics

コマンド モード

特権 EXEC モード

例

次に、QoS 統計情報カウンタをクリアする例を示します。

```
switchxxxxxx(config)#  clear qos statistics
```

qos statistics policer

qos statistics policer インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用すると、プロファイル内外のカウントを有効にできます。カウントを無効にするには、このコマンドの **no** 形式を使用します。

このコマンドは、ポリサーが定義されている場合にのみ関係します。

構文

qos statistics policer *policy-map-name class-map-name*

no qos statistics policer *policy-map-name class-map-name*

パラメータ

- **policy-map-name**：ポリシー マップ名を指定します。（長さ：1 ～ 32 文字）
- **class-map-name**：クラス マップ名を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

インプロファイルおよびアウトオブプロファイルのカウントは無効です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次の例では、インターフェイスでのインプロファイルおよびアウトオブプロファイルのカウントを有効にします。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# qos statistics policer policy1 class1
```

qos statistics aggregate-policer

qos statistics aggregate-policer グローバル コンフィギュレーション モード コマンドを使用すると、プロファイル内外のカウントを有効にできます。カウントを無効にするには、このコマンドの **no** 形式を使用します。

構文

qos statistics aggregate-policer *aggregate-policer-name*

no qos statistics aggregate-policer *aggregate-policer-name*

パラメータ

aggregate-policer-name：集約ポリサー名を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

インプロファイルおよびアウトオブプロファイルのカウントは無効です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、インターフェイスでのインプロファイルおよびアウトオブプロファイルのカウントを有効にします。

```
switchxxxxxx(config)# qos statistics aggregate-policer policer1
```

clear queue statistics

キュー統計情報をクリアするには、**clear queue statistics** 特権 EXEC モードコマンドを使用します。

構文

clear queue statistics [*interface-id*]

パラメータ

- ***interface-id***：キュー統計情報をクリアするイーサネットポートを指定します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

特定のポートのキュー統計情報をクリアするには、**clear queue statistics** *interface-id* コマンドを使用します。

すべてのポートのキュー統計情報をクリアするには、**clear queue statistics** コマンドを使用します。

例

次に、イーサネットポート gi1/0/2 のキュー統計情報をクリアする例を示します。

```
switchxxxxxx# clear queue statistics gi1/0/2
```

show queue statistics

キューの統計情報を表示するには、**show queue statistics** 特権 EXEC モードコマンドを使用します。

構文

show queue statistics [*interface-id*] [**detailed**]

パラメータ

- ***interface-id***：キュー統計情報を表示するイーサネットポートを指定します。
- ***detailed***：（オプション）すべてのインターフェイスとキューの情報を表示します。detailed オプションが指定されていない場合、コマンドの出力には、表示されるカウンタのいずれかの値がゼロ以外のインターフェイスとキューのみが含まれます。

デフォルト設定

デフォルトでは、このコマンドは、表示されるカウンタのいずれかがゼロ以外のポートとキューの情報のみを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

特定のポートのキュー統計情報を表示するには、**show queue statistics** *interface-id* コマンドを使用します。detailed オプションが指定されていない場合、コマンドの出力には、表示されるカウンタのいずれかの値がゼロ以外のインターフェイスキューのみが含まれます。

すべてのインターフェイスとキューの統計を表示するには、**show queue statistics detailed** コマンドを使用します。detailed オプションが指定されていない場合、コマンドの出力には、表示されるカウンタのいずれかの値がゼロ以外のインターフェイスとキューのみが含まれます。

例

例 1：

次の例では、表示されるカウンタのいずれかにゼロ以外の値を持つイーサネットポート gi1/0/2 のキューのキュー統計が表示されます。

```
switchxxxxxx# show queue statistics gi1/0/2
```

Interface	Queue	Tx Pkts	Tx Bytes	テールドロップパケット	テールドロップバイト
---	---	---	---	---	---
gi1/0/2	1	2700221	0	44543278	0
gi1/0/2	4	1850	257369	0	0
gi1/0/2	5	233017	50313150	12	10234
gi1/0/2	8	50	25600	0	0

例 2：次の例では、イーサネットポート gi1/0/2 のすべてのキューのキュー統計が表示されます。

Interface	Queue	Tx Pkts	Tx Bytes	テールドロップパケット	テールドロップバイト
---	---	---	---	---	---
gi1/0/2	1	2700221	0	44543278	0
gi1/0/2	2	0	0	0	0
gi1/0/2	3	0	0	0	0
gi1/0/2	4	1850	257369	12	10234
gi1/0/2	5	233017	50313150	0	0
gi1/0/2	6	0	0	0	0
gi1/0/2	7	0	0	0	0
gi1/0/2	8	0	0	0	0

show qos statistics

show qos statistics 特権 EXEC モード コマンドを使用すると、Quality of Service 統計情報を表示できます。

構文

show qos statistics

コマンド モード

特権 EXEC モード

使用上のガイドライン

QoS 統計情報を表示するには、**show qos statistics** コマンドを使用します。

ポリサーに対して最大 16 セットのカウンタを有効にできます。カウンタは、ポリサーの作成時に有効にすることができます。

例

次の例では、Quality of Service 統計情報を表示します。

```
switchxxxxxx# show qos statistics
Policers
---------
```

Interface	Policy Map	Class Map	In-Profile Bytes	Peak Bytes	Violate Bytes
gi1/0/1	----------	----------	---------	--------	---------
gi1/0/1	Policy1	Class1	756457	5427	12
gi1/0/2	Policy1	Class2	8759	14	12
gi1/0/2	Policy1	Class1	75457	5	2
	Policy1	Class2	5326		12

```
Aggregate Policers

------------------
```

Name	In-Profile Bytes	Peak Bytes	Violate Bytes
----------	---------	--------	---------
Policer	756457	5427	12

RADIUS コマンド

この章は、次の項で構成されています。

- radius-server host （1132 ページ）
- radius-server key （1134 ページ）
- radius-server retransmit （1135 ページ）
- radius-server host source-interface （1136 ページ）
- radius-server host source-interface-ipv6 （1137 ページ）
- radius-server timeout （1138 ページ）
- radius-server deadtime （1139 ページ）
- show radius-servers （1140 ページ）
- show radius-servers key （1141 ページ）

radius-server host

radius-server host グローバル コンフィギュレーション モード コマンドを使用すると、RADIUS サーバ ホストを設定できます。指定した RADIUS サーバ ホストを削除するには、コマンドの no 形式を使用します。

構文

radius-server host {*ip-address* | *hostname*} [**auth-port** *auth-port-number*] [**acct-port** *acct-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**priority** *priority*] [**usage** {**login** | **dot1.x** | **all**}]

encrypted radius-server host {*ip-address* | *hostname*} [**auth-port** *auth-port-number*] [**acct-port** *acct-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *encrypted-key-string*] [**priority** *priority*] [**usage** {**login** | **dot1.x** | **all**}]

no radius-server host {*ip-address* | *hostname*}

パラメータ

- ***ip-address***：RADIUS サーバ ホストの IP アドレスを指定します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。
- ***hostname***：RADIUS サーバ ホスト名を指定します。IPv4 アドレスへの変換のみがサポートされています。（長さ：1 ～ 158 文字、ホスト名の各部分の最大ラベル長は 63 文字です）
- **auth-port** *auth-port-number*：認証要求のポート番号を指定します。ポート番号を 0 に設定すると、そのホストは認証に使用されません。（範囲：0 ～ 65535）
- **acct-port** *acct-port-number*：アカウンティング要求のポート番号。0 に設定すると、ホストはアカウンティングに使用されません。指定しない場合、ポート番号はデフォルトの 1813 になります。
- **timeout** *timeout*：タイムアウト値を秒単位で指定します。(範囲：1 ～ 30)
- **retransmit** *retries*：再試行の再送信の数を指定します（範囲：1 ～ 15）
- **deadtime** *deadtime*：RADIUS サーバがトランザクション要求によって省略される間の期間を分単位で指定します。(範囲：0 ～ 2000)
- **key** *key-string*：デバイスと RADIUS サーバ間のすべての RADIUS 通信の認証および暗号化キーを指定します。キーは RADIUS デーモンで使用する暗号に一致している必要があります。空の文字列を指定するには、"" と入力します。（長さ：0 ～ 128 文字）。このパラメータを省略した場合は、グローバルに設定されている radius キーが使用されます。
- **key** encrypted-*key-string*：key-string と同じですが、キーは暗号化された形式です。
- **priority** *priority*：サーバを使用する順序を指定します。0 は最高の優先度です。（範囲：0 ～ 65535）

- **usage** {**login** | **dot1.x** | **all**}：RADIUS サーバ使用タイプを指定します。次の値が可能です。

  login：RADIUS サーバをユーザ ログインパラメータ認証用として指定します。

  dot1.x：RADIUS サーバを 802.1x ポート認証用として指定します。

  all：RADIUS サーバをユーザ ログイン認証用と 802.1x ポート認証用として指定します。

デフォルト設定

デフォルトの認証ポート番号は 1812 です。

timeout が指定されていない場合は、グローバル値（radius-server timeout コマンド）が使用されます。

retransmit が指定されていない場合は、グローバル値（radius-server retransmit コマンド）が使用されます。

key-string が指定されていない場合は、グローバル値（radius-server key コマンド）が使用されます。

usage キーワードが指定されていない場合は、**all** 引数が適用されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

複数のホストを指定するには、このコマンドはホストごとに使用されます。

例

次の例では、IP アドレス 192.168.10.1 の RADIUS サーバ ホスト、認証要求ポート番号 20、20 秒タイムアウト期間を指定します。

```
switchxxxxxx(config)# radius-server host 192.168.10.1 auth-port 20 timeout 20
```

radius-server key

radius-server key グローバル コンフィギュレーション モード コマンドを使用すると、デバイスと RADIUS デーモン間の RADIUS 通信の認証キーを設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

radius-server key [*key-string*]

encrypted radius-server key [*encrypted-key-string*]

no radius-server key

パラメータ

- ***key-string***：デバイスと RADIUS サーバ間のすべての RADIUS 通信に認証および暗号キーを指定します。キーはRADIUSデーモンで使用する暗号に一致している必要があります。（範囲：0 ～ 128 文字）
- ***encrypted-key-string***：key-string パラメータと同じですが、キーは暗号化された形式です。

デフォルト設定

key-string は空の文字列です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、デバイスと RADIUS デーモン間のすべての RADIUS 通信の認証キーを定義します。

```
switchxxxxxx(config)# radius-server key enterprise-server
```

radius-server retransmit

radius-server retransmit グローバル コンフィギュレーション モード コマンドを使用すると、ソフトウェアが RADIUS サーバ ホストのリストを検索する回数を指定できます。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

radius-server retransmit *retries*

no radius-server retransmit

パラメータ

- **retransmit** *retries*：再試行再送信の回数を指定します（範囲：1 ～ 15）。

デフォルト設定

ソフトウェアは RADIUS サーバ ホストのリストを 3 回検索します。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、ソフトウェアがすべての RADIUS サーバ ホストを検索する回数を 5 回に設定します。

```
switchxxxxxx(config)# radius-server retransmit 5
```

radius-server host source-interface

radius-server host source-interface グローバル コンフィギュレーション モード コマンドを使用すると、IPv4 アドレスが IPv4 RADIUS サーバとの通信用の送信元 IPv4 アドレスとして使用される送信元インターフェイスを指定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

radius-server host source-interface *interface-id*

no radius-server host source-interface

パラメータ

- ***interface-id***：送信元インターフェイスを指定します。

デフォルト設定

送信元 IPv4 アドレスは、発信インターフェイスで定義され、ネクスト ホップ IPv4 サブネットに属する IPv4 アドレスです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスの場合は、ネクスト ホップ IPv4 サブネットに属するインターフェイス IP アドレスが適用されます。

送信元インターフェイスが発信インターフェイスでない場合は、送信元インターフェイスで定義された最小 IPv4 アドレスが適用されます。

使用可能な IPv4 送信元アドレスがない場合は、IPv4 RADIUS サーバと通信しようとすると、SYSLOG メッセージが発行されます。

送信元インターフェイスとして OOB は定義できません。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# radius-server host source-interface vlan 100
```

radius-server host source-interface-ipv6

radius-server host source-interface-ipv6 グローバル コンフィギュレーション モード コマンドを使用すると、IPv6 アドレスが IPv6 RADIUS サーバとの通信用の送信元 IPv6 アドレスとして使用される送信元インターフェイスを指定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

radius-server host source-interface-ipv6 *interface-id*

no radius-server host source-interface-ipv6

パラメータ

- ***interface-id***：送信元インターフェイスを指定します。

デフォルト設定

IPv6 送信元アドレスは、発信インターフェイスで定義された IPv6 アドレスであり、RFC6724 に従って選択されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスである場合は、送信元 IPv6 アドレスはインターフェイスで定義され、RFC 6724 に従って選択された IPv6 アドレスです。

送信元インターフェイスが発信インターフェイスでない場合は、送信元 IPv6 アドレスは送信元インターフェイス上で定義され、宛先 IPv6 アドレスの範囲と一致します。

使用可能な送信元 IPv6 アドレスがない場合は、IPv6 RADIUS サーバとの通信を試行する際に SYSLOG メッセージが発行されます。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# radius-server host source-interface-ipv6 vlan 100
```

radius-server timeout

デバイスがサーバ ホストからの応答を待つ時間を設定するには、**radius-server timeout** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

radius-server timeout *timeout-seconds*

no radius-server timeout

パラメータ

- **timeout** *timeout-seconds*：タイムアウト値を秒単位で指定します。（範囲：1 ～ 30）。

デフォルト設定

デフォルトのタイムアウト値は 3 秒です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、すべての RADIUS サーバのタイムアウト間隔を 5 秒に設定します。

```
switchxxxxxx(config)# radius-server timeout 5
```

radius-server deadtime

radius-server deadtime グローバル コンフィギュレーション モード コマンドを使用すると、使用不可能なRADIUSサーバがトランザクション要求によって省略される時間を設定できます。これにより、サーバが使用不可能な場合のRADIUSの応答所要時間が改善されます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

radius-server deadtime *deadtime*

no radius-server deadtime

パラメータ

- ***deadtime***：RADIUS サーバがトランザクション要求によって省略される間の間隔を分単位で指定します。（範囲：0 ～ 2000）。

デフォルト設定

デフォルトのデッドタイム間隔は 0 です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、すべての RADIUS サーバのデッドタイムを 10 分に設定します。

```
switchxxxxxx(config)# radius-server deadtime 10
```

show radius-servers

show radius-servers 特権 EXEC モード コマンドを使用すると、RADIUS サーバ設定を表示できます。

構文

show radius-servers

コマンド モード

特権 EXEC モード

例

次の例では、RADIUS サーバ設定を表示します。

```
switchxxxxxx# show radius-servers
IP address  Port Port Time                Dead    Deadtime
            Auth Acc  Out   Retransmission time    status     Priority Usage
----------  ---- ---- ----  ------------- ------    ------     -------- -----
172.16.1.1  1812 1813  125  Global        Global     Dead        1      All
172.16.1.2  1812 1813  102  8             Global      Up         2      All
Global values
--------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10
```

show radius-servers key

show radius-servers key 特権 EXEC モード コマンドを使用すると、RADIUS サーバのキー設定を表示できます。

構文

show radius-servers key

コマンド モード

特権 EXEC モード

例

次に、RADIUS サーバのキー設定を表示する例を示します。

```
switchxxxxxx# show radius-servers key

IP address                                  Key (Encrypted)
----------                                  ---------------
172.16.1.1                                  1238af77aaca17568f1298cced165fec
172.16.1.2                                  1238af77aaca17568f12988601fcabed

Global key (Encrypted)
----------------------
1238af77aaca17568f1298bc5476ddad
```

RADIUS サーバコマンド

この章は、次の項で構成されています。

- allowed-time-range （1144 ページ）
- clear radius server accounting （1145 ページ）
- clear radius server rejected users （1146 ページ）
- clear radius server statistics （1147 ページ）
- clear radius server unknown nas （1148 ページ）
- privilege-level （1149 ページ）
- radius server accounting-port （1150 ページ）
- radius server authentication-port （1151 ページ）
- radius server enable （1152 ページ）
- radius server group （1153 ページ）
- radius server nas secret （1154 ページ）
- radius server traps accounting （1156 ページ）
- radius server traps authentication success （1157 ページ）
- radius server user （1158 ページ）
- show radius server accounting （1160 ページ）
- show radius server configuration （1162 ページ）
- show radius server group （1163 ページ）
- show radius server rejected users （1164 ページ）
- show radius server statistics （1166 ページ）
- show radius server nas secret （1168 ページ）
- show radius server user （1169 ページ）
- show radius server unknown nas （1170 ページ）
- vlan （1171 ページ）

allowed-time-range

ユーザが接続できる時間を定義するには、RADIUS サーバ グループ コンフィギュレーション モードで **allowed-time-range** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

allowed-time-range *time-range-name*

no allowed-time-range

パラメータ

- ***time-range-name***：time range コマンドで設定した時間範囲名を指定します。

コマンド モード

RADIUS サーバ グループ コンフィギュレーション モード

使用上のガイドライン

ユーザが接続できる時間を定義するには、**allowed-time-range** コマンドを使用します。

デフォルトに戻すには、このコマンドの **no** 形式を使用します。

例

次に、定期的な時間間隔を割り当てる例を示します。

```
switchxxxxxx(config)# time-range connection-time
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00
switchxxxxxx(config-time-range)# exit
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)# allowed-time-range connection-time
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)#
```

clear radius server accounting

RADIUS アカウンティングキャッシュをクリアするには、特権 EXEC モードで **clear radius server accounting** コマンドを使用します。

構文

clear radius server accounting

コマンド モード

特権 EXEC モード

使用上のガイドライン

RADIUS アカウンティングキャッシュをクリアするには、**clear radius server accounting** コマンドを使用します。

例

次に、RADIUS アカウンティングキャッシュをクリアする例を示します。

```
switchxxxxxx(config)# clear radius server accounting
```

clear radius server rejected users

RADIUS 拒否済みユーザキャッシュをクリアするには、特権 EXEC モードで **clear radius server rejected users** コマンドを使用します。

構文

clear radius server rejected users

コマンド モード

特権 EXEC モード

使用上のガイドライン

RADIUS 拒否済みユーザキャッシュをクリアするには、**clear radius server rejected users** コマンドを使用します。

例

次に、RADIUS 拒否済みユーザキャッシュをクリアする例を示します。

```
switchxxxxxx(config)# clear radius server rejected users
```

clear radius server statistics

RADIUS サーバのカウンタをクリアするには、特権 EXEC モードで **clear radius server statistics** コマンドを使用します。

構文

clear radius server statistics [*ip-address*]

パラメータ

- *ip-address*：RADIUS クライアントのホスト IP アドレスを指定します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

すべてのカウンタをクリアするには、パラメータを指定せずに **clear radius server statistics** コマンドを使用します。

特定の NAS のカウンタをクリアするには、パラメータを指定して **clear radius server statistics** コマンドを使用します。

例

次に、RADIUS サーバのカウンタをクリアする例を示します。

```
switchxxxxxx(config)# clear radius server statistics
```

clear radius server unknown nas

RADIUS の不明な NAS キャッシュをクリアするには、特権 EXEC モードで **clear radius server unknown nas** コマンドを使用します。

構文

clear radius server unknown nas

コマンド モード

特権 EXEC モード

使用上のガイドライン

RADIUS の不明な NAS キャッシュをクリアするには、**clear radius server unknown nas** コマンドを使用します。

例

次に、RADIUS の不明な NAS キャッシュをクリアする例を示します。

```
switchxxxxxx(config)# clear radius server unknown nas
```

privilege-level

ユーザ特権レベルを定義するには、RADIUS サーバ グループ コンフィギュレーション モードで **privilege-level** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

privilege-level *level*

no privilege-level

パラメータ

- ***level***：ユーザ特権レベルを指定します。（範囲：1 ～ 15）

デフォルト設定

1

コマンド モード

RADIUS サーバ グループ コンフィギュレーション モード

使用上のガイドライン

特定のグループのユーザの特権レベルを定義するには、**privilege-level** コマンドを使用します。

デフォルトに戻すには、このコマンドの **no** 形式を使用します。

特権レベルの値は、Vendor-Specific(26) 属性の Access-Accept メッセージで RADIUS クライアントに渡されます。この属性は、ログインユーザにのみ渡されます。

例

次に、開発者グループのユーザに指定した特権レベル 15 を指定する例を示します。

```
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)# privilege-level 15
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)#
```

radius server accounting-port

アカウンティング要求に使用するアカウンティング UDP ポートを定義するには、グローバル コンフィギュレーション モードで **radius server accounting-port** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

radius server accounting-port udp-port

no radius server accounting-port

パラメータ

- *udp-port*：アカウンティング要求の UDP ポート番号を指定します。（範囲：1 ー 59999）

デフォルト設定

1813

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

アカウンティング要求用の UDP ポートを定義するには、**radius server accounting-port** コマンドを使用します。

デフォルトの UDP アカウンティングポートを復元するには、**no radius server accounting-port** コマンドを使用します。

例

次に、ポート 2083 をアカウンティング UDP ポートとして定義する例を示します。

```
switchxxxxxx(config)# accounting-port 2083
```

radius server authentication-port

認証要求に使用する認証 UDP ポートを定義するには、グローバル コンフィギュレーション モードで **radius server authentication-port** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

radius server authentication-port udp-port

no radius server authentication-port

パラメータ

- *udp-port*：認証要求用の UDP ポート番号を指定します。（範囲：1 ー 59999）

デフォルト設定

1812

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

認証要求用の UDP ポートを定義するには、**radius server authentication-port** コマンドを使用します。

デフォルトの UDP 認証ポートを復元するには、**no radius server authentication-port** コマンドを使用します。

例

次に、認証 UDP ポートとしてポート 2083 を定義する例を示します。

```
switchxxxxxx(config)# authentication-port 2083
```

radius server enable

組み込み RADIUS サーバを有効にするには、グローバル コンフィギュレーション モードで **radius server enable** を使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

radius server enable

no radius server enable

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

組み込み RADIUS サーバを有効にするには、**radius server enable** コマンドを使用します。

組み込み RADIUS サーバを無効にするには、**no radius server enable** コマンドを使用します。

例

次に、組み込み RADIUS サーバを有効にする例を示します。

```
switchxxxxxx(config)# radius server enable
```

radius server group

RADIUS サーバ グループ コンフィギュレーション モードを開始して、このグループが存在しない場合に作成するには、グローバル コンフィギュレーション モードで **radius server group** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

radius server group group-name

no radius server group *[group-name*]

パラメータ

- ***group-name***：グループの名前を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

グループは存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

RADIUS サーバ グループ コンフィギュレーション モードを開始するには、**radius server group** コマンドを使用します。このグループが存在しない場合は自動的に作成されます。

1 つのグループを削除するには、**no radius server group group-name** コマンドを使用します。

すべてのグループを削除するには、**no radius server group** コマンドを使用します。

このグループを参照しているユーザが存在する場合は、グループを削除できません。

RADIUS サーバは、最大 50 個のグループをサポートします。

例

次に、グループ開発者が存在しない場合は作成し、そのコンテキストを開始する例を示します。

```
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)#
```

radius server nas secret

秘密鍵を作成するには、グローバル コンフィギュレーション モードで **radius server nas secret key** コマンドを使用します。鍵を削除するには、このコマンドの **no** 形式を使用します。

構文

radius server nas secret key key {**default** | *ip-address*}

radius server nas secret ip-address

encrypted radius server nas secret key *encrypted-key* {**default** | *ip-address*}

no radius server nas secret *[***default** | *ip-address*]

パラメータ

- ***key***：特定のグループのデバイスとユーザ間の通信に認証と暗号キーを指定します。（範囲：0 ～ 128 文字）
- ***encrypted-key***：key-string パラメータと同じですが、キーは暗号化形式です。
- **default**：秘密キーを持たないNASとの通信に適用するデフォルトの秘密鍵を指定します。
- *ip-address*：RADIUS クライアントのホスト IP アドレスを指定します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。

デフォルト設定

秘密鍵が存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

秘密キーを持たないNAS間の通信に適用するキーを定義するには、**radius server nas secret key** key **default** コマンドを使用します。

指定したNASとの通信に適用するキーを定義するには、**radius server nas secret key** key *ip-address* コマンドを使用します。

指定したNASとの通信に適用するデフォルトの秘密鍵を定義するには、**radius server nas secret** ip-address コマンドを使用します。

このコマンドでNASを定義しない場合は、このNASから受信するすべてのメッセージがドロップされます。

RADIUS サーバは、最大 50 の NAS をサポートします。

デフォルトのキーを削除するには、**no radius server nas secret default** コマンドを使用します。

特定の NAS とその秘密鍵を削除するには、**no radius server nas secret** ip-address コマンドを使用します。

すべての NAS とすべての秘密鍵を削除するには、**no radius server nas secret** コマンドを使用します。

例 1。次に、デフォルトの秘密鍵を定義する例を示します。

```
switchxxxxxx(config)# radius server nas secret key qrBut56$#qw default
```

例 2。次に、デフォルトの秘密鍵を定義する例を示します。

```
switchxxxxxx(config)# radius server nas secret key qrBut56$#qw default
```

例 3。次に、デフォルトの秘密鍵を使用して NAS を定義する例を示します。

```
switchxxxxxx(config)# radius server nas secret 10.05.10.1
```

radius server traps accounting

アカウンティングトラップの送信を有効にするには、グローバル コンフィギュレーション モードで **radius server traps accounting** コマンドを使用します。このトラップを無効にするには、このコマンドの **no** 形式を使用します。

構文

radius server traps accounting

no radius server traps accounting

デフォルト設定

アカウンティングトラップが無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

トラップには次のようにレート制限が適用されます。このタイプでは、10秒間に複数のトラップを送信できません。

例

次に、アカウンティングトラップの送信を有効にする例を示します。

```
switchxxxxxx(config)# radius server traps accounting
```

radius server traps authentication success

ユーザが正常に承認されたときにトラップの送信を有効にするには、グローバル コンフィギュレーション モードで **radius server traps authentication success** コマンドを使用します。このトラップを無効にするには、このコマンドの **no** 形式を使用します。

構文

radius server traps authentication success

no radius server traps authentication success

デフォルト設定

成功トラップが無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

トラップには次のようにレート制限が適用されます。このタイプでは、10秒間に複数のトラップを送信できません。

例

次に、ユーザが正常に承認されたときにトラップの送信を有効にする例を示します。

```
switchxxxxxx(config)# radius server traps authentication success
```

radius server user

ユーザを作成するには、グローバル コンフィギュレーション モードで **radius server user** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

radius server user username user-name **group** group-name **password** *unencrypted-password*

encrypted radius server user username user-name **group** *group-name* **password***encrypted-password*

no radius server user *[***username** user-name | **group** group-name]

パラメータ

- ***user-name***：ユーザ名を指定します。（長さ：1 ～ 32 文字）
- ***group-name***：ユーザグループ名を指定します。（長さ：1 ～ 32 文字）
- ***unencrypted-password***：ユーザーパスワードを指定します。（長さ：1 ～ 64 文字）
- ***encrypted-password***：*unencrypted-password* パラメータと同じですが、パスワードは暗号化された形式です。

デフォルト設定

ユーザが存在しません。

RADIUS サーバは、最大 1,024 人のユーザをサポートします。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

新しいユーザを作成するには、**radius server user** コマンドを使用します。

1 人のユーザを削除するには、**no radius server user username user-name** コマンドを使用します。

特定のグループのユーザを削除するには、**no radius server user group group-name** コマンドを使用します。

すべてのユーザを削除するには、**no radius server user** コマンドを使用します。

例

例 1。次に、グループ開発者の名前に bob、パスワードに Aerv#136dSsT を指定して新しいユーザを作成する例を示します。

```
switchxxxxxx(config)# radius server user username bob group developers password
Aerv#136dSsT
```

例2。次に、bill of group finance という名前の新しいユーザーを作成し、パスワードを暗号化形式で指定する例を示します。

```
switchxxxxxx(config)# encrypted radius server user username bill group
finance password bCWG7DnKMNUaik4S0TkLDkJVYIsQcwQkRFVYj7VNvAI=
```

show radius server accounting

ユーザアカウンティング情報を表示するには、特権 EXEC モードで **show radius server accounting** コマンドを使用します。

構文

show radius server accounting *[***username** *user-name*]

パラメータ

- ***user-name***：ユーザ名を指定します。（長さ：1 ～ 32 文字）

コマンド モード

特権 EXEC モード

使用上のガイドライン

RADIUS サーバは、フラッシュのサイクルファイルに最新の 1024 個のアカウンティングログを保存します。

1 人のユーザのアカウンティング情報を表示するには、**show radius server accounting username** *user-name* コマンドを使用します。

すべてのユーザのアカウンティング情報を表示するには、**show radius server accounting** コマンドを使用します。

例 1。次に、すべてのユーザのアカウンティング情報を表示する例を示します。

```
switchxxxxxx# show radius server accounting
29-Jun-14, 16:00, Stop
  User: Bob
  Accounting Session Time: 6 hours,15 minutes
  Authenticated by: local
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
  Termination Reason: User Request
29-Jun-14, 12:04, Start
  User: Alisa
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 00:12:cf:00:1c:25
  NAS Port: 10
29-Jun-14, 12:04, Stop
  User: Alisa
  Accounting Session Time: 2 days,2 hours,10 minutes
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 00:12:cf:00:1c:25
  Termination Reason: User Request
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-2014, 9:05, Start
  User: Bob
  Authenticated by: local
```

```
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
*20-Feb-2008, 9:00, Reboot
```

例 2。次に、Bob という 1 人のユーザのアカウンティング情報を表示する例を示します。

```
switchxxxxxx# show radius server accounting username Bob:
29-Jun-14, 16:00, Stop
  User: Bob
  Accounting Session Time: 6 hours,15 minutes
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
  Termination Reason: User Request
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-2014, 9:05, Start
  User: Bob
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
*20-Feb-2008, 9:00, Reboot
```

show radius server configuration

RADIUS サーバのグローバル設定を表示するには、特権 EXEC モードで **show radius server configuration** コマンドを使用します。

構文

show radius server configuration

コマンド モード

特権 EXEC モード

使用上のガイドライン

RADIUS サーバのグローバル設定を表示するには、**show radius server configuration** コマンドを使用します。

例

次に、RADIUS サーバのグローバル設定を表示する例を示します。

```
switchxxxxxx# show radius server configuration
Radius Server Status: Enabled
Authentication UDP port: 1812 (default)
Accounting UDP port: 1813 (default)
Authentication failure traps are enabled
Authentication success traps are enabled
Accounting traps are enabled
```

show radius server group

RADIUS サーバのグループ設定を表示するには、特権 EXEC モードで **show radius server group** コマンドを使用します。

構文

show radius server group *[group-name]*

パラメータ

- ***group-name***：グループの名前を指定します。（長さ：1 ～ 32 文字）

コマンド モード

特権 EXEC モード

使用上のガイドライン

1 つのグループを表示するには、**show radius server group** *group-name* コマンドを使用します。

すべてのグループを表示するには、**show radius server group** コマンドを使用します。

例

次に、RADIUS サーバグループを表示する例を示します。

```
switchxxxxxx# show radius server group
Group gr1
  VLAN: 124
  Privilege Level: 15
  Time Range: ConnectionTime
  Group Users: develop, designers
Group gr2
  Privilege Level: 1 (default)
  Group Users: bob
```

show radius server rejected users

拒否されたユーザを表示するには、特権 EXEC モードで **show radius server rejected users** コマンドを使用します。

構文

show radius server rejected users *[***username** *user-name*]

パラメータ

- ***user-name***：ユーザ名を指定します。（長さ：1 ～ 32 文字）

コマンド モード

特権 EXEC モード

使用上のガイドライン

RADIUS サーバは、フラッシュのサイクルファイルに最後の 1024 の拒否された認証要求を保存します。

RADIUS サーバは、フラッシュのサイクルファイルに最新の 1024 個のアカウンティングログを保存します。

拒否された 1 人のユーザを表示するには、**show radius server rejected users** *user-name* コマンドを使用します。

拒否されたすべてのユーザを表示するには、**show radius server rejected users** コマンドを使用します。

例 1。次に、拒否されたすべてのユーザを表示する例を示します。

```
switchxxxxxx# show radius server rejected users
30-Jun-14 16:44
  User Name: Jack
  User Type: Login
  NAS Address: 10.1.1.1
  User Address: 10.23.4.3
  Reason: Unknown user
30-Jun-14 16:04
  User Name: Bob
  User Type: Login
  NAS Address: 10.1.1.1
  User Address: 10.23.4.3
  Reason: Illegal password
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-08 16:24
  User Name: Robert
  User Type: 802.1x
  NAS Address: 10.1.1.1
  NAS Port: 2
  User Address: 00:67:67:96:ac:21
  Reason: Not Supported EAP method
```

```
20-Feb-08 14:14
  User Name: Alisa
  User Type: 802.1x
  NAS Address: 10.1.1.1
  NAS Port: 2
  User Address: 00:67:67:96:ac:21
  Reason: Not allowed at this time
*20-Feb-2008, 9:00, Reboot
```

例 2。次に、リジェクトされた Bob という 1 人のユーザを表示する例を示します。

```
switchxxxxxx# show radius server rejected users 30-Jun-14 16:04
  User Name: Bob
  User Type: Login
  NAS Address: 10.1.1.1
  User Address: 10.23.4.3
  Reason: Illegal password
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
*20-Feb-2008, 9:00, Reboot
```

show radius server statistics

RADIUS サーバカウンタを表示するには、ユーザ EXEC モードで **show radius server statistics** コマンドを使用します。

構文

show radius server statistics [***ip-address***]

パラメータ

- ***ip-address***：RADIUS クライアントのホスト IP アドレスを指定します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

RFC4669 と RFC4671 で定義されている RADIUS サーバカウンタを表示するには、**show radius server statistics** コマンドを使用します。

グローバルカウンタを表示するには、パラメータを指定せずに **show radius server statistics** コマンドを使用します。

特定の NAS のカウンタを表示するには、パラメータを指定して **show radius server statistics** コマンドを使用します。

例 1。次に、RADIUS サーバのグローバルカウンタを表示する例を示します。

```
switchxxxxxx# show radius server statistics
Number of incoming packets on the authentication port: 120
Number of incoming Access-Requests from unknown addresses: 0
Number of duplicate incoming Access-Requests: 3
Number of sent Access-Accepts: 100
Number of sent Access-Rejects: 17
Number of sent Access-Challenges: 0
Number of incoming malformed Access-Requests: 0
Number of incoming Authentication-Requests with Bad Authenticator: 0
Number of incoming Authentication packets with other mistakes: 0
Number of incoming Authentication packets of unknown type: 0
Number of incoming packets on the accounting port: 80
Number of incoming Accounting-Requests from unknown addresses: 12
Number of incoming Accounting-Requests from unknown addresses: 0
Number of incoming duplicate Accounting-Requests: 0
Number of sent Accounting-Responses: 0
Number of incoming malformed Accounting-Requests: 0
Number of incoming Accounting-Requests with Bad Authenticator: 0
Number of incoming Accounting packets with other mistakes: 0
Number of incoming not recorded Accounting-Requests: 0
Number of incoming Accounting packets of unknown type: 0
```

例 2。次に、特定の SNA：秘密鍵の RADIUS サーバカウンタを表示する例を示します。

```
switchxxxxxx# show radius server statistics 1.1.1.1
NAS: 1.1.1.1
Number of incoming packets on the authentication port: 120
Number of duplicate incoming Access-Requests: 3
Number of sent Access-Accepts: 100
Number of sent Access-Rejects: 17
Number of sent Access-Challenges: 0
Number of incoming malformed Access-Requests: 0
Number of incoming Authentication-Requests with Bad Authenticator: 0
Number of incoming Authentication packets with other mistakes: 0
Number of incoming Authentication packets of unknown type: 0
Number of incoming packets on the accounting port: 80
Number of incoming Accounting-Requests from unknown addresses: 0
Number of incoming duplicate Accounting-Requests: 0
Number of sent Accounting-Responses: 0
Number of incoming malformed Accounting-Requests: 0
Number of incoming Accounting-Requests with Bad Authenticator: 0
Number of incoming Accounting packets with other mistakes: 0
Number of incoming not recorded Accounting-Requests: 0
Number of incoming Accounting packets of unknown type: 0
```

show radius server nas secret

秘密鍵を表示するには、特権 EXEC モードで **show radius server nas secret** コマンドを使用します。

構文

show radius server nas secret *[***default** | ***ip-address***]

パラメータ

- **default**：秘密キーを持たないNASとの通信に適用するデフォルトの秘密鍵を指定します。
- ***ip-address***：RADIUS クライアントのホスト IP アドレスを指定します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

デフォルトの秘密鍵を表示するには、**show radius server nas secret default** コマンドを使用します。

特定の NAS 秘密鍵を表示するには、**show radius server nas secret** ip-address コマンドを使用します。

すべての秘密鍵を表示するには、**show radius server nas secret** コマンドを使用します。

例 1。次に、すべての秘密鍵を表示する例を示します。

```
switchxxxxxx# show radius server nas secret
Default Secret Key's MD5:1238af77aaca17568f1298cced1255cc
    NAS Address                 Secret Key’s MD5
-------------------------  --------------------------------
10.1.35.3                  1238af77aaca17568f1298cced165fec
10.2.37.6                  default
3000:1231:1230:9cab:1384   1238af77aaca17568f12988601fcabed
3001:ab11::9cda:0981       1238af77aaca17568f1298bc5476ddad
```

例 2。次に、デフォルトの秘密鍵を表示する例を示します。

```
switchxxxxxx# show radius server nas secret default
Default Secret Key's MD5:1238af77aaca17568f1298cced1255cc
```

例 3。次に、特定の NAS の秘密鍵を表示する例を示します。

```
switchxxxxxx# show radius server nas secret 10.1.35.3
            NAS ID                  Secret Key’s MD5
-------------------------  --------------------------------
10.1.35.3                  1238af77aaca17568f1298cced165fec
```

show radius server user

RADIUS サーバのユーザ設定を表示するには、特権 EXEC モードで **show radius server user** コマンドを使用します。

構文

show radius server user *[***username** *user-name*] | [**group** *group-name*]

パラメータ

- ***user-name***：ユーザ名を指定します。（長さ：1 ～ 32 文字）
- ***group-name***：グループの名前を指定します。（長さ：1 ～ 32 文字）

コマンド モード

特権 EXEC モード

使用上のガイドライン

1 人のユーザを表示するには、**show radius server user username** *user-name* コマンドを使用します。

特定のグループのすべてのユーザを表示するには、**show radius server user group** *group-name* コマンドを使用します。

すべてのユーザを表示するには、**show radius server user** コマンドを使用します。

例

次に、bob という 1 人のユーザを表示する例を示します。

```
switchxxxxxx# show radius server user username bob
User bob
  Group: developers
  Password's MD5: 1238af77aaca17568f1298cced1255cc
```

show radius server unknown nas

不明な NAS を表示するには、特権 EXEC モードで **show radius server unknown nas** コマンドを使用します。

構文

show radius server unknown nas

コマンド モード

特権 EXEC モード

使用上のガイドライン

RADIUS サーバは、最後の 100 個の不明な NAS をサイクルキャッシュに保存します。

例

次に、不明な NAS から受信した RADIUS 要求を表示する例を示します。

```
switchxxxxxx# show radius server unknown nas
30-Jun-14 16:44 NAS Address: 10.1.1.1
30-Jun-14 16:04 NAS Address: 10.1.1.1
*20-Feb-08, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-08 16:24 NAS Address: 10.1.1.1
20-Feb-08 14:14 NAS Address: 10.1.1.1
*20-Feb-08, 9:00, Reboot
```

vlan

RADIUS割り当て済みVLANを定義するには、RADIUSサーバグループコンフィギュレーションモードで**vlan**コマンドを使用します。デフォルト設定に戻すには、このコマンドの**no**形式を使用します。

構文

vlan {**id** *vlan-id* | **name** *vlan-name*}

no vlan

パラメータ

- ***vlan-id***：VLAN ID を指定します。（範囲：1 ～ 4094）
- ***vlan-name***：VLAN 名を指定します。（長さ：1 ー 32 文字）

デフォルト設定

RADIUS 割り当て済み VLAN なし

コマンド モード

RADIUS サーバ グループ コンフィギュレーション モード

使用上のガイドライン

vlan コマンドを使用して、RADIUS クライアントに VLAN を割り当てます。この RADIUS 割り当て済み VLAN は、次の属性の Access-Accept メッセージで RADIUS クライアントに渡されます。

- Tunnel-Type(64)
- Tunnel-Medium-Type（65）
- Tunnel-Private-Group-ID(81)

VLAN が割り当てられていない場合、これらの属性は Access-Accept メッセージに含まれません。

VLAN の割り当てを削除するには、このコマンドの **no** 形式を使用します。

例

次に、開発者グループのユーザに VLAN 100 を割り当てて、マネージャグループのユーザの VLAN 名前管理を指定する例を示します。

```
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)# vlan id 100
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)# radius server group managers
```

```
switchxxxxxx(config-radser-group)# vlan name management
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)#
```

レート制限コマンドとストームコマンド

この章は、次の項で構成されています。

- clear storm-control counters （1174 ページ）
- rate-limit（イーサネット） （1176 ページ）
- rate-limit vlan （1177 ページ）
- storm-control （1178 ページ）
- show rate-limit interface （1180 ページ）
- show rate-limit vlan （1181 ページ）
- show storm-control interface （1182 ページ）

clear storm-control counters

すべてのストーム制御カウンタをクリアするには、特権 EXEC モードで **clear storm-control counters** コマンドを使用します。

構文

clear storm-control counters [**broadcast** | **multicast** | **unicast**] [interface *interface-id*]

パラメータ

- **broadcast**：（オプション）ブロードキャスト ストーム制御カウンタをクリアします。
- **multicast**：（オプション）マルチキャスト ストーム制御カウンタをクリアします。
- **unicast**：（オプション）ユニキャスト不明ストーム制御カウンタをクリアします。
- **interface** *interface-id*：（オプション）指定されたイーサネット ポートのストーム制御カウンタをクリアします。

コマンド モード

特権 EXEC モード

使用上のガイドライン

ポートの指定のトラフィックの種類のストーム制御が有効の場合、スイッチは、このトラフィックの種類のポート カウンタをクリアします。

ストーム制御の実行中にストーム制御カウンタをクリアするには、このコマンドを使用します。

すべてのイーサネット ポートのすべてのストーム制御カウンタをクリアするには、**clear storm-control counters** コマンドを使用します。

特定のポートのすべてのストーム制御カウンタをクリアするには、**clear storm-control counters interface** *interface-id* コマンドを使用します。

すべてのイーサネットポートの特定のトラフィックタイプのすべてのストーム制御カウンタをクリアするには、**clear storm-control counters broadcast** | **multicast** | **unicast** コマンドを使用します。

特定のトラフィックタイプで、特定のポートの 1 つのストーム制御カウンタをクリアするには、**clear storm-control counters broadcast** | **multicast** | **unicast interface** *interface-id* コマンドを使用します。

例 1。次の例では、すべてのポートのすべてのストーム制御カウンタをクリアします。

```
switchxxxxxx# clear storm-control counters
```

例 2。次に、ポート gi1/0/1 のすべてのストーム制御カウンタをクリアする例を示します。

```
switchxxxxxx# clear storm-control counters interface gi1/0/1
```

例 3。次の例では、すべてのポートのブロードキャスト ストーム制御カウンタをクリアします。

```
switchxxxxxx# clear storm-control counters broascat
```

例 4。次に、ポート gi1/0/1 のマルチキャストストーム制御カウンタをクリアする例を示します。

```
switchxxxxxx# clear storm-control counters multicast interface gi1/0/1
```

rate-limit（イーサネット）

ポートの着信トラフィック レートを制限するには、インターフェイス（イーサネット）コンフィギュレーション モードで **rate-limit** コマンドを使用します。レート制限を無効にするには、このコマンドの **no** 形式を使用します。

構文

rate-limit *committed-rate-kbps* **[burst** *committed-burst-bytes***]**

no rate-limit

パラメータ

- ***committed-rate-kbps***：ポートの入力トラフィックのキロビット/秒の最大数を指定します。範囲は、3 ～ 最大ポート速度です。
- **burst** *committed-burst-bytes*：（オプション）バースト サイズ（バイト単位）。（範囲：3000 ～ 19173960）。指定しない場合、デフォルトは 128K に設定されています。

デフォルト設定

レート制限が無効になります。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

計算されたレートには、イーサネット フレーミングのオーバーヘッド（プリアンブル＋SFD＋IPG）の 20 バイトが含まれています。

レート制限は、ストーム制御によって制御されるトラフィックは計算しません。実際の許可されるレートは、コマンドで指定されたレートと特定のトラフィックの種類のストーム制御コマンドで指定されたレートの合計になります。

例

次に、gi1/0/1 で着信トラフィック レートを 150,000 kbps に制限する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# rate-limit 150000
```

rate-limit vlan

VLAN の着信トラフィック レートを制限するには、グローバル コンフィギュレーション モードで **rate-limit vlan** コマンドを使用します。レート制限を無効にするには、このコマンドの **no** 形式を使用します。

構文

rate-limit vlan *vlan-id committed-rate committed-burst-bytes*

no rate-limit vlan *vlan-id*

パラメータ

- ***vlan-id***：VLAN ID を指定します。
- ***committed-rate***：平均トラフィック レート（CIR）を kbits/秒（kbps）で指定します。（範囲：3 ～ 57982058）
- ***committed-burst***：最大バースト サイズ（CBS）をバイト単位で指定します。（範囲：3000 ～ 19173960）。

デフォルト設定

レート制限が無効になります。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

計算されたレートには、イーサネット フレーミングのオーバーヘッド（プリアンブル＋SFD＋IPG）の 20 バイトが含まれています。

ポリシー マップのトラフィック ポリシングは、VLAN のレート制限よりも優先されます。パケットがポリシー マップのトラフィック ポリシングの対象で、レートが制限される VLAN に関連付けられている場合、パケットはポリシー マップのトラフィック ポリシングでのみカウントされます。

VLAN レート制限は、スタック内のユニットごとに別個に計算されます。

IP ソース ガードと連携しては機能しません。

例

次に、VLAN 11 のレートを 150,000 kbps に、コミット済みバーストサイズを 9,600 バイトに制限します。

```
switchxxxxxx(config)# rate-limit vlan 11 150000 9600
```

storm-control

ポートのブロードキャスト、マルチキャスト、またはユニキャストストーム制御を有効にするには、インターフェイス（イーサネット）コンフィギュレーション モードで **storm-control** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

storm-control broadcast {**level** *level* | **kbps** *kbps***} [trap**] [**shutdown**]

no storm-control broadcast

storm-control multicast [**registered** | **unregistered**] {**level** *level* | **kbps** *kbps***} [trap**] [**shutdown**]

no storm-control multicast

storm-control unicast {**level** *level* | **kbps** *kbps***} [trap**] [**shutdown**]

no storm-control unicast

no storm-control

パラメータ

- **broadcast**：ポートでブロードキャスト ストーム制御を有効にします。
- **multicast** [**registered** | **unregistered**]：すべてのマルチキャスト、登録済みマルチキャストのみ、または未登録のマルチキャストストーム制御のみのいずれかをポートで有効にします。
- **unicast**：ポートでユニキャスト不明ストーム制御を有効にします。
- **level** *level*：抑制レベル（%）。指定した level の値に達した場合、ストーム パケットのフラッディングをブロックします。（範囲：1 ～ 100）
- **kbps** *kbps*：ポートにおける最大ブロードキャスト トラフィック（キロビット/秒）。（範囲：1 ～ 10000000）
- **trap**：（オプション）ストームがポートで発生したときにトラップを送信します。このキーワードが指定されないと、トラップは送信されません。
- **shutdown**：（オプション）ストームがポートで発生したときに、ポートをシャットダウンします。このキーワードが指定されないと、余剰トラフィックは廃棄されます。

デフォルト設定

ストーム制御は無効です。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

計算されたレートには、イーサネット フレーミングのオーバーヘッド（プリアンブル＋SFD＋IPG）の 20 バイトが含まれています。

ポートのレート制限では、このポートのストーム制御によって制御されるトラフィックは計算されません。

ポートですべてのトラフィックの種類のストーム制御を無効にするには、**no storm-control** コマンドを使用します。

例

次に、ポート gi1/0/1 でブロードキャスト、マルチキャスト、およびユニキャストの不明ストーム制御を、ポート gi1/0/2 で未登録マルチキャスト、および不明ユニキャストを有効にする例を示します。

インターフェイス gi1/0/1 上で登録済みおよび未登録のマルチキャストトラフィックのグループ 1 を有効にします。余剰トラフィックは廃棄されます。

switchxxxxxx(config)# **interface gi1/0/1** switchxxxxxx(config-if)# **storm-control broadcast kbps 10000 shutdown** switchxxxxxx(config-if)# **storm-control multicast level 20 trap** switchxxxxxx(config-if)# **storm-control unicast level 5 trap shutdown** switchxxxxxx(config-if)# **exit** switchxxxxxx(config)# **interface gi1/0/2** switchxxxxxx(config-if)# **storm-control multicast unregistered level 5 trap shutdown** switchxxxxxx(config-if)# **storm-control unicast level 5 trap** switchxxxxxx(config-if)# **exit**

show rate-limit interface

インターフェイスのレート制限設定を表示するには、特権 EXEC モードで **show rate-limit interface** コマンドを使用します。

構文

show rate-limit interface [*interface-id***]**

パラメータ

- ***interface-id***：（オプション）イーサネット ポートを指定します。引数が設定されていない場合、すべてのイーサネット ポートのレート制限設定が表示されます。

コマンド モード

特権 EXEC モード

例

次に、**show rate-limit interface** の出力例を示します。

```
switchxxxxxx> show rate-limit interface
```

Interface	Rate Limit (kbps)	Burst (Bytes)
----------	----------	----------
gi1/0/1gi1/0/2	80000	512
	100000	1024

show rate-limit vlan

VLAN のレート制限設定を表示するには、特権 EXEC モードで **show rate-limit vlan** コマンドを使用します。

構文

show rate-limit vlan [*vlan-id***]**

パラメータ

- ***vlan-id***：（オプション）VLAN ID を指定します。引数を設定しない場合、すべての VLAN のレート制限設定が表示されます。

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード

例

次に、**show rate-limit vlan** の出力例を示します。

```
switchxxxxxx> show rate-limit vlan 1075
```

VLAN	Rate Limit (kbps)	Burst (Bytes)
--------	----------	----------
1075	100000	1024

show storm-control interface

インターフェイスのストーム制御情報を表示するには、特権EXECモードで**show storm-control interface** コマンドを使用します。

構文

show storm-control interface [*interface-id***]**

パラメータ

- ***interface-id***：（オプション）イーサネット ポートを指定します。引数が設定されていない場合、すべてのイーサネット ポートのストーム制御情報が表示されます。

コマンド モード

特権 EXEC モード

例

次に、**show storm-control interface** の出力例を示します。

```
switchxxxxxx> show storm-control interface
gi1/0/1
 Broadacst
 Rate: 5%
 Action: Shutdown
 Passed Counter (Bytes): 124997
 Dropped Counter (Bytes): 10
 Last drop time: 27-Jan-2014, 09:00:01
 Multicast
 Rate: 1000 kbps
 Action: Drop, Trap
 Passed Counter (Bytes):112876
 Dropped Counter (Bytes):1272
 Last drop time: 20-Jan-2014, 11:00:01
 Unicast
 Rate: 10%
 Action: drop
 Passed Counter (Bytes): 27653
 Dropped Counter (Bytes):1
 Last drop time: 27-Feb-2014, 09:00:01
gi1/0/2
 Broadacst
 Rate: 5%
 Action: Shutdown
 Passed Counter (Bytes): 124997
 Dropped Counter (Bytes): 0
 Last drop time:
 Multicast Unregistred
 Rate: 5%
 Action: Shutdown
 Traffic Type:Broadcast
 Passed Counter (Bytes): 124997
 Dropped Counter (Bytes): 3
 Last drop time: 26-Jan-2014, 10:00:01
```

RIP コマンド

この章は、次の項で構成されています。

- clear rip statistics （1184 ページ）
- default-information originate （1185 ページ）
- default-metric （1186 ページ）
- ip rip authentication key-chain （1187 ページ）
- ip rip authentication mode （1188 ページ）
- ip rip authentication-key （1189 ページ）
- ip rip default-information originate （1190 ページ）
- ip rip distribute-list in （1191 ページ）
- ip rip distribute-list out （1192 ページ）
- ip rip offset （1193 ページ）
- ip rip passive-interface （1194 ページ）
- ip rip distribute-list in （1195 ページ）
- ip rip distribute-list out （1196 ページ）
- ip rip offset （1197 ページ）
- ip rip passive-interface （1198 ページ）
- ip rip shutdown （1199 ページ）
- network （1200 ページ）
- passive-interface（RIP） （1201 ページ）
- redistribute（RIP） （1202 ページ）
- router rip （1204 ページ）
- show ip rip database （1205 ページ）
- show ip rip peers （1208 ページ）
- shutdown （1209 ページ）

clear rip statistics

clear rip statistics 特権 EXEC モード コマンドは、すべてのインターフェイスおよびすべてのピアの統計カウンタをクリアします。

構文

clear rip statistics

パラメータ

該当なし

コマンド モード

特権 EXEC モード

例

次に、すべてのカウンタをクリアする例を示します。

```
switchxxxxxx# clear rip statistics
```

default-information originate

RIP（Routing Information Protocol）へのデフォルト ルートを生成するには、ルータ コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

default-information originate

no default-information originate

デフォルト設定

デフォルト ルートは RIP によって生成されません。

コマンド モード

ルータ RIP コンフィギュレーション モード

使用上のガイドライン

デフォルト ルートの生成を有効にするには、コマンドを使用します。

例 1：次の例では、デフォルト ルートを生成する方法を示します。

switchxxxxxx(config)# router rip switchxxxxxx(config-rip)# default-information originate
switchxxxxxx(config-rip)# exit

default-metric

default-metric ルータ RIP コンフィギュレーション モード コマンドは、他のプロトコルによって（たとえばスタティック設定）RIP アドバタイズ ルートが取得された場合のデフォルト メトリック値を設定します。このコマンドの **no** 形式を使用すると、デフォルト値が設定されます。

構文

default-metric [*metric-value*]

no default-metric

パラメータ

- ***metric-value***：デフォルト メトリック値。範囲：1 ～ 15。

デフォルト設定

metric-value：1。

コマンド モード

ルータ RIP コンフィギュレーション モード

例

次の例は、デフォルト メトリックを 2 に設定する方法を示します。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# default-metric 2
switchxxxxxx(config-rip)# exit
```

ip rip authentication key-chain

ip rip authentication key-chain IP インターフェイス コンフィギュレーション モード コマンドは、認証の種類に使用でき、認証の種類を指定する一連のキーを指定します。このコマンドの **No** 形式を使用するとデフォルトに戻ります。

構文

ip rip authentication key-chain *name-of-chain*

no ip rip authentication key-chain

パラメータ

- ***name-of-chain***：キー セットの名前を指定します。名前変更パラメータは、**key chain** CLI コマンドで指定されたキーのリストを指定します。

デフォルト設定

キー チェーンは定義されていません。

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

キー チェーン名を定義するには、**ip rip authentication key-chain** IP インターフェイス コンフィギュレーション モード コマンドを使用します。IP インターフェイスごとに 1 つのキー チェーンのみ定義できます。各 **ip rip authentication key-chain** コマンドは、以前の定義をオーバーライドします。

キー チェーン内のキーを円滑にロール オーバーするため、キーに以前のキーの有効期限が切れる数分前に開始する有効期限を設定する必要があります。

例

次に、チェーン名を定義する例を示します。

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip authentication key-chain alpha
switchxxxxxx(config-route-map)# exit
```

ip rip authentication mode

ip rip authentication mode IP インターフェイス コンフィギュレーション モード コマンドは、認証を有効にします。このコマンドの **No** 形式を使用するとデフォルトに戻ります。

構文

ip rip authentication mode {**text** | **md5**}

no ip rip authentication mode

パラメータ

- **text**：クリア テキスト認証を指定します。
- **md5**：MD5 認証を指定します。

デフォルト設定

認証なし

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

MD5 認証を有効にする場合、**ip rip authentication key-chain** インターフェイス コマンドでキーチェーンの名前を設定する必要があります。IP インターフェイスのキー チェーンが定義されていないか、有効なキーがない場合は、その IP インターフェイスでは RIP パケットが送信されず、受信した IP インターフェイスのパケットはドロップされます。

クリア テキスト認証を有効にする場合、**ip rip authentication-key** インターフェイス コマンドでパスワードを設定する必要があります。IPインターフェイスのパスワードが定義されていない場合は、その IP インターフェイスでは RIP パケットが送信されず、受信した IP インターフェイスのパケットはドロップされます。

例

次に、md5 モードを設定する例を示します。

switchxxxxxx(config)# **interface ip** 1.1.1.1

```
switchxxxxxx(config-route-map)# ip rip authentication mode md5
switchxxxxxx(config-route-map)# exit
```

ip rip authentication-key

RIPクリアテキスト認証を使用している隣接ルータが使用するパスワードを割り当てるには、インターフェイス コンフィギュレーション モードで **ip rip authentication-key** コマンドを使用します。RIP パスワードを削除するには、このコマンドの **no** 形式を使用します。

構文

ip rip authentication-key *password*

no ip rip authentication-key

パラメータ

- ***password***：キーボードから入力可能な最大 16 文字の文字列。

デフォルト設定

パスワードは指定されません。

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

このコマンドで作成するパスワードは「キー」として使用され、このキーはスイッチ ソフトウェアによるルーティング プロトコル パケットの発信時にRIPヘッダーに直接挿入されます。各サブネットワークに別のパスワードを割り当てることができます。RIP 情報を交換するには、同じサブネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。

IPインターフェイスごとに 1 つのパスワードのみ定義できます。各 **ip rip authentication-key** コマンドは、以前の定義をオーバーライドします。

例

次に、パスワードを定義する例を示します。

switchxxxxxx(config)# **interface ip** 1.1.1.1

```
switchxxxxxx(config-route-map)# ip rip authentication mode text
switchxxxxxx(config-route-map)# ip rip authentication-key alph$$12
switchxxxxxx(config-route-map)# exit
```

ip rip default-information originate

ip rip default-information originate IP インターフェイスは、RIP のデフォルト ルートのメトリックを生成します。機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip rip default-information originate {disable | *metric*}

no ip rip default-information originate

パラメータの範囲

- **disable**：デフォルト ルートを送信しません。
- ***metric***：デフォルト ルートのメトリック値。範囲：1 ～ 15。

デフォルト設定

RIP の動作は **default-information originate** コマンドによって指定されます。

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

特定の IP インターフェイス上で **default-information originate** コマンドによって指定された RIP 動作をオーバーライドするには、このコマンドを使用します。

例

次の例では、メトリック 3 のデフォルト ルートの送信を有効にする方法を示します。

switchxxxxxx(config)# **interface ip** 1.1.1.1

```
switchxxxxxx(config-route-map)# ip rip default-information originate 3
switchxxxxxx(config-route-map)# exit
```

ip rip distribute-list in

ip rip distribute-list in IP コンフィギュレーション モード コマンドは、着信 RIP アップデート メッセージ内のルートのフィルタリングを有効にします。このコマンドの **no** 形式は、フィルタリングを無効にします。

構文

ip rip distribute-list access *access-list-name* **in**

no ip rip distribute-list in

パラメータ

- *access-list-name*：最大 32 文字の標準 IP アクセス リスト名。このリストは、着信 RIP アップデート メッセージ内のどのルートを承認し、どのルートを抑制するかを定義します。

デフォルト設定

フィルタリングなし

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

受信した RIP アップデート メッセージから各ネットワークがアクセス リストによって評価され、リストによって許可されている場合にのみ承認されます。詳細については、**ip access-list (IP standard)** および **ip prefix-list** コマンドを参照してください。

例

次に、入力フィルタリングを定義する例を示します。

```
witchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip distribute-list access 5 in
switchxxxxxx(config-route-map)# exit
```

ip rip distribute-list out

ip rip distribute-list out IP コンフィギュレーション モード コマンドは、発信 RIP アップデート メッセージ内のルートのフィルタリングを有効にします。このコマンドの **no** 形式は、フィルタリングを無効にします。

構文

ip rip distribute-list access *access-list-name* **out**

no ip rip distribute-list out

パラメータ

- ***access-list-name***：最大 32 文字の標準 IP アクセス リスト名。このリストは、発信 RIP アップデート メッセージ内のどのルートを送信し、どのルートを抑制するかを定義します。

デフォルト設定

フィルタリングなし

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

IP フォワーディング テーブルから各ネットワークがリストによって評価され、リストによって許可される場合にのみ RIP アップデート メッセージに含められます。**ip access-list (IP standard)** および **ip prefix-list** コマンドを参照してください。

例

次に、発信フィルタリングを定義する例を示します。

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip distribute-list access 5 out
switchxxxxxx(config-route-map)# exit
```

ip rip offset

ip rip offset IP コンフィギュレーション モード コマンドは、着信ルートへの追加のメトリックを定義します。このコマンドの **No** 形式を使用するとデフォルトに戻ります。

構文

ip rip offset *offset*

no ip rip offset

パラメータ

- ***offset***：受信したルートに適用するオフセットを指定します。範囲：1 ～ 15。

デフォルト設定

offset：1。

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

例

次の例は、オフセットを 2 に設定する方法を示します。

switchxxxxxx(config)# **interface ip** 1.1.1.1

```
switchxxxxxx(config-route-map)# ip rip offset 2
switchxxxxxx(config-route-map)# exit
```

ip rip passive-interface

ip rip passive-interface IP インターフェイス コンフィギュレーション モード コマンドは、IP インターフェイス上の RIP パケットの送信を無効にします。このコマンドの **no** 形式は、RIP パケットの送信を再び有効にします。

構文

ip rip passive-interface

no ip rip passive-interface

デフォルト設定

RIP メッセージは送信されます。

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

特定の IP インターフェイスで RIP メッセージの送信を停止するには、**ip rip passive-interface** コマンドを使用します。すべてのインターフェイスでRIPメッセージの送信を停止するには、**passive-interface** コマンドを使用します。

注。no ip rip passive-interface コマンドは、**passive-interface** コマンドをオーバーライドしません。

例

次の例では、RIP メッセージの送信を停止する方法を示します。

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip passive-interface
switchxxxxxx(config-route-map)# exit
```

ip rip distribute-list in

ip rip distribute-list in IP コンフィギュレーション モード コマンドは、着信 RIP アップデート メッセージ内のルートのフィルタリングを有効にします。このコマンドの **no** 形式は、フィルタリングを無効にします。

構文

ip rip distribute-list access *access-list-name* **in**

no ip rip distribute-list in

パラメータ

- *access-list-name*：最大 32 文字の標準 IP アクセス リスト名。このリストは、着信 RIP アップデート メッセージ内のどのルートを承認し、どのルートを抑制するかを定義します。

デフォルト設定

フィルタリングなし

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

受信した RIP アップデート メッセージから各ネットワークがアクセス リストによって評価され、リストによって許可されている場合にのみ承認されます。詳細については、**ip access-list (IP standard)** および **ip prefix-list** コマンドを参照してください。

例

次に、入力フィルタリングを定義する例を示します。

```
witchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip distribute-list access 5 in
switchxxxxxx(config-route-map)# exit
```

ip rip distribute-list out

ip rip distribute-list out IP コンフィギュレーション モード コマンドは、発信 RIP アップデート メッセージ内のルートのフィルタリングを有効にします。このコマンドの **no** 形式は、フィルタリングを無効にします。

構文

ip rip distribute-list access *access-list-name* **out**

no ip rip distribute-list out

パラメータ

- ***access-list-name***：最大 32 文字の標準 IP アクセス リスト名。このリストは、発信 RIP アップデート メッセージ内のどのルートを送信し、どのルートを抑制するかを定義します。

デフォルト設定

フィルタリングなし

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

IP フォワーディング テーブルから各ネットワークがリストによって評価され、リストによって許可される場合にのみRIPアップデートメッセージに含められます。**ip access-list (IP standard)** および **ip prefix-list** コマンドを参照してください。

例

次に、発信フィルタリングを定義する例を示します。

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip distribute-list access 5 out
switchxxxxxx(config-route-map)# exit
```

ip rip offset

ip rip offset IP コンフィギュレーション モード コマンドは、着信ルートへの追加のメトリックを定義します。このコマンドの **No** 形式を使用するとデフォルトに戻ります。

構文

ip rip offset *offset*

no ip rip offset

パラメータ

- ***offset***：受信したルートに適用するオフセットを指定します。範囲：1 ～ 15。

デフォルト設定

offset：1。

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

例

次の例は、オフセットを 2 に設定する方法を示します。

switchxxxxxx(config)# **interface ip** 1.1.1.1

```
switchxxxxxx(config-route-map)# ip rip offset 2
switchxxxxxx(config-route-map)# exit
```

ip rip passive-interface

ip rip passive-interface IP インターフェイス コンフィギュレーション モード コマンドは、IP インターフェイス上の RIP パケットの送信を無効にします。このコマンドの **no** 形式は、RIP パケットの送信を再び有効にします。

構文

ip rip passive-interface

no ip rip passive-interface

デフォルト設定

RIP メッセージは送信されます。

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

特定の IP インターフェイスで RIP メッセージの送信を停止するには、**ip rip passive-interface** コマンドを使用します。すべてのインターフェイスでRIPメッセージの送信を停止するには、**passive-interface** コマンドを使用します。

注。no ip rip passive-interface コマンドは、**passive-interface** コマンドをオーバーライドしません。

例

次の例では、RIP メッセージの送信を停止する方法を示します。

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip passive-interface
switchxxxxxx(config-route-map)# exit
```

ip rip shutdown

ip rip shutdown IP インターフェイス コンフィギュレーション モード コマンドは、RIP インターフェイスの状態を **enabled** から **disabled** に変更します。このコマンドの **no** 形式は、状態を **enabled** の値に戻します。

構文

ip rip shutdown

no ip rip shutdown

デフォルト設定

有効

コマンド モード

IP コンフィギュレーション モード

使用上のガイドライン

設定を削除せずに IP インターフェイスの RIP を無効にするには、**ip rip shutdown** CLI コマンドを使用します。**ip rip shutdown** CLI コマンドは、**network** CLI コマンドによって作成された RIP インターフェイスだけに適用できます。**ip rip shutdown** CLI コマンドは、RIP インターフェイス設定を削除しません。

例

次の例では、1.1.1.1 の IP インターフェイスで RIP メッセージを無効にする方法を示します。

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip shutdown
switchxxxxxx(config-route-map)# exit
```

network

network ルータ RIP コンフィギュレーション モード コマンドは、特定の IP インターフェイスで RIP を有効にします。このコマンドの **no** 形式は、特定の IP インターフェイスで RIP を無効にして、そのインターフェイス設定を削除します。

構文

network *ip-address* [**shutdown**]

no network *ip-address*

パラメータ

- ***ip-address***：スイッチの IP インターフェイスの IP アドレス。
- **shutdown**：シャットダウン状態のインターフェイスで RIP が有効です。

コマンド モード

ルータ RIP コンフィギュレーション モード

使用上のガイドライン

RIP は、手動で設定された IP インターフェイスでのみ定義できます。これは、DHCP で定義された IP アドレス、またはデフォルトの IP アドレスでは RIP を定義できないことを意味します。

RIP 設定のデフォルト値を変更して、**no ip rip shutdown** CLI コマンドを使用し、インターフェイスで RIP を作成する場合は、**shutdown** キーワードを指定して **network** CLI コマンドを使用します。

IP インターフェイスの RIP を削除し、そのインターフェイス設定を削除するには、**no network** CLI コマンドを使用します。

例 1。次の例では、デフォルトのインターフェイス構成の IP インターフェイス 1.1.1.1 で RIP を有効にする方法を示します。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 1.1.1.1
switchxxxxxx(config-rip)# exit
```

例 2。次の例では、シャットダウン状態の 1.1.1.1 で RIP を有効にして、メトリックを設定し RIP を開始します。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 1.1.1.1 shutdown
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip offset 2
switchxxxxxx(config-route-map)# no ip rip shutdown
switchxxxxxx(config-route-map)# exit
```

passive-interface（RIP）

すべてのRIP IPインターフェイスでルーティング アップデートの送信を無効にするには、ルータ RIP コンフィギュレーション モードで **passive-interface** コマンドを使用します。RIP ルーティング アップデートの送信を再び有効にするには、このコマンドの **no** 形式を使用します。

構文

passive-interface

no passive-interface

デフォルト設定

ルーティング アップデートは、すべての IP RIP インターフェイスで送信されます。

コマンド モード

ルータ RIP コンフィギュレーション モード

使用上のガイドライン

passive-interface コマンドを使用した後、**no ip rip passive-interface** コマンドを使用して隣接関係が必要な個々のインターフェイスを設定できます。

例

次の例では、すべての IP インターフェイスをパッシブとして設定し、次に IP インターフェイス 1.1.1.1 を除外します。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# passive-interface
switchxxxxxx(config-rip)# network 1.1.1.1
switchxxxxxx(config-rip)# network 2.2.2.2
switchxxxxxx(config-rip)# network 3.3.3.3
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# no ip rip passive-interface
switchxxxxxx(config-route-map)# exit
```

redistribute（RIP）

ルーティング ドメインから別の RIP ルーティング ドメインに ルートを再配布するには、ルータ RIP コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を無効にするには、このコマンドの **no** 形式を使用します。

構文

redistribute *protocol* [**metric** {*metric-value* | **transparent**}]

no redistribute *protocol*

パラメータ

- ***protocol***：ルートの再配布元のプロトコルです。**connected** または **static** のいずれかのキーワードを指定できます。
- **metric transparent**：RIP で RIP メトリックとして再配布ルートの配布元プロトコル メトリックを使用します。16 よりも小さいメトリックを持つルートのみが再配布されます。
- **metric** *metric-value*：再配布されたルートに割り当てられたメトリックを指定します。この値は、**default-metric** コマンドを使用して指定したメトリック値よりも優先されます。

デフォルト設定

ルート再配布は無効です。

コマンド モード

ルータ RIP コンフィギュレーション モード

使用上のガイドライン

配布元プロトコルに配布されたルートは、これにより再配布されることはありません。

connected キーワードは、RIP が有効になっていない定義済みの IP インターフェイスに対応する RIP ルートへ再配布するために使用します。デフォルトでは、RIP ルーティング テーブルには、有効になっている IP インターフェイスのみに対応するルートのみが含まれています。

static キーワードは、RIP スタティック ルートを再配布する場合に使用します。デフォルトでは、スタティック ルートは RIP に再配布されません。

メトリック値をルート マップで（**set metric** コマンドで）設定する場合、この値は *metric-value* 引数で指定されたメトリック値よりも優先されます。

metric キーワードが定義されていない場合、**default-metric** CLI コマンドで指定されたメトリックが、再配布されたルートに割り当てられます。ルートマップによって設定されたメトリック値が 16 以上の場合、ルートは再配布ではありません。

キーワードを変更または無効にしても、他のキーワードの状態には影響しません。

redistribute コマンドに設定したオプションを削除するには、期待する結果が得られるように **redistribute** コマンドの **no** 形式を慎重に使用する必要があります。

例 1。次の例では、透過的なメトリックでの RIP によるスタティック ルートの再配布を有効にします。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# exit
```

例 2。次の例では、透過的なメトリックでの RIP によるスタティック ルートの再配布を有効にして、次にメトリックをデフォルトに変更します。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# no redistribute static metric transparent
switchxxxxxx(config-rip)# exit
```

例 3。次の例では、デフォルトのメトリックでの RIP によるスタティック ルートの再配布を有効にして、次にメトリックを透過的に変更します。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# exit
```

例 4。次の例では、透過的なメトリックでの RIP によるスタティック ルートの再配布を有効にします。2 番目の再配布コマンドの影響はありません。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# redistribute static
switchxxxxxx(config-rip)# exit
```

例 5。次の例では、RIP によるスタティック ルートの再配布を無効にします。

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# no redistribute static
switchxxxxxx(config-rip)# exit
```

router rip

router rip グローバル コンフィギュレーション モード コマンドは、ルータ RIP モードを指定し、無効になっている場合は有効にします。このコマンドの **no** 形式は、RIP をグローバルに無効にして、その設定を削除します。

構文

router rip

no router rip

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

RIP は次のグローバル状態をサポートしています。

- disabled
- enabled
- shutdown

RIP グローバル状態の値が **disabled**（デフォルト値）の場合、RIP は動作せず、設定できません。この状態が設定されている場合、RIP 設定は削除されます。任意の RIP グローバル状態から **no router rip** CLI コマンドによって状態を設定できます。

RIP グローバル状態の値が **shutdown** の場合、RIP は動作しませんが、設定はできます。この状態が設定されている場合は、RIP 設定は変更されません。**enabled** RIP グローバル状態から **shutdown** CLI コマンドによって状態を設定できます。

RIP グローバル状態の値が **enabled** の場合、RIP は動作しており、設定できます。状態は、**disabled** RIP グローバル状態から **router rip** CLI コマンドによって、また **shutdown** RIP グローバル状態から **no shutdown** CLI コマンドによって設定できます。

例

次の例は、RIP をグローバルに有効にする方法を示します。

```
router rip
```

show ip rip database

show ip rip database 特権 EXEC モード コマンドは、RIP データベースに関する情報を表示します。

構文

show ip rip database [all | brief | *ip-address*]

パラメータ

- **all**：すべての RIP インターフェイスに関する完全な RIP データベース情報を提供します。オプションはパラメータを省略した場合を想定しています。
- **brief**：RIP データベース情報の一覧ビューを提供します。
- ***ip-address***：指定した IP アドレスに関する完全な RIP データベース情報を提供します。

コマンド モード

特権 EXEC モード

例 1：次の例では、すべての RIP インターフェイスに関する完全な RIP データベース情報を表示します。

```
switchxxxxxx# show ip rip database
RIP is enabled
RIP Administrative state is UP
Default metric value is 1
Redistributing is enabled from
Connected:
Metric is default-metric
Static:

Metric is transparent
IP Interface: 1.1.1.1
Administrative State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwitew%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is List12
IP Interface: 2.2.2.2
Administrative State is enabled
IP Interface Offset is 2
No Default Originate Metric
Authentication Type is MD5
Key Chain Name is chain1
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is 12
IP Interface: 3.3.3.3
```

```
Administrative State is enabled
IP Interface Offset is 1
IP Interface is passive
Default Originate Metric 3, on passive too
No Authentication
No IN Filtering
No OUT Filtering
IP Interface: 4.4.4.4
Administrative State is shutdown
IP Interface Offset is 1
No Authentication
No IN Filtering
No OUT Filtering
```

例 2：次の例では、指定した IP アドレスに関する完全な RIP データベース情報を表示します。

```
switchxxxxxx# show ip rip database 1.1.1.1
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: on passive only
Default metric value is 1
Redistributing is enabled from
Connected
Metric is default-metric
Static
Metric is transparent

IP Interface: 1.1.1.1
Administrative State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwitew%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is List12
```

例 3：次の例では、すべての RIP インターフェイスに関する簡単な RIP データベース情報を表示します。

```
switchxxxxxx# show ip rip database brief
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: route-map is condition
Default metric value is 1
Redistributing is enabled from
Connected
Metric is default-metric
Static
Metric is transparent


IP Interface    Admin    Offset  Passive   Default Auth.  IN Filt. OUT Filt.
                State            Interface Metric  Type   Type     Type
--------------- -------- ------- --------  ------- -----  -------  ---------
100.100.100.100 enabled    10      No          12   Text   Access   Access
2.2.2.2         enabled     2      No               MD5    Access   Access
3.3.3.3         enabled     1      Yes
4.4.4.4         shutdown    1      No
```

例 4：次の例では、RIP が無効の場合の出力を示します。

```
switchxxxxxx# show ip rip database
RIP is disabled
```

show ip rip peers

show ip rip peers 特権 EXEC モード コマンドは、RIP ピアに関する情報を表示します。

構文

show ip rip peers

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# show ip rip peers
RIP is enabled
Static redistributing is enabled with Default metric
Default redistributing metric is 1
Address       Last          Received       Received
              Update        Bad Packets    Bad Route
------------  ---------     -----------    ---------
1.1.12        00:10:17          -                1
2.2.2.3       00:10:01          -             -
```

shutdown

shutdown ルータ RIP コンフィギュレーション モード コマンドは、RIP グローバル状態を **shutdown** に設定します。このコマンドの **no** 形式は、RIP グローバル状態を **enabled** に設定します。

構文

shutdown

no shutdown

デフォルト設定

有効

コマンド モード

ルータ RIP コンフィギュレーション モード

使用上のガイドライン

設定を削除せずに RIP をグローバルに停止するには、**shutdown** CLI コマンドを使用します。

例

次の例は、RIP をグローバルにシャットダウンする方法を示します。

```
router rip
  shutdown
exit
```

RMON コマンド

この章は、次の項で構成されています。

- rmon alarm （1212 ページ）
- show rmon alarm-table （1214 ページ）
- show rmon alarm （1215 ページ）
- rmon event （1217 ページ）
- show rmon events （1218 ページ）
- show rmon log （1219 ページ）
- rmon table-size （1220 ページ）
- show rmon statistics （1221 ページ）
- rmon collection stats （1224 ページ）
- show rmon collection stats （1225 ページ）
- show rmon history （1226 ページ）

rmon alarm

アラーム条件を設定するには、**rmon alarm** グローバル コンフィギュレーション モード コマンドを使用します。アラームを削除するには、このコマンドの **no** 形式を使用します。

構文

rmon alarm *index mib-object-id interval rising-threshold falling-threshold rising-event falling-event [***type** *{***absolute** | **delta***}] [***startup** *{***rising** | **rising-falling** | **falling***}] [***owner** *name]*

no rmon alarm *index*

パラメータ

- **index**：アラーム インデックスを指定します。（範囲：1 ～ 65535）
- **mib-object-id**：サンプリングする変数のオブジェクト識別子を指定します。（有効なOID）
- **interval**：データをサンプリングして上昇しきい値および下限しきい値と比較する間隔（秒単位）。（範囲：1 ～ 2147483647）
- **rising-threshold**：上昇しきい値を指定します。（範囲：0 ～ 2147483647）
- **falling-threshold**：下限しきい値を指定します。（範囲：0 ～ 2147483647）
- **rising-event**：上昇しきい値を超えるとトリガーされるイベントのインデックスを指定します。（範囲：0 ～ 65535）
- **falling-event**：下限しきい値を超えるとトリガーされるイベントのインデックスを指定します。（範囲：0 ～ 65535）
- **type** {**absolute** | **delta**}：（オプション）選択された変数をサンプリングし、しきい値と比較される値を計算するのに使用される方式。次の値が可能です。

  absolute：選択した変数値をサンプリング間隔の最後にしきい値と直接比較することを指定します。

  delta：最後のサンプルの選択した変数値を現在の値から差し引き、その差異をしきい値と比較することを指定します。

- **startup** {**rising** | **rising-falling** | **falling**}：（オプション）このエントリが有効になったときに送信できるアラームを指定します。次の値が可能です。

  rising：最初のサンプル（このエントリが有効になった後）が **rising-threshold** 以上であれば、単一の上昇アラームを生成することを指定します。

  rising-falling：最初のサンプル（このエントリが有効になった後）が ***rising-threshold*** 以上であれば、単一の上昇アラームを生成することを指定します。最初のサンプル（このエントリが有効になった後）が **falling-threshold** 以下の場合は、単一の下限アラームを生成します。

falling：最初のサンプル（このエントリが有効になった後）が **falling-threshold** 以下であれば、単一の下限アラームを生成することを指定します。

- **owner** *name*：（オプション）このアラームを設定した人の名前を指定します。（有効な文字列）

デフォルト設定

デフォルトの方式タイプは **absolute** です。

デフォルトの **startup** 方向は **rising-falling** です。

所有者名が指定されていない場合は、デフォルトで空の文字列になります。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、インデックス 1000、MIB オブジェクト ID D-Link、サンプリング間隔 360000 秒（100 時間）、上昇しきい値 1000000、下限しきい値 1000000、上昇しきい値イベント インデックス 10、下限しきい値イベント インデックス 10、absolute 方式タイプ、および上昇下限アラームでアラームを設定しています。

```
switchxxxxxx(config)#  rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10
 20
```

show rmon alarm-table

アラーム テーブルのサマリーを表示するには、**show rmon alarm-table** 特権 EXEC モード コマンドを使用します。

構文

show rmon alarm-table

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

次に、アラーム テーブルを表示する例を示します。

```
switchxxxxxx#  show rmon alarm-table

Index       OID                      Owner
-----       ----------------------   -------
1           1.3.6.1.2.1.2.2.1.10.1   CLI
2           1.3.6.1.2.1.2.2.1.10.1   Manager
3           1.3.6.1.2.1.2.2.1.10.9   CLI
```

次の表に、この出力で表示される重要なフィールドについて説明します。

フィールド	説明
Index	エントリを一意に識別するインデックス。
OID	モニタ対象の変数の OID。
Owner	このエントリを設定したエンティティです。

show rmon alarm

アラーム設定を表示するには、**show rmon alarm** 特権 EXEC モード コマンドを使用します。

構文

show rmon alarm *number*

パラメータ

alarm *number*：アラーム インデックスを指定します。（範囲：1 ～ 65535）

コマンド モード

特権 EXEC モード

例

次に、RMON 1 アラームを表示する例を示します。

```
switchxxxxxx#  show rmon alarm 1
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

次の表に、この出力で表示される重要なフィールドについて説明します。

フィールド	説明
Alarm	アラーム インデックス。
OID	モニタ対象の変数の OID。
Last Sample Value	最後のサンプリング期間の統計値。たとえば、サンプル タイプが **delta** の場合、この値は、その期間の開始時のサンプルと終了時のサンプルの差となります。サンプル タイプが **absolute** の場合、この値は、その期間の終了時にサンプリングされた値になります。
Interval	データを上昇しきい値および下限しきい値と比較するためのデータのサンプリング間隔の秒数。

フィールド	説明
Sample Type	変数をサンプリングし、しきい値と比較される値を計算する方式。値が **absolute** の場合、変数値をサンプリング間隔の最後にしきい値と直接比較します。値が **delta** の場合、最後のサンプルの変数値を現在の値から差し引き、その差異をしきい値と比較します。
Startup Alarm	このエントリを最初に設定したときに送信されるアラーム。最初のサンプルが上昇しきい値以上で、スタートアップアラームが上昇または上昇下限である場合、単一の上昇アラームが生成されます。最初のサンプルが上昇しきい値以下で、スタートアップアラームが下限または上昇下限である場合、単一の下限アラームが生成されます。
Rising Threshold	サンプリング統計上昇しきい値。現在のサンプリング値がこのしきい値以上で、最後のサンプリング期間の値がこのしきい値未満である場合、単一のイベントが生成されます。
Falling Threshold	サンプリング統計下限しきい値。現在のサンプリング値がこのしきい値以下で、最後のサンプリング期間の値がこのしきい値を超えた場合、単一のイベントが生成されます。
Rising Event	上昇しきい値を超えると使用されるイベント インデックス。
Falling Event	下限しきい値を超えると使用されるイベント インデックス。
Owner	このエントリを設定したエンティティ。

rmon event

イベントを設定するには、**rmon event** グローバル コンフィギュレーション モード コマンドを使用します。イベントを削除するには、このコマンドの **no** 形式を使用します。

構文

rmon event *index {***none** | **log** | **trap** | **log-trap***} [***community** *text] [***description** *text] [***owner** *name]*

no rmon event *index*

パラメータ

- **index**：イベント インデックスを指定します。（範囲：1 ～ 65535）
- **none**：このイベントについてはデバイスによって通知が生成されないことを指定します。
- **log**：このイベントについてはデバイスによって通知エントリがログ テーブルに生成されることを指定します。
- **trap**：このイベントについてはデバイスによってSNMP トラップが 1 つ以上の管理ステーションに送信されることを指定します。
- **log-trap**：このイベントについてはデバイスによってエントリがログテーブルに生成され、SNMP トラップが 1 つ以上の管理ステーションに送信されることを指定します。
- **community text**：（オプション）SNMP トラップの送信時に使用される SNMP コミュニティ（パスワード）を指定します。（オクテット文字列の長さ：0 ～ 127 文字）これは、「snmp-server host」コマンドを使用してSNMP ホストを定義する際に使用されたコミュニティである必要があります。
- **description text**：（オプション）このイベントについて説明するコメントを指定します。（長さ：0 ～ 127 文字）
- **owner name**：（オプション）このイベントを設定した人の名前を指定します。（有効な文字列）

デフォルト設定

所有者名が指定されていない場合は、デフォルトで空の文字列になります。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、インデックス 10 として識別されるイベントを設定しています。このイベントについて、デバイスはログ テーブルに通知を生成します。

```
switchxxxxxx(config)#  rmon event 10 log
```

show rmon events

RMON イベント テーブルを表示するには、**show rmon events** 特権 EXEC モード コマンドを使用します。

構文

show rmon events

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

次に、RMON イベント テーブルを表示する例を示します。

```
switchxxxxxx#  show rmon events

Index   Description     Type      Community   Owner     Last time sent
-----1  ----------Errors------Log---------   ------    ------------------
2       High Broadcast  Log       router      CLI       Jan 18 2006 23:58:17
                        Trap                  Manager   Jan 18 2006 23:59:48
```

次の表に、この出力で表示される重要なフィールドについて説明します。

フィールド	説明
Index	このイベントを識別する一意のインデックス。
説明	このイベントについて説明するコメント。
Type	このイベントに関してデバイスが生成する通知のタイプ。**none**、**log**、**trap**、**log-trap** のいずれかの値を設定できます。ログの場合、イベントごとにエントリがログ テーブルに作成されます。トラップの場合は、SNMP トラップが 1 つ以上の管理ステーションに送信されます。
Community	SNMP トラップが送信される場合は、このオクテット文字列で指定された SNMP コミュニティ文字列も一緒に送信されます。
Owner	このイベントを設定したエンティティ。
Last time sent	このエントリがイベントを最後に生成した時間。このエントリがイベントを 1 つも生成していない場合、この値は 0 になります。

show rmon log

RMON ログ テーブルを表示するには、**show rmon log** 特権 EXEC モード コマンドを使用します。

構文

show rmon log [*event*]

パラメータ

event：（オプション）イベント インデックスを指定します。（範囲：0 ～ 65535）

コマンド モード

特権 EXEC モード

例

次に、RMON ログ テーブルにイベント 1 を表示する例を示します。

```
switchxxxxxx#  show rmon log 1
Maximum table size: 500 (800 after reset)

Event          Description                 Time
-----          -------------               -------------------
1              MIB Var.:                   Jan 18 2006 23:48:19
               1.3.6.1.2.1.2.2.1.10.53,
               Delta, Rising, Actual Val:
                800, Thres.Set: 100,
               Interval (sec):1
```

rmon table-size

RMON テーブルの最大サイズを設定するには、**rmon table-size** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトのサイズに戻すには、no 形式のコマンドを使用します。

構文

rmon table-size {**history** *entries* | **log** *entries*}

no rmon table-size {**history** | **log**}

パラメータ

- **history** *entries*：履歴テーブルのエントリの最大数を指定します。（範囲：20 ～ 32767）
- **log** *entries*：ログ テーブルのエントリの最大数を指定します。（範囲：20 ～ 32767）

デフォルト設定

履歴テーブルのデフォルト サイズは 270 エントリです。

ログ テーブルのデフォルト サイズは 200 エントリです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

設定したテーブル サイズは、デバイスのリブート後に有効になります。

例

次に、RMON 履歴テーブルの最大サイズを 100 エントリに設定する例を示します。

```
switchxxxxxx(config)#  rmon table-size history 100
```

show rmon statistics

RMON イーサネット統計を表示するには、**show rmon statistics** 特権 EXEC モード コマンドを使用します。

構文

show rmon statistics *{interface-id}*

パラメータ

interface-id：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

特権 EXEC モード

例

次に、ポート gi1/0/1 の RMON イーサネットの統計情報を表示する例を示します。

```
switchxxxxxx#  show rmon statistics gi1/0/1
Port gi1/0/1
Dropped: 0
Octets: 0                       Packets: 0
Broadcast: 0                    Multicast: 0
CRC Align Errors: 0             Collisions: 0
Undersize Pkts: 0               Oversize Pkts: 0
Fragments: 0                    Jabbers: 0
64 Octets: 0                    65 to 127 Octets: 1
128 to 255 Octets: 1            256 to 511 Octets: 1
512 to 1023 Octets: 0           1024 to max Octets: 0
```

次の表では、表示される重要なフィールドについて説明します。

フィールド	説明
Dropped	リソース不足のためにプローブによってパケットがドロップされたイベントの合計数。この数は、必ずしもドロップされたパケットの数ではないことに注意してください。この条件が検出された回数です。
Octets	ネットワーク上での受信データ（不良パケット内のデータを含む）のオクテットの合計数（フレーミング ビットを除くが、FCS オクテットは含む）。
Packets	受信したパケットの合計数（不良パケット、ブロードキャスト パケット、マルチキャスト パケットを含む）。
Broadcast	ブロードキャストアドレスに送信された受信正常パケットの合計数。マルチキャスト パケットは含まれません。

フィールド	説明
Multicast	マルチキャストアドレスに送信された受信正常パケットの合計数。この数には、ブロードキャスト アドレス宛てのパケットは含まれていません。
CRC Align Errors	長さが 64 ～ 1518 オクテットの範囲（フレーミング ビットを除くが、FCS オクテットは含む）で、オクテットの整数倍のフレーム チェック シーケンス（FCS）不良（FCS エラー）またはオクテットの整数倍でない FCS 不良（アライメント エラー）が含まれる受信されたパケットの合計数。
Collisions	このイーサネット セグメントにおける合計衝突数の最小推定値。
Undersize Pkts	長さ（フレーミング ビットは除くが、FCS オクテットは含む）が 64 オクテット未満であるが、それ以外の形式は良好であった、受信パケットの合計数。
Oversize Pkts	長さ（フレーミング ビットは除くが、FCS オクテットは含む）が 1518 オクテットを超えるが、それ以外の形式は良好であった、受信パケットの合計数。
Fragments	長さ（フレーミング ビットは除くが、FCS オクテットは含む）が 64 オクテット未満で、オクテット数が整数でフレーム チェック シーケンス（FCS）が不正であるか（FCS エラー）、オクテット数が整数でなく FCS が不正な（アライメント エラー）、受信パケット数の合計。
Jabbers	1518 オクテットより長く（フレーミング ビットは除くが、FCS オクテットは含む）、オクテット数が整数でフレーム チェック シーケンス（FCS）が不正であるか（FCS エラー）、オクテット数が整数でなく FCS が不正な（アライメント エラー）、受信パケット数の合計。
64 Octets	長さ（フレーミング ビットは除くが、FCS オクテットは含む）が 64 オクテットの受信パケット（フレーミング ビットは除くが、FCS オクテットは含む）の合計数。
65 to 127 Octets	長さが 65 オクテット以上 127 オクテット以下（フレーミング ビットを除くが、FCS オクテットは含む）の受信パケット（不良パケットを含む）の合計数。
128 to 255 Octets	長さが 128 オクテット以上 255 オクテット以下（フレーミング ビットを除くが、FCS オクテットは含む）の受信パケット（不良パケットを含む）の合計数。
256 to 511 Octets	長さが 256 オクテット以上 511 オクテット以下（フレーミング ビットを除くが、FCS オクテットは含む）の受信パケット（不良パケットを含む）の合計数。

フィールド	説明
512 to 1023 Octets	長さが 512 オクテット以上 1023 オクテット以下（フレーミング ビットを除くが、FCS オクテットは含む）の受信パケット（不良パケットを含む）の合計数。
1024 to max	長さが 1024 オクテットから最大フレーム サイズの範囲（フレーミング ビットは除くが、FCS オクテットは含む）にある受信パケット（不良パケットを含む）の合計数。

rmon collection stats

RMON MIB にインターフェイスの履歴統計を収集するには（グループ化）、**rmon collection stats**インターフェイス コンフィギュレーション モード コマンドを使用します。指定したRMON履歴統計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。

構文

rmon collection stats index *[***owner** *ownername] [***buckets** *bucket-number] [***interval** *seconds]*

no rmon collection stats *index*

パラメータ

- **index**：要求した統計グループのインデックス。（範囲：1 ～ 65535）
- **owner** *ownername*：（オプション）RMON 統計グループの所有者名を記録します。未指定の場合、名前は空の文字列になります。(範囲：有効な文字列)
- **buckets** *bucket-number*：（オプション）RMON コレクション履歴統計グループに指定されているバケットの数に関連付けられた値。指定しない場合、デフォルトは 50 です。（範囲：1 ～ 50）
- **interval** *seconds*：（オプション）各ポーリング サイクルの秒数。指定しない場合、デフォルトは 1800 です。（範囲：1 ～ 3600）

コマンド モード

インターフェイス コンフィギュレーション モード.

show rmon collection stats

要求した RMON 履歴グループ統計を表示するには、**show rmon collection stats** 特権 EXEC モード コマンドを使用します。

構文

show rmon collection stats *[interface-id]*

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

特権 EXEC モード

例

次に、すべての RMON 履歴グループ統計を表示する例を示します。

```
switchxxxxxx#  show rmon collection stats

Index   Interface   Interval   Requested   Granted   Owner
                               Samples     Samples
-----   ---------   --------   ---------   -------   -------
1       gi1/0/1     30         50          50        CLI
2       gi1/0/1     1800       50          50        Manager
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

フィールド	説明
Index	エントリを一意に識別するインデックス。
Interface	サンプリングしたイーサネット インターフェイス。
Interval	サンプル間の秒単位の間隔。
Requested Samples	保存するサンプルの要求数。
Granted Samples	保存するサンプルの許可数。
Owner	このエントリを設定したエンティティです。

show rmon history

RMON イーサネット履歴統計を表示するには、**show rmon history** 特権 EXEC モード コマンドを使用します。

構文

show rmon history *index {***throughput** | **errors** | **other***} [***period** *seconds*]

パラメータ

- **index**：表示するサンプルのセットを指定します。（範囲：1 ～ 65535）
- **throughput**：スループット カウンタを表示します。
- **errors**：エラー カウンタを表示します。
- **other**：ドロップ カウンタおよび衝突カウンタを表示します。
- **period** *seconds*：（オプション）表示する期間を秒単位で指定します。（範囲：1 ～ 2147483647）

コマンド モード

特権 EXEC モード

例

次に、インデックス 1 の RMON イーサネット履歴統計を表示する例を示します。

```
switchxxxxxx#  show rmon history 1 throughput

Sample Set: 1                          Owner: CLI
Interface: gi1/0/1                     Interval: 1800
Requested samples: 50                  Granted samples: 50

Maximum table size: 500

Time                 Octets     Packets   Broadcast   Multicast   Util
-------------------  --------   -------   ---------   ---------   ----
Jan 18 2005 21:57:00 303595962  357568    3289        7287        19%
Jan 18 2005 21:57:30 287696304  275686    2789        5878        20%

switchxxxxxx#  show rmon history 1 errors

Sample Set: 1                          Owner: Me
Interface:gi1/0/1                      Interval: 1800
Requested samples: 50                  Granted samples: 50

Maximum table size: 500 (800 after reset)
```

```
Time                  CRC Align  Under     Oversize  Fragments  Jabbers
------------          -------    size      --------  ---------  ----
Jan 18 2005 21:57:00  1          -----     0         49         0
Jan 18 2005 21:57:30  1          1         0         27         0
                                 1
```

```
switchxxxxxx#  show rmon history 1 other
```

```
Sample Set: 1                          Owner: Me
Interface: gi1/0/1                     Interval: 1800
Requested samples: 50                  Granted samples: 50
```

```
Maximum table size: 500
```

```
Time                  Dropped   Collisions
--------------------  ------    ----------
Jan 18 2005 21:57:00  3         0
Jan 18 2005 21:57:30  3         0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

フィールド	説明
Time	エントリが記録される日付と時刻。
Octets	ネットワーク上で受信したデータ（不良パケット内のデータは含み、フレーミング ビットは除くが、FCS オクテットは含む）のオクテットの合計数。
Packets	このサンプリング間隔中に受信したパケットの数（不良パケットを含む）。
Broadcast	このサンプリング間隔中に受信したブロードキャストアドレス宛ての正常パケットの数。
Multicast	このサンプリング間隔中に受信したマルチキャストアドレス宛ての正常パケットの数。この数には、ブロードキャストアドレス宛てのパケットは含まれていません。
Utilization	このサンプリング間隔中にこのインターフェイスで測定される平均物理層ネットワーク使用率の最小推定値（百分率）。
CRC Align	このサンプリング間隔中に受信したパケットのうち、長さが 64 ～ 1518 オクテットの範囲（フレーミング ビットを除くが、FCS オクテットは含む）で、オクテットの整数倍のフレーム チェック シーケンス（FCS）不良（FCS エラー）またはオクテットの整数倍でない FCS 不良（アライメント エラー）があったパケットの数。
Undersize	このサンプリング間隔中に受信したパケットのうち、長さが 64 オクテット未満（フレーミング ビットを除くが、FCS オクテットは含む）で、それ以外は適切な形式であったパケットの数。

フィールド	説明
Oversize	このサンプリング間隔中に受信したパケットのうち、長さが 1518 オクテットより長く（フレーミング ビットを除くが、FCS オクテットは含む）で、それ以外は適切な形式であったパケットの数。
Fragments	このサンプリング間隔中に受信したパケットのうち、長さ（フレーミング ビットは除くが、FCS オクテットは含む）が 64 オクテット未満で、オクテットの整数倍のフレーム チェック シーケンス（FCS）不良（FCS エラー）またはオクテットの整数倍でない FCS 不良（アライメント エラー）があったパケットの数。ラント（コリジョンによる正常な発生）とノイズ ヒットの両方がカウントされるため、etherHistoryFragments が増加するのは正常です。
Jabbers	このサンプリング間隔中に受信したパケットのうち、1518 オクテットより長く（フレーミング ビットを除くが、FCS オクテットは含む）、オクテットの整数倍のフレーム チェック シーケンス（FCS）不良（FCS エラー）またはオクテットの整数倍でない FCS 不良（アライメント エラー）があったパケットの数。
Dropped	このサンプリング間隔中にリソース不足のためにプローブによってパケットがドロップされたイベントの合計数。この数は、必ずしもドロップされたパケット数ではありません。この状態が検出された回数です。
Collisions	このサンプリング間隔中におけるこのイーサネット セグメントでの合計衝突数の最小推定値。

ルータ リソース コマンド

この章は、次の項で構成されています。

- show system resources （1230 ページ）
- set router hardware-routing active （1232 ページ）
- show router hardware-routing status （1234 ページ）
- system resources （1235 ページ）

show system resources

IP エントリ、ポリシーベースのルート、および VLAN マッピングに現在使用されているエントリと最大許容エントリを表示するには、ユーザ EXEC モードで **show system resources** コマンドを使用します。

構文

show system resources

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

現在使用している IP エントリおよび最大許容 IP エントリ、ポリシーベースのルート、ならびに VLAN マッピングエントリを表示するには、**show system resources** コマンドを使用します。

コマンド出力の「in use」エントリの数は、次のように計算されます。

「*policy routes*」エントリ：作成したポリシーマップごとに 1 つのエントリが消費されます。

- 「*vlan mapping*」エントリ：8 つのエントリがシステム用に予約されています。
  - インターフェイスに適用される VLAN マッピングエントリごとに 1 つのエントリが消費されます。
- 「*IP entries*」エントリ：IP エントリ数にはさまざまなタイプのエントリを含めることができます。次の表に、各エントリタイプごとの IP エントリの消費数の詳細を示します。

論理エンティティ	消費した IP エントリの数
IP ホスト/ネイバー	ネイバーあたり 1 エントリ
IPv4 インターフェイス	インターフェイスあたり 2 エントリ
IPv4（リモート）ルート	ルートあたり 1 エントリ
IPv4 マルチキャストグループ	グループあたり 2 エントリ
IPv6 ホスト/ネイバー	ネイバーあたり 4 エントリ
IPv6 インターフェイス	インターフェイスあたり 8 エントリ
リンクプレフィックスの IPv6	プレフィックスあたり 4 エントリ

論理エンティティ	消費した IP エントリの数
IPv6（リモート）ルート	ルートあたり 4 エントリ
IPv6 マルチキャストグループ	グループあたり 8 エントリ

例

次に、タイプごとに使用中のエントリと最大エントリを表示する例を示します。

```
switchxxxxxx# show system resources
                        In-Use              Max
                        ------             --------
IP Entries                 10                500
IPv4 policy Routes         0                 16
IPv6 policy Routes         16                32
VLAN Mapping Entries       48                64
```

set router hardware-routing active

デバイスでハードウェアベースのルーティングを再アクティブ化するプロセスを開始するには、**set router hardware-routing active** 特権 EXEC モードコマンドを使用します。

構文

set router hardware-routing active

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

IPv4 ルートまたは IPv6 ルートが有効になると、デバイスでハードウェアベースのルーティングが自動的にサポートされます。ただし、デバイスハードウェアのリソースが IPv4 エントリまたは IPv6 エントリ、あるいはその両方の数量をサポートできない場合、ハードウェアベースのルーティングはソフトウェアによって自動的に非アクティブ化されます。

IPv4 エントリ：IPv4 インターフェイス/アドレスとルート、および IPv4 マルチキャストエントリ。

IPv6 エントリ：IPv6 インターフェイス/アドレスとルート、および IPv6 マルチキャストエントリ。

ハードウェアベースのルーティングがシステムによって非アクティブ化されると、ユーザは **set router hardware-routing active** コマンドを適用してデバイスのハードウェアベースのルーティングを再アクティブ化する必要があります。デバイスのハードウェア機能に一致するように、デバイス上の IPv4 エントリまたは IPv6 エントリ、あるいはその両方の数を調整することを推奨します。

コマンドが適用されると、デバイスはデバイスのハードウェアテーブルに対する既存のすべての IP エントリの更新を開始します。プロセスが成功すると、ハードウェアベースのルーティングが再アクティブ化されます。プロセスが失敗した場合（たとえば、デバイスハードウェアのリソースが現在のデバイス IP エントリをサポートするのに十分でない場合）、ハードウェア ルーティング ステータスは非アクティブのままになります。

syslog メッセージは、ハードウェアテーブルの更新プロセスの開始と、そのような更新の成功または失敗をユーザに示します。

例 1。次に、ハードウェアベースのルーティングの再アクティブ化プロセスを適用する例を示します。

```
switchxxxxxx# set router hardware-routing active
This operation may take a few moments...
```

例2。次に、ハードウェアベースのルーティングがデバイスですでにアクティブになっている場合にコマンドを適用する例を示します。

```
switchxxxxxx# set router hardware-routing active
Hardware based routing aleady active
```

show router hardware-routing status

ハードウェアベースのルーティングのステータスを表示するには、ユーザ EXEC モードで **show router hardware-routing status** コマンドを使用します。

構文

show router hardware-routing status

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

例 1。次に、ハードウェアルーティングのステータスが非アクティブとして表示される例を示します。

```
switchxxxxxx# show system router resources
Hardware routing status: inactive
```

例 2。次に、ハードウェアルーティングのステータスが「in activation」として表示される例を示します（これは通常、コマンド set router hardware-routing active （1232 ページ） のアクティブ化に続いて更新されたハードウェアテーブルが処理中であることを示します）。

```
switchxxxxxx# show system router resources
Hardware routing status: in activation
```

system resources

ポリシーベースのルーティングや VLAN マッピングのハードウェアリソースの割り当てを設定するには、グローバル コンフィギュレーション モードで **system resources** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

system resources [**policy-ip-routes** max-number] [**policy-ipv6-routes** max-number] [**vlan-mapping-entries** max-number]

no system resources

パラメータ

- **policy-ip-routes** max-number：（オプション）設定可能な IPv4 ポリシールートの最大数。（範囲：0 ー 32）
- **policy-ipv6-routes max-number**：（オプション）設定可能な IPv6 ポリシールートの最大数。（範囲：12 ～ 32）
- **vlan-mapping-entries max-number**：（オプション）設定可能な VLAN マッピングエントリの最大数。（範囲：0 ー 228）

デフォルト設定

- policy-ip-routes：12
- policy-ipv6-routes：12
- vlan-mapping-entries：0

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ポリシーベースのルートや VLAN マッピングエントリのサポートされる最大数の新しい設定を入力するには、**system resources** コマンドを使用します。コマンドを再入力すると現在の設定が表示され、ユーザは新しい設定をスタートアップ コンフィギュレーションに保存したことを確認するように求められ、その後にシステムをリブートして変更を適用する必要があります。

デバイスにダウンロードされるコンフィギュレーションファイルにこのコマンドが含まれている場合、コマンドが実行コンフィギュレーションファイルにダウンロードされると、コマンドは拒否されます。スタートアップ コンフィギュレーションファイルにダウンロードした場合、デバイスは自動的にリブートしません。新しい設定は、デバイスを手動でリブートした後で使用されます。

ポリシーベースのルートや VLAN マッピングエントリに追加のリソースを割り当てると、IP タイプのエントリで使用されるリソースが少なくなります。

VLANマッピングに割り当てられたエントリのうちの8つのエントリはシステム用に予約されており、ユーザベースの VLAN マッピング設定には使用できません。

データの検証：

新しいポリシーベースのルートやVLANマッピング値をデバイスがサポートできない場合（関連するリソースが他のアプリケーションで使用されているため）、コマンドは拒否され、メッセージがユーザに表示されます。

新しいmax-numberパラメータが現在使用中の設定の実際のエントリ数よりも少ない場合、（保存確認メッセージの前に）確認メッセージがユーザに表示されます。

デフォルトの設定を復元するには、**no system resources** コマンドを使用します。

例

例 1：次に、IPv4ポリシーベースのルート、IPv6ポリシーベースのルート、またはVLANマッピングでサポートされるエントリの数を定義する例を示します。

```
switchxxxxxx(config)# system resources policy-ip-routes 20 policy-ipv6-routes 32
vlan-mapping-entries 100
                           In-Use  Reserved (Current)  Reserved (New)
                           ------  ------------------  --------------
IPv4 policy Routes             8             16                  20
IPv6 policy Routes             8             16                  32
VLAN Mapping Entries            32            32                  100
Setting the new configuration of entries requires saving the running-configuration file
 to startup-configuration file and rebooting the system, do you want to continue? (Y/N)
 [N] Y
```

例 2：次に、デバイスで現在使用しているエントリよりも設定したエントリが少ない例を示します。この設定を使用すると、既存のネットワークにはシステムを再度実行するためのリソースが不足します。

```
switchxxxxxx(config)# system resources policy-ip-routes 8 policy-ipv6-routes 8
vlan-mapping-routes 16
                            In-Use   Reserved (Current)  Reserved (New)
                            ------   ------------------  --------------
IPv4 policy Routes            10             20                   8
IPv6 policy Routes            10              32                  8
VLAN Mapping Entries            50            100                    16
1) In one or more of the parameters, the new max entry configuration is less than the
entries which are currently in use by the system, do you want to continue?

2) Setting the new configuration of entries requires saving the running-configuration
file to startup-configuration file and rebooting the system.
Do you want to continue?
Do you want to continue? (Y/N) [N] Y
```

ルートマップコマンド

この章は、次の項で構成されています。

- match ip address（ポリシールーティング） （1238 ページ）
- match ipv6 address（ポリシールーティング） （1239 ページ）
- route-map（ポリシールーティング） （1240 ページ）
- set ip next-hop （1242 ページ）
- set ipv6 next-hop （1243 ページ）
- show route-map （1244 ページ）

match ip address（ポリシールーティング）

IP ポリシールーティングを実行するために IP パケットを一致させるには、ルート マップ コンフィギュレーション モードで **match ip address** コマンドを使用します。**match ip address** エントリを移動するには、このコマンドの **no** 形式を使用します。

構文

match ip address access-list *extended-access-list-name*

no match ip address access-list

パラメータ

- **access-list** *extended-access-list-name*：拡張 IP ACL を指定します。

デフォルト設定

なし。このコマンドは設定されません。

コマンド モード

ルート マップ コンフィギュレーション モード

使用上のガイドライン

match ip address コマンドは、拡張 IP アクセスリスト（プロトコル、プロトコル サービス、送信元または宛先の IP アドレスなど）による一致基準に基づいたパケットのポリシールーティングを可能にします。

extended-access-list-name 引数で指定された ACL リストには次のキーワードを含めることはできません。

- **time-range**
- **disable-port**
- **log-input**

例

次に、IPv4 ポリシーベースのルーティングを設定する例を示します。

```
switchxxxxxx(config)# ip access-list extended acl1
switchxxxxxx(config-ip-al)# permit ip 176.212.0.0 00.255.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr
switchxxxxxx(config-route-map)# match ip address access-list acl1
switchxxxxxx(config-route-map)# set ip next-hop 173.23.13.20
switchxxxxxx(config-route-map)# exit
```

match ipv6 address（ポリシールーティング）

IPv6 ポリシールーティングを実行するように IPv6 パケットを一致させるには、ルート マップ コンフィギュレーション モードで **match ipv6 address** コマンドを使用します。**match ipv6 address** エントリを移動するには、このコマンドの **no** 形式を使用します。

構文

match ipv6 address access-list *extended-access-list-name*

no match ipv6 address access-list

パラメータ

- **access-list** *extended-access-list-name*：拡張 IPv6 アクセスリストを指定します。

デフォルト設定

なし。このコマンドは設定されません。

コマンド モード

ルート マップ コンフィギュレーション モード

使用上のガイドライン

match ipv6 address コマンドは、拡張アクセスリスト（プロトコル、プロトコル サービス、送信元または宛先の IPv6 アドレスなど）と一致させることができる基準に基づいて IPv6 パケットのポリシールーティングを可能にします。

extended-access-list-name 引数で指定された ACL リストには次のキーワードを含めることはできません。

- **time-range**
- **disable-port**
- **log-input**

例

次に、IPv4 ポリシーベースのルーティングを設定する例を示します。

```
switchxxxxxx(config)# ipv6 access-list acl1
switchxxxxxx(config-ip-al)# permit ipv6 3211:1297::  ::/32 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr
switchxxxxxx(config-route-map)# match ipv6 address access-list acl1
switchxxxxxx(config-route-map)# set ipv6 next-hop 3003:17ac::20
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config-ip-al)# exit
```

route-map（ポリシールーティング）

ポリシールーティングの条件を定義するには、グローバル コンフィギュレーション モードでは **route-map** コマンド、ルート マップ コンフィギュレーション モードでは **match** コマンドと **set** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

構文

route-map *map-tag* [*sequence-number*]

no route-map *map-tag* [*sequence-number*]

パラメータ

- ***map-tag***：ルート マップ用のわかりやすい名前を指定します。redistribute ルータ コンフィギュレーション コマンドはこの名前を使用して、このルート マップを参照します。複数のルート マップで同じマップ タグ名を共有できます。
- ***sequence-number***：同じ名前ですでに設定されているルートマップのリストに新しいルートマップがある位置を示す正の整数の番号。このパラメータをこのコマンドの **no** 形式で使用すると、ルートマップの位置が削除されます。**route-map** コマンドでパラメータを省略すると、値 10 が適用されます。**no** 形式でパラメータを省略すると、同じマップタグ名を共有するすべてのルートマップが削除されます。

デフォルト設定

ポリシールーティングの条件が設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

route-map コマンドを使用して、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。**route map** コマンドの目的は、ポリシールーティングを定義することです。

match コマンドは、ポリシールーティングが実行される条件を指定し、**set** コマンドは match コマンドで適用された基準が満たされた場合に実行されるルーティングアクションを指定します。

- 発信パケットが許可アクションで ACL と一致する場合、パケットは **set** コマンド（ポリシーベースのルーティング）によって転送されます。
- 発信パケットが拒否アクションで ACL と一致する場合、フレームは転送テーブル（通常のルーティング）によって転送されます。

ルートマップには、同じマップタグを使用して個別の **route-map** コマンドで設定された複数のセクションを含めることができます。ルーティングされたパケットがルートマップによって確認されると、基準が強制される最初のセクションが適用されます。一致するセクションがない場合は、転送テーブルを使用した明らかな最短パスが適用されます。

例 1。次に、1 つのセクションを持つルートマップの例を示します。サブネット 156.12.5.0/24 に送信された TCP パケットは、ネクストホップ 56.1.1.1 に渡されます。

```
switchxxxxxx(config)# ip access-list extended pr-acl1
switchxxxxxx(config-ip-al)# permit tcp any any 156.12.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr
switchxxxxxx(config-route-map)# match ip address access-list pr-acl1
switchxxxxxx(config-route-map)# set ip next-hop 56.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip policy route-map pbr
switchxxxxxx(config-if)# exit
```

例 2。次に、2 つのセクションを持つルートマップの例を示します。サブネット 156.12.5.0/24 に送信される TCP パケットはネクストホップ 56.1.1.1 に渡され、サブネット 156.122.5.0/24 に送信される CP パケットはネクストホップ 50.1.1.1 に渡されます。

```
switchxxxxxx(config)# ip access-list extended pr-acl1
switchxxxxxx(config-ip-al)# permit tcp any any 156.12.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# ip access-list extended pr-acl2
switchxxxxxx(config-ip-al)# permit tcp any any 156.122.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr 10
switchxxxxxx(config-route-map)# match ip address access-list pr-acl1
switchxxxxxx(config-route-map)# set ip next-hop 56.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# route-map pbr 20
switchxxxxxx(config-route-map)# match ip address access-list pr-acl2
switchxxxxxx(config-route-map)# set ip next-hop 50.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip policy route-map pbr
switchxxxxxx(config-if)# exit
```

set ip next-hop

ネクストホップポリシールーティングのIPアドレスを指定するには、ルートマップコンフィギュレーションモードで **set ip next-hop** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

構文

set ip next-hop *next-hop*

no set ip next-hop

パラメータ

- ***next-hop***：ネクストホップルータの IPv4 アドレス。

デフォルト設定

このコマンドは、デフォルトで無効になっています。

コマンド モード

ルート マップ コンフィギュレーション モード

使用上のガイドライン

ネクスト ホップ ポリシー ルーティングの IP アドレスを設定するには、**set ip next-hop** コマンドを使用します。

例

次に、IP アドレス 192.168.30.1 をネクストホップ IP アドレスとして設定する例を示します。

```
switchxxxxxx(config)# route-map bpr
switchxxxxxx(config-route-map)# match ip address access-list acl
switchxxxxxx(config-route-map)# set ip next-hop 192.168.30.1
switchxxxxxx(config-route-map)# exit
```

set ipv6 next-hop

ネクスト ホップ ポリシー ルーティングの IPv6 アドレスを指定するには、ルート マップ コンフィギュレーション モードで **set ipv6 next-hop** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

構文

set ipv6 next-hop *next-hop*

no set ipv6 next-hop

パラメータ

- ***next-hop***：ネクストホップルータの IPv6 アドレス、またはポイントツーポイントの発信インターフェイスの発信インターフェイス ID。

デフォルト設定

このコマンドは、デフォルトで無効になっています。

コマンド モード

ルート マップ コンフィギュレーション モード

使用上のガイドライン

ネクスト ホップ ポリシー ルーティングの IPv6 アドレスを設定するには、**set ip next-hop** コマンドを使用します。

例

例 1。次に、IPv6 アドレス **3003:17ac::20** をネクストホップ IPv6 アドレスとして設定する例を示します。

```
switchxxxxxx(config)# route-map pbr
switchxxxxxx(config-route-map)# match ipv6 address access-list acl1
switchxxxxxx(config-route-map)# set ipv6 next-hop 3003:17ac::20
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config-ip-al)# exit
```

例 2。次に、インターフェイス tunnel1 をネクストホップとして設定する例を示します。

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# tunnel source 132.1.1.1
switchxxxxxx(config-if)# tunnel destination 192.168.30.1
switchxxxxxx(config-if)# tunnel mode ipv6ip
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# route-map bpr
switchxxxxxx(config-route-map)# match ipv6 address access-list acl
switchxxxxxx(config-route-map)# set ipv6 next-hop tunnel 1
switchxxxxxx(config-route-map)# exit
```

show route-map

ルートマップを表示するには、特権 EXEC モードで **show route-map** コマンドを使用します。

構文

show route-map [*map-name*]

パラメータ

- ***map-name***：特定のルートマップの名前。

デフォルト設定

コマンド モード

特権 EXEC モード

使用上のガイドライン

特定の 1 つのルートマップを表示するには、**show route-map** *map-name* コマンドを使用します。

設定したすべてのルートマップを表示するには、**show route-map** コマンドを使用します。

例

次に、show route-map コマンドの出力例を示します。

```
switchxxxxxx# show route-map
route-map POLICY-ROUTING, permit, sequence 10
  Match clauses:
    ip address access-lists: acl1
  Set clauses:
    ip next-hop: 192.12.34.5
route-map POLICY-ROUTING, permit, sequence 20
  Match clauses:
    ip address access-lists: acl2
  Set clauses:
    ip next-hop: 192.122.23.15
route-map POLICY-ROUTING-IPv6, permit, sequence 10
  Match clauses:
    ipv6 address access-lists: acl3
  Set clauses:
    ipv6 next-hop: 3003:17ac::20
route-map POLICY-ROUTING-IPv6, permit, sequence 20
  Match clauses:
    ipv6 address access-lists: acl4
  Set clauses:
    interface next-hop: tunnel 1
```

RSA および証明書コマンド

この章は、次の項で構成されています。

- crypto key generate dsa （1246 ページ）
- crypto key generate rsa （1247 ページ）
- crypto key import （1248 ページ）
- show crypto key （1250 ページ）
- crypto certificate generate （1251 ページ）
- crypto certificate request （1253 ページ）
- crypto certificate import （1255 ページ）
- show crypto certificate （1259 ページ）

crypto key generate dsa

crypto key generate dsa グローバル コンフィギュレーション モード コマンドは、SSH 公開キーの認証用に DSA キーペアを生成します。

構文

crypto key generate dsa

デフォルト設定

アプリケーションがデフォルト キーを自動的に作成します。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

作成された DSA キーのサイズは 1,024 ビットです。

DSA キーはペアで作成されます。1 つは DSA 公開キー、もう 1 つは DSA 秘密キーです。

デバイスにすでにデフォルトまたはユーザ定義の DSA キーがある場合は、警告が表示され、既存のキーを新しいキーに置き換えるように求められます。

スタートアップ コンフィギュレーションを消去するか、工場出荷時の初期状態に戻すと、デフォルト キーは自動的に削除され、これらはデバイスの初期化中に再作成されます。

このコマンドは、実行コンフィギュレーション ファイルに保存されません。ただし、このコマンドで生成されたキーは実行コンフィギュレーション ファイルに保存されます。

例

次の例では、DSA キー ペアを生成しています。

```
switchxxxxxx(config)# crypto key generate dsa
The SSH service is generating a private DSA key.
This may take a few minutes, depending on the key size.
.....
```

crypto key generate rsa

crypto key generate rsa グローバル コンフィギュレーション モード コマンドは SSH 公開キー認証の RSA キーペアを生成します。

構文

crypto key generate rsa

デフォルト設定

アプリケーションがデフォルト キーを自動的に作成します。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

作成した RSA キーのサイズは 2048 ビットです。

RSA キーはペアで作成されます。1 つは RSA 公開キー、もう 1 つは RSA 秘密キーです。

デバイスにデフォルトまたはユーザ定義の RSA キーがすでにある場合は、警告が表示され、既存のキーを新しいキーに置換するように求められます。

スタートアップ コンフィギュレーションを消去するか、工場出荷時の初期状態に戻すと、デフォルト キーは自動的に削除され、これらはデバイスの初期化中に再作成されます。

このコマンドは、実行コンフィギュレーション ファイルに保存されません。ただし、このコマンドで生成されたキーは実行コンフィギュレーション ファイルに保存されます。

例

次の例では、RSA キーがすでに存在している場合に、RSA キー ペアを生成しています。

```
switchxxxxxx(config)# crypto key generate rsa
Replace Existing RSA Key [y/n]? N
switchxxxxxx(config)#
```

crypto key import

crypto key import グローバル コンフィギュレーション モード コマンドは、DSA/RSA キー ペアをインポートします。

ユーザ キーを削除し、代わりに新しいデフォルトを生成するには、このコマンドの no 形式を使用します。

構文

crypto key import {dsa| rsa}

encrypted crypto key import {dsa| rsa}

no crypto key {**dsa| rsa**}

デフォルト設定

DSA および RSA キー ペアは存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

インポートされるキーは、RFC 4716 で定義されている形式に従う必要があります。

インポートの DSA キーサイズは 512 ～ 1024 ビットです。

インポートの RSA キーサイズは 1024 ー 2048 ビットです。

DSA/RSA キーはペアでインポートされます。1 つは DSA/RSA 公開キーで、もう 1 つは DSA/RSA 秘密キーです。

デバイスにすでに DSA/RSA キーがある場合は、警告が表示され、既存のキーを新しいキーに置き換えるように求められます。

このコマンドは、実行コンフィギュレーション ファイルに保存されます。

暗号化されたキーワードを使用すると、秘密キーがその暗号化形式でインポートされます。

例

```
switchxxxxxx(config)# encrypted crypto key import rsa
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
switchxxxxxx(config)# encrypted crypto key import rsa
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key
84et9C2XUfcRlpemuGINAygnLwfkKJcDM6m2OReALHScqqLhi0wMSSYNlT1IWFZP1kEVHH
Fpt1aECZi7HfGLcp1pMZwjn1+HaXBtQjPDiEtbpScXqrg6ml1/OEnwpFK2TrmUy0Iifwk8
E/mMfX3i/2rRZLkEBea5jrA6Q62gl5naRw1ZkOges+GNeibtvZYSk1jzr56LUr6fT7Xu5i
KMcU2b2NsuSD5yW8R/x0CW2elqDDz/biA2gSgd6FfnW2HV48bTC55eCKrsId2MmjbExUdz
+RQRhzjcGMBYp6HzkD66z8HmShOU+hKd7M1K9U4Sr+Pr1vyWUJlEkOgz9O6aZoIGp4tgm4
VDy/K/G/sI5nVL0+bR8LFUXUO/U5hohBcyRUFO2fHYKZrhTiPT5Rw+PHt6/+EXKG9E+TRs
```

```
lUADMltCRvs+lsB33IBdvoRDdl98YaA2htZay1TkbMqCUBdfl0+74UOqa/b+bp67wCYKe9
yen418MaYKtcHJBQmF7sUQZQGP34VPmOMyZzon68S/ZoT77cy0ihRZx9wcI1yYhJnDiYxP
dgXHYhW6kCTcTj6LrUSQuxCJ9su89ZIWNn5OwdgonLSpvfnabv2GHmmelaveL7JJ/7UcfO
61q5D4PJ67Vk2xL7PqyHXN931rseTzPuJplkSLCFZ5uqTMbWWyQEKmHDlOx35vlGou5tky
9LgIwG4d+9edctZZaggeq5cgjnsZWJgUoB4Bn4hIreyOdHDiFUPPRxkoyhGOGnJuvxC9T9
K6BF1wBTdDQS+Gu47/0/gRoD/50q4sGkzqHsRJJ53WOT0Q1bHMTMLPpwn2nXzvfGxWL/bu
QhZZSqRonG6MX1cP7KT7i4TPq2w2k3TGtNBnVYHx6OoNcaTHmg1N2s5OgRsyXD9tF++6nY
RfMN8CsV+9jQKQP7ZaGc8Ju+d72jvSwppSr032HY+IpzZ4ujkK+/X5oawZL5NnkaEQTQKX
RSL55S4O5NPOjS/pC9hg7GaVjoY2mQ7HDpSUBeTIDTlvOwC2kskA9C6aF/Axj2dXLweQd5
lxk7m0/mMNaiJsNk6y33LcuKjIxpNNjK9n9KzRPkGNMFObprfenWKteDftjQ==
---- END SSH2 PRIVATE KEY ----
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAvRHsKry6NKMKymb+yWEp9042vupLvYVq3ngt1sB9JH
OcdK/2nw7lCQguy1mLsX8/bKMXYSk/3aBEvaoJQ82+r/nRf0y3HTy4Wp9zV0SiVC8jLD+7
7t0aHejzfUhr0FRhWWcLnvYwr+nmrYDpS6FADMC2hVA85KZRye9ifxT7otE=
---- END SSH2 PUBLIC KEY ----
```

show crypto key

show crypto key 特権 EXEC モード コマンドは、デフォルトとユーザ定義の両方のキーについて、デバイスの SSH 秘密キーおよび公開キーを表示します。

構文

show crypto key [*mypubkey*] [**dsa**| **rsa**]

パラメータ

- ***mypubkey***：公開キーのみを表示します。
- **rsa**：RSA キーを表示します。
- **dsa**：DSA キーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このキーペアを表示およびコピーする方法については、「**キーおよび証明書**」を参照してください。

例

次に、デバイスの SSH 公開 DSA キーを表示する例を示します。

```
switchxxxxxx# show crypto key mypubkey dsa
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAzN31fu56KSEOZdrGVPIJHpAs8G8NDIkB
dqZ2q0QPiKCnLPw0Xsk9tTVKaHZQ5jJbXn81QZpolaPLJIIH3B1cc96D7IFf
VkbPbMRbz24dpuWmPVVLUlQy5nCKdDCui5KKVD6zj3gpuhLhMJor7AjAAu5e
BrIi2IuwMVJuak5M098=
---- END SSH2 PUBLIC KEY ----
Public Key Fingerprint: 6f:93:ca:01:89:6a:de:6e:ee:c5:18:82:b2:10:bc:1e
```

crypto certificate generate

crypto certificate generate グローバル コンフィギュレーション モード コマンドは、HTTPS 用の自己署名証明書を生成します。

構文

crypto certificate *number* **generate** [**key-generate** [*length*]] [**cn** *common- name*] [**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*] [**duration** *days*]

パラメータ

- ***number***：証明書番号を指定します。(範囲：1 ～ 2)
- **key-generate rsa** *length*：SSL RSA キーを再生成してキー長を指定します（サポートされる長さ：2048（ビット）または 3092（ビット））。

  次の要素は、キーに関連付けることができます。キーが表示されると、それらも表示されます。

  cn *common- name*：完全修飾デバイス URL または IP アドレスを指定します。（長さ：1 ～ 64 文字）。指定しない場合、デフォルトでデバイスの最小の IP アドレスになります（証明書が生成されるとき）。

  ou *organization-unit*：部門または部署名を指定します。（長さ：1 ～ 64 文字）

  or *organization*：組織名を指定します。（長さ：1 ～ 64 文字）

  loc *location*：場所または市区町村名を指定します。（長さ：1 ～ 64 文字）

  st *state*：都道府県名を指定します。（長さ：1 ～ 64 文字）

  cu *country*：国名を指定します。（長さ：2 文字）

  duration *days*：証明書が有効な日数を指定します。（範囲：30 ー 1095）

デフォルト設定

key-generate パラメータを使用しない場合、証明書は既存のキーを使用して生成されます。

SSL の RSA キーのデフォルト長は 2048 です。

デフォルト SSL の EC キーの長さは 256 です。

cn *common- name* を指定しないと、デフォルトでは（証明書の生成時に）デバイスの最小のスタティック IPv6 アドレス、スタティック IPv6 アドレスがない場合にはデバイスの最小のスタティック IPv4 アドレス、スタティック IP アドレスがない場合には 0.0.0.0 に設定されます。

duration *days* を指定しない場合、デフォルトは 730 日です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

特定の証明書キーが存在しない場合は、**key-generate** パラメータを使用する必要があります。

証明書 1 と 2 の両方が生成されている場合は、**ip https certificate** コマンドを使用して、どちらか一方の証明書を有効化します。

このキーペアを表示およびコピーする方法については、「**キーおよび証明書**」を参照してください。

スタートアップ コンフィギュレーションを消去するか、工場出荷時の初期状態に戻すと、デフォルト キーは自動的に削除され、これらはデバイスの初期化中に再作成されます。

例

次に、キーの長さが 2048 バイトの HTTPS の自己署名証明書を生成する例を示します。

```
switchxxxxxx(config)# crypto certificate 1 generate key-generate 2048
```

crypto certificate request

crypto certificate request 特権 EXEC モード コマンドは、HTTPS 用の証明書要求を生成して表示します。

構文

crypto certificate *number* **request** *[***cn** *common- name*] [**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country]*

パラメータ

- ***number***：証明書番号を指定します。(範囲：1 ～ 2)
- 次の要素は、キーに関連付けることができます。キーが表示されると、それらも表示されます。

  cn *common- name*：完全修飾デバイス URL または IP アドレスを指定します。（長さ：1 ～ 64 文字）。指定しない場合、デフォルトでデバイスの最小の IP アドレスになります（証明書が生成されるとき）。

  ou *organization-unit*：部門または部署名を指定します。（長さ：1 ～ 64 文字）

  or *organization*：組織名を指定します。（長さ：1 ～ 64 文字）

  loc *location*：場所または市区町村名を指定します。（長さ：1 ～ 64 文字）

  st *state*：都道府県名を指定します。（長さ：1 ～ 64 文字）

  cu *country*：国名を指定します。（長さ：2 文字）

デフォルト設定

cn common-name を指定しない場合、デフォルトでは（証明書が生成されたときの）デバイスの最小静的 IPv6 アドレスに設定されるか、または静的 IPv6 アドレスがない場合はデバイスの最小静的 IPv4 アドレスに、静的 IP アドレスがない場合は 0.0.0.0 に設定されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、証明機関に証明書要求をエクスポートする場合に使用します。証明書要求は、Base64 でエンコードされた X.509 形式で生成されます。

証明書要求を生成する前に、まず **crypto cerificate generate** コマンドを使用して、自己署名証明書を生成してキーを生成します。証明書のフィールドを再入力する必要があります。

証明機関から証明書を受信したら、**crypto cerificate import** コマンドを使用して、デバイスに証明書をインポートします。この証明書は、自己署名証明書と置き換わります。

例

次の例では、HTTPS 用の証明書要求を表示します。

```
switchxxxxxx# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAxCzAJBgNVBAgTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm
/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
MRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBBAUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa
g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----
```

crypto certificate import

crypto certificate import グローバル コンフィギュレーション モード コマンドは、HTTPS 用の証明機関によって署名された証明書をインポートします。さらに、関連するキーペアもインポートできます。

ユーザ定義のキーおよび証明書を削除するには、このコマンドの no 形式を使用します。

構文

crypto certificate *number* **import**

encrypted crypto certificate *number* **import**

no crypto certificate *number*

パラメータ

- ***number***：証明書番号を指定します。（範囲：1 ～ 2）。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

証明書は PEM エンコーディング/ファイル拡張子からインポートする必要があります

セッションを終了する（コマンドラインに戻って次のコマンドを入力する）には、空白行を入力します。

インポートする証明書は、**crypto cerificate request** コマンドで作成される証明書要求に基づく必要があります。

証明書のみをインポートする場合に、証明書にある公開キーがデバイスの SSL キーに一致しないと、コマンドは失敗します。公開キーと証明書の両方をインポートする場合で、証明書にある公開キーがインポートしたキーに一致しない場合、コマンドは失敗します。

このコマンドは、実行コンフィギュレーション ファイルに保存されます。

このコマンドの暗号化形式を使用するときは、秘密キーのみを暗号化形式にする必要があります。

例 1：次の例では、HTTPS の証明機関によって署名された証明書をインポートしています。

```
switchxxxxxx(config)# crypto certificate 1 import
Please paste the input now, add a period (.) on a separate line after the input,and press
 Enter.
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
```

```
OOg9XM1AxfOiqLlQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5sO4lv0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
.
-----END CERTIFICATE-----
Certificate imported successfully.
Issued by : C=  , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
 SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

例 2：次の例では、HTTPS の証明機関によって署名された証明書、および RSA キーペアをインポートしています。

```
switchxxxxxx(config)# crypto certificate 1 import
Please paste the input now, add a period (.) on a separate line after the input,and press
 Enter.

-----BEGIN RSA PRIVATE KEY-----
ACnrqImEGlXkwxBuZUlAO9nHq9IGJsnkf7/MauGPVqxt5vfDf77uQ5CPf49JWQhu07cVXh
2OwrBhJgB69vLUlJujM9p1IXFpMk8qR3NS7JzlInYAWjHKKbEZBMsKSA6+t/UzVxevKK6H
TGB7vMxi+hv1bL9zygvmQ6+/6QfqA51c4nP/8a6NjO/ZOAgvNAMKNr2Wa+tGUOoAgL0b/C
11EoqzpCq5mT7+VOFhPSO4dUU+NwLv1YCb1Fb7MFoAa0N+y+2NwoGp0pxOvDA9ENYl7qsZ
MWmCfXu52/IxC7fD8FWxEBtks4V81Xqa7K6ET657xS7m8yTJFLZJyVawGXKnIUs6uTzhhW
dKWWc0e/vwMgPtLlWyxWynnaP0fAJ+PawOAdsK75bo79NBim3HcNVXhWNzqfg2s3AYCRBx
WuGoazpxHZ0s4+7swmNZtS0xI4ek43d7RaoedGKljhPqLHuzXHUon7Zx15CUtP3sbHl+XI
B3u4EEcEngYMewy5obn1vnFSot+d5JHuRwzEaRAIKfbHa34alVJaN+2AMCb0hpI3IkreYo
A8Lk6UMOuIQaMnhYf+RyPXhPOQs01PpIPHKBGTi6pj39XMviyRXvSpn5+eIYPhve5jYaEn
UeOnVZRhNCVnruJAYXSLhjApf5iIQr1JiJb/mVt8+zpqcCU9HCWQqsMrNFOFrSpcbHu5V4
ZX4jmd9tTJ2mhekoQf1dwUZbfYkRYsK70ps8u7BtgpRfSRUr7g0LfzhzMuswoDSnB65pkC
ql7yZnBeRS0zrUDgHLLRfzwjwmxjmwObxYfRGMLp4=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMVuFgfJYLbUzmbm6UoLD3ewHYd1ZMXY4A3KLF2SXUd1TIXq84aME8DIitSfB2
Cqy4QB5InhgAobBKC96VRsUe2rzoNG4QDkj2L9ukQOvoFBYNmbzHc7a+7043wfVmH+QOXf
TbnRDhIMVrZJGbzl1c9IzGky1l21Xmicy0/nwsXDAgEj

-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
OOg9XM1AxfOiqLlQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5sO4lv0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
-----END CERTIFICATE-----
.
Certificate imported successfully.
Issued by : C=  , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
 SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

例 3：暗号化されたキーで証明書をインポートしています。

```
switchxxxxxx(config)# encrypted crypto certificate 1 import
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
```

```
wJIjj/tFEI/Z3GFkTl5C+SFOeSyTxnSsfssNo9CoHJ6X9Jg1SukjtXU49kaUbTjoQVQatZ
AdQwgWM5mnjUhUaJ1MM3WfrApY7HaBL3iSXS9jDVrf++Q/KKhVH6Pxlv6cKvYYzHg43Unm
CNI2n5zf9oisMH0U6gsIDs4ysWVD1zNgoVQwD7RqKpL9wo3+YVFVS6XCB7pDb7iPePefa6
GD/crN28vTLGf/NpyKoOhdAMRuwEQoapMo0Py2Cvy+sqLiv4ZKck1FPlsVFV7X7sh+zVa3
We84pmzyjGiY9S0tPdBSGhJ2xDNcqTyvUpffFEJJYrdGKGybqD0o3tD/ioUQ3UJgxDbGYw
aLlLoavSjMYiWkdPjfcbn5MVRdU5iApCQJXWv3MYC8GQ4HDa6UDN6aoUBalUhqjT+REwWO
DXpJmvmX4T/u5W4DPvELqTHyETxgQKNErlO7gRi2yyLcybUokh+SP+XuRkG4IKnn8KyHtz
XeoDojSe6OYOQww2R0nAqnZsZPgrDzj0zTDL8qvykurfW4jWa4cv1Sc1hDEFtHH7NdDLjQ
FkPFNAKvFMcYimidapG+Rwc0m3lKBLcEpNXpFEE3v1mCeyN1pPe6eSqMcBXa2VmbInutuP
CZM927oxkb41g+U5oYQxGhMK7OEzTmfS1FdLOmfqv0DHZNR4lt4KgqcSjSWPQeYSzB+4PW
Qmy4fTF4wQdvCLy+WlvEP1jWPbrdCNxIS13RWucNekrm9uf5Zuhd1FA9wf8XwSRJWuAq8q
zZFRmDMHPtey9ALO2alpwjpHOPbJKiCMdjHT94ugkF30eyeni9sGN6Y063IvuKBy0nbWsA
J0sxrvt3q6cbKJYozMQE5LsgxLNvQIH4BhPtUz+LNgYWb3V5SI8D8kRejqBM9eaCyJsvLF
+yAI5xABZdTPqz0l7FNMzhIrXvCqcCCCx+JbgP1PwYTDyD+m2H5v8Yv6sT3y7fZC9+5/Sn
Vf8jpTLMWFgVF9U1Qw9bA8HA7K42XE3R5Zr1doOeUrXQUkuRxLAHkifD7ZHrE7udOmTiP9
W3PqtJzbtjjvMjm5/C+hoC6oLNP6qp0TEn78EdfaHpMMutMF0leKuzizenZQ==
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMoCaK+b9hTgrzEeWjdz55FoWwV8s54k5VpuRtv1e5r1zp7kzIL6mvCCXk6J9c
kkr+TMfX63b9t5RgwGPgWeDHw3q5QkaqInzz1h7j2+A++mwCsHui1BhpFNFY/gmENiGq9f
puukcnoTvBNvz7z3VOxv6hw1UHMTOeO+QSbe7WwVAgMBAAE=
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIICHDCCAYUCEFCcI4/dhLsUhTWxOwbzngMwDQYJKoZIhvcNAQEEBQAwTzELMAkG
A1UEBhMCICAxCjAIBgNVBAgTASAxCjAIBgNVBAcTASAxEDAOBgNVBAMTBzAuMC4w
LjAxCjAIBgNVBAoTASAxCjAIBgNVBAsTASAwHhcNMTIwNTIxMTI1NzE2WhcNMTMw
NTIxMTI1NzE2WjBPMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEQMA4GA1UEAxMHMC4wLjAuMDEKMAgGA1UEChMBIDEKMAgGA1UECxMBIDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAygJor5v2FOCvMR5aN3PnkWhbBXyzniTl
Wm5G2/V7mvXOnuTMgvqa8IJeTon1ySSv5Mx9frdv23lGDAY+BZ4MfDerlCRqoifP
PWHuPb4D76bAKwe6LUGGkU0Vj+CYQ2Iar1+m66RyehO8E2/PvPdU7G/qHDVQcxM5
475BJt7tbBUCAwEAATANBgkqhkiG9w0BAQQFAAOBgQBOknTzas7HniIHMPeC5yC0
2rd7c+zqQOe1e4CpEvVlOC0QGvPa72pz+m/zvoFmAC5WjQngQMMwH8rNdvrfaSyE
dkB/761PpeKkUtgyPHfTzfSMcJdBOPPnpQcqbxCFh9QSNa4ENSXqC5pND02RHXFx
wS1XJGrhMUoNGz1BY5DJWw==
-----END CERTIFICATE-----
.
Certificate imported successfully.
Issued by : C=  , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
 SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
Example 3 - Import certificate with encrypted key
encrypted crypto certificate 1 import
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
wJIjj/tFEI/Z3GFkTl5C+SFOeSyTxnSsfssNo9CoHJ6X9Jg1SukjtXU49kaUbTjoQVQatZ
AdQwgWM5mnjUhUaJ1MM3WfrApY7HaBL3iSXS9jDVrf++Q/KKhVH6Pxlv6cKvYYzHg43Unm
CNI2n5zf9oisMH0U6gsIDs4ysWVD1zNgoVQwD7RqKpL9wo3+YVFVS6XCB7pDb7iPePefa6
GD/crN28vTLGf/NpyKoOhdAMRuwEQoapMo0Py2Cvy+sqLiv4ZKck1FPlsVFV7X7sh+zVa3
We84pmzyjGiY9S0tPdBSGhJ2xDNcqTyvUpffFEJJYrdGKGybqD0o3tD/ioUQ3UJgxDbGYw
aLlLoavSjMYiWkdPjfcbn5MVRdU5iApCQJXWv3MYC8GQ4HDa6UDN6aoUBalUhqjT+REwWO
DXpJmvmX4T/u5W4DPvELqTHyETxgQKNErlO7gRi2yyLcybUokh+SP+XuRkG4IKnn8KyHtz
XeoDojSe6OYOQww2R0nAqnZsZPgrDzj0zTDL8qvykurfW4jWa4cv1Sc1hDEFtHH7NdDLjQ
FkPFNAKvFMcYimidapG+Rwc0m3lKBLcEpNXpFEE3v1mCeyN1pPe6eSqMcBXa2VmbInutuP
CZM927oxkb41g+U5oYQxGhMK7OEzTmfS1FdLOmfqv0DHZNR4lt4KgqcSjSWPQeYSzB+4PW
Qmy4fTF4wQdvCLy+WlvEP1jWPbrdCNxIS13RWucNekrm9uf5Zuhd1FA9wf8XwSRJWuAq8q
zZFRmDMHPtey9ALO2alpwjpHOPbJKiCMdjHT94ugkF30eyeni9sGN6Y063IvuKBy0nbWsA
J0sxrvt3q6cbKJYozMQE5LsgxLNvQIH4BhPtUz+LNgYWb3V5SI8D8kRejqBM9eaCyJsvLF
+yAI5xABZdTPqz0l7FNMzhIrXvCqcCCCx+JbgP1PwYTDyD+m2H5v8Yv6sT3y7fZC9+5/Sn
Vf8jpTLMWFgVF9U1Qw9bA8HA7K42XE3R5Zr1doOeUrXQUkuRxLAHkifD7ZHrE7udOmTiP9
W3PqtJzbtjjvMjm5/C+hoC6oLNP6qp0TEn78EdfaHpMMutMF0leKuzizenZQ==
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
```

```
MIGJAoGBAMoCaK+b9hTgrzEeWjdz55FoWwV8s54k5VpuRtv1e5r1zp7kzIL6mvCCXk6J9c
kkr+TMfX63b9t5RgwGPgWeDHw3q5QkaqInzz1h7j2+A++mwCsHui1BhpFNFY/gmENiGq9f
puukcnoTvBNvz7z3VOxv6hw1UHMTOeO+QSbe7WwVAgMBAAE=
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIICHDCCAYUCEFCcI4/dhLsUhTWxOwbzngMwDQYJKoZIhvcNAQEEBQAwTzELMAkG
A1UEBhMCICAxCjAIBgNVBAgTASAxCjAIBgNVBAcTASAxEDAOBgNVBAMTBzAuMC4w
LjAxCjAIBgNVBAoTASAxCjAIBgNVBAsTASAwHhcNMTIwNTIxMTI1NzE2WhcNMTMw
NTIxMTI1NzE2WjBPMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEQMA4GA1UEAxMHMC4wLjAuMDEKMAgGA1UEChMBIDEKMAgGA1UECxMBIDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAygJor5v2FOCvMR5aN3PnkWhbBXyzniTl
Wm5G2/V7mvXOnuTMgvqa8IJeTon1ySSv5Mx9frdv23lGDAY+BZ4MfDerlCRqoifP
PWHuPb4D76bAKwe6LUGGkU0Vj+CYQ2Iar1+m66RyehO8E2/PvPdU7G/qHDVQcxM5
475BJt7tbBUCAwEAATANBgkqhkiG9w0BAQQFAAOBgQBOknTzas7HniIHMPeC5yC0
2rd7c+zqQOe1e4CpEvV1OC0QGvPa72pz+m/zvoFmAC5WjQngQMMwH8rNdvrfaSyE
dkB/761PpeKkUtgyPHfTzfSMcJdBOPPnpQcqbxCFh9QSNa4ENSXqC5pND02RHXFx
wS1XJGrhMUoNGz1BY5DJWw==
-----END CERTIFICATE-----
.
Certificate imported successfully.
Issued by : C=  , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
 SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

show crypto certificate

show crypto certificate 特権 EXEC モード コマンドを使用すると、デフォルト キーとユーザ定義キーの両方について、デバイスの SSH 証明書とキーペアが表示されます。

構文

show crypto certificate [mycertificate] [*number*]

パラメータ

- ***number***：証明書番号を指定します。（範囲：1、2）
- **mycertificate**：証明書のみを表示することを指定します。

デフォルト設定

両方のキーを表示します。

コマンド モード

特権 EXEC モード

例

次に、デバイスに存在する SSL 証明書番号 1 およびキー ペアを表示する例を示します。

```
switchxxxxxx# show crypto certificate 1
Certificate 1:
Certificate Source: Default
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----

----BEGIN RSA PRIVATE KEY-----
ACnrqImEGlXkwxBuZUlAO9nHq9IGJsnkf7/MauGPVqxt5vfDf77uQ5CPf49JWQhu07cVXh
2OwrBhJgB69vLUlJujM9p1IXFpMk8qR3NS7JzlInYAWjHKKbEZBMsKSA6+t/UzVxevKK6H
TGB7vMxi+hv1bL9zygvmQ6+/6QfqA51c4nP/8a6NjO/ZOAgvNAMKNr2Wa+tGUOoAgL0b/C
11EoqzpCq5mT7+VOFhPSO4dUU+NwLv1YCb1Fb7MFoAa0N+y+2NwoGp0pxOvDA9ENYl7qsZ
MWmCfXu52/IxC7fD8FWxEBtks4V81Xqa7K6ET657xS7m8yTJFLZJyVawGXKnIUs6uTzhhW
dKWWc0e/vwMgPtLlWyxWynnaP0fAJ+PawOAdsK75bo79NBim3HcNVXhWNzqfg2s3AYCRBx
WuGoazpxHZ0s4+7swmNZtS0xI4ek43d7RaoedGKljhPqLHuzXHUon7Zx15CUtP3sbHl+XI
B3u4EEcEngYMewy5obn1vnFSot+d5JHuRwzEaRAIKfbHa34alVJaN+2AMCb0hpI3IkreYo
A8Lk6UMOuIQaMnhYf+RyPXhPOQs01PpIPHKBGTi6pj39XMviyRXvSpn5+eIYPhve5jYaEn
UeOnVZRhNCVnruJAYXSLhjApf5iIQr1JiJb/mVt8+zpqcCU9HCWQqsMrNFOFrSpcbHu5V4
ZX4jmd9tTJ2mhekoQf1dwUZbfYkRYsK70ps8u7BtgpRfSRUr7g0LfzhzMuswoDSnB65pkC
ql7yZnBeRS0zrUDgHLLRfzwjwmxjmwObxYfRGMLp4=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMVuFgfJYLbUzmbm6UoLD3ewHYd1ZMXY4A3KLF2SXUd1TIXq84aME8DIitSfB2
```

```
Cqy4QB5InhgAobBKC96VRsUe2rzoNG4QDkj2L9ukQOvoFBYNmbzHc7a+7043wfVmH+QOXf
TbnRDhIMVrZJGbzl1c9IzGky1l21Xmicy0/nwsXDAgEj

-----END RSA PUBLIC KEY-----
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

Smartport コマンド

この章は、次の項で構成されています。

- macro auto（グローバル） （1262 ページ）
- macro auto built-in parameters （1264 ページ）
- macro auto persistent （1265 ページ）
- macro auto processing cdp （1266 ページ）
- macro auto processing lldp （1267 ページ）
- macro auto processing type （1268 ページ）
- macro auto resume （1269 ページ）
- macro auto smartport（インターフェイス） （1270 ページ）
- macro auto smartport type （1271 ページ）
- macro auto trunk refresh （1273 ページ）
- macro auto user smartport macro （1274 ページ）
- show macro auto ports （1276 ページ）
- show macro auto processing （1278 ページ）
- show macro auto smart-macros （1279 ページ）
- smartport storm-control （1281 ページ）

macro auto（グローバル）

macro auto グローバル コンフィギュレーション モード コマンドは、Auto Smartport のグローバル管理状態を設定します。デフォルト値に戻すには、このコマンドの**no**形式を使用します。

構文

macro auto {enabled | disabled | controlled}

no macro auto

パラメータ

- **enabled**：Auto Smartport のグローバル管理状態および動作状態が有効になります。
- **disabled**：Auto Smartport のグローバル管理状態および動作状態が無効になります。
- **controlled**：自動音声 VLAN の動作時に、Auto Smartport のグローバル管理状態および動作状態が有効になります。

デフォルト設定

管理状態は**無効**です

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

Auto Smartport の状態にかかわらず、Smartport マクロを関連付けられた Smartport タイプにいつでも手動で適用できます。Smartport マクロは、組み込みマクロまたはユーザ定義マクロです。「マクロ コマンド」セクションに示されている CLI コマンドを使用して、マクロを定義し、適用することができます。

Auto Smartport の管理状態が制御されている場合、Auto Smartport の動作状態は音声 VLAN マネージャによって管理され、次のように設定されます。

- OUI 音声 VLAN が有効になっている場合、Auto Smartport の動作状態は無効になります。

  自動音声 VLAN が有効になっている場合、Auto Smartport の動作状態は有効になります。

OUI 音声 VLAN が有効になっている場合、ユーザは Auto Smartport をグローバルに有効にすることはできません。

例

この例では、controlled モードで Auto Smartport 機能をグローバルに有効にしようとしています。OUI 音声機能が有効になっているため、これはできません。その後、音声 VLAN 状態が

無効になり、Auto Smartport を有効にできるようになります。これらの VLAN 上で Auto Smartport 用のポートが設定されているため、適切な VLAN が自動的に有効になります。

```
switchxxxxxx(config)# macro auto controlled
switchxxxxxx(config)# macro auto enabled
Auto smartports cannot be enabled because OUI voice is enabled.
switchxxxxxx(config)# voice vlan state disabled
switchxxxxxx(config)# macro auto enabled
switchxxxxxx(config)#
10-Apr-2011 16:11:31 %LINK-I-Up:  Vlan 20
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 5
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 6
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 7
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 8
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 9
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 10
```

macro auto built-in parameters

macro auto built-in parameters グローバル コンフィギュレーション モード コマンドは、組み込み Smartport マクロのデフォルトの Auto Smartport の値を置き換えます。このコマンドの **no** 形式を使用すると、デフォルト値に戻ります。

構文

macro auto built-in parameters *smartport-type* [*parameter-name value* [*parameter-name value* [*parameter-name value*]]]

no macro auto built-in parameters *smartport-type*

パラメータ

- **smartport-type**：Smartport タイプ（範囲：*printer*、**desktop**、**guest**、**server**、**host**、**ip_camera**、**ip_phone**、**ip_phone_desktop**、**switch**、**router**、または **ap**（ワイヤレス アクセス ポイント））。
- ***parameter-name value***：パラメータ名とその値を指定します。これらは、**macro auto user smartport macro** コマンドで定義された組み込みマクロまたはユーザ定義マクロのパラメータです

デフォルト設定

組み込み Smartport マクロのパラメータ $native_vlan のデフォルト値は 1 です。

その他のパラメータのデフォルト値は、パラメータのデフォルト値です。たとえば、パラメータがネイティブ VLAN の場合、デフォルト値はデフォルトのネイティブ VLAN です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

デフォルトでは、各 Smartport タイプは組み込みマクロのペアに関連付けられています。これは、設定を適用するマクロと、設定を削除するアンチマクロ（no形式のマクロ）のペアです。Smartport タイプは対応する組み込み Smartport マクロの名前と同じで、アンチマクロには **no_** のプレフィックスが付いています。

パラメータ **$voice_vlan** の値は、このコマンドでは変更できません。

例

組み込みマクロのパラメータを変更するには、次のようにします。

```
switchxxxxxx(config)# macro auto built-in parameters switch $native_vlan 2
```

macro auto persistent

macro auto persistent インターフェイス コンフィギュレーション モード コマンドは、インターフェイスを Smartport の永続インターフェイスとして設定します。このコマンドの **no** 形式を使用すると、デフォルトに戻ります。

構文

macro auto persistent

no macro auto persistent

パラメータ

このコマンドには、パラメータやキーワードはありません。

デフォルト設定

Persistent は設定されています。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

Smartport の永続インターフェイスは、リンク ダウン/アップ、接続デバイスのエージアウト、および再起動が行われた場合に、その動的設定を保持します。永続化と Smartport 設定を再起動後も有効にするには、実行コンフィギュレーションファイルをスタートアップ コンフィギュレーション ファイルに保存する必要があります。

例

この例では、2 つのポート範囲を確立して、片方は永続化し、もう片方は永続化しません。

```
switchxxxxxx(config)# interface range gi1/0/1-2
switchxxxxxx(config-if-range)# macro auto persistent
switchxxxxxx(config-if-range)# exit
switchxxxxxx(config)# interface range gi1/0/3-4
switchxxxxxx(config-if-range)# no macro auto persistent
```

macro auto processing cdp

macro auto processing cdp グローバル コンフィギュレーション モード コマンドを使用すると、CDP 機能情報を使用して接続デバイスのタイプを識別できます。

Auto Smartport がインターフェイスで有効になっており、このコマンドが実行されると、接続デバイスがアドバタイズする CDP 機能に基づいて、スイッチは自動的に対応する Smartport タイプをインターフェイスに適用します。

機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

macro auto processing cdp

no macro auto processing cdp

パラメータ

このコマンドには、パラメータやキーワードはありません。

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、CDP をグローバルに有効にします。

```
switchxxxxxx(config)# macro auto processing cdp
```

macro auto processing lldp

macro auto processing lldp グローバル コンフィギュレーション モード コマンドを使用すると、LLDP 機能情報を使用して接続デバイスのタイプを識別できます。

インターフェイス上で Auto Smartport が有効になっている場合にこのコマンドが実行されると、スイッチは接続デバイスによってアドバタイズされた LLDP 機能に基づいて、対応する Smartport タイプをインターフェイスに自動的に適用します。

機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

macro auto processing lldp

no macro auto processing lldp

パラメータ

このコマンドには、パラメータやキーワードはありません。

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

例

LLDP をグローバルに有効にする場合：

```
switchxxxxxx(config)# macro auto processing lldp
```

macro auto processing type

macro auto processing type グローバル コンフィギュレーション モード コマンドは、指定されたタイプのデバイスの自動検出を有効または無効にします。コマンドのno形式を使用すると、デフォルトに戻ります。

構文

macro auto processing type *smartport-type* {**enabled** | **disabled**}

no macro auto processing type *smartport-type*

パラメータ

- ***smartport-type***：Smartport タイプ（範囲：**host**、**ip_phone**、**ip_phone_desktop**、**switch**、**router**、または **ap**（ワイヤレス アクセス ポイント））。

デフォルト設定

デフォルトでは、ip_phone、ip_phone_desktop、switch、および ap（ワイヤレス アクセス ポイント）の自動検出が有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

この例では、ap（ワイヤレス アクセス ポイント）の自動検出が有効になっています。

```
switchxxxxxx(config)# macro auto processing type ?
  host                set type to host
  ip_phone            set type to ip_phone
  ip_phone_desktop    set type to ip_phone_desktop
  switch              set type to switch
  router              set type to router
  ap                  set type to access point
switchxxxxxx(config)# macro auto processing type ap enabled
```

macro auto resume

macro auto resume インターフェイス コンフィギュレーション モード コマンドは、Smartport タイプを **unknown** から **default** に変更し、指定したインターフェイスで Smartport 機能を再開します（ただし、Smartport マクロを再適用しません。これを実行するには **macro auto trunk refresh** コマンドを使用します）。

構文

macro auto resume

パラメータ

このコマンドには、パラメータやキーワードはありません。

デフォルト設定

なし

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

インターフェイスで Smartport マクロが失敗すると、インターフェイスの Smartport タイプが **Unknown** になります。インターフェイスや Smartport マクロでの失敗の理由を診断し、エラーを修正する必要があります。

例

Smartport タイプを **unknown** から **default** に変更し、ポート 1 の Smartport 機能を再開します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# macro auto resume
```

macro auto smartport（インターフェイス）

macro auto smartport インターフェイス コンフィギュレーション モード コマンドは、指定されたインターフェイスで Auto Smartport 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、インターフェイスでこの機能が無効化されます。

構文

macro auto smartport

no macro auto smartport

パラメータ

このコマンドには、パラメータやキーワードはありません。

デフォルト設定

有効

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドは、Auto Smartport がグローバルに有効になっている場合にのみ有効です。

例

ポート 1 の Auto Smartport 機能を有効にします。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# macro auto smartport
```

macro auto smartport type

macro auto smartport type インターフェイス コンフィギュレーション モード コマンドは、Smartport タイプをインターフェイスに手動で（静的に）割り当てます。このコマンドの **no** 形式を使用すると、手動で設定したタイプが削除され、**default** に戻ります。

構文

macro auto smartport type *smartport-type* [*parameter-name value* [*parameter-name value* [*parameter-name value*]]]

no macro auto smartport type

パラメータ

- ***smartport-type***：Smartport タイプ。
- ***parameter-name value***：パラメータ名とその値を指定します（範囲：printer、desktop、guest、server、host、ip_camera、ip_phone、ip_phone_desktop、switch、router、または ap（ワイヤレス アクセス ポイント））

デフォルト設定

parameter-name *value*：パラメータのデフォルト値。たとえば、パラメータが音声 VLAN の場合、デフォルト値はデフォルトの音声 VLAN です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドにより設定された静的タイプは、動的タイプにより変更できません。

例

この例では、ポート 1 の Smartport タイプを printer（静的）に設定しようとしています。このマクロは行 10 で失敗します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# macro auto smartport type printer
30-May-2011 15:02:45 %AUTOSMARTPORT-E-FAILEDMACRO: Macro printer for auto smar
port type Printer on interface gi1/0/1 failed at command number 10
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# do show parser macro name printer
Macro name : printer
Macro type : default interface
  1. #macro description printer
  2. #macro keywords $native_vlan
  3. #
  4. #macro key description:  $native_vlan: The untag VLAN which will be configu
red on the port
```

```
  5. #Default Values are
  6. #$native_vlan = Default VLAN
  7. #
  8. #the port type cannot be detected automatically
  9. #
 10. switchport mode access
 11. switchport access vlan $native_vlan
 12. #
 13. #single host
 14. port security max 1
 15. port security mode max-addresses
 16. port security discard trap 60
 17. #
 18. smartport storm-control broadcast level 10
 19. smartport storm-control include-multicast
 20. smartport storm-control broadcast enable
switchxxxxxx(config)#
```

macro auto trunk refresh

macro auto trunk refresh グローバル コンフィギュレーション コマンドは、指定したインターフェイスまたは指定した Smartport タイプのすべてのインターフェイスに Smartport マクロを再適用します。

構文

macro auto trunk refresh [*smartport-type*] [*interface-id*]

パラメータ

- ***smartport-type***：Smartport タイプ（**switch**、**router**、**ap**（ワイヤレス アクセス ポイント））。
- ***interface-id***：インターフェイス識別子（ポートまたはポート チャネル）。

デフォルト設定

ユーザ ガイドラインを参照してください。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

macro auto smartport コマンドは、Auto Smartport がグローバルに有効になっている場合にのみ有効になります。

smartport-type と *interface-id* の両方が定義されている場合、アタッチされた Smartport マクロは、指定された Smartport タイプを持つインターフェイスで実行されます。

smartport-type のみが定義されている場合、アタッチされた Smartport マクロは、指定された Smartport タイプを持つすべてのインターフェイスで実行されます。

interface-id のみが定義されている場合、インターフェイスが **switch**、**router**、または **ap**（ワイヤレス アクセス ポイント）の Smartport タイプを持つ場合は、対応するアタッチされた Smartport マクロが実行されます。

Smartport マクロに、1 台以上のインターフェイスで最新ではなくなったコンフィギュレーション コマンドが含まれている場合は、インターフェイスに Smartport マクロを再適用して設定を更新できます。

例

関連付けられた Smartport マクロを実行して、Smartport タイプ **switch** のポートを既存のすべての VLAN に追加します。

```
switchxxxxxx(config)# macro auto trunk refresh switch
```

macro auto user smartport macro

macro auto user smartport macro グローバル コンフィギュレーション モード コマンドは、ユーザ定義の Smartport マクロを Smartport タイプにリンクします。これは、組み込みマクロへのリンクをユーザ定義マクロへのリンクに置き換えることにより行われます。このコマンドの **no** 形式を使用すると、リンクがデフォルトの組み込み Smartport マクロに戻ります。

構文

macro auto user smartport macro *smartport-type user-defined-macro-name* [*parameter-name value* [*parameter-name value* [*parameter-name value*]]]

no macro auto user smartport macro *smartport-type*

パラメータ

- ***smartport-type***：Smartport タイプ（範囲：**printer**、**desktop**、**guest**、**server**、**host**、**ip_camera**、**ip_phone**、**ip_phone_desktop**、**switch**、**router**、または **ap**（ワイヤレス アクセス ポイント））。
- ***user-defined-macro-name***：組み込み Smartport マクロを置き換えるユーザ定義マクロ名を指定します。
- ***parameter-name value***：ユーザ定義のマクロのパラメータ名とその値を指定します。

デフォルト設定

parameter-name *value*：パラメータのデフォルト値。たとえば、パラメータがネイティブ VLAN の場合、デフォルト値はデフォルトのネイティブ VLAN です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

各パラメータの対象範囲は、定義されているマクロです。パラメータ **$voice_vlan** は例外で、グローバル パラメータであり、その値はスイッチにより指定され、マクロでは定義できません。

このコマンドでマクロをリンクする前に、マクロを定義する必要があります。

（このコマンドの **no** バージョンを使用して）Smartport マクロを削除する前に、Smartport タイプから Smartport マクロの接続を解除する必要があります。

Smartport タイプをユーザ定義マクロに関連付けるには、マクロのペアを定義する必要があります。片方は設定を適用するためのマクロで、もう片方（アンチマクロ）は設定を削除するためのマクロです。このマクロは名前でペアになっています。アンチマクロの名前は、**no_** と対応

するマクロの名前を連結したものになります。マクロの定義の詳細については、「マクロ コマンド」セクションを参照してください。

例

ユーザ定義マクロ my_ip_phone_desktop を Smartport タイプ ip_phone_desktop にリンクして、その 2 つのパラメータに値を指定するには、次のようにします。

```
switchxxxxxx(config)# macro auto user smartport macro ip_phone_desktop my_ip_phone_desktop
 $p1 1 $p2 2
```

show macro auto ports

show macro auto ports EXEC モード コマンドは、すべての Smartport ポートまたは特定の Smartport ポートに関する情報を表示します。ポートでマクロが実行されて失敗した場合、そのポートのタイプは Unknown と表示されます。

構文

show macro auto ports [*interface-id* | **detailed**]

パラメータ

- ***interface-id***：インターフェイス識別子（イーサネット インターフェイス、ポート チャネル）。
- **detailed**：現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのポートに関する情報が表示されます。

コマンド モード

ユーザ EXEC モード

例

例 1：switch タイプと phone タイプの Smartport が自動的に設定されていることに注目してください。ルータの Smartport は静的に設定されています。Auto Smartport はグローバルに有効になります。

```
switchxxxxxx# show macro auto ports
Smartport is enabled
Administrative Globally Auto Smartport is enabled
Operational Globally Auto Smartport is enabled
```

Interface	Auto Smartport Admin State	Persistent State	Smartport Type
gi1/0/1	disabled	enabled	router(static)
gi1/0/2	disabled	enabled	switch default
gi1/0/3	enabled	disabled	phone
gi1/0/4	enabled	enabled	

例 2：switch タイプと phone タイプの Smartport が自動的に設定されていることに注目してください。ルータの Smartport は静的に設定されています。Auto Smartport はグローバルに有効になります。

```
switchxxxxxx# show macro auto ports
Smartport is enabled
```

```
Administrative Globally Auto Smartport is disabled
Operational Globally Auto Smartport is disabled
```

Interface	Auto Smartport Admin State	Persistent State	Smartport Type
gi1/0/1	disabled	enabled	router(static)
gi1/0/2	disabled	enabled	switch
gi1/0/3	enabled	disabled	default
gi1/0/4	enabled	enabled	phone

例 3：gi1/0/2 の Auto SmartPort を無効にします。

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# no macro auto smartport
switchxxxxxx(config-if)# end
switchxxxxxx# show macro auto ports gi1/0/2
SmartPort is Enabled
Administrative Globally Auto SmartPort is controlled
Operational Globally Auto SmartPort is enabled
Auto SmartPort is disabled on gi1/0/2
Persistent state is not-persistent
Interface type is default
No macro has been activated
```

例 4：gi1/0/1 の Auto Smartport を有効にします。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# macro auto smartport
switchxxxxxx(config-if)# end
switchxxxxxx# show macro auto ports gi1/0/1
SmartPort is Enabled
Administrative Globally Auto SmartPort is enabled
Operational Globally Auto SmartPort is enabled
Auto SmartPort is enabled on gi1/0/1
Persistent state is persistent
Interface type is switch
Last activated macro is switch
```

show macro auto processing

show macro auto processing EXEC モード コマンドは、どちらのプロトコル（CDP または LLDP）が有効で、どのデバイス タイプを自動的に検出できるかに関する情報を表示します。

構文

show macro auto processing

パラメータ

このコマンドには、パラメータやキーワードはありません。

デフォルト設定

なし

コマンド モード

ユーザ EXEC モード

例

```
switchxxxxxx# show macro auto processing
CDB: enabled
LLDP: enabled
host            :disabled
ip_phone        :enabled
ip_phone_desktop:enabled
switch          :enabled
router          :disabled
ap              :enabled
```

show macro auto smart-macros

show macro auto smart-macros EXEC モード コマンドは、Smartport マクロの名前、そのタイプ（組み込みまたはユーザ定義）、およびそのパラメータを表示します。この情報は、すべての Smartport タイプまたは指定されたタイプについて表示されます。

構文

show macro auto smart-macros [*smartport-type*]

パラメータ

- ***smartport-type***：Smartport タイプ（範囲：**printer**、**desktop**、**guest**、**server**、**host**、**ip_camera**、**ip_phone**、**ip_phone_desktop**、**switch**、**router**、または **ap**（ワイヤレス アクセス ポイント））。

デフォルト設定

なし

コマンド モード

ユーザ EXEC モード

例

```
switchxxxxxx# show macro auto smart-macros
SG300-52-R#show macro auto smart-macros
SmartPort type : printer
Parameters     : $native_vlan=1
SmartPort Macro: printer (Built-In)
SmartPort type : desktop
Parameters     : $max_hosts=10 $native_vlan=1
SmartPort Macro: desktop (Built-In)
SmartPort type : guest
Parameters     : $native_vlan=1
SmartPort Macro: guest (Built-In)
SmartPort type : server
Parameters     : $max_hosts=10 $native_vlan=1
SmartPort Macro: server (Built-In)
SmartPort type : host
Parameters     : $max_hosts=10 $native_vlan=1
SmartPort Macro: host (Built-In)
SmartPort type : ip-camera
Parameters     : $native_vlan=1
SmartPort Macro: ip_camera (Built-In)
SmartPort type : ip-phone
Parameters     : $max_hosts=10 $native_vlan=1 $voice_vlan=1
SmartPort Macro: ip_phone (Built-In)
SmartPort type : ip-phone-desktop
Parameters     : $max_hosts=10 $native_vlan=1 $voice_vlan=1
SmartPort Macro: ip_phone_desktop (Built-In)
SmartPort type : switch
Parameters     : $native_vlan=1 $voice_vlan=1
SmartPort Macro: switch (Built-In)
```

```
SmartPort type : router
Parameters     : $native_vlan=1 $voice_vlan=1
SmartPort Macro: router (Built-In)
SmartPort type : ap
Parameters     : $native_vlan=1 $voice_vlan=1
SmartPort Macro: ap (Built-In)
SG300-52-R#
```

smartport storm-control

インターフェイスでブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を有効にするには、インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モードで **storm-control** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

smartport storm-control broadcast {**level** *level* | **kbps** kbps} [**trap**] [**shutdown**]

no **smartport** storm-control broadcast

smartport storm-control multicast [**registred** | **unregistred**] {**level** *level* | **kbps** *kbps*} [**trap**] [**shutdown**]

no **smartport** storm-control multicast

smartport storm-control unicast {level *level* | kbps *kbps*} [trap] [shutdown]

no **smartport** storm-control unicast

no **smartport** storm-control

パラメータ

- **broadcast**：ポートでブロードキャスト ストーム制御を有効にします。
- **multicast** [**registred** | **unregistred**]：すべてのマルチキャスト、登録済みマルチキャストのみ、未登録マルチキャスト ストーム制御のみのいずれかをポートで有効にします。
- **unicast**：ポートでユニキャスト不明ストーム制御を有効にします。
- **level** *level*：抑制レベル（%）。指定した level の値に達した場合、ストーム パケットのフラッディングをブロックします。（範囲：1 ～ 100）
- **kbps** *kbps*：ポートにおける最大ブロードキャスト トラフィック（キロビット/秒）。（範囲：1 ～ 10000000）
- **trap**：（オプション）ストームがポートで発生したときにトラップを送信します。このキーワードが指定されないと、トラップは送信されません。
- **shutdown**：（オプション）ストームがポートで発生したときに、ポートをシャットダウンします。このキーワードが指定されないと、余剰トラフィックは廃棄されます。

デフォルト設定

ストーム制御は無効です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例 1：ポート 1 でのブロードキャスト トラフィックのキロビット/秒の最大数を 10000 に設定します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# smartport storm-control broadcast kpbs 10000
```

例 2：ポート 1 のブロードキャスト トラフィック（キロビット/秒）の最大パーセンテージを 30% に設定します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# smartport storm-control broadcast level 30
```

sFlow コマンド

この章は、次の項で構成されています。

- sflow receiver （1284 ページ）
- sflow flow-sampling （1285 ページ）
- sflow counters-sampling （1286 ページ）
- clear sflow statistics （1287 ページ）
- show sflow configuration （1288 ページ）
- sflow receiver source-interface （1289 ページ）
- sflow receiver source-interface-ipv6 （1290 ページ）

sflow receiver

sFlow コレクタを定義するには、**sflow receiver** グローバル コンフィギュレーション モード コマンドを使用します。コレクタの定義を削除するには、このコマンドの**no**形式を使用します。

構文

sflow receiver *index {ipv4-address | ipv6-address | hostname} [port port] [max-datagram-size bytes]*

no sflow receiver *index*

パラメータ

- **index**：受信者のインデックス。（範囲：1 ～ 8）
- **ipv4-address**：sFlow コレクタとして使用されるホストの IPv4 アドレス。
- **ipv6-address**：sFlow コレクタとして使用されるホストの IPv6 アドレス。IPv6 アドレスがリンク ローカルアドレス（IPv6Zアドレス）である場合、発信インターフェイス名を指定する必要があります。インターフェイス名の構文については、「ユーザガイドライン」を参照してください。
- **hostname**：sFlow コレクタとして使用されるホストのホスト名。
- **port**：（オプション）sFlow メッセージのポート番号。指定しない場合、ポート番号はデフォルトの 6343 になります。範囲は 1 ～ 65535 です。
- **bytes** ：（オプション）送信可能な最大データグラムサイズを指定します。指定しない場合は、デフォルトで 1400 が設定されます。

デフォルト

受信者が定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

sFlow レシーバの IP アドレスを 0.0.0.0 に設定した場合、sFlow データグラムは送信されません。

sflow flow-sampling

sFlow フローサンプリングを有効にし、特定のポートの平均サンプリングレートを設定するには、**sflow flow-sampling** インターフェイス コンフィギュレーション モード コマンドを使用します。フローサンプリングを無効にするには、このコマンドの **no** 形式を使用します。

構文

sflow flow-sampling *rate receiver-index [max-header-size bytes]*

no sflow flow-sampling

パラメータ

rate：平均サンプリングレートを指定します。サンプリングレートは、1/**レート**として計算されます（範囲：1024 ー 1073741823）。

receiver-index：レシーバ/コレクタのインデックス（範囲：1 ー 8）。

max-header-size bytes：（オプション）サンプリングされたパケットからコピーされる最大バイト数を指定します。指定しない場合は、デフォルトで 128 が設定されます。（範囲：20 ー 256）。

デフォルト

無効

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

インターフェイスのサンプリングレートを設定します。サンプリングレートは、1/レート（コマンドで指定された値）として計算されます。

デバイスには最大3つのレートを設定できます。同じレートを複数のインターフェイスに設定でき、それは単一のレートと見なされます。3つを超えるレートが設定されている場合、コマンドは拒否されます。

sFlow サンプリングは、モニターセッションの送信元インターフェイスとして設定されたインターフェイスでは有効にできません。

新しいサンプリングレート設定は、ハードウェアにすぐにはロードされません。次のパケットが（現在のサンプリングレートに基づいて）サンプリングされた後にのみ、ハードウェアにロードされます。

sflow counters-sampling

sFlow カウンタのサンプリングを有効にし、特定のポートの最大間隔を設定するには、**sflow counters-sampling** インターフェイス コンフィギュレーション モード コマンドを使用します。sFlow カウンタのサンプリングを無効にするには、このコマンドの **no** 形式を使用します。

構文

sflow counters-sampling *interval receiver-index*

no sflow counters-sampling

パラメータ

interval：インターフェイスカウンタの連続するサンプル間の最大秒数を指定します。（範囲：15 ー 86400）

receiver-index：受信者/コレクタのインデックス。（範囲：1 〜 8）

デフォルト

無効

コマンド モード

インターフェイス コンフィギュレーション モード

clear sflow statistics

sFlow 統計情報をクリアするには、**clear sFlow statistics** 特権 EXEC モードコマンドを使用します。

構文

clear sflow statistics *[interface-id]*

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID はイーサネット ポートである必要があります。

コマンド モード

特権 EXEC モード

使用上のガイドライン

ユーザがインターフェイスを指定しない場合、このコマンドはすべての sFlow 統計情報カウンタ（送信されたデータグラムを含む）をクリアします。ユーザがインターフェイスを指定した場合、このコマンドは特定のインターフェイスのカウンタのみをクリアします。

show sflow configuration

フローサンプリングまたはカウンタサンプリングが有効になっているポートの sFlow 設定を表示するには、**show sflow configuration** 特権 EXEC モードコマンドを使用します。

構文

show sflow configuration *[interface-id]*

パラメータ

interface-id：（オプション）インターフェイス ID を指定します。インターフェイス ID はイーサネット ポートである必要があります。

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx#  show sflow configuration
sFlow Agent Address 172.16.1.1
Receivers
Index      IP Address        Port   Max Datagram Size
----- -------------------- -------- ----------------
  1         0.0.0.0          6343         1400
  2         172.16.1.2       6343         1400
  3         0.0.0.0          6343         1400
  4         0.0.0.0          6343         1400
  5         0.0.0.0          6343         1400
  6         0.0.0.0          6343         1400
  7         0.0.0.0          6343         1400
  8         0.0.0.0          6343         1400
Interfaces
Inter-  Flow          Counters  Max Header  Flow      Counters Collector
face    Sampling      Sampling  Size        Collector Index    Index
----- -----------     --------- ---------   ---------- -----   ------------
gi1/0/1   1/2048     60 sec    128         1                  1
gi1/0/2   1/4096     Disabled  128         0                  2
Global values
--------------
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10
```

sflow receiver source-interface

IPv4 アドレスが sFlow 受信者との通信に送信元 IPv4 アドレスとして使用される送信元インターフェイスを指定するには、**sflow receiver source-interface** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sflow receiver source-interface *interface-id*

no sflow receiver source-interface

パラメータ

- ***interface-id***：送信元インターフェイスを指定します。

デフォルト設定

送信元 IPv4 アドレスは、発信インターフェイスで定義され、ネクスト ホップ IPv4 サブネットに属する IPv4 アドレスです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスの場合は、ネクスト ホップ IPv4 サブネットに属するインターフェイス IP アドレスが適用されます。

送信元インターフェイスが発信インターフェイスでない場合は、送信元インターフェイスで定義された最小 IPv4 アドレスが適用されます。

使用可能な IPv4 送信元アドレスがない場合は、IPv4 sFlow サーバとの通信を試行する際に SYSLOG メッセージが発行されます。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# sflow receiver source-interface vlan 100
```

sflow receiver source-interface-ipv6

IPv6 アドレスを IPv6 sFlow 受信者との通信の送信元 IPv6 アドレスとして使用する送信元インターフェイスを指定するには、**sflow receiver source-interface-ipv6** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

sflow receiver source-interface-ipv6 *interface-id*

no sflow receiver source-interface-ipv6

パラメータ

- ***interface-id***：送信元インターフェイスを指定します。

デフォルト設定

IPv6 送信元アドレスは、発信インターフェイスで定義された IPv6 アドレスであり、RFC6724 に従って選択されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスである場合は、送信元 IPv6 アドレスはインターフェイスで定義され、RFC 6724 に従って選択された IPv6 アドレスです。

送信元インターフェイスが発信インターフェイスでない場合は、送信元 IPv6 アドレスは送信元インターフェイス上で定義され、宛先 IPv6 アドレスの範囲と一致します。

使用可能な送信元IPv6アドレスがない場合にIPv6 sFlow受信者との通信を試行すると、SYSLOG メッセージが発行されます。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# sflow receiver source-interface-ipv6 vlan 100
```

SPAN および RSPAN コマンド

この章は、次の項で構成されています。

- monitor session destination （1292 ページ）
- monitor session source （1295 ページ）
- remote-span （1298 ページ）
- show monitor session （1300 ページ）
- show vlan remote-span （1302 ページ）

monitor session destination

新しくスイッチドポートアナライザ（SPAN）またはリモートSPAN（RSPAN）の宛先セッションを作成するには、グローバル コンフィギュレーション モードで **monitor session destination** コマンドを使用します。宛先セッションを削除するには、このコマンドの **no** 形式を使用します。

構文

monitor session *session_number* **destination** {{**interface** *interface-id* [**network**]} | {**remote vlan** *vlan-id* **reflector-port** *interface-id*} **network**}

no monitor session *session_number* destination

パラメータ

- ***session_number***：SPAN、RSPAN、またはフローミラーセッションで識別したセッション番号を指定します。指定できる範囲は 1 ～ 4 です。
- **interface** *interface-id*：SPAN、RSPAN、またはフローミラーセッション（イーサネットポート）の宛先インターフェイスを指定します。送信元インターフェイスが RSPAN VLAN の場合は、インターフェイスにコピーされたすべてのフレームから RSPAN VLAN_ID が削除されます。
- **network**：宛先ポートがネットワークポートとしても機能するように指定します。
- **remote vlan** *vlan-id*：RSPAN 宛先セッションの RSPAN VLAN を指定します。定義できる RSPAN 宛先 VLAN は 1 つのみです。
- **reflector-port** *interface-id*：RSPANセッション（イーサネットポート）の宛先インターフェイスを指定します。RSPAN VLAN_ID は、インターフェイスにコピーされたすべてのフレームに追加されます。

デフォルト設定

SPAN セッションと RSPAN セッションは設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

SPAN、ローカルフローミラー、最終 RSPAN または 最終フローミラーの宛先セッションを作成してトラフィックを宛先ポートにコピーするには、**monitor session** *session_number* **destination interface** *interface-id* を使用します。

開始RSPAN宛先セッションを作成してトラフィックをリフレクタポート経由でRSPAN VLANにコピーするには、**monitor session** *session_number* **destination remote vlan** *vlan-id* **reflector-port** *interface-id* コマンドを使用します。

送信元ポートを宛先ポートまたはリフレクタポートに指定することはできません。

OOB ポートを接続再ポートまたはリフレクタポートに指定することはできません。

network キーワードを定義しない場合は、宛先ポートで送信されたミラートラフィックとすべての入力トラフィックが破棄され、その動作ステータスとして DOWN の値がそのポートで実行しているすべてのアプリケーションにアドバタイズされます。

network キーワードを指定せずに設定した宛先ポートには、次の制限があります。

- そのポートで UDLD を有効にすることができない。
- そのポートで 802.1x を有効にできない。

次のいずれかの条件に該当する場合、**network** キーワードを使用してポートを宛先ポートとして設定することはできません。

- 送信元 VLAN に属する場合
- リモート VLAN に属する場合

送信元/リモート VLAN に宛先ポートを追加しないでください。

リモート VLAN に属するポートは、リフレクタとして設定できません。

リモート VLAN は送信元 VLAN として設定できません。

最終スイッチでのみ、リモート VLAN を送信元リモート VLAN として設定できます。

network キーワードまたはリフレクタポートを持つ宛先ポートは、エッジポート（**vlan-mapping** モードのいずれかを持つポート）では設定できません。

ミラーリングされたトラフィックは、宛先ポートのキュー番号 1 に送信されます。

1 つの宛先セッションを削除するには、**no monitor** *session session_number* **destination** コマンドを使用します。

例 1。次に、3 つの送信元セッションと 1 つの宛先セッションで構成される SPAN セッションを設定する例を示します。最初の送信元セッションは送信元ポート gi1/0/2 から両方向のトラフィックをコピーし、2 番目の送信元セッションは VLAN 100 からブリッジトラフィックをコピーし、3 番目の送信元セッションは送信元ポート gi1/0/3 で受信したトラフィックをコピーします。宛先セッションは、ポート gi1/0/1 を宛先ポートとして定義します。

```
switchxxxxxx(config)# monitor session 1 source interface gi1/0/2 both
switchxxxxxx(config)# monitor session 1 source vlan 100
switchxxxxxx(config)# monitor session 1 source interface gi1/0/3 rx
witchxxxxxx(config)# monitor session 1 destination interface gi1/0/1
```

例 2。次に、フローミラーセッションを設定する例を示します。

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# mirror 1
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
```

例 3。次に、2 つの送信元セッションと 1 つの宛先セッションから構成される RSPAN 開始セッションを設定する例を示します。最初の送信元セッションは送信元ポート gi1/0/2 からの両方向のトラフィックをコピーし、2 番目のセッションは VLAN 100 からのトラフィックをコピーします。宛先セッションは、VLAN 2 を RSPAN VLAN として定義し、ポート gi1/0/1 をリフレクタポートとして定義します。

```
switchxxxxxx(config)# monitor session 1 source interface gi1/0/2 both
switchxxxxxx(config)# monitor session 1 source vlan 100
switchxxxxxx(config)# monitor session 1 destination remote vlan 2 reflector-port gi1/0/1
 network
```

例 4。次に、トラフィックを RSPAN VLAN 2 から宛先ポート gi1/0/1 にコピーする最終 RSPAN セッションを設定する例を示します。

```
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# monitor session 1 source remote vlan 2
switchxxxxxx(config)# monitor session 1 destination interface gi1/0/1
```

monitor session source

スイッチドポートアナライザ（SPAN）またはリモート SPAN（RSPAN）の送信元セッションを新しく作成するには、グローバル コンフィギュレーション モードで **monitor session source** コマンドを使用します送信元セッションを削除するには、このコマンドの **no** 形式を使用します。

構文

monitor session *session_number* **source** {**interface** *interface-id* [**both** | **rx** | **tx**]} | {**vlan** *vlan-id*} | {**remote vlan** *vlan-id*}

no monitor session [*session_number*] **source** [{**interface** *interface-id*} | {**vlan** *vlan-id*} | {**remote vlan** *vlan-id*}]

パラメータ

- ***session_number***：SPAN セッションまたは RSPAN セッションで識別したセッション番号を指定します。指定できる範囲は 1 ～ 4 です。
- **interface** *interface-id*：SPAN セッションまたは RSPAN セッションの送信元インターフェイス（イーサネットポート）を指定します。
- **both**, **rx**, **tx**：モニタするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。
- **vlan** *vlan-id*：SPAN 送信元インターフェイスを VLAN ID として指定します。この場合、*session_number* 引数に指定できる値は 1 のみです。
- **remote vlan** *vlan-id*：送信元 RSPAN 送信元 VLAN ID を指定します。

デフォルト設定

SPAN セッションと RSPAN セッションは設定されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元モートに発着信するトラフィックをモニタするために SPAN または RSPAN の開始送信元セッションを作成するには、**monitor session** *session_number* **source interface** *interface-id* [**both** | **rx** | **tx**] コマンドを使用します。

送信元 VLAN にブリッジされるトラフィックをモニタするために SPAN または RSPAN の開始送信元セッションを作成するには、**monitor session** *session_number* **source vlan** *vlan-id* コマンドを使用します。

RSPAN VLAN を介して渡されるトラフィックをモニタするために最終 RSPAN 送信元セッションを作成するには、**monitor session** *session_number* **source remote vlan** *vlan-id* コマンドを使用します。

SPAN または RSPAN セッションは、同じセッション番号を持つ最大 8 つの送信元と 1 つの宛先で構成されます。

各 **monitor session source** コマンドは、1 つの送信元ポートまたは VLAN を定義します。異なる **monitor session source** コマンドは、異なる送信元を定義する必要があります。同じセッション番号と同じ送信元を持つ新しいコマンドは、以前に定義されたコマンドをオーバーライドします。

1 つのセッションで最大 8 つのソースを定義できます。

パケットがポートベースの入力ミラーリングメカニズムと、他の入力ミラーリングメカニズムのいずれかによってミラーリングされた場合、選択したセッションはセッション番号が大きいセッションになります。

同じ送信元セッションの異なる送信元ポートのすべての定義は、同じタイプ（SPAN、start RSPAN start、または RSPAN final）である必要があります。

送信元モートは宛先ポートにすることはできません。

送信元ポートを OOB ポートにすることはできません。

RSPAN 送信元スイッチの送信元インターフェイスは、リモート VLAN のメンバーシップにすることはできません。

1 つの送信元を削除するには、**no monitor session** *session_number* **source** {**interface** *interface-id*} | {**vlan** *vlan-id*} | {**remote vlan** *vlan-id*} コマンドを使用します。

特定の送信元セッションのすべての送信元ポートを削除するには、**no monitor session** *session_number* **source** コマンドを使用します。

例 1。次に、3 つの送信元セッションと 1 つの宛先セッションで構成される SPAN セッションを設定する例を示します。最初の送信元セッションは送信元ポート gi1/0/2 から両方向のトラフィックをコピーし、2 番目の送信元セッションは VLAN 100 からブリッジトラフィックをコピーし、3 番目の送信元セッションは送信元ポート gi1/0/3 で受信したトラフィックをコピーします。宛先セッションは、ポート gi1/0/1 を宛先ポートとして定義します。

```
switchxxxxxx(config)# monitor session 1 source interface gi1/0/2 both
switchxxxxxx(config)# monitor session 1 source vlan 100
switchxxxxxx(config)# monitor session 1 source interface gi1/0/3 rx
switchxxxxxx(config)# monitor session 1 destination interface gi1/0/1
```

例 2。次に、2 つの送信元セッションと 1 つの宛先セッションから構成される RSPAN 開始セッションを設定する例を示します。最初の送信元セッションは送信元ポート gi1/0/2 からの両方向のトラフィックをコピーし、2 番目のセッションは VLAN 100 からのトラフィックをコピーします。宛先セッションは、VLAN 2 を RSPAN VLAN として、ポート gi1/0/1 をリフレクタポートとして定義します。

```
switchxxxxxx(config)# monitor session 1 source interface gi1/0/2 both
switchxxxxxx(config)# monitor session 1 source vlan 100
```

```
switchxxxxxx(config)# monitor session 1 destination remote vlan 2 reflector-port gi1/0/1
 network
```

例 3。次に、トラフィックを RSPAN VLAN 2 から宛先ポート gi1/0/1 にコピーする最終 RSPAN セッションを設定する例を示します。

```
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# monitor session 1 source remote vlan 2
switchxxxxxx(config)# monitor session 1 destination interface gi1/0/1
```

remote-span

仮想ローカルエリアネットワーク（VLAN）を RSPAN リモート VLAN として設定するには、VLAN コンフィギュレーション モードで **remote-span** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

remote-span

no remote-span

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

VLAN は RSPAN リモート VLAN ではありません。

コマンド モード

VLAN コンフィギュレーション モード

ユーザ ガイドライン

VLAN を RSPAN リモート VLAN として定義するには、**remote-span** コマンドを使用します。

スイッチごとに定義できるリモート VLAN は 1 つのみです。

リモート VLAN は、**remote-span** コマンドを設定する前に手動で作成する必要があります。

ゲスト VLAN はリモート VLAN として設定できません。

RSPLAN VLAN へのトラフィックはすべてタグ付けされ、MAC ラーニングは RSPAN VLAN では無効になります。

remote-span コマンドは、設定された VLAN のすべてのポートが出力タグ付きポートであることを確認し、MAC ラーニングを無効にします。**no remote-span** コマンドは、MAC ラーニングをリセットします。

注。RSPAN リモート VLAN のメンバーシップは、定義されている場所によって異なります。

- 送信元または開始スイッチ：RSPAN リモート VLAN にメンバーシップがないことを推奨します。
- 中間スイッチ：不要なフラッディングを回避するために、ミラートラフィックの受け渡しに使用されないトランクポートから RSPAN リモート VLAN を削除することを推奨します。通常、RSPAN リモート VLAN には 2 つのポートが含まれます。

- 宛先または最終スイッチ：RSPAN リモート VLAN には、この VLAN を介してミラーリングされたトラフィックが着信するメンバーシップが含まれている必要があります。宛先インターフェイスをこの VLAN のメンバーシップにすることはできません。

例 1。次に、送信元スイッチで RSPAN リモート VLAN を設定する例を示します。

```
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# monitor session 1 source interface gi1/0/2 both
switchxxxxxx(config)# monitor session 1 destination remote vlan 2 reflector-port gi1/0/1
```

例 2。次に、最終スイッチで RSPAN リモート VLAN を設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/3
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed none
switchxxxxxx(config-if)# switchport trunk allowed add 2
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# monitor session 1 source remote vlan 2
switchxxxxxx(config)# monitor session 1 destination interface gi1/0/1
```

例 3。次に、中間スイッチで RSPAN リモート VLAN を設定する例を示します。

```
switchxxxxxx(config)# interface range gi1/0/3,4
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed none
switchxxxxxx(config-if)# switchport trunk allowed add 2
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
```

show monitor session

スイッチ上でのスイッチドポートアナライザ（SPAN）とリモート SPAN（RSPAN）セッションに関する情報を表示するには、ユーザ EXEC モードで **show monitor** コマンドを使用します。

構文

show monitor session [*session_number*]

パラメータ

- *session_number*：SPAN セッションまたは RSPAN セッションで識別したセッション番号を指定します。指定できる範囲は 1 ～ 4 です。引数を定義しない場合は、すべてのセッションに関する情報が表示されます。

デフォルト設定

このコマンドには、デフォルト設定がありません。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

1 つのセッションに関する情報を表示するには、**show monitor session** *session_number* コマンドを使用します。

すべてのセッションに関する情報を表示するには、**show monitor session** コマンドを使用します。

例 1。次に、スイッチに定義されているすべての SPAN セッションに関する情報を表示する例を示します。

```
switchxxxxxx> show monitor session
Session 1
  Type: SPAN
  Source: gi1/0/2, rx only
  Source: VLAN 100
  Source: flow mirrow, policy-map: alpha class-maps: ip-http,  ipv6-http
  Destination: gi1/0/1, network port
```

例 2。次に、スイッチに定義されているすべての開始 RSPAN セッションに関する情報を表示する例を示します。

```
switchxxxxxx> show monitor session
Session 1
  Type: RSPAN Start
  Source: gi1/0/3, both
  Source: VLAN 100
  Source: flow mirrow, policy-map: alpha class-maps: ip-http,  ipv6-http
  Destination: RSPAN VLAN 2, reflector-port gi1/0/1, network port
```

例 3。次に、スイッチに定義されているすべての最終 RSPAN セッションに関する情報を表示する例を示します。

```
switchxxxxxx> show monitor session
Session 1
  Type: RSPAN Final
  Source: RSPAN VLAN 10
  Source: RSPAN VLAN 20
  Destination: gi1/0/1
```

フィールドの定義：

- **Type**：セッションのタイプ。
- **Source**：セッションの送信元。次のオプションがサポートされます。

  送信元：*interface-id*、*traffic-direction*（rx only、tx only、またはその両方）

  ```
  The Source is an interface.
  ```

  送信元：vlan *vlan-id*

  ```
  The Source is a VLAN.
  ```

  送信元：remote vlan *vlan-id*

  ```
  The Source is a RSPAN VLAN (in the RSPAN session final switch).
  ```

  送信元：flow mirrow, policy-map: *policy-map-name*, class-maps: *class-map-name1*, *class-map-name2*

  ```
  The Source is a flow mirror, only attached policy-names are displayed.
  ```

- **Destination**：セッションの宛先。次のオプションがサポートされます。

  宛先：*interface-id*

  ```
  The Destination is an interface, regular forwarding on the interface is not supported.
  ```

  宛先：*interface-id*、network

  ```
  The Destination is an interface, regular forwarding on the interface is supported.
  ```

  宛先：RSPAN VLAN *vlan-id*、reflector-port *interface-id*

  ```
  The switch is the first switch in the RSPAN session, regular forwarding on the
  interface is not supported.
  ```

  宛先：RSPAN VLAN *vlan-id*、reflector-port *interface-id*、network

  ```
  The switch is the first switch in the RSPAN session, regular forwarding on the
  interface is supported.
  ```

show vlan remote-span

リモート スイッチド ポート アナライザ（RSPAN）の VLAN のリストを表示するには、ユーザ EXEC モードで **show vlan remote-span** を使用します。

構文

show vlan remote-span

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

このコマンドには、デフォルト設定がありません。

コマンド モード

ユーザ EXEC モード

例次に、RSPAN VLAN のリストを表示する例を示します。

```
switchxxxxxx> show vlan remote-span
Remote SPAN VLAN: 20
```

スパニングツリーコマンド

この章は、次の項で構成されています。

- spanning-tree （1305 ページ）
- spanning-tree mode （1306 ページ）
- spanning-tree forward-time （1307 ページ）
- spanning-tree hello-time （1308 ページ）
- spanning-tree max-age （1309 ページ）
- spanning-tree priority （1310 ページ）
- spanning-tree disable （1311 ページ）
- spanning-tree cost （1312 ページ）
- spanning-tree port-priority （1313 ページ）
- spanning-tree portfast （1314 ページ）
- spanning-tree link-type （1315 ページ）
- spanning-tree pathcost method （1316 ページ）
- spanning-tree bpdu（グローバル） （1317 ページ）
- spanning-tree bpdu（インターフェイス） （1318 ページ）
- spanning-tree guard root （1319 ページ）
- spanning-tree bpduguard （1320 ページ）
- clear spanning-tree counters （1321 ページ）
- clear spanning-tree detected-protocols （1322 ページ）
- spanning-tree mst priority （1323 ページ）
- spanning-tree mst max-hops （1324 ページ）
- spanning-tree mst port-priority （1325 ページ）
- spanning-tree mst cost （1326 ページ）
- spanning-tree mst configuration （1327 ページ）
- instance (MST) （1328 ページ）
- name (MST) （1330 ページ）
- revision (MST) （1331 ページ）
- show (MST) （1332 ページ）
- exit (MST) （1333 ページ）

- abort (MST) （1334 ページ）
- spanning-tree mst instance （1335 ページ）
- show spanning-tree （1337 ページ）
- show spanning-tree bpdu （1349 ページ）
- spanning-tree loopback-guard （1350 ページ）
- spanning-tree vlan forward-time （1351 ページ）
- spanning-tree vlan hello-time （1352 ページ）
- spanning-tree vlan max-age （1353 ページ）
- spanning-tree vlan priority （1354 ページ）
- spanning-tree vlan cost （1355 ページ）
- spanning-tree vlan port-priority （1356 ページ）

spanning-tree

スパニングツリー機能を有効にするには、**spanning-tree** グローバル コンフィギュレーション モード コマンドを使用します。スパニングツリー機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

spanning-tree

no spanning-tree

デフォルト設定

スパニングツリーが有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、スパニング ツリー機能を有効にしています。

```
switchxxxxxx(config)#  spanning-tree
```

spanning-tree mode

どのスパニング ツリー プロトコル（STP）プロトコルを実行するかを選択するには、**spanning-tree mode** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree mode {**stp**| **rstp** | **mst** | **pvst** | **rapid-pvst**}

no spanning-tree mode

パラメータ

- **stp**：STP が有効であることを指定します。
- **rstp**：Rapid STP が有効であることを指定します。
- **mst**：複数の STP を有効にすることを指定します。
- **pvst**：PVST+ が有効であることを指定します。
- **rapid-pvst**：Rapid PVST+ が有効であることを指定します。

デフォルト設定

デフォルトは RSTP です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

RSTP モードでは、デバイスはネイバーデバイスが STP を使用する場合はポートで STP を使用するように指定します。

MSTP モードでは、デバイスはネイバー デバイスが RSTP を使用している場合は RSTP を使用し、ネイバー デバイスが STP を使用している場合は STP を使用します。

PVST モードまたは Rapid PVST モードが有効な場合、スイッチは最大 126 の VLAN をサポートできます。

Rapid PVST モードでは、ネイバーデバイスが PVST を使用する場合、デバイスはポート上の VLAN に PVST を使用します。

例

次の例では、MSTP を有効にしています。

```
switchxxxxxx(config)#  spanning-tree mode mst
```

spanning-tree forward-time

スパニング ツリー ブリッジ転送時間（ポートがフォワーディング ステートになる前にリスニング ステートおよびラーニング ステートのままである時間）を設定するには、**spanning-tree forward-time** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree forward-time *seconds*

no spanning-tree forward-time

パラメータ

- ***seconds***：スパニングツリーの転送時間を秒単位で指定します。(範囲：4 ～ 30)

デフォルト設定

15 秒

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

転送時間を設定するときは、次の関係を維持する必要があります。

2*(Forward-Time - 1) >= Max-Age

例

次の例では、スパニング ツリー ブリッジ転送時間を 25 秒に設定しています。

```
switchxxxxxx(config)#  spanning-tree forward-time 25
```

spanning-tree hello-time

どのくらいの頻度でデバイスが他のデバイスに Hello メッセージをブロードキャストするかを設定するには、**spanning-tree hello-time** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree hello-time *seconds*

no spanning-tree hello-time

パラメータ

- ***seconds***：スパニングツリーの hello タイムを秒単位で指定します。（範囲：1 ～ 10）

デフォルト設定

2 秒

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

hello タイムを設定するときは、次の関係を維持する必要があります。

- Max-Age >= 2*(Hello-Time + 1)

例

次の例では、スパニング ツリー ブリッジ hello タイムを 5 秒に設定しています。

```
switchxxxxxx(config)#  spanning-tree hello-time 5
```

spanning-tree max-age

STP最大有効期間を設定するには、**spanning-tree max-age**グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree max-age *seconds*

no spanning-tree max-age

パラメータ

- ***seconds***：スパニング ツリー ブリッジ最大有効期間を秒単位で指定します。(範囲：6～40)

デフォルト設定

デフォルトの最大経過時間は 20 秒です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

最大有効期間を設定するときは、次の関係を維持する必要があります。

- 2*(Forward-Time - 1) >= Max-Age
- Max-Age >= 2*(Hello-Time + 1)

例

次の例では、スパニング ツリー ブリッジ最大有効期間を 10 秒に設定しています。

```
switchxxxxxx(config)#  spanning-tree max-age 10
```

spanning-tree priority

デバイスのSTP優先順位を設定するには、**spanning-tree priority** グローバル コンフィギュレーション モード コマンドを使用します。この優先順位は、どのブリッジをルート ブリッジとして選択するかを決定するために使用されます。デフォルトのデバイス スパニング ツリー優先順位に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree priority *priority*

no spanning-tree priority

パラメータ

- ***priority***：ブリッジ優先順位を指定します。(範囲：0 ～ 61440)

デフォルト設定

デフォルトの優先順位は 32768 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

priority 値は 4096 の倍数にする必要があります。

優先順位が最も低いスイッチが、スパニング ツリーのルートです。複数のスイッチが最低優先順位になっている場合は、MACアドレスの最も小さいスイッチがルートとして選択されます。

例

次の例では、スパニング ツリー優先順位を 12288 に設定しています。

```
switchxxxxxx(config)#  spanning-tree priority 12288
```

spanning-tree disable

特定のポートでスパニング ツリーを無効にするには、**spanning-tree disable** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。ポートでスパニング ツリーを有効にするには、このコマンドの **no** 形式を使用します。

構文

spanning-tree disable

no spanning-tree disable

デフォルト設定

スパニング ツリーは、すべてのポートで有効になっています。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、gi1/0/5 でスパニングツリーを無効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/5
switchxxxxxx(config-if)#  spanning-tree disable
```

spanning-tree cost

ポートのスパニング ツリー パス コストを設定するには、**spanning-tree cost** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree cost *cost*

no spanning-tree cost

パラメータ

- ***cost***：ポート パス コストを指定します。(範囲：1 ～ 200000000)

デフォルト設定

デフォルトのパスコストは、次のように、ポート速度とパスコスト方式（long または short）によって決まります。

Interface	Long	short
Port-channel	ポートチャネル インターフェイス速度に基づくデフォルトコストの半分	ポートチャネル インターフェイス速度に基づくデフォルトコストの半分
TenGigabit Ethernet（10000 Mbps）	2000	2
5 **Gigabit Ethernet（5000 Mbps）**	12,000	3
2.5 **Gigabit Ethernet（2500 Mbps）**	17,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet（100 Mbps）	200,000	19
Ethernet（10 Mbps）	2,000,000	100

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、gi1/0/15 でのスパニングツリーコストを 35000 に設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/15
switchxxxxxx(config-if)#  spanning-tree cost 35000
```

spanning-tree port-priority

ポート優先順位を設定するには、**spanning-tree port-priority** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree port-priority *priority*

no spanning-tree port-priority

パラメータ

- ***priority***：ポートの優先順位を指定します。(範囲：0 ～ 240)

デフォルト設定

デフォルトのポートの優先順位は 128 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

priority 値は 16 の倍数にする必要があります。

例

次に、gi1/0/15 でスパニング優先順位を 96 に設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/15
switchxxxxxx(config-if)#  spanning-tree port-priority 96
```

spanning-tree portfast

PortFast モードを有効にするには、**spanning-tree portfast** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。PortFast モードを無効にするには、このコマンドの **no** 形式を使用します。

構文

spanning-tree portfast [**auto**]

no spanning-tree portfast

パラメータ

- **auto**：インターフェイスを PortFast モードにする前の遅延を指定します。

デフォルト設定

PortFast モードは auto に設定されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

PortFast モードでは、インターフェイスはリンクアップ時に標準の転送時間遅延を待機せずにただちに転送状態になります。

PortFast モードをただちに有効にするには、**spanning-tree portfast** コマンドを使用します。

PortFast モードを 3 秒間遅らせるには、**spanning-tree portfast auto** を使用します。この間隔でスパニング ツリー プロトコル メッセージを受信しない場合、インターフェイスはPortFastモードになります。

例

次に、gi1/0/15 で PortFast モードを有効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/15
switchxxxxxx(config-if)#  spanning-tree portfast
```

spanning-tree link-type

ポートのデュプレックスモードによって決定されたデフォルトのリンク タイプ設定をオーバーライドし、RSTP をフォワーディング ステートに遷移するには、**spanning-tree link-type** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree spanning-tree link-type

パラメータ

- **point-to-point**：ポートのリンク タイプをポイントツーポイントにすることを指定します。
- **shared**：ポートのリンク タイプが共有であることを指定します。

デフォルト設定

デバイスは、デュプレックス モードからポートのリンク タイプを導き出します。つまり、全二重ポートはポイントツーポイント リンク、半二重ポートは共有リンクであると見なされます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、gi1/0/15 で共有スパニングツリーを有効にする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/15
switchxxxxxx(config-if)#  spanning-tree link-type shared
```

spanning-tree pathcost method

デフォルトのパス コスト方式を設定するには、**spanning-tree pathcost method** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

パラメータ

- **long**：デフォルトのポート パス コストを 1 ～ 200,000,000 の範囲内にすることを指定します。
- **short**：デフォルトのポートパスコストの範囲を 1 ～ 65,535 に指定します。

デフォルト設定

ロング パス コスト方式。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、スイッチのすべてのスパニング ツリー インスタンスに適用されます。

- ショート方式を選択すると、スイッチはデフォルトのコストを 100 と計算します。
- ロング方式を選択すると、スイッチはデフォルトのコストを 20000 と計算します。

例

次の例では、デフォルトのパス コスト方式をロングに設定しています。

```
switchxxxxxx(config)#  spanning-tree pathcost method long
```

spanning-tree bpdu（グローバル）

スパニングツリーがグローバルに無効であるか、または単一のインターフェイスで無効である場合にブリッジプロトコルデータユニット（BPDU）処理を定義するには、**spanning-tree bpdu** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree bpdu {**filtering** | **flooding**}

no spanning-tree bpdu

パラメータ

- **filtering**：インターフェイスでスパニング ツリーが無効になっているときに BPDU パケットをフィルタ処理することを指定します。
- **flooding**：スパニング ツリーが無効で、BPDU 処理モードがフラッディングの場合、タグなしBPDUパケットをすべてのポートに無条件に（VLANルールの適用なし）フラッディングすることを指定します。タグ付きの BPDU パケットはフィルタ処理されます。

デフォルト設定

デフォルト設定は **flooding** です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

filtering モードおよび **flooding** モードが意味を持つのは、スパニング ツリーがグローバルに無効であるか、または単一のインターフェイスで無効である場合です。

例

次に、スパニングツリーがインターフェイスで無効になっている場合に、BPDUパケット処理モードを **flooding** として定義する例を示します。

```
switchxxxxxx(config)#  spanning-tree bpdu flooding
```

spanning-tree bpdu（インターフェイス）

スパニング ツリーが単一のインターフェイスで無効になっている場合に BPDU 処理を定義するには、**spanning-tree bpdu** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree bpdu {**filtering** | **flooding**}

no spanning-tree bpdu

パラメータ

- **filtering**：インターフェイスでスパニング ツリーが無効になっているときに BPDU パケットをフィルタ処理することを指定します。
- **flooding**：スパニング ツリーが無効で、BPDU 処理モードがフラッディングの場合、タグなしBPDUパケットをポートに無条件に（VLANルールの適用なし）フラッディングすることを指定します。タグ付きの BPDU パケットはフィルタ処理されます。

デフォルト設定

spanning-tree bpdu（グローバル） （1317 ページ） コマンドによって、デフォルトの設定が決定されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、スパニングツリーが gi1/0/3 で無効になっている場合に BPDU パケットを **flooding** として定義する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/3
switchxxxxxx(config-if)#  spanning-tree bpdu flooding
```

spanning-tree guard root

インターフェイスのすべてのスパニング ツリー インスタンスでルートガードを有効にするには、**spanning-tree guard root** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。ルート ガードを使用すると、インターフェイスがデバイスのルート ポートになるのを阻止できます。インターフェイスでルート ガードを無効にするには、このコマンドの **no** 形式を使用します。

構文

spanning-tree guard root

no spanning-tree guard root

デフォルト設定

ルート ガードは無効です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

ルートガードは、デバイスがスパニングツリーモードで動作している場合に有効にできます。

ルート ガードを有効にすると、スパニング ツリー計算によってポートがルート ポートとして選択された場合に、ポートが代替状態に変化します。

例

次に、gi1/0/1 がデバイスのルートポートになることを阻止する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  spanning-tree guard root
```

spanning-tree bpduguard

インターフェイスでスパニングツリーメッセージを受信した場合にそのインターフェイスをシャットダウンするには、**spanning-tree bpduguard** インターフェイス（イーサネット、ポートチャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree bpduguard {**enable** | **disable**}

no spanning-tree bpduguard

パラメータ

- **enable**：BPDU ガードを有効にします。
- **disable**：BPDU ガードを無効にします。

デフォルト設定

BPDU Guard は無効です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

このコマンドは、スパニング ツリーが有効の場合でも（ポートが PortFast モードのときに便利）無効の場合でも有効にできます。

例

次に、gi1/0/5 で BPDU を受信した場合に gi1/0/5 をシャットダウンする例を示します。

```
switchxxxxxx(config)#  interface gi1/0/5
switchxxxxxx(config-if)#  spanning-tree bpduguard enable
```

clear spanning-tree counters

すべてのインターフェイスまたは指定したインターフェイスの STP カウンタをクリアするには、**clear spanning-tree counters** 特権 EXEC モードコマンドを使用します。

構文

clear spanning-tree counters [**interface** *interface-id*]

パラメータ

- ***interface-id***：（任意）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

デフォルト設定

すべてのインターフェイス。

コマンド モード

特権 EXEC モード

使用上のガイドライン

clear spanning-tree counters コマンドは、スイッチ全体または指定したインターフェイスから送受信された STP BPDU カウンタをクリアします。

例

次に、すべてのインターフェイスの STP カウンタをクリアする例を示します。

switchxxxxxx# **clear spanning-tree counters**

clear spanning-tree detected-protocols

すべてのスパニング ツリー インターフェイスまたは指定されたインターフェイスで、STP 移行プロセスを再開する（ネイバー スイッチと強制的に再ネゴシエーションさせる）には、**clear spanning-tree detected-protocols** 特権 EXEC モード コマンドを使用します。

構文

clear spanning-tree detected-protocols [**interface** *interface-id*]

パラメータ

- ***interface-id***：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

デフォルト設定

すべてのインターフェイス。

コマンド モード

特権 EXEC モード

使用上のガイドライン

この機能は、RSTP、MSTP、または Rapid PVST モードで動作している場合にのみ使用できます。

例

これは、すべてのインターフェイスで STP 移行プロセスを再開しています。

```
switchxxxxxx#  clear spanning-tree detected-protocols
```

spanning-tree mst priority

指定したスパニング ツリー インスタンスのデバイス優先順位を設定するには、**spanning-tree mst priority** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

パラメータ

- ***instance-id***：スパニング ツリー インスタンス ID を指定します。（範囲：1 ー 7）
- ***priority***：指定したスパニング ツリー インスタンスのデバイス優先順位を指定します。この設定によって、スイッチがルート スイッチとして選択される可能性が決まります。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高まります。(範囲：0 ～ 61440)

デフォルト設定

デフォルトの優先順位は 32768 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

priority 値は 4096 の倍数にする必要があります。

優先順位が最も低いスイッチが、スパニング ツリーのルートです。

例

次の例では、インスタンス 1 のスパニング ツリー優先順位を 4096 に設定しています。

```
switchxxxxxx(config)#  spanning-tree mst 1 priority 4096
```

spanning-tree mst max-hops

BDPU が破棄されてポート情報がエージ アウトされるまでの MST リージョン内のホップ数を設定するには、**spanning-tree mst max-hops** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

パラメータ

- ***hop-count***：BDPU を破棄するまでの MST リージョン内のホップ数を指定します。(範囲：1 ～ 40)

デフォルト設定

デフォルトのホップ数は 20 です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、パケットが MST リージョン内を移動するホップの最大数を 10 に設定しています。それを超えると、パケットは破棄されます。

```
switchxxxxxx(config)#  spanning-tree mst max-hops 10
```

spanning-tree mst port-priority

ポートの優先順位を設定するには、**spanning-tree mst port-priority** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

パラメータ

- ***instance-id***：スパニングツリー インスタンスの ID を指定します。（範囲：1 ー 7）
- ***priority***：ポートの優先順位を指定します。（範囲：0 ～ -240 で、16 の倍数）

デフォルト設定

デフォルトのポートの優先順位は 128 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

priority 値は 16 の倍数にする必要があります。

例

次に、gi1/0/1 のポート優先順位を 144 に設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  spanning-tree mst 1 port-priority 144
```

spanning-tree mst cost

MST を計算するためのパス コストを設定するには、**spanning-tree mst cost** インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード コマンドを使用します。ループが発生した場合、スパニング ツリー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際にパス コストを考慮します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

パラメータ

- ***instance-id***：スパニング ツリー インスタンス ID を指定します。（範囲：1 ー 7）
- ***cost***：ポート パス コストを指定します。(範囲：1 ～ 200000000)

デフォルト設定

デフォルトのパス コストは、次のように、ポート速度およびパス コスト方式（long または short）によって決まります。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、ポート gi1/0/9 ～ 4 の MSTP インスタンス 1 パスコストを設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/9
switchxxxxxx(config-if)#  spanning-tree mst 1 cost 4
```

spanning-tree mst configuration

MSTモードにしてMSTリージョンを設定できるようにするには、**spanning-tree mst configuration** グローバル コンフィギュレーション モード コマンドを使用します。

構文

spanning-tree mst configuration

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

2 台以上のスイッチが同一 MST リージョン内に存在する場合、同じ VLAN マッピング、同じコンフィギュレーション リビジョン番号、および同じ名前が含まれている必要があります。

例

次の例では、MST リージョンを設定しています。

```
switchxxxxxx(config)#  spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
switchxxxxxx(config-mst)# name region1
switchxxxxxx(config-mst)# revision 1
```

instance (MST)

MST インスタンスに VLAN をマップするには、**instance** MST コンフィギュレーション モード コマンドを使用します。デフォルト マッピングに戻すには、このコマンドの **no** 形式を使用します。

構文

instance *instance-id* ***vlan*** *vlan-range*

no **instance** *instance-id* ***vlan*** *vlan-range*

パラメータ

- ***instance-id***：MST インスタンス（範囲：1 ～ 7）
- ***vlan-range***：指定した VLAN 範囲が既存の範囲に追加されます。範囲を指定するには、ハイフンを使用します。シリーズを指定するには、カンマを使用します。（範囲：1～4094）

デフォルト設定

すべての VLAN は、Common and Internal Spanning Tree（CIST）インスタンス（インスタンス 0）にマップされます。

コマンド モード

MST コンフィギュレーション モード

使用上のガイドライン

VLAN をインスタンスにマッピングする前に、spanning-tree mst instance （1335 ページ） コマンドを使用してインスタンスを作成する必要があります（最大 15 個のインスタンスを作成できます）。

明示的に MST インスタンスにマッピングされていないすべての VLAN は、Common and Internal Spanning Tree（CIST）インスタンス（インスタンス 0）にマッピングされ、CIST から解除できません。

2 台以上のデバイスが同一 MST リージョン内に存在する場合、同じ VLAN マッピング、同じコンフィギュレーション リビジョン番号、および同じ名前が設定されている必要があります。

例

例 1。次の例では、VLAN 10 ～ 20 を MST インスタンス 1000 にマッピングしています。

```
switchxxxxxx(config)# spanning-tree mst instance 1000
switchxxxxxx(config)#  spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1000 vlan 10-20
```

例 2。次の例では、ユーザーがインスタンス ID 1001 を作成していないため、VLAN を MST インスタンス ID 1001 にマッピングしようとすると失敗します。

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1000 vlan 30-40
Cannot map VLANs to instance 1001. Instance 1001 does not exist.
```

name (MST)

MST リージョン名を定義するには、**name** MST コンフィギュレーション モード コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

構文

name *string*

no name

パラメータ

- ***string***：MST リージョン名を指定します。（長さ：1 ～ 32 文字）

デフォルト設定

デフォルト名はブリッジの MAC アドレスです。

コマンド モード

MST コンフィギュレーション モード

例

次に、リージョン名を Region1 として定義する例を示します。

```
switchxxxxxx(config)#  spanning-tree mst configuration
switchxxxxxx(config-mst)# name region1
```

revision (MST)

MST コンフィギュレーション リビジョン番号を定義するには、**revision** MST コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

revision *value*

no revision

パラメータ

- ***value***：MST コンフィギュレーション リビジョン番号を指定します。（範囲：0 ～ 65535）

デフォルト設定

デフォルトのコンフィギュレーション リビジョン番号は 0 です。

コマンド モード

MST コンフィギュレーション モード

例

次の例では、コンフィギュレーション リビジョンを 1 に設定しています。

```
switchxxxxxx(config)#  spanning-tree mst configuration
switchxxxxxx(config-mst) # revision 1
```

show (MST)

現在または保留中の MST リージョン コンフィギュレーションを表示するには、**show** MST コンフィギュレーション モード コマンドを使用します。

構文

show {**current** | **pending**}

パラメータ

- **current**：現在の MST リージョン コンフィギュレーションを表示します。
- **pending**：保留中の MST リージョン コンフィギュレーションを表示します。

コマンド モード

MST コンフィギュレーション モード

例

次に、保留中の MST リージョン コンフィギュレーションを表示する例を示します。

```
switchxxxxxx(config-mst)# show pending
Gathering information ..........
Current MST configuration
Name: Region1
Revision: 1
Digest: 0xB41829F9030A054FB74EF7A8587FF58D
Instance  VLANs Mapped               State
--------  -------------------------  -----
0         1-4094                     Disabled
switchxxxxxx(config-mst)#
```

exit (MST)

MST リージョン コンフィギュレーション モードを終了し、すべての設定変更を適用するには、**exit** MST コンフィギュレーション モード コマンドを使用します。

構文

exit

コマンド モード

MST コンフィギュレーション モード

例

次の例では、MST コンフィギュレーション モードを終了し、変更を保存しています。

```
switchxxxxxx(config)#  spanning-tree mst configuration
switchxxxxxx(config-mst)# exit
switchxxxxxx(config)#
```

abort (MST)

設定変更を適用しないで MST コンフィギュレーション モードを終了するには、**abort** MST コンフィギュレーション モード コマンドを使用します。

構文

abort

コマンド モード

MST コンフィギュレーション モード

例

次の例では、変更を保存しないで MST コンフィギュレーション モードを終了しています。

```
switchxxxxxx(config)#  spanning-tree mst configuration
switchxxxxxx(config-mst)# abort
```

spanning-tree mst instance

VLAN をマッピングできる MST インスタンスを作成するには、spanning-tree mst instance グローバル コンフィギュレーション モード コマンドを使用します。インスタンスを削除するには、コマンドの no 形式を使用します。

構文

spanning-tree mst instance *instance-id*

no spanning-tree mst instance *instance-id*

パラメータ

- ***instance-id***：スパニング ツリー インスタンス ID を指定します。（範囲：1 ～ 4094）

デフォルト設定

インスタンス ID 1 ～ 4094 は存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

MST インスタンスを作成するには、spanning-tree mst instance コマンドを使用します。最大 15 個作成できます。インスタンス 0（共通および内部スパニングツリー（CIST）インスタンス）はデフォルトでデバイスに存在しており、削除できません。

MST インスタンスを作成すると、MST コンフィギュレーション モードで VLAN をこのインスタンスにマッピングし、作成したインスタンスで次の設定を行うことができます。

- インスタンスの優先順位の設定：コマンド spanning-tree mst priority （1323 ページ）。
- インスタンスごとのポートの優先順位の設定：コマンド spanning-tree mst port-priority （1325 ページ）
- インスタンスごとのポートコストの設定：コマンド spanning-tree mst cost （1326 ページ）

インスタンスを削除するには、コマンドの no 形式を使用します。1 つ以上の VLAN がマッピングされたままのインスタンスは削除できません。インスタンスを削除すると、そのインスタンスに関連するすべての STP 設定が削除されます。

例

例 1。次の例では、インスタンス ID が 248 の MST インスタンスを作成しています。

```
switchxxxxxx(config)#spanning-tree mst instance 248
```

例 2：次の例では、デバイスから MST インスタンス 248 を削除しています。

```
switchxxxxxx(config)# no spanning-tree mst instance 248
```

例 3：次の例では、VLAN がまだこのインスタンスにマッピングされているため、インスタンス ID 365 の削除は失敗します。

```
switchxxxxxx(config)# no spanning-tree mst instance 365
Cannot delete instance 365. One or more VLANs are mapped to this instance.
```

show spanning-tree

スパニング ツリー設定を表示するには、**show spanning-tree** 特権 EXEC モード コマンドを使用します。

構文

show spanning-tree [*interface-id*] [**{instance** *instance-id*} | {**vlan** *vlan-id*}]

show spanning-tree [**detail**] [**active** | **blockedports**] [**{instance** *instance-id*} | {**vlan** *vlan-id*}]

show spanning-tree inconsistentports

show spanning-tree mst-configuration

show spanning-tree mst-configuration digest

パラメータ

- ***interface-id***（オプション）インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。
- **detail**：詳細情報を表示します。
- **active**：アクティブなポートのみを表示します。アクティブポートは、STP が有効で、動作ステータスが up のポートです。デバイスモードが PVST+ または Rapid PVST+ の場合、ポートも表示された VLAN のメンバーである必要があります。
- **blockedports**：ブロックされたポートのみを表示します。
- ***instance-id***：MST インスタンス（範囲：1 ～ 7）。パラメータは、モード MSTP が有効な場合にのみ定義できます。
- **vlan** *vlan-id*：VLAN ID を指定します。（範囲：1 ～ 4094）パラメータは、モード PVST または RPVST が有効な場合にのみ定義できます。
- **inconsistentports**：STP の状態が整合しないポートを表示します。コマンドは、PVST+ モードまたは Rapid PVST モードの場合にのみ適用されます。
- **mst-configuration**：MST 設定の情報を表示します。
- **mst-configuration digest**：MST 設定のダイジェスト情報を表示します。

デフォルト設定

インターフェイスを指定しない場合、デフォルトはすべてのインターフェイスです。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、MST が有効の場合にのみ機能します。

例

次の例では、さまざまな設定のスパニングツリー情報を表示します。

- **STP モードまたは RSTP モードのデバイスの表示例**：

```
switchxxxxxx#  show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled
```

Root ID	Priority Address Cost Port	32768 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority Address	36864 00:02:4b:29:7a:00		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio. No	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	FRW	Root		P2p (RSTP)
gi1/0/2	Enabled	128.2	20000	FRW	Desg	No	Shared (STP)
gi1/0/3	Disabled	128.3	20000	-	-	No	-
gi1/0/4	Enabled	128.4	20000	BLK	Altn	-	Shared (STP)
gi1/0/5	Enabled	128.5	20000	DIS	-	No	-
						-	

```
switchxxxxxx# show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long
Loopback guard: Disabled
Interfaces
```

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	FRW	Desg	No	P2p (RSTP)
gi1/0/2	Enabled	128.2	20000	FRW	Desg	No	Shared (STP)
gi1/0/3	Disabled	128.3	20000	-	-	-	-
gi1/0/4	Enabled	128.4	20000	FRW	Desg	No	Shared (STP)
gi1/0/5	Enabled	128.5	20000	DIS	-	-	-

```
switchxxxxxx#  show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long
Loopback guard: Disabled
```

Root ID	Priority Address Path Cost Root Port Hello Time	N/A N/A N/A N/A N/A	Max Age N/A	Forward Delay N/A
Bridge ID	Priority Address	36864 00:02:4b:29:7a:00		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nb	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	-	-	-	-
gi1/0/2	Enabled	128.2	20000	-	-	-	-
gi1/0/3	Disabled	128.3	20000	-	-	-	-
gi1/0/4	Enabled	128.4	20000	-	-	-	-
gi1/0/5	Enabled	128.5	20000	-	-	-	-

```
switchxxxxxx#  show spanning-tree active
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled
```

Root ID	Priority Address Path Cost Root Port	32768 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority Address	36864 00:02:4b:29:7a:00		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	FRW	Root	No	P2P (RSTP)
gi1/0/2	Enabled	128.2	20000	FRW	Desg	No	Shared (STP)
gi1/0/4	Enabled	128.4	20000	BLK	Altn	No	Shared (STP)

```
switchxxxxxx#  show spanning-tree blockedports
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled
```

Root ID	Priority Address Path Cost Root Port	32768 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority	36864		
	Address	00:02:4b:29:7a:00		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
gi1/0/4	Enabled	128.4	19	BLK	Altn	No	Shared (STP)

```
switchxxxxxx#  show spanning-tree detail
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled
```

Root ID	Priority Address Path Cost Root Port	32768 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority Address	36864 00:02:4b:29:7a:00		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Number of topology changes 2 last change occurred 2d18h ago				
Times:	hold 1, topology change 35, notification 2 hello 2, max age 20, forward delay 15			

Port 1 (gi1/0/1) enabled State: Forwarding Port id: 128.1 Type: P2p (configured: auto) RSTP Designated bridge Priority: 32768 Designated port id: 128.25 Guard root: Disabled	Role: Root Port cost: 20000 Port Fast: No (configured:no) Address: 00:01:42:97:e0:00 Designated path cost: 0 BPDU guard: Disabled
Number of transitions to forwarding state: 1 BPDU: sent 2, received 120638	

Port 2 (gi1/0/2) enabled State: Forwarding Port id: 128.2 Type: Shared (configured: auto) STP Designated bridge Priority: 32768 Designated port id: 128.2 Guard root: Disabled	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000 BPDU guard: Disabled
Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	
Port 3 (gi1/0/3) disabled State: N/A Port id: 128.3 Type: N/A (configured: auto) Designated bridge Priority: N/A Designated port id: N/A Guard root: Disabled	Role: N/A Port cost: 20000 Port Fast: N/A (configured:no) Address: N/A Designated path cost: N/A BPDU guard: Disabled
Number of transitions to forwarding state: N/A BPDU: sent N/A, received N/A	
Port 4 (gi1/0/4) enabled State: Blocking Port id: 128.4 Type: Shared (configured:auto) STP Designated bridge Priority: 28672 Designated port id: 128.25 Guard root: Disabled	Role: Alternate Port cost: 20000 Port Fast: No (configured:no) Address: 00:30:94:41:62:c8 Designated path cost: 20000 BPDU guard: Disabled
Number of transitions to forwarding state: 1 BPDU: sent 2, received 120638	
Port 5 (gi1/0/5) enabled State: Disabled Port id: 128.5 Type: N/A (configured: auto) Designated bridge Priority: N/A Designated port id: N/A Guard root: Disabled	Role: N/A Port cost: 20000 Port Fast: N/A (configured:no) Address: N/A Designated path cost: N/A BPDU guard: Disabled

```
Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A
switchxxxxxx#  show spanning-tree ethernet gi1/0/1
```

Port 1 (gi1/0/1) enabled State: Forwarding Port id: 128.1 Type: P2p (configured: auto) RSTP Designated bridge Priority: 32768 Designated port id: 128.25 Guard root: Disabled	Role: Root Port cost: 20000 Port Fast: No (configured:no) Address: 00:01:42:97:e0:00 Designated path cost: 0 BPDU guard: Disabled

```
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
```

- **PVST モードまたは Rapid PVST モードのデバイスの表示例**：

```
switchxxxxxx#  show spanning-tree
Spanning tree enabled mode Rapid-PVST
Default port cost method: long
Loopback guard: Disabled
VLAN 1
```

Root ID	Priority Address Path Cost Root Port	4096 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority Address	36864 00:02:4b:29:7a:00		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
						No	
gi1/0/1	Enabled	128.1	20000	Frw	Root	No	P2P (RPVST)
gi1/0/2	Enabled	128.2	20000	DSCR	Bkup	No	P2P (RVPST)
gi1/0/3	Disabled	128.3	20000	-	-	No	-
gi1/0/4	Enabled	128.4	20000	Dsbl	Dsbl	No	-
gi1/0/5	Enabled	128.5	20000	DSCR	Altn	Yes	P2P (RPVST)
gi1/0/6	Enabled	128.6	20000	Frw	Desg		Shared(PVST)

* Port Type or PVID Inconsistency
VLAN 20

Root ID	Priority Address	4096 00:02:4b:29:7a:00		
	This switch is the root			
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
						No	
gi1/0/1	Enabled	128.1	20000	FRW	Desg	No	P2p (RPVST)
gi1/0/2	Enabled	128.2	20000	Dscr*	Desg	No	P2p (RPVST)
gi1/0/3	Disabled	128.3	20000	Dsbl	Dsbl	No	-
gi1/0/4	Enabled	128.4	20000	Dsbl	Dsbl	no	-
gi1/0/5	Enabled	128.5	20000	Dsbl	Dsbl	Yes	P2P (RPVST)
gi1/0/6	Enabled	128.6	20000	Frw	Desg		Shared(PVST)

* Port Type or PVID Inconsistency
switchxxxxxx# **show spanning-tree active**
Spanning tree enabled mode Rapid-PVST
Default port cost method: long
Loopback guard: Disabled
VLAN 1

Root ID	Priority Address Path Cost Root Port	4096 00:01:42:97:e0:00 20000 gi1/0/1

	Hello Time 2 sec	Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority Address	36864 00:02:4b:29:7a:00	
	Hello Time 2 sec	Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
						No	
gi1/0/1	Enabled	128.1	20000	Frw	Root	No	P2p (RPVST)
gi1/0/2	Enabled	128.2	20000	DSCR	Bkup	No	P2p (RPVST)
gi1/0/5	Enabled	128.5	20000	DSCR	Altn	Yes	P2p (RPVST)
gi1/0/6	Enabled	128.6	20000	Frw	Desg		Shared(PVST)

* Port Type or PVID Inconsistency
VLAN 20

Root ID	Priority Address	4096 00:02:4b:29:7a:00
	This switch is the root	
	Hello Time 2 sec	Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
						No	
gi1/0/1	Enabled	128.1	20000	FRW	Desg	No	P2p (RPVST)
gi1/0/2	Enabled	128.2	20000	Dscr*	Desg	Yes	P2p (RPVST)
gi1/0/6	Enabled	128.6	20000	Frw	Desg		Shared(PVST)

* Port Type or PVID Inconsistency
switchxxxxxx# **show spanning-tree VLAN 20**
Spanning tree enabled mode PVST
Default port cost method: long
Loopback guard: Disabled
VLAN 20

Root ID	Priority Address	4096 00:02:4b:29:7a:00
	This switch is the root	
	Hello Time 2 sec	Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
						No	
gi1/0/1	Enabled	128.1	20000	FRW	Desg	No	P2p (RPVST)
gi1/0/2	Enabled	128.2	20000	Dscr*	Desg	No	P2p (RPVST)
gi1/0/3	Disabled	128.3	20000	Dsbl	Dsbl	No	-
gi1/0/4	Enabled	128.4	20000	Dsbl	Dsbl	no	-
gi1/0/5	Enabled	128.5	20000	Dsbl	Dsbl	Yes	P2P (RPVST)
gi1/0/6	Enabled	128.6	20000	Frw	Desg		Shared(PVST)

```
* Port Type or PVID Inconsistency
switchxxxxxx#  show spanning-tree gi1/0/2
```

VLAN	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
						No	
1	Enabled	128.1	2000	FRW	Root	No	P2p (RPVST)
2	Enabled	128.2	2000	Dscr*	Desg	No	P2p (RPVST)
3	Enabled	128.3	2000	Dscr	Altr	Yes	P2p (RPVST)
6	Enabled	128.6	2000	Frw	Desg		Shared(PVST)

```
* Port Type or PVID Inconsistency
switchxxxxxx#  show spanning-tree gi1/0/2 vlan 3
```

(gi1/0/2) enabled	Role: Alternate
State: Discarding	Port cost: 2000
Port id: 128.3	Port Fast: No (configured:Auto)
Type: P2p (configured: auto) RPVST	Address: 00:01:42:97:e0:00
Designated bridge Priority: 32768	Designated path cost: 0
Designated port id: 128.22	BPDU guard: Disabled
Guard root: Disabled	

```
switchxxxxxx#  show spanning-tree inconsistentports
```

name	interface	inconsistency
VLAN 10	gi1/0/2	Port Type Inconsistency
VLAN 10	gi1/0/7	PVID Inconsistency
VLAN 20	gi1/0/7	PVID Inconsistency
VLAN 20	gi1/0/8	Port Type Inconsistency

```
Number of inconsistent ports (segments) in the system : 4
```

- **MSTP モードのデバイスの表示例**：

```
switchxxxxxx#  show spanning-tree mst-configuration
Name: Region1
Revision: 1
```

Instance	Vlans mapped	State
--------	------------	---------
1	1-9, 21-4094	Enabled
2	10-20	Enabled

```
switchxxxxxx#  show spanning-tree mst-configuration digest
Name: Region1
Revision: 1
Format selector: 0
Digest: 0xB41829F9030A054FB74EF7A8587FF58D
Number of instances configured: 3
switchxxxxxx#  show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
Loopback guard: Disabled
###### MST 0 Vlans Mapped: 1-9
```

CST Root ID	Priority Address Path Cost Root Port	32768 00:01:42:97:e0:00 20000 gi1/0/1	
	Hello Time 2 sec	Max Age 20 sec	Forward Delay 15 sec
IST Master ID	Priority Address	32768 00:02:4b:29:7a:00	
	This switch is the IST master.		
	Hello Time 2 sec	Max Age 20 sec	Forward Delay 15 sec
	Max hops 20		

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
----	-------	--------	-----	---	----	--------	-------------
gi1/0/1	Enabled	128.1	20000	FRW	Root	No	P2p Bound
gi1/0/2	Enabled	128.2	20000	FRW	Desg	No	(RSTP)
gi1/0/3	Enabled	128.3	20000	FRW	Desg	No	Shared Bound
gi1/0/4	Enabled	128.4	20000	FRW	Desg	No	(STP)
							P2p
							P2p

```
###### MST 1 Vlans Mapped: 10-20
```

Root ID	Priority Address Path Cost Root Port Rem hops	24576 00:02:4b:29:89:76 20000 gi1/0/4 19
Bridge ID	Priority Address	32768 00:02:4b:29:7a:00

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	FRW	Boun	No	P2p Bound
gi1/0/2	Enabled	128.2	20000	FRW	Boun	No	(RSTP)
gi1/0/3	Enabled	128.3	20000	BLK	Altn	No	Shared Bound
gi1/0/4	Enabled	128.4	20000	FRW	Root	No	(STP)
							P2p
							P2p

```
switchxxxxxx#  show spanning-tree detail
Spanning tree enabled mode MSTP
Default port cost method: long
Loopback guard: Disabled
###### MST 0 Vlans Mapped: 1-9
```

CST Root ID	Priority Address Path Cost Root Port	32768 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
IST Master ID	Priority Address	32768 00:02:4b:29:7a:00		
	This switch is the IST master.			
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
	Max hops 20 Number of topology changes 2 last change occurred 2d18h ago Times: hold 1, topology change 35, notification 2 hello 2, max age 20, forward delay 15			

Port 1 (gi1/0/1) enabled State: Forwarding Port id: 128.1 Type: P2p (configured: auto) Boundary RSTP Designated bridge Priority: 32768 Designated port id: 128.25 Number of transitions to forwarding state: 1 BPDU: sent 2, received 120638	Role: Root Port cost: 20000 Port Fast: No (configured:no) Address: 00:01:42:97:e0:00 Designated path cost: 0
Port 2 (gi1/0/2) enabled State: Forwarding Port id: 128.2 Type: Shared (configured: auto) Boundary STP Designated bridge Priority: 32768 Designated port id: 128.2 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000

Port 3 (gi1/0/3) enabled State: Forwarding Port id: 128.3 Type: Shared (configured: auto) Internal Designated bridge Priority: 32768 Designated port id: 128.3 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000
Port 4 (gi1/0/4) enabled State: Forwarding Port id: 128.4 Type: Shared (configured: auto) Internal Designated bridge Priority: 32768 Designated port id: 128.2 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000

MST 1 Vlans Mapped: 10-20

Root ID	Priority Address Path Cost Root Port	24576 00:02:4b:29:89:76 20000 gi1/0/4
	Rem hops 19	
Bridge ID	Priority Address	32768 00:02:4b:29:7a:00
	Number of topology changes 2 last change occurred 1d9h ago	
	Times: hold 1, topology change 2, notification 2 hello 2, max age 20, forward delay 15	

Port 1 (gi1/0/1) enabled State: Forwarding Port id: 128.1 Type: P2p (configured: auto) Boundary RSTP Designated bridge Priority: 32768 Designated port id: 128.1 Number of transitions to forwarding state: 1 BPDU: sent 2, received 120638	Role: Boundary Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000
Port 2 (gi1/0/2) enabled State: Forwarding Port id: 128.2 Type: Shared (configured: auto) Boundary STP Designated bridge Priority: 32768 Designated port id: 128.2 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000

Port 3 (gi1/0/3) disabled State: Blocking Port id: 128.3 Type: Shared (configured: auto) Internal Designated bridge Priority: 32768 Designated port id: 128.78 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Alternate Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:1a:19 Designated path cost: 20000
Port 4 (gi1/0/4) enabled State: Forwarding Port id: 128.4 Type: Shared (configured: auto) Internal Designated bridge Priority: 32768 Designated port id: 128.2 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000

show spanning-tree bpdu

スパニング ツリーが無効の場合に BPDU 処理を表示するには、**show spanning-tree bpdu** ユーザ EXEC モード コマンドを使用します。

構文

show spanning-tree bpdu [*interface-id* | **detailed**]

パラメータ

- ***interface-id***：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。
- **detailed**：現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

すべてのインターフェイスの情報を表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

ユーザ EXEC モード

例

次に、スパニング ツリー BPDU 情報を表示する例を示します。

```
switchxxxxxx#  show spanning-tree bpdu

The following is the output if the global BPDU handling command is
not supported.

Interface         Admin Mode        Oper Mode
---------         ----------        ---------
gi1/0/1           Filtering         Filtering
gi1/0/2           Filtering         Filtering
gi1/0/3           Filtering         Guard

The following is the output if both the global BPDU handling command
 and the per-interface BPDU handling command are supported.

Global: Flooding

Interface         Admin Mode        Oper Mode
---------         ----------        ---------
gi1/0/1           Global            Flooding
gi1/0/2           Global            STP
gi1/0/3           Flooding          STP
```

spanning-tree loopback-guard

ループバック BPDU を受信した場合にインターフェイスをシャットダウンするには、**spanning-tree loopback-guard global configuration** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree loopback-guard

no spanning-tree loopback-guard

コマンド モード

グローバル

使用上のガイドライン

これにより、インターフェイスでループバック BPDU を受信した場合に、すべてのインターフェイスをシャットダウンできます。

例

```
switchxxxxxx(config)#  spanning-tree loopback-guard
```

spanning-tree vlan forward-time

VLANのスパニングツリーのブリッジ転送時間を設定するには、グローバル コンフィギュレーション モードで **spanning-tree vlan forward-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree vlan *vlan-range* **forward-time** *seconds*

no spanning-tree vlan *vlan-range* **forward-time**

パラメータ

- ***vlan-range***：設定する VLAN の範囲を指定します。範囲を指定するには、ハイフンを使用します。シリーズを指定するには、カンマを使用します。（範囲：2 ～ 4094）
- ***seconds***：スパニングツリーの転送時間を秒単位で指定します。(範囲：4 ～ 30)

デフォルト設定

デフォルトの転送時間は 15 秒です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

スパニングツリーのブリッジ転送時間は、ポートが転送状態に入るまでのリスニング状態とラーニング状態に留まっている時間です。

転送時間を設定するときは、次の関係を維持する必要があります。

- 2*(Forward-Time - 1) >= Max-Age

指定した VLAN インスタンスの転送時間を設定するには、このコマンドを使用します。設定は、スパニングツリーモードが PVST または Rapid PVST に設定されている場合に有効になります。

例

次に、VLAN 100 のスパニングツリーのブリッジ転送時間を 25 秒に設定する例を示します。

```
switchxxxxxx(config)#  spanning-tree vlan 100 forward-time 25
```

spanning-tree vlan hello-time

VLAN のスパニングツリーのブリッジ hello タイムを設定するには、グローバル コンフィギュレーション モードで **spanning-tree vlan hello-time** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree vlan *vlan-range* **hello-time** *seconds*

no spanning-tree vlan *vlan-range* **hello-time**

パラメータ

- ***vlan-range***：設定する VLAN の範囲を指定します。範囲を指定するには、ハイフンを使用します。シリーズを指定するには、カンマを使用します。（範囲：2 ～ 4094）
- ***seconds***：スパニングツリーの hello タイムを秒単位で指定します。（範囲：1 ～ 10）

デフォルト設定

デフォルトの hello タイムは 2 秒です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

スパニングツリーのブリッジ hello タイムは、連続して送信される 2 つの hello メッセージ間の時間です。

hello タイムを設定するときは、次の関係を維持する必要があります。

Max-Age >= 2*(Hello-Time + 1)

指定した VLAN インスタンスの hello タイムを設定するには、このコマンドを使用します。設定は、スパニングツリーモードが PVST または Rapid PVST に設定されている場合に有効になります。

例

次に、VLAN 100 ～ 101 に対してスパニングツリーのブリッジ hello タイムを 5 秒に設定する例を示します。

```
switchxxxxxx(config)#  spanning-tree vlan 100-101 hello-time 5
```

spanning-tree vlan max-age

VLANのスパニングツリーブリッジの最大有効期間を設定するには、グローバル コンフィギュレーション モードで **spanning-tree vlan max-age** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree vlan *vlan-range* **max-age** *seconds*

no spanning-tree vlan *vlan-range* **max-age**

パラメータ

- ***vlan-range***：設定する VLAN の範囲を指定します。範囲を指定するには、ハイフンを使用します。シリーズを指定するには、カンマを使用します。（範囲：2 ～ 4094）
- ***seconds***：スパニング ツリー ブリッジ最大有効期間を秒単位で指定します。(範囲：6～40)

デフォルト設定

デフォルトの max-age 値は 15 秒です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

最大有効期間を設定するときは、次の関係を維持する必要があります。

2*(Forward-Time - 1) >= Max-Age

Max-Age >= 2*(Hello-Time + 1)

指定した VLAN インスタンスの最大有効期限を設定するには、このコマンドを使用します。設定は、スパニングツリーモードが PVST または Rapid PVST に設定されている場合に有効になります。

例

次に、VLAN 100 に対してスパニングツリーブリッジの最大有効期限を 10 秒に設定する例を示します。

```
switchxxxxxx(config)#  spanning-tree vlan 100 max-age 10
```

spanning-tree vlan priority

VLAN のスパニングツリーの優先順位を設定するには、グローバル コンフィギュレーション モードで **spanning-tree vlan priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree vlan *vlan-range* **priority** *priority*

no spanning-tree vlan *vlan-range* **priority**

パラメータ

- ***vlan-range***：設定する VLAN の範囲を指定します。範囲を指定するには、ハイフンを使用します。シリーズを指定するには、カンマを使用します。（範囲：2 ～ 4094）
- ***priority***：ブリッジ優先順位を指定します。(範囲：0 ～ 61440)

デフォルト設定

デフォルトの優先順位は 32768 に相当します。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

priority 値は 4096 の倍数にする必要があります。

優先順位が最も低いスイッチが、スパニング ツリーのルートです。複数のスイッチが最低優先順位になっている場合は、MACアドレスの最も小さいスイッチがルートとして選択されます。

指定した VLAN インスタンスのブリッジ優先順位を設定するには、このコマンドを使用します。設定は、スパニングツリーモードが PVST または Rapid PVST に設定されている場合に有効になります。

例

次に、スパニングツリーの優先順位を VLAN 100-105 に対して 12288 に設定する例を示します。

```
switchxxxxxx(config)#  spanning-tree vlan 100-105 priority 12288
```

spanning-tree vlan cost

ポートのスパニングツリーのブリッジパスコストを設定するには、インターフェイス（イーサネット、ポートチャネル）コンフィギュレーション モードで **spanning-tree vlan cost** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree vlan *vlan-range* **cost** *cost*

no spanning-tree vlan *vlan-range* **cost**

パラメータ

- ***vlan-range***：設定する VLAN の範囲を指定します。範囲を指定するには、ハイフンを使用します。シリーズを指定するには、カンマを使用します。（範囲：2 ～ 4094）
- ***cost***：ポート パス コストを指定します。(範囲：1 ～ 200000000)

デフォルト設定

デフォルトのパスコストは、ポート速度とパスコスト方式（long または short）によって決まります。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

指定した VLAN インスタンスのポートコストを設定するには、このコマンドを使用します。設定は、スパニングツリーモードが PVST または Rapid PVST に設定されている場合に有効になります。

指定できる VLAN インスタンスは VLAN ID 2 ～ 4094 です。

例

次に、スパニングツリーのコストをポート gi1/0/15 と VLAN 100 で 35000 に設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/15
switchxxxxxx(config-if)#  spanning-tree vlan 100 cost 35000
```

spanning-tree vlan port-priority

VLANのスパニングツリーのポート優先順位を設定するには、インターフェイス（イーサネット、ポートチャネル）コンフィギュレーション モードで **spanning-tree vlan port-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

spanning-tree vlan *vlan-range* **port-priority** *priority*

no spanning-tree vlan *vlan-range* **port-priority**

パラメータ

- ***vlan-range***：設定する VLAN の範囲を指定します。範囲を指定するには、ハイフンを使用します。シリーズを指定するには、カンマを使用します。（範囲：2 ～ 4094）
- ***priority***：ポートの優先順位を指定します。(範囲：0 ～ 240)

デフォルト設定

デフォルトのポートの優先順位は 128 です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

priority 値は 16 の倍数にする必要があります。

指定したVLANインスタンスのポート優先順位を設定するには、このコマンドを使用します。設定は、スパニングツリーモードが PVST または Rapid PVST に設定されている場合に有効になります。

例

次に、VLAN 100 ー 102 の gi1/0/15 のスパニング優先順位を 16 に設定する例を示します。

```
switchxxxxxx(config)#  interface gi1/0/15-16
switchxxxxxx(config-if)#  spanning-tree vlan 100-102 port-priority 96
```

SSH クライアント コマンド

この章は、次の項で構成されています。

- ip ssh-client authentication （1358 ページ）
- ip ssh-client change server password （1359 ページ）
- ip ssh-client key （1360 ページ）
- ip ssh-client password （1363 ページ）
- ip ssh-client server authentication （1364 ページ）
- ip ssh-client server fingerprint （1365 ページ）
- ip ssh-client source-interface （1367 ページ）
- ipv6 ssh-client source-interface （1368 ページ）
- ip ssh-client username （1369 ページ）
- show ip ssh-client （1370 ページ）
- show ip ssh-client server （1372 ページ）

ip ssh-client authentication

リモート SSH サーバによる認証のためにローカル SSH クライアントで使用される SSH クライアント認証方式を定義するには、グローバル コンフィギュレーション モードで **ip ssh-client authentication** コマンドを使用します。

デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

ip ssh-client authentication {**password** | **public-key** {**rsa** | **dsa**}}

no ip ssh-client authentication

パラメータ

- **password**：認証にユーザ名とパスワードを使用します。
- **public-key rsa**：認証にユーザ名と RSA 公開キーを使用します。
- **public-key dsa**：認証にユーザ名と DSA 公開キーを使用します。

デフォルト設定

ローカル SSH クライアントは、認証にユーザ名とパスワードを使用します。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

SSH 認証が公開キーによって行われる場合、ユーザは **ip ssh-client key** コマンドを使用して RSA/DSA キーを生成/設定できます。そうしない場合、スイッチによって生成されたデフォルトのキーが使用されます。

例

次の例では、認証にユーザ名と公開キーを使用することを指定しています。

```
switchxxxxxx(config)# ip ssh-client authentication public-key rsa
```

ip ssh-client change server password

リモート SSH サーバで SSH クライアントのパスワードを変更するには、グローバル コンフィギュレーション モードで **ip ssh-client change server password** コマンドを使用します。

構文

ip ssh-client change server password server {*host* | *ip-address* | *ipv6-address*} **username** *username* **old-password** *old-password* **new-password** *new-password*

パラメータ

- ***host***：リモート SSH サーバの DNS 名。
- ***ip-address***：リモート SSH サーバの IP アドレスを指定します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。「IPv6z アドレスの表記法」を参照してください。
- ***username***：ローカル SSH クライアントのユーザ名（1 ～ 70 文字）。
- ***old-password***：ローカル SSH クライアントの古いパスワード（1 ～ 70 文字）。
- ***new-password***：ローカル SSH クライアントの新しいパスワード（1 ～ 70 文字）。パスワードに文字「@」と「:」を含めることはできません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、リモート SSH サーバでパスワードを変更する場合に使用します。**ip ssh-client password** コマンドは、スイッチの SSH クライアントの SSH クライアント パスワードを、リモート SSH サーバに設定された新しいパスワードに一致するように変更する場合に使用します。

例

次の例では、ローカル SSH クライアントのパスワードを変更しています。

```
switchxxxxxx(config)# ip ssh-client change server password server 10.7.50.155 username
john old-password &&&@@@aaff new-password &&&@@@aaee
```

ip ssh-client key

公開キーによる SSH クライアント認証のキー ペアを（キーを生成するか、キーをインポートすることで）作成するには、グローバル コンフィギュレーション モードで **ip ssh-client key** コマンドを使用します。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。

構文

ip ssh-client key {**dsa** | **rsa**} {**generate | key-pair** *privkey pubkey***}**

encrypted ip ssh-client key {**dsa** | **rsa**} **key-pair** *encrypted-privkey pubkey*

no ip ssh-client key [**dsa** | **rsa**]

パラメータ

- **dsa**：DSA キー タイプ。
- **rsa**：RSA キー タイプ。
- **key-pair**：デバイスにインポートされるキー。

  privkey：プレーン テキストの秘密キー。

  encrypted-privkey：プライベートキーは暗号化形式です。

  pubkey：プレーン テキストの公開キー。

デフォルト設定

アプリケーションは、キーを自動的に作成します。これがデフォルトのキーになります。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

キーワード **generate** を使用すると、指定したタイプ（RSA/DSA）の秘密キーと公開キーが SSH クライアント用に生成されます。キー生成コマンドでコンフィギュレーション ファイルをダウンロードすることはできません。このようなダウンロードは失敗します。

キーワード **key-pair** を使用すると、ユーザは別のデバイスによって作成されたキー ペアをインポートできます。この場合、キーは RFC 4716 で指定されている形式に従う必要があります。

指定したキーがすでに存在する場合は、既存のキーを新しいキーに置き換える前に、警告が発行されます。

キー ペアを削除するには、**no ip ssh-client key** コマンドを使用します。両方のキー ペアを削除する場合は、このコマンドにキー タイプを指定しないでください。

表 *4:* キー、デフォルトおよびユーザ

送信元/先	表示	表示（詳細）	実行コンフィギュレーションのコピー/アップロード	スタートアップコンフィギュレーションのコピー/アップロード	テキダウバッ
スタートアップコンフィギュレーション	ユーザ定義のみ	該当なし	すべてのキー（デフォルトとユーザ）	該当なし	すべルト
ランニング コンフィギュレーション	キーは表示されません。	すべてのキー（デフォルトとユーザ）	該当なし	ユーザ定義のみ。	ユー
テキストベースの CLI（TFTP/バックアップ）	そのままコピーされました。	該当なし	すべてのキー（デフォルトとユーザ）	ユーザ定義のみ。	テキて。

テキストベースのコンフィギュレーション ファイルにキーが含まれていない場合、デバイスは初期化時に自身のキーを生成します。実行コンフィギュレーションに（ユーザ定義ではなく）デフォルトのキーが含まれている場合、同じデフォルトのキーのままになります。

例 1：次の例では、RSA タイプのキー ペアを作成しています。

```
switchxxxxxx(config)# ip ssh-client key rsa generate
The SSH service is generating a private RSA key.
This may take a few minutes, depending on the key size.
```

例 2：次の例では、RSA タイプの公開キーと秘密キーの両方をインポートしています（秘密キーはプレーン テキストとして）。

```
switchxxxxxx(config)# ip ssh-client key rsa key-pair
Please paste the input now, add a period (.) on a separate line after the input
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDH6CU/2KYRl8rYrK5+TIvwS4zvhBmiC4I31m9cR/1iRTFViMRuJ++TEr
p9ssqWyI1Ti9d0jzmG0N3jHzp2je5/DUTHZXvYaUzchBDnsPTJo8dyiBl4YBqYHQgCjUhk
tXqvloy+1uxRJTAaLVXCBAmuIU/kMLoEox8/zwjB/jsF9wIBIwKBgC2xZ5mQmvy0+yo2GU
FwlQO5f0yweuM11J8McTmqDgfVTRrdbroXwbs3exVqsfaUPY9wa8Le6JPX+DPp4XovEfC/
iglZBSC8SeDmI2U7D6HrkAyD9HHf/r32jukB+5Z7BlHPz2Xczs2clOOwrnToy+YTzjLUxy
WS7V/IxbBllipLAkEA/QluVSCfFmdMlZxaEfJVzqPO1cF8guovsWLteBf/gqHuvbHuNy0t
OWEpObKZs1m/mtCWppkgcqgrB0oJaYbUFQJBAMo/cCrkyhsiV/+ZsryeD26NbPEKiak16V
Tz2ayDstidGuuvcvm2YF7DjM6n6NYz3+/ZLyc5n82okbld1NhDONsCQQCmSAas+C4HaHQn
zSU+/lWlDI88As4qJN2DMmGJbtsbVHhQxWIHAG4tBVWa8bV12+RPyuan/jnk8irniGyVza
FPAkEAiq8oV+1XYxA8V39V/a42d7FvRjMckUmKDl4Rmt32+u9i6sFzaWcdgs87+2vS3AZQ
afQDE5U6YSMiGLVewC4YWwJBAOFZmhO+dIlxT8Irzf2cUZGggopfnX6Y+L+Yl09MuZHbwH
tXaBGj6ayMYvXnloONecnApBjGEm37YVwKjO2DV2w=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMfoJT/YphGXytisrn5Mi/BLjO+EGaILgjfWb1xH/WJFMVWIxG4n75MSun2yyp
bIjVOL13SPOYbQ3eMfOnaN7n8NRMdle9hpTNyEEOew9Mmjx3KIGXhgGpgdCAKNSGS1eq+W
jL7W7FElMBotVcIECa4hT+QwugSjHz/PCMH+OwX3AgEj
-----END RSA PUBLIC KEY-----
```

例 3：次の例では、DSA タイプの公開キーと秘密キーの両方をインポートしています（秘密キーは暗号化されます）。

```
switchxxxxxx(config)# encrypted ip ssh-client key rsa key-pair
(Need to encrypted SSH client RSA key pair, for example:)
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
gxeOjs6OzGRtL4qstmQg1B/4gexQblfa56RdjgHAMejvUT02elYmNi+m4aTu6mlyXPHmYP
lXlXny7jZkHRvgg8EzcppEB0O3yQzq3kNi756cMg4Oqbkm7TUOtdqYFEz/h8rJJ0QvUFfh
BsEQ3e16E/OPitWgK43WTzedsuyFeOoMXR9BCuxPUJc2UeqQVM2IJt5OM0FbVt0S6oqXhG
sEEdoTlhlDwHWg97FcV7x+bEnPfzFGrmbrUxcxOxlkFsuCNo3/94PHK8zEXyWtrx2KoCDQ
qFRuM8uecpjmDh6MO2GURUVstctohEWEIVCIOr5SBCbciaxv5oS0jIzXMrJA==
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBALLOeh3css8tBL8ujFt3trcX0XJyJLlxxt4sGp8Q3ExlSRN25+Mcac6togpIEg
tIzk6t1IEJscuAih9Brwh1ovgMLRaMe25j5YjO4xG6Fp42nhHiRcie+YTS1o309EdZkiXa
QeJtLdnYL/r3uTIRVGbXI5nxwtfWpwEgxxDwfqzHAgEj
-----END RSA PUBLIC KEY-----
```

例 4：次の例では、DSA キー ペアを削除しています。

```
switchxxxxxx(config)# no ip ssh-client key dsa
```

例 5：次の例では、すべてのキー ペア（RSA タイプと DSA タイプ）を削除しています。

```
switchxxxxxx(config)# no ip ssh-client key
```

ip ssh-client password

パスワードによるSSHクライアント認証用にパスワードを設定するには、グローバル コンフィギュレーション モードで **ip ssh-client password** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

ip ssh-client password *string*

encrypted ip ssh-client password *encrypted-string*

no ip ssh-client password

パラメータ

- ***string***：SSH クライアントのパスワード（1 ～ 70 文字）。パスワードに文字「@」と「:」を含めることはできません。
- ***encrypted-string***：暗号化形式の SSH クライアントのパスワード。

デフォルト設定

デフォルトのパスワードは anonymous です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

パスワードを使用するように認証を設定している場合は（コマンド **ip ssh-client authentication** を使用）、**ip ssh-client password** コマンドを使用してパスワードを定義します。

encrypted キーワードを使用している場合、パスワードは暗号化形式である必要があります。

リモート SSH サーバ上のパスワードを、SSH クライアントの新しいパスワードに一致するように変更するには、コマンド **ip ssh-client change server password** を使用します。

例

次の例では、ローカル SSH クライアントに対してプレーン テキストのパスワードを指定しています。

```
switchxxxxxx(config)# ip ssh-client password &&&111aaff
```

ip ssh-client server authentication

SSHクライアントによるリモートSSHサーバ認証を有効にするには、グローバル コンフィギュレーション モードで **ip ssh-client server authentication** コマンドを使用します。

リモート SSH サーバ認証を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip ssh-client server authentication

no ip ssh-client server authentication

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

SSH サーバ認証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

リモート SSH サーバ認証が無効になっている場合、いずれのリモート SSH サーバも受け入れられます（これは、SSH の信頼できるリモート サーバ テーブルにリモート SSH サーバのエントリがない場合でも同じです）。

リモート SSH サーバ認証が有効になっている場合は、信頼できる SSH サーバのみが受け入れられます。**ip ssh-client server fingerprint** コマンドは、信頼できる SSH サーバを設定する場合に使用します。

例

次の例では、SSH サーバ認証を有効にしています。

```
switchxxxxxx(config)# ip ssh-client server authentication
```

ip ssh-client server fingerprint

信頼できるリモート SSH サーバ テーブルに信頼できるサーバを追加するには、グローバル コンフィギュレーション モードで **ip ssh-client server fingerprint** コマンドを使用します。信頼できるリモート SSH サーバ テーブルから 1 つのエントリまたはすべてのエントリを削除するには、このコマンドの **no** 形式を使用します。

構文

ip ssh-client server fingerprint {*host* | *ip-address*} *fingerprint*

no ip ssh-client server fingerprint [*host* | *ip-address*]

パラメータ

- ***host***：SSH サーバの DNS 名。
- ***ip-address***：SSH サーバのアドレスを指定します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。「IPv6z アドレスの表記法」を参照してください。
- ***fingerprint***：SSH サーバ公開キーのフィンガー プリント（32 個の 16 進数文字）。

デフォルト設定

信頼できるリモート SSH サーバ テーブルが空です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

フィンガープリントを作成するには、公開キーに暗号学的ハッシュ関数を適用します。フィンガープリントは、参照先のキーよりも短いため簡単に使用できます（元のキーよりも手動で入力するのが容易です）。スイッチは、SSH サーバの公開キーを認証する必要があるたびに、受信したキーのフィンガープリントを計算して、以前に設定されたフィンガープリントと比較します。

フィンガープリントは、SSH サーバから取得できます（フィンガープリントは、SSH サーバで公開キーが生成されるときに計算されます）。

no ip ssh-client server fingerprint コマンドは、信頼できるリモート SSH サーバ テーブルからすべてのエントリを削除します。

例

次の例では、信頼できるサーバを信頼できるサーバ テーブルに追加しています（区切り記号 ":" あり/なし）。

```
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1
DC789788DC88A988127897BCBB789788
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1
DC:78:97:88:DC:88:A9:88:12:78:97:BC:BB:78:97:88
```

ip ssh-client source-interface

IPv4 SSH サーバと通信するために IPv4 アドレスを送信元 IPv4 アドレスとして使用する送信元インターフェイスを指定するには、**ip ssh-client source-interface** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ip ssh-client source-interface *interface-id*

no ip ssh-client **source-interface**

パラメータ

- ***interface-id***：送信元インターフェイスを指定します。

デフォルト設定

送信元 IPv4 アドレスは、発信インターフェイスで定義され、ネクスト ホップ IPv4 サブネットに属する IPv4 アドレスです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスである場合、ネクストホップの IPv4 サブネットに属しているインターフェイスの IP アドレスが適用されます。

送信元インターフェイスが発信インターフェイスでない場合、送信元インターフェイスで定義されている最小の IPv4 アドレスが適用されます。

使用可能な IPv4 送信元アドレスがない場合は、IPv4 SSH サーバとの通信を試行する際に SYSLOG メッセージが発行されます。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# ip ssh-client source-interface vlan 100
```

ipv6 ssh-client source-interface

IPv6 SSH サーバと通信するために IPv6 アドレスを送信元 IPv6 アドレスとして使用する送信元インターフェイスを指定するには、**ipv6 ssh-client source-interface** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ipv6 ssh-client source-interface *interface-id*

no ipv6 ssh-client **source-interface**

パラメータ

- ***interface-id***：（オプション）送信元インターフェイスを指定します。

デフォルト設定

IPv6 送信元アドレスは、発信インターフェイスに定義され、RFC6724 に従って選択される IPv6 アドレスです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスである場合、インターフェイスで定義され、RFC 6724 に準拠して選択された IPv6 アドレス。

送信元インターフェイスが発信インターフェイスでない場合、送信元インターフェイスで定義されている、宛先 IPv6 アドレスの範囲で最小の IPv4 アドレスが適用されます。

使用可能な IPv6 送信元アドレスがない場合は、IPv6 SSH サーバとの通信を試行する際に SYSLOG メッセージが発行されます。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# ipv6 ssh-client source-interface vlan 100
```

ip ssh-client username

スイッチの SSH クライアント ユーザ名を設定するには、グローバル コンフィギュレーション モードで **ip ssh-client username** コマンドを使用します。

デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

ip ssh-client username *string*

no ip ssh-client username

パラメータ

- ***string***：SSH クライアントのユーザ名。長さは 1 ～ 70 文字です。ユーザ名には、「@」と「:」の文字は使用できません。

デフォルト設定

デフォルトのユーザ名は anonymous です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

設定したユーザ名は、SSH クライアント認証がパスワードとキーの両方またはいずれか一方で行われるときに使用されます。

例

次の例では、SSH クライアントのユーザ名を指定しています。

switchxxxxxx(config)# **ip ssh-client username jeff**

show ip ssh-client

SSHクライアントのクレデンシャル（デフォルトのキーとユーザ定義のキーの両方）を表示するには、特権 EXEC モードで **show ip ssh-client** コマンドを使用します。

構文

show ip ssh-client

show ip ssh-client {mypubkey | key} {dsa | rsa}

パラメータ

- **dsa**：DSA キー タイプを表示することを指定します。
- **rsa**：RSA キー タイプを表示することを指定します。
- **mypubkey**：公開キーのみを表示することを指定します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、特定のキー タイプを指定して SSH クライアント キーを表示する場合に使用します。公開キーと秘密キーのどちらか一方を表示したり、noパラメータを指定して秘密キーと公開キーの両方を表示したりできます。キーは、RFC 4716 で指定されている形式で表示されます。

例 1。次に、認証方式および RSA 公開キーを表示する例を示します。

```
switchxxxxxx# show ip ssh-client mypubkey rsa
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:   DSA key
Username:                john
Key Source:              User Defined
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAudGEIaPARsKoVJVjs8XALAKqBN1WmXnY
kUf5oZjGY3QoMGDvNipQvdN3YmwLUBiKk31WvVwFB3N2K5a7fUBjoblkdjns
QKTKZiu4V+IL5rds/bD6LOEkJbjUzOjmp9hlIkh9uc0ceZ3ZxMtKhnORLrXL
aRyxYszO5FuirTo6xW8=
---- END SSH2 PUBLIC KEY ----
Public Key Fingerprint: 84:f8:24:db:74:9c:2d:51:06:0a:61:ef:82:13:88:88
```

例 2。次に、認証方式および暗号化形式の DSA 秘密キーを表示する例を示します。

```
switchxxxxxx# show ip ssh-client key DSA
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:   DSA key
Username:                john
Key Source:              User Defined
```

```
Public Key Fingerprint: 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
---- BEGIN SSH2 PRIVATE KEY ----
Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PRIVATE KEY ----
```

例 3。次に、SSH クライアント認証方式、ユーザ名、およびパスワードを表示する例を示します。

```
switchxxxxxx# show ip ssh-client
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:   DSA key
Username:                anonymous (default)
Password:                anonymous (default)
password(Encrypted):     KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5nsxSxwic=
```

show ip ssh-client server

SSH リモート サーバ認証方式および信頼できるリモート SSH サーバ テーブルを表示するには、特権 EXEC コンフィギュレーション モードで **show ip ssh-client server** コマンドを使用します。

構文

show ip ssh-client server [*host* | *ip-address*]

パラメータ

- ***host***：（オプション）SSH サーバの DNS 名。
- ***ip-address***：（オプション）SSH サーバの IP アドレス。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。「IPv6z アドレスの表記法」を参照してください。

デフォルト設定

なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

特定の SSH サーバを指定すると、その SSH サーバのフィンガープリントのみが表示されます。それ以外の場合は、既知のすべてのサーバが表示されます。

例 1：次の例では、SSH リモート サーバ認証方式およびすべての信頼できるリモート SSH サーバを表示しています。

```
switchxxxxxx# show ip ssh-client server
SSH Server Authentication is enabled
server address: 11.1.0.1
  Server Key Fingerprint: 5a:8d:1d:b5:37:a4:16:46:23:59:eb:44:13:b9:33:e9
server address: 192.165.204.111
  Server Key Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
server address: 4002:0011::12
  Server Key Fingerprint: a5:34:44:44:27:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

例 2：次に、認証方式および暗号化形式の DSA 秘密キーを表示する例を示します。

```
switchxxxxxx# show ip ssh-client key DSA
Authentication method:   DSA key
Username:                john
Key Source:              Default
Public Key Fingerprint: 77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
```

```
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
---- BEGIN SSH2 PRIVATE KEY ----
Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PRIVATE KEY ----
```

例 3：次に、SSH クライアント認証方式、ユーザ名、およびパスワードを表示する例を示します。

```
switchxxxxxx# show ip ssh-client
Authentication method: password (default)
Username: anonymous (default)
password(Encrypted): KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5
```

SSD コマンド

この章は、次の項で構成されています。

- ssd config （1376 ページ）
- passphrase （1377 ページ）
- ssd rule （1378 ページ）
- show SSD （1380 ページ）
- ssd session read （1382 ページ）
- show ssd session （1383 ページ）
- ssd file passphrase control （1384 ページ）
- ssd file integrity control （1386 ページ）

ssd config

セキュア センシティブ データ（SSD）コマンド モードを開始するには、グローバル コンフィギュレーション モードで **ssd config** を使用します。このコマンド モードでは、管理者はデバイス上のセンシティブ データ（キーやパスワードなど）をどのように保護するかを設定できます。

構文

ssd config

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

十分な権限を持つユーザのみが、このコマンドを使用して、SSD設定を編集および表示できます。これらの権限の説明については、ssd rule （1378 ページ） を参照してください。

例

```
switchxxxxxx(config)# ssd config
switchxxxxxx(config-ssd)#
```

passphrase

システムのパスフレーズを変更するには、SSD コンフィギュレーション モードで **passphrase** を使用します。デバイスは、パスフレーズから生成されたキーを使用して自身のセンシティブデータを暗号化して保護します。

パスフレーズをデフォルトのパスフレーズにリセットするには、**no passphrase** を使用します。

構文

passphrase *{passphrase}*

encrypted passphrase *{encrypted-passphrase}*

no passphrase

パラメータ

- **passphrase**：新しいシステム パスフレーズ。
- **encrypted-passphrase**：その暗号化形式のパスフレーズ。

デフォルトの使用

このコマンドを入力しない場合は、デフォルトのパスフレーズが使用されます。

コマンド モード

SSD コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用するには、passphrase と Enter を入力します。確認メッセージが表示され、ユーザはパスフレーズを変更する意思を確認する必要があります。その後、パスフレーズを入力することができます（例を参照）。

パスフレーズの暗号化は、スタートアップ コンフィギュレーション ファイルにコピーされるソース ファイルの SSD 制御ブロックでのみ許可されます（ユーザがこのコマンドを手動で入力することはできません）。

パスフレーズを生成する場合、ユーザは4種類の文字クラスを使用する必要があります（強力なパスワード/パスワードの複雑さに似ています）。標準のキーボードから入力できる大文字、小文字、数値、および特殊文字を使用できます。

例

次の例では、パスフレーズの復号化を定義しています。

```
switchxxxxxx(config-ssd)# passphrase
This operation will change the system SSD passphrase. Are you sure? (Y/N)[N] Y
Please enter SSD passphrase:**********
Please reenter SSD passphrase:**********
```

ssd rule

SSD ルールを設定するには、SSD コンフィギュレーション モードで **ssd rule** を使用します。デバイスは、SSD ルールに基づいてユーザにセンシティブ データの読み取りアクセス許可を付与します。**Both** または **Plaintext** 読み取りアクセス許可を付与されているユーザは、SSD コンフィギュレーション モードを開始する権限も付与されます。

ユーザ定義のルールを削除し、デフォルトのルールに戻すには、**no ssd rule** を使用します。

構文

[encrypted] SSD rule {***all*** **|** *level-15* **|** *default-user* **|** *user user-name*}

{***secure*** **|** *insecure* | ***secure-xml-snmp*** **|** *insecure-xml-snmp}*

permission {***encrypted-only*** **| plaintext-only | both |** *exclude*}

default*-read* **{***encrypted* | ***plaintext*** **|** *exclude*}

no ssd rule [{***all*** **|** *level-15* **|** *default-user* **|** *user user-name*}

{***secure*** **|** *insecure* | ***secure-xml-snmp*** **|** *insecure-xml-snmp*}]

コマンド モード

SSD コンフィギュレーション モード。

デフォルト ルール

デバイスには、次のような工場出荷時のデフォルト ルールがあります。

表 *5:* デフォルトの *SSD* ルール

ルール キー		規則アクション	
ユーザ	チャネル	読み取り権限	デフォルト読み取りモード
level-15	secure-xml-snmp	Plaintext Only	Plaintext
level-15	secure	Both	Encrypted
level-15	insecure	Both	Encrypted
all	insecure-xml-snmp	Exclude	Exclude
all	secure	Encrypted Only	Encrypted
all	insecure	Encrypted Only	Encrypted

使用上のガイドライン

ユーザ定義のルールを削除したり、変更したデフォルト ルールをデフォルトに戻したりするには、**no ssd rule** を使用します。

すべての SSD ルールを削除し、デフォルトの SSD ルールに戻すには、**no ssd rule**（パラメータなし）を使用します。確認メッセージが表示され、これを行うための権限が求められます。特定のルールを削除するには（対象となるのはユーザ定義のルール）、パラメータを使用してチャネルのユーザおよびセキュリティを指定します。

encrypted SSD rule は、安全な方法によりデバイス間で SSD ルールをコピーするために使用します。

デフォルトの SSD ルールは、変更することはできますが削除することはできません。次に、SSD ルールが適用される順序を示します。

- 指定した *users* に対する SSD ルール。
- **default-user**（**cisco**）に対する SSD ルール。
- **level-15** ユーザの SSD ルール。
- **all** に対する残りの SSD ルール。

ユーザは、コマンドを任意の順序で入力できます。順序付けは、デバイスによって暗黙的に行われます。

例 1：次の例では、ルールを変更しています。

```
switchxxxxxx(config-ssd)# ssd rule level-15 secure permission encrypted-only default-read
 encrypted
```

例 2：次の例では、ルールを追加しています。

```
switchxxxxxx(config-ssd)# ssd rule user james secure permission both default-read encrypted
```

例 3：次の例では、ルールを暗号化形式として追加しています。

```
switchxxxxxx(config-ssd)# encrypted ssd rule iurwe874jho32iu9ufjo32i83232fdefsd
```

例 4：次の例では、デフォルト ルールを削除しています。

```
switchxxxxxx(config-ssd)# no ssd rule all secure
```

例 5：次の例では、ユーザ定義のルールを削除しています。

```
switchxxxxxx(config-ssd)# no ssd rule user james secure
```

例 6：次の例では、すべてのルールを削除しています。

```
switchxxxxxx(config-ssd)# no ssd rule
This operation will delete all user-defined rules and retrieve the default rules instead.
Are you sure (Y/N): N
```

show SSD

現在のSSDのルールを表示するには（ルールはプレーンテキストとして表示されます）、SSDコンフィギュレーション モードで **show ssd rules** を使用します。

構文

show SSD [***rules*** | ***brief***]

パラメータ

- **rules**：（オプション）SSD ルールのみを表示します。
- **brief**：（オプション）暗号化パスフレーズ、ファイル パスフレーズ制御、およびファイル整合性の属性を表示します。

コマンド モード

SSD コンフィギュレーション モード

デフォルト設定

すべての SSD 情報を表示します。

例 1：次の例では、すべての SSD 情報を表示しています。

```
switchxxxxxx(config-ssd)# show ssd
SSD current parameters:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
SSD parameters after reset:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
 User Type   User Name      Channel      Read Permission Default Read    Type
------------ --------- ----------------- --------------- ------------ -----------
  Specific    admin11       secure            Both        Encrypted   User-Define
  Specific    admin2        secure       Encrypted-Only   Encrypted   User-Define
  Level-15              secure-xml-snmp  Plaintext-Only   Plaintext     Default
  Level-15                  secure            Both        Encrypted     Default
  Level-15                 insecure           Both        Encrypted     Default
    All                     secure       Encrypted-Only   Encrypted     Default
    All                    insecure      Encrypted-Only   Encrypted     Default
    All                insecure-xml-snmp Plaintext-Only   Plaintext    *Default
* Modified default entry
```

例 2：次の例では、SSD ルールを表示しています。

```
switchxxxxxx(config-ssd)# show ssd rules
 User Type   User Name      Channel      Read Permission Default Read    Type
------------ --------- ----------------- --------------- ------------ -----------
  Specific    admin11       secure            Both        Encrypted   User-Define
  Specific    admin2        secure       Encrypted-Only   Encrypted   User-Define
  Level-15              secure-xml-snmp  Plaintext-Only   Plaintext     Default
```

```
  Level-15                  secure            Both        Encrypted     Default
  Level-15                insecure            Both        Encrypted     Default
    All                     secure       Encrypted-Only   Encrypted     Default
    All                   insecure       Encrypted-Only   Encrypted     Default
    All               insecure-xml-snmp Plaintext-Only    Plaintext    *Default
* Modified default entry
```

例 3：次の例では、SSD 属性を表示しています。

```
switchxxxxxx(config-ssd)# show ssd brief
SSD current parameters:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
SSD parameters after reset:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
```

ssd session read

現在のセッションにおける SSD 読み取りの現在のデフォルトをオーバーライドするには、グローバル コンフィギュレーション モードで **ssd session read** を使用します。

構文

ssd session read {***encrypted*** | ***plaintext*** | ***exclude***}

no **ssd session** read

パラメータ

- **encrypted**：SSD のデフォルトのオプションを encrypted にオーバーライドします。
- **plaintext**：SSD のデフォルトのオプションを plaintext にオーバーライドします。
- **exclude**：SSD のデフォルトのオプションを exclude にオーバーライドします。

コマンド モード

グローバル コンフィギュレーション モード。

デフォルト

このコマンド自体にデフォルトはありません。ただし、セッション自体の読み取りモードは、デフォルトではデバイスがセッションのユーザに SSD 権限を付与するために使用する SSD ルールのデフォルトの読み取りモードに設定されます。

使用上のガイドライン

SSD ルールの読み取りオプションをデフォルトに戻すには、**no ssd session read** を使用します。この設定が許可されるのは、現在のセッションのユーザが十分な読み取りアクセス許可を持っている場合のみです。それ以外の場合、コマンドは失敗し、エラーが表示されます。設定は、ただちに有効になり、ユーザが設定を元に戻すかセッションを終了すると終了します。

例

```
switchxxxxxx(config)# ssd session read plaintext
```

show ssd session

現在のセッションのユーザに対する SSD 読み取りアクセス許可およびデフォルトの読み取りモードを表示するには、特権 EXEC モードで **show ssd session** を使用します。

構文

show ssd session

コマンド モード

特権 EXEC モード

デフォルト

なし

例

```
switchxxxxxx# show ssd session
User Name/Level: James / Level 15
User Read Permission:  Both
Current Session Read mode: Plaintext
```

ssd file passphrase control

コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルにコピーするときに保護のレベルを高めるには、SSD コンフィギュレーション モードで **ssd file passphrase control** を使用します。コンフィギュレーション ファイル内のパスフレーズは、常にデフォルトのパスフレーズ キーで暗号化されます。

構文

ssd file passphrase control {***restricted*** | ***unrestricted***}

no ssd file passphrase control

パラメータ

- **Restricted**：このモードでは、デバイスは自身のパスフレーズがコンフィギュレーション ファイルにエクスポートされるのを制限します。制限モードは、パスフレーズがないデバイスからコンフィギュレーション ファイル内の暗号化されたセンシティブ データを保護します。このモードは、ユーザがコンフィギュレーション ファイルにパスフレーズを公開しないようにする場合に使用します。
- **Unrestricted**：このモードでは、デバイスはコンフィギュレーション ファイルを作成するときに自身のパスフレーズを含めます。これにより、コンフィギュレーション ファイルを受け入れるすべてのデバイスがそのファイルからパスフレーズを学習できます。

デフォルト

デフォルトは **unrestricted** です。

コマンド モード

SSD コンフィギュレーション モード。

使用上のガイドライン

デフォルトの状態に戻すには、**no ssd file passphrase control** コマンドを使用します。

デバイスを工場出荷時の設定にリセットすると、そのローカル パスフレーズがデフォルトのパスフレーズに設定されることに注意してください。そのため、このままではデバイスは自身のコンフィギュレーション ファイルにあるユーザ定義のパスフレーズ キーで暗号化されたセンシティブ データを復号化できません。これを行うには、ユーザ パスフレーズで再度デバイスを手動で設定するか、コンフィギュレーション ファイルを無制限モードで作成します。

無制限モードのユーザ定義のパスフレーズを設定する場合は、SSD ファイル整合性制御を有効にすることを強く推奨します。SSD ファイル整合性制御を有効にすると、コンフィギュレーション ファイルを改ざんから保護できます。

例

```
console(ssd-config)# ssd file passphrase control restricted
console(ssd-config)# no ssd file passphrase control
```

ssd file integrity control

暗号化されたセンシティブ データが含まれている新規生成のコンフィギュレーション ファイルを改ざんから保護するようにデバイスに指示するには、SSD コンフィギュレーション モードで **ssd file integrity control** コマンドを使用します。

Integrity Control を無効にするには、**no ssd file integrity control** を使用します。

構文

ssd file integrity control ***enabled***

no ssd file integrity control

パラメータ

- **enabled**：ファイル整合性制御を有効にして、新規生成のコンフィギュレーション ファイルを改ざんから保護します。

デフォルト

デフォルトのファイル入力制御は**無効**になっています。

コマンド モード

SSD コンフィギュレーション モード。

使用上のガイドライン

TAユーザは、ファイル整合性制御を有効にしたファイルを作成することで、コンフィギュレーション ファイルを改ざんから保護できます。ファイル パスフレーズ制御を無制限にしたユーザ定義のパスフレーズをデバイスで使用する場合には、ファイル整合性制御を有効にすることを推奨します。

デバイスは、コンフィギュレーションファイルでファイル整合性制御コマンドを調べて、コンフィギュレーションファイルの整合性が保護されているかどうかを判別します。ファイルの整合性を保護するようになっているのに、ファイルの整合性が維持されていないことをデバイスが検出した場合、デバイスはファイルを拒否します。そうでない場合、ファイルは受け入れられて、さらに処理が加えられることになります。

例

```
switchxxxxxx(config-ssd)#  ssd file integrity control enabled
```

File Integrityが有効である場合、コンフィギュレーション ファイル全体の末尾に内部のダイジェストコマンドを追加します。これは、スタートアップ コンフィギュレーションにコンフィギュレーション ファイルをダウンロードする場合に使用します。

```
config-file-digest 0AC78001122334400AC780011223344
```

スタック コマンド

この章は、次の項で構成されています。

- set stack unit-type （1388 ページ）
- stack unit （1390 ページ）
- stack configuration （1391 ページ）
- show stack configuration （1392 ページ）
- show stack （1393 ページ）
- show stack links （1394 ページ）

set stack unit-type

スタックメンバーのユニットタイプを設定するには、**set stack unit-type** 特権 EXEC モードコマンドを使用します。

set stack unit-type unit *unit-id* **network** *network-type* **uplink** *uplink-type*

パラメータ

- **unit** unit-id：設定を適用するユニット ID を定義します。（範囲：1 ～ **4**）
- **network** network-type：ユニットのネットワークポートのタイプ。次の値をサポートしています。
  - gi（すべてのネットワークポートタイプが Gigabitethernet であるデバイス用）
  - tw（すべてのネットワークポートタイプが TwoPointFiveGigabitEthernet であるデバイスの場合）。
  - te（すべてのネットワークポートタイプが Tengigabitethernet であるデバイスの場合）。
- **uplink** *uplink-type*：ユニットのアップリンクポートのタイプ。次の値をサポートしています。
  - te（Tengigabitethernet アップリンクポートを備えたデバイスの場合）
  - none（アップリンクポートのないデバイスの場合）

デフォルト設定

ユーザ定義タイプが設定されていません

コマンド モード

特権 EXEC モード

使用上のガイドライン

「存在しない」スタックユニットのタイプを定義するには、**set stack unit-type** コマンドを使用します（以下を参照）。スタック内のユニットのタイプは、このユニットのインターフェイス命名のタイプを定義し、適用できるインターフェイスレベルのコマンドを決定します。

ユニットが存在するか、またはスタックに挿入されている場合、ユニットタイプは識別されたユニットのタイプにソフトウェアによって自動的に設定されます。存在していたユニットがその後スタックから削除されると、ユニットは「not-present」になりますが、既存のユニットタイプは保持されます。ユニットが「not-present」で、以前に識別されたタイプがない（ユニットが以前スタックに存在していなかった）場合、そのユニットタイプは自動的にアクティブユニットと同じユニットタイプに設定されます。

- **network** ポートタイプが te に設定されている場合は、**uplink** ポートタイプを none に設定する必要があります。
- **network** ポートタイプが gi または tw に設定されている場合、**uplink** ポートタイプは te に設定する必要があります。
- コマンドがスタック内に存在するユニットに適用されると、そのコマンドは「Unit ID X is present in stack - cannot manually set unit type」というエラーメッセージで失敗します。
- 各ユニットのユニットタイプは、リブート後にも保存され、設定ファイルヘッダーの一部として「**unit-type unit** X **network** *network-type* **uplink** *uplink-type*」の形式で表示されます。

例 1：次に、ユニット 3 のユニットタイプを設定する例を示します。

```
switchxxxxxx# set stack unit-type unit 3 network gi uplink te
```

stack unit

指定したスタック ユニットまたはすべてのスタック ユニットのコンテキストにユーザを配置するには、**stack unit** グローバル コンフィギュレーション コマンドを使用します。

構文

stack unit {*unit-id* | ***all***}

パラメータ

- **unit-id**：特定のユニットを選択します。このコマンドの後のすべてのコマンドは、このユニットを参照します。ユニットは、スタックのメンバーである必要があります。（範囲：1 ～ **4**）。
- ***all***：スタック内のすべてのユニットを**選択します。**

デフォルト設定

なし

コマンド モード

グローバル コンフィギュレーション モード

例 1：次に、ユニット コンテキストを 2 に設定し、以降のすべてのスタック コマンドがユニット 2 に適用される例を示します。

```
switchxxxxxx(config)# stack unit 2
```

例 2：次に、ユニット コンテキストをスタックのすべてのユニットに設定し、以降のすべてのスタック コマンドがすべてのユニットに適用される例を示します。

```
switchxxxxxx(config)# stack unit all
```

stack configuration

リブート後のポートとユニット ID を設定するには、**stack configuration** コマンドを使用します。

構文

stack configuration {[***links*** *ports-list*] [***unit-id*** {*unit-id* | ***auto***}] *}*

no stack configuration

パラメータ

- ***links***：リロード後にスタック リンクとして使用するポート リストを選択します。
- ***ports-list***：カンマで区切られた1つ以上のスタックポートのリスト、またはダッシュでマークされた連続的なポートの範囲。

  no-links：リブート後のスタック リンクのないスタック ユニットを設定します。
- ***unit-id***：リロード後に使用するユニットを選択します。（範囲：1 ～ **4**）。スタック自動番号付け機能を有効にするには、***auto*** を使用します。

コマンド モード

グローバル コンフィギュレーション モード

スタック ユニット モード。

使用上のガイドライン

- このコマンドをグローバル コンフィギュレーション モードで実行すると、現在のスタックのアクティブユニットが設定されます。
- リロード後にスタック設定を工場出荷時に戻すには、**no stack configuration** を使用します（ユニットをリブートするには **reload** コマンドを使用します）。
- **stack unit** *all* コンテキストで ***unit-id*** パラメータの設定を ***auto*** 以外でコマンドを実行するとエラーが生成されます（複数のユニットを同じ ID に設定しないようにするため）。
- コマンドで指定しないオプションのパラメータは変更されません。

例 1：次に、アクティブユニットをスタックの工場出荷時の設定にする例を示します。

```
switchxxxxxx(config)# no stack configuration
```

例 2：次に、ユニット 3 が自動のユニット ID でスタックリンク（ポート）te3-4 を持つように設定する例を示します。

```
switchxxxxxx(config)# stack unit 3
switchxxxxxxunit# stack configuration links te3-4 unit-id auto
```

show stack configuration

スタック設定（リブート後に設定される設定を含む）パラメータを表示するには、**show stack configuration** EXEC モード コマンドを使用します。

構文

show stack configuration

コマンド モード

ユーザ EXEC モード

例

スタック全体のスタック設定情報を表示します。

```
switchxxxxxx# show stack configuration
```

Unit Id	After Reboot Configuration	
	Unit Id	Stack Links
----------	----------	----------
1	1	te1-2
2	auto	te3-4
3	4	te1-2

show stack

スタックの動作状態を表示するには、**show stack** EXEC モード コマンドを使用します。

構文

show stack

コマンド モード

ユーザ EXEC モード

例

スタック全体のスタック情報を表示します。

```
switchxxxxxx# show stack
Topology is Ring
Units stack mode: Hybrid
```

Unit Id	MAC Address	Role	Network Port Type	Uplink Port Type
-------	------------------	---------	--------	---------
1	00:00:b0:00:10:00	アクティブ	te	none
2	00:00:b0:00:20:00	Standby	gi	te
3	00:00:b0:00:30:00	メンバ	gi	te
4	00:00:b0:00:40:00	メンバ	tw	te

show stack links

スタック リンクの動作状態を表示するには、**show stack links** EXEC モード コマンドを使用します。

構文

show stack links [details]

コマンド モード

ユーザ EXEC モード

例 1：スタック全体のスタック リンク情報を表示します。

```
switchxxxxxx# show stack links
```

Topology is Ring

Unit Id	Active Links	Neighbor Links	Operational Link Speed	Down/Standby Links
----------	----------	----------	----------	----------
1	te1/1-2	te3/4,te2/1	10G	te1/3,te1/4
2	te2/1-2	te1/2,te3/3	10G	
3	te3/3-4	te2/2,te1/1	10G	

例 2：スタック全体のスタック リンク情報を詳細とともに表示します。

.

```
switchxxxxxx# show stack links details
```

Unit Id	Link	Status	Speed	Neighbor Unit Id	Neighbor Link	Neighbor Mac Address
----------	----------	----------	----------	----------	----------	----------
1	te1	Active	10G	2	te2	00:00:b0:00:20:00
1	te2	ダウン	該当なし	該当なし	該当なし	該当なし
2	te1	ダウン	該当なし	該当なし	該当なし	該当なし
2	te2	Active	10G	1	te1	00:00:b0:00:10:00

Topology is Ring

監視 VLAN

この章は、次の項で構成されています。

- surveillance-vlan vlan-id （1396 ページ）
- surveillance-vlan cos （1397 ページ）
- surveillance-vlan aging-timeout （1398 ページ）
- Surveillance-vlan traffic-source （1399 ページ）
- surveillance-vlan enable（インターフェイス） （1400 ページ）
- Show surveillance-vlan （1402 ページ）
- show surveillance-vlan interface （1403 ページ）

surveillance-vlan vlan-id

ASV（自動監視VLAN）機能をグローバルに有効にし、監視VLAN IDを選択するには、グローバル コンフィギュレーション モードで Surveillance-vlan コマンドを使用します。この機能をディセーブルにする場合は、このコマンドの no 形式を使用します。

構文

surveillance-vlan vlan-id *vlan-id*

no surveillance-vlan vlan-id

パラメータ

vlan-id：監視 VLAN の ID

デフォルト設定

ASV 機能は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

ASV として割り当てられる VLAN は、既存の静的 VLAN である必要があります。

ASV 機能をアクティブにすると、IGMP および MLD のスヌーピングおよびクエリア機能が、VLAN 上およびグローバルで有効になります（無効になっている場合）。さらに、ブリッジ マルチキャスト フィルタ処理のグローバル設定が有効になります（無効になっている場合）。

監視 VLAN は、次の VLAN とは異なる必要があります。

- Voice VLAN
- 非認証 VLAN
- ゲスト VLAN
- プライベート VLAN

コマンドを使用して、既存の ASV VLAN の VLAN ID を変更できます。この場合、ASV VLAN ID の変更により、ASV が有効になっているインターフェイスの VLAN メンバーシップが変更される可能性があるため、ユーザーは設定を確認するように求められます（コマンド survance-vlan enable（インターフェイス））。

例

次の例では、VLAN 3 で ASV 機能が有効になります。

```
switchxxxxxx(config)# surveillance-vlan vlan-id 3
```

surveillance-vlan cos

有効になっているインターフェイスで検出された監視トラフィックの VLAN 優先順位タグ（CoS）を再マーキングするためのCoS値を定義するには、グローバル コンフィギュレーション モードでsurveillance-vlan cosコマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

surveillance-vlan cos *cos*

no surveillance-vlan *cos*

パラメータ

- cos：監視トラフィックに適用されるサービスクラス。（範囲：0 ～ 7）

デフォルト設定

デフォルトでは、監視トラフィックは CoS 5 で再マークされます。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、CoS を 3 に設定しています。

```
switchxxxxxx(config)# surveillance-vlan cos 3
```

surveillance-vlan aging-timeout

監視 VLAN メンバーシップのエージングタイムアウトを設定するには、グローバル コンフィギュレーション モードで surveillance-vlan aging-timeout コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

surveillance-vlan aging-timeout minutes

no surveillance-vlan aging-timeout

- minutes：インターフェイスで監視トラフィックが停止してから、そのインターフェイスが ASV から削除されるまでの時間。（範囲：1 ～ 43200）

パラメータ

minutes：インターフェイスで監視トラフィックが停止してから、そのインターフェイスが ASV から削除されるまでの時間（分）。（範囲：1 ～ 43200）

デフォルト設定

1440 分。

コマンド モード

グローバル コンフィギュレーション モード

例

次に、ASV エージングタイムアウトを 12 時間に設定する例を示します。

```
switchxxxxxx(config)# surveillance-vlan aging-timeout 720
```

Surveillance-vlan traffic-source

ASV 機能で追跡するトラフィック送信元を追加するには、グローバル コンフィギュレーション モードでsurvance-vlan traffic-source コマンドを使用します。テーブルからトラフィック送信元を削除するには、このコマンドの no 形式を使用します。

構文

surveillance-vlan traffic-source default | {**mac** *mac-address*|**oui** *OUI*} [**description** description]}

no surveillance-vlan traffic-source {**mac** *mac-address*|**oui** *OUI*}

パラメータ

- *mac-address*：トラフィック送信元テーブルに追加されるユニキャスト MAC アドレス。
- *oui*：トラフィック送信元テーブルに追加される 3 オクテットの MAC アドレスプレフィックス。
- *description*：監視トラフィック送信元の説明（長さ：最大 32 文字）。

デフォルト設定

テーブルは空です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

トラフィック送信元テーブルには、MAC エントリと OUI エントリが含まれています。これらのエントリに一致する送信元からのトラフィックを、ASV 機能が有効になっているインターフェイスで受信した場合、そのインターフェイスは自動監視 VLAN に追加されます。

例

次の例では、テーブルに OUI エントリを追加しています。

```
switchxxxxxx(config)# surveillance-vlan traffic-source oui a0:bb:cc
```

次の例では、テーブルに説明とともに MAC エントリを追加しています。

```
switchxxxxxx(config)# surveillance-vlan traffic-source mac 12:44:4a:4c:13:ec
description floor1_sec
```

次の例では、テーブルから MAC ベースのエントリを削除しています。

```
switchxxxxxx(config)# no surveillance-vlan traffic-source mac
12:44:4a:4c:13:ec
```

surveillance-vlan enable（インターフェイス）

インターフェイスの ASV 機能を有効にするには、surveillance-vlan enable インターフェイス コンフィギュレーション モード コマンドを使用します。インターフェイスでこの機能を無効にするには、このコマンドの no 形式を使用します。

構文

surveillance-vlan enable

no surveillance-vlan enable

デフォルト設定

ASV 機能は、すべてのインターフェイスで無効になっています。

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

ASV機能は、スイッチポートモードがアクセスまたは一般であるインターフェイスでのみ有効にできます。

アクセスモードは、単一の監視デバイスに接続されるインターフェイスに使用する必要があります。

一般モードは、その後複数の監視デバイスに接続される可能性のある他のネットワークノードに接続されているインターフェイスで使用する必要があります。

監視送信元として定義された送信元からのトラフィックが、ASV機能が有効になっているインターフェイスで検出された場合、そのインターフェイスは監視VLANのメンバーになります。

このインターフェイスで転送される監視トラフィックの VLAN 優先順位タグは、survance-vlan cos コマンドで定義された CoS 値に設定されます。

監視送信元からのトラフィックが停止し、エージングタイムアウト機能の期間が経過すると、インターフェイスは監視VLANから削除され、元の静的VLANメンバーシップを再開します。

アクセスモードでは、インターフェイスが監視VLANに追加されると、監視VLANのメンバーである間は元のメンバーシップから削除されます。

一般モードでは、監視トラフィックは監視 VLAN でルーティングされますが、非監視トラフィックはインターフェイスの元の VLAN メンバーシップを使用します。

RADIUSによってVLANに割り当てられている場合、この機能をインターフェイスで有効にすることはできません。

例

次の例では、gi1/0/2 で ASV 機能が有効になります。

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# surveillance-vlan enable
```

Show surveillance-vlan

ASVのグローバル設定とステータス、およびトラフィック送信元テーブルを表示するには、特権 EXEC モードで show threat-vlan コマンドを使用します。

構文

show surveillance-vlan

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、ASV機能とトラフィック送信元テーブルのグローバル設定を表示します。トラフィック送信元テーブルには、次の列があります。

- [MAC/OUI]：このトラフィック送信元の MAC または OUI プレフィックス。
- [Description]：トラフィック送信元の説明。
- [Active]：エージングタイムアウトによってタイムアウトしていない、ASV 機能が有効になっているインターフェイスで、この送信元からのトラフィックが検出された場合、この値は [Yes] になります。
- [Interface]：この送信元からのトラフィックを検出した、ASV 機能が有効になっているインターフェイスのリスト。

例

このコマンドは、ASV 機能のグローバルステータスと設定を表示します。

[Surveillance Traffic Sources] テーブルの [Active] 列は、FDB からまだエージアウトしていないこの送信元からの現在のフローがあることを示します。[Interfaces] 列には、この送信元OUIまたはMAC に一致するトラフィックを現在受信しているインターフェイスが表示されます。

次の例は、コマンドの出力を示しています。

```
switchxxxxxx# show surveillance-vlan
Surveillance VLAN is enabled on VLAN 5
Aging timeout: 1440 minutes
CoS: 5
Surveillance-Traffic sources
MAC/OUI Description Active Interface
================ =========== ====== =========
00:03:C5 Mobotix Yes ge1/2, LAG8
00:04:7D Pelco No
10:22:33:12:44:22 RND-Server Yes ge1/4
```

show surveillance-vlan interface

このコマンドは、ASV 機能に関連するインターフェイスのステータスと設定を表示します。

ASV インターフェイスの設定とステータスを表示するには、特権 EXEC モードで show surveillance-vlan interface コマンドを使用します。

構文

show surveillance-vlan interface

コマンド モード

特権 EXEC モード。

使用上のガイドライン

このコマンドは、デバイスのインターフェイスの ASV 機能のインターフェイス設定を表示します。

設定テーブルには、次の列があります。

- [Interface]：行にステータスが表示されるインターフェイス。
- [Enabled]：インターフェイスで ASV 機能が有効になっているかどうかを示す boolean 値。
- [Active]：インターフェイスが ASV VLAN のメンバーになった場合（MAC アドレス転送テーブルに監視トラフィックの送信元アドレスのエントリが含まれていない場合でも）、この値は [Yes] になります。

例

次の例は、コマンドの出力を示しています。

```
Switchxxxxxx# show surveillance-vlan interface
Interface Enabled Active
========= ======= ======
ge1/1     Yes     No
ge1/2     Yes     Yes
ge1/3     No      No
```

SYSLOG コマンド

この章は、次の項で構成されています。

- aaa logging （1406 ページ）
- clear logging （1407 ページ）
- clear logging file （1408 ページ）
- file-system logging （1409 ページ）
- logging buffered （1410 ページ）
- logging console （1411 ページ）
- logging file （1412 ページ）
- logging host （1413 ページ）
- logging on （1415 ページ）
- logging source-interface （1416 ページ）
- logging source-interface-ipv6 （1417 ページ）
- logging aggregation on （1418 ページ）
- logging aggregation aging-time （1419 ページ）
- logging origin-id （1420 ページ）
- logging cbd module （1421 ページ）
- logging cbd level （1422 ページ）
- show logging （1423 ページ）
- show logging file （1424 ページ）
- show syslog-servers （1425 ページ）

aaa logging

AAA ログインのロギングを有効にするには、**aaa logging** グローバル コンフィギュレーション モード コマンドを使用します。AAA ログインのロギングを無効にするには、このコマンドの **no** 形式を使用します。

構文

aaa logging {**login**}

no aaa logging {**login**}

パラメータ

login：成功した AAA ログイン イベント、失敗した AAA ログイン イベント、およびその他の AAA ログイン関連のイベントに関連するメッセージのロギングを有効にします。

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、正常に完了したログイン イベント、失敗したログイン イベント、およびその他のログイン関連のイベントに関連するメッセージのロギングを有効にします。他のタイプの AAA イベントは、このコマンドの対象になりません。

例

次の例では、AAA ログイン イベントのロギングを有効にしています。

```
switchxxxxxx(config)# aaa logging login
```

clear logging

内部ロギング バッファからメッセージをクリアするには、**clear logging** 特権 EXEC モード コマンドを使用します。

構文

clear logging

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

特権 EXEC モード

例

次の例では、内部ロギング バッファからメッセージをクリアしています。

```
switchxxxxxx# clear logging
Clear Logging Buffer ? (Y/N)[N]
```

clear logging file

ロギング ファイルからメッセージをクリアするには、**clear logging file** 特権 EXEC モード コマンドを使用します。

構文

clear logging file

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

特権 EXEC モード

例

次の例では、ロギング ファイルからメッセージをクリアしています。

```
switchxxxxxx# clear logging file
Clear Logging File [y/n]
```

file-system logging

ファイル システム イベントのロギングを有効にするには、**file-system logging** グローバル コンフィギュレーション モード コマンドを使用します。ファイル システム イベントのロギングを無効にするには、このコマンドの **no** 形式を使用します。

構文

file-system logging *{***copy** | **delete-rename***}*

no file-system logging *{***copy** | **delete-rename***}*

パラメータ

- **copy**：ファイル コピー操作に関連するメッセージのロギングを指定します。
- **delete-rename**：ファイル削除操作および名称変更操作に関連するメッセージのロギングを指定します。

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、ファイル コピー操作に関連するメッセージのロギングを有効にしています。

```
switchxxxxxx(config)# file-system logging copy
```

logging buffered

SYSLOG メッセージの出力を特定のシビラティ（重大度）のメッセージに制限し、バッファ サイズ（保存できるメッセージの数）を定義するには、**logging buffered** グローバル コンフィギュレーション モード コマンドを使用します。SYSLOG メッセージの出力をキャンセルし、バッファ サイズをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

logging buffered [*buffer-size*] [*severity-level* | *severity-level-name*]

no logging buffered

パラメータ

- **buffer-size**：（オプション）バッファに保存されるメッセージの最大数を指定します。（範囲：20 ～ 1000）
- **severity-level**：（オプション）バッファにロギングするメッセージのシビラティ（重大度）を指定します。設定できる値は 1 ～ 7 です。
- **severity-level-name**：（オプション）バッファにロギングするメッセージのシビラティ（重大度）を指定します。設定可能な値は、emergencies（緊急）、alerts（アラート）、critical（重大）、errors（エラー）、warnings（警告）、notifications（通知）、informational（情報）、debugging（デバッグ）です。

デフォルト設定

デフォルトのシビラティ（重大度）レベルは informational です。

デフォルトのバッファ サイズは 1000 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

すべての SYSLOG メッセージが内部バッファにロギングされます。このコマンドは、ユーザに表示されるメッセージを制限します。

例

次の例では、内部バッファからの SYSLOG メッセージの出力をシビラティ（重大度）が **debugging** のメッセージに制限する 2 つの方法を示しています。2 番目の例では、バッファ サイズを 100、シビラティ（重大度）を **informational** に設定しています。

```
switchxxxxxx(config)# logging buffered debugging
switchxxxxxx(config)# logging buffered 100 informational
```

logging console

コンソールにロギングするメッセージを特定のシビラティ（重大度）のメッセージに制限するには、**logging console** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

構文

logging console *level*

no logging console

パラメータ

level：ロギングしたメッセージのうちコンソールに表示するメッセージのシビラティ（重大度）を指定します。設定可能な値は、emergencies（緊急）、alerts（アラート）、critical（重大）、errors（エラー）、warnings（警告）、notifications（通知）、informational（情報）、debugging（デバッグ）です。

デフォルト設定

Informational

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、コンソールに表示するロギング メッセージをシビラティ（重大度）が **errors** のメッセージに制限しています。

```
switchxxxxxx(config)# logging console errors
```

logging file

ロギング ファイルに送信されるSYSLOGメッセージを特定のシビラティ（重大度）のメッセージに制限するには、**logging file** グローバル コンフィギュレーション モード コマンドを使用します。ファイルへのメッセージの送信をキャンセルするには、このコマンドの **no** 形式を使用します。

構文

logging file *level*

no logging file

パラメータ

level：ロギング ファイルに送信される SYSLOG メッセージのシビラティ（重大度）を指定します。設定可能な値は、emergencies（緊急）、alerts（アラート）、critical（重大）、errors（エラー）、warnings（警告）、notifications（通知）、informational（情報）、debugging（デバッグ）です。

デフォルト設定

デフォルトのシビラティ（重大度）レベルは **errors** です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、ロギング ファイルに送信される SYSLOG メッセージをシビラティ（重大度）が **alerts** のメッセージに制限しています。

```
switchxxxxxx(config)# logging file alerts
```

logging host

指定したSYSLOGサーバにメッセージをロギングするには、**logging host** グローバル コンフィギュレーション コマンドを使用します。SYSLOG サーバの一覧から指定したアドレスを持つSYSLOG 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。

構文

logging host *{ip-address | ipv6-address | hostname}* [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]

no logging host *{ipv4-address | ipv6-address | hostname}*

パラメータ

- **ip-address**：SYSLOGサーバとして使用するホストのIPアドレス。IPアドレスには、IPv4、IPv6 または IPv6z アドレスを使用できます。
- **hostname**：SYSLOG サーバとして使用するホストのホスト名。IPv4 アドレスへの変換のみがサポートされています。（範囲：1 ～ 158 文字。ホスト名の各部分の最大ラベル サイズ：63）。
- ***port*** *port*：（オプション）SYSLOG メッセージのポート番号。指定しない場合、ポート番号はデフォルトの 514 になります。（範囲：1 ～ 65535）
- ***severity*** *level*：（オプション）SYSLOG サーバへのメッセージのロギングを指定されたシビラティ（重大度）に制限します。Emergencies、Alerts、Critical、Errors、Warnings、Notifications、Informational、Debugging のいずれかです。
- ***facility*** *facility*：（オプション）メッセージに示されているファシリティ。local0、local1、local2、local3、local4、local5、local6、local7 のいずれかの値になります。指定しない場合、ポート番号はデフォルトの local7 になります。
- ***description*** *text*：（オプション）SYSLOG サーバの説明。（範囲：最大 64 文字）

デフォルト設定

メッセージは、SYSLOG サーバにロギングされません。

指定しない場合、**シビラティ（重大度）**はデフォルトの Informational になります。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

複数の SYSLOG サーバを使用できます。

例

```
switchxxxxxx(config)# logging host 1.1.1.121
switchxxxxxx(config)# logging host 3000::100/SYSLOG1
```

logging on

メッセージのロギングを有効にするには、**logging on** グローバル コンフィギュレーション モード コマンドを使用します。このコマンドは、デバッグ メッセージまたはエラー メッセージを指定の場所に非同期に送信します。ロギングを無効にするには、このコマンドの **no** 形式を使用します。

構文

logging on

no logging on

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

メッセージのロギングは有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、エラー メッセージのロギングを有効にしています。

```
switchxxxxxx(config)# logging on
```

logging source-interface

IPv4 SYSLOG サーバと通信するために IPv4 アドレスを送信元 IPv4 アドレスとして使用する送信元インターフェイスを指定するには、**logging source-interface** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

logging source-interface *interface-id*

no logging source-interface

パラメータ

interface-id：送信元インターフェイスを指定します。

デフォルト設定

送信元 IPv4 アドレスは、発信インターフェイスで定義され、ネクスト ホップ IPv4 サブネットに属する IPv4 アドレスです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスの場合は、ネクスト ホップ IPv4 サブネットに属するインターフェイス IP アドレスが適用されます。

送信元インターフェイスが発信インターフェイスでない場合は、送信元インターフェイスで定義された最小 IPv4 アドレスが適用されます。

使用可能な IPv4 送信元アドレスがない場合は、IPv4 SYSLOG サーバと通信しようとすると、SYSLOG メッセージが発行されます。

送信元インターフェイスとして OOB は定義できません。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# logging source-interface vlan 100
```

logging source-interface-ipv6

IPv6 SYSLOG サーバと通信するために IPv6 アドレスを送信元 IPv6 アドレスとして使用する送信元インターフェイスを指定するには、**logging source-interface-ipv6** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

logging source-interface-ipv6 *interface-id*

no logging source-interface-ipv6

パラメータ

interface-id：送信元インターフェイスを指定します。

デフォルト設定

IPv6 送信元アドレスは、発信インターフェイスの定義済みの IPv6 アドレスであり、RFC6724 に従って選択されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスの場合は、このインターフェイスに定義された IPv6 アドレスになり、RFC 6724 に従って選択されます。

送信元インターフェイスが発信インターフェイスでない場合は、送信元インターフェイス上で宛先 IPv6 アドレスの範囲で定義された最小 IPv6 アドレスが適用されます。

使用可能な IPv6 送信元アドレスがない場合は、IPv6 SYSLOG サーバとの通信を試行する際に SYSLOG メッセージが発行されます。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# logging source-interface-ipv6 vlan 100
```

logging aggregation on

SYSLOG メッセージの集約を制御するには、**logging aggregation on** グローバル コンフィギュレーション モード コマンドを使用します。集約を有効にすると、ロギング メッセージが時間間隔ごとに（logging aggregation aging-time （1419 ページ） で指定されているエージング タイムに従って）表示されます。SYSLOG メッセージの集約を無効にするには、このコマンドの **no** 形式を使用します。

構文

logging aggregation on

no logging aggregation on

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

例

SYSLOG メッセージの集約をオフにするには、次のようにします。

```
switchxxxxxx(config)# no logging aggregation on
```

logging aggregation aging-time

集約した SYSLOG メッセージのエージング タイムを設定するには、**logging aggregation aging-time** グローバル コンフィギュレーション モード コマンドを使用します。SYSLOG メッセージは、aging-time パラメータによって設定された時間間隔の間集約されます。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

logging aggregation aging-time *sec*

no logging aggregation aging-time

パラメータ

aging-time *sec*：秒単位（範囲：15 ～ 3600）のエージング タイム。

デフォルト設定

300 秒

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# logging aggregation aging-time 300
```

logging origin-id

SYSLOG サーバに送信される SYSLOG メッセージ パケット ヘッダーの origin フィールドを設定するには、**logging origin-id** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

logging origin-id {***hostname*** | ***IP*** | ***IPv6*** | ***string*** *user-defined-id*}

no logging origin-id

パラメータ

- **hostname**：システム ホスト名は、メッセージ発信元識別子として使用されます。
- **IP**：メッセージ発信元識別子として使用される送信インターフェイスの IP アドレス。
- **IPv6**：メッセージ発信元識別子として使用される送信インターフェイスの IPv6 アドレス。送信インターフェイスが IPv4 の場合は、代わりに IPv4 アドレスが使用されます。
- **string** *user-defined-id*：ユーザが選択する識別説明を指定します。*user-defined-id* 引数は、識別子を説明する文字列です。

デフォルト設定

ヘッダーは、PRI フィールドと別に送信されません。

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# logging origin-id string “Domain 1, router B”
```

logging cbd module

Cisco Business Dashboard（CBD）ロギングでサポートされるモジュールを定義するには、**logging cbd module** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

構文

logging cbd module {*module* [*module2 … module6*] | ***none*** | **all}**

no logging cbd module

パラメータ

- ***module*** - list includes: ***call-home, discovery, northbound, services, southbound, system***. このリストは、以前に設定されたリストを置き換えます。
- **none**：すべてのモジュールのロギングを無効にします。
- **all**：すべてのモジュールのロギングを有効にします。

デフォルト設定

CBD のロギングはすべてのモジュールで有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

この設定は、CBD エージェントのロギングに影響します。

例

次に、すべての CBD モジュールのロギングメッセージを有効にする例を示します。

```
switchxxxxxx(config)# logging cbd module all
```

logging cbd level

Cisco Business Dashboard（CBD）に記録されるメッセージを特定のシビラティ（重大度）レベルのメッセージに制限するには、**logging cbd level** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

構文

logging cbd level *level*

no logging cbd level

パラメータ

level：ロギングしたメッセージのうちコンソールに表示するメッセージのシビラティ（重大度）を指定します。使用可能な値は、errors、warnings、informational、および debugging です。これにより、このレベル以上のメッセージのロギングが有効になります。

デフォルト設定

Informational

コマンド モード

グローバル コンフィギュレーション モード

例

次に、CBD のメッセージのロギングをシビラティ（重大度）レベル **errors** のメッセージに制限する例を示します。

```
switchxxxxxx(config)# logging cbd errors
```

show logging

内部バッファに保存されているロギング ステータスおよび SYSLOG メッセージを表示するには、**show logging** 特権 EXEC モード コマンドを使用します。

構文

show logging

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

特権 EXEC モード

例

次に、内部バッファに保存されているロギング ステータスおよび SYSLOG メッセージを表示する例を示します。

```
switchxxxxxx# show logging
Logging is enabled.
```

Origin id: hostname

```
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200 Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged
Application filtering control
Application            Event                 Status
--------------------   -----------------     ---------
AAA                    Login                 Enabled
File system            Copy                  Enabled
File system            Delete-Rename         Enabled
Management ACL         Deny                  Enabled
Aggregation: Disabled.
Aggregation aging time: 300 Sec
Logging cbd level: Informational
Logging cbd  modules Enabled: call-home
01-Jan-2010 05:29:46 :%INIT-I-Startup: Warm Startup
01-Jan-2010 05:29:02 :%LINK-I-Up:  Vlan 1
01-Jan-2010 05:29:02 :%LINK-I-Up:  SYSLOG6
01-Jan-2010 05:29:02 :%LINK-I-Up:  SYSLOG7
01-Jan-2010 05:29:00 :%LINK-W-Down:  SYSLOG8
```

show logging file

ロギング ファイルに保存されているロギング ステータスおよび SYSLOG メッセージを表示するには、**show logging file** 特権 EXEC モード コマンドを使用します。

構文

show logging file

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

特権 EXEC モード

例

次に、ロギング ファイルに保存されているロギング ステータスおよび SYSLOG メッセージを表示する例を示します。

```
switchxxxxxx# show logging file
Logging is enabled.
```

Origin id: hostname

```
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200 Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged
Application filtering control
Application            Event                Status
--------------------   -----------------    ---------
AAA                    Login                Enabled
File system            Copy                 Enabled
File system            Delete-Rename        Enabled
Management ACL         Deny                 Enabled
Aggregation: Disabled.
Aggregation aging time: 300 Sec
1-Jan-2010 05:57:00 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:56:36 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:55:37 :%SSHD-E-ERROR: SSH error: key_read: type mismatch: encoding error
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_read: key_from_blob bgEgGnt9
z6NHgZwKI5xKqF7cBtdl1xmFgSEWuDhho5UedydAjVkKS5XR2... failed
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_from_blob: invalid key type.
01-Jan-2010 05:56:34 :%SSHD-E-ERROR: SSH error: bad sigbloblen 58 != SIGBLOB_LEN
console#
```

show syslog-servers

SYSLOG サーバ設定を表示するには、**show syslog-servers** 特権 EXEC モード コマンドを使用します。

構文

show syslog-servers

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

特権 EXEC モード

例

次の例では、SYSLOG サーバに関する情報を提供しています。

```
switchxxxxxx# show syslog-servers
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Device Configuration
--------------------
IP address    Port   Facility Severity  Description
------------- ----   --------- -------- --------------
1.1.1.121     514    local7    info
3000::100     514    local7    info
OOB host Configuration
----------------------
IP address    Port   Facility Severity  Description
------------- ----   --------- -------- --------------
2.1.1.200     514    local7    warning
```

システム管理コマンド

この章は、次の項で構成されています。

- disable ports leds （1429 ページ）
- dying-gasp enable （1430 ページ）
- hostname （1431 ページ）
- reload （1432 ページ）
- reload factory-default （1434 ページ）
- resume （1436 ページ）
- service cpu-utilization （1437 ページ）
- show cpld version （1438 ページ）
- show cpu input rate （1439 ページ）
- show cpu utilization （1440 ページ）
- show dying-gasp packets （1441 ページ）
- show dying-gasp status （1442 ページ）
- show environment （1443 ページ）
- show inventory （1445 ページ）
- show platform certificate （1447 ページ）
- show platform hardware integrity （1452 ページ）
- show platform integrity （1454 ページ）
- show reload （1456 ページ）
- show sessions （1457 ページ）
- show software versions （1459 ページ）
- show system （1461 ページ）
- show system languages （1463 ページ）
- show system tcam utilization （1464 ページ）
- show services tcp-udp （1465 ページ）
- show tech-support （1466 ページ）
- show system fans （1468 ページ）
- show system sensors （1471 ページ）
- show system id （1473 ページ）

- show ports leds configuration （1474 ページ）
- show users （1475 ページ）
- show hardware version （1476 ページ）
- show hardware components （1477 ページ）
- system light （1479 ページ）
- system recovery （1480 ページ）
- system reset-button disable （1481 ページ）

disable ports leds

デバイス上のすべてのポートのLEDを**オフ**にするには、**disable ports leds** グローバル コンフィギュレーション モード コマンドを使用します。

デバイス上にあるすべてのポートのLEDをポートの現在の動作状態に設定するには、**no disable ports leds** コマンドを使用します。

構文

disable **ports leds**

no disable **ports leds**

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

デフォルトは **no disable port leds** です。つまり、すべてのポート LED はそれぞれの現在の状態を反映しています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、ポート LED をオフにしています。

```
switchxxxxxx(config)# disable ports leds
```

dying-gasp enable

このコマンドは、Dying Gasp機能を有効にし、メッセージの送信に使用するメソッドとその優先順位を選択します。このコマンドの no 形式を使用すると、デフォルト設定に戻ります（機能を無効にします）。

構文

dying-gasp enable *method1 [method2…]*

no dying-gasp enable

パラメータ

Method1 [method2…]：Dying Gaspメッセージの送信に使用するメソッドのリスト。メソッドの順序は、メソッド間の優先順位を示します。この機能を有効にするには、少なくとも1つのメソッドを入力する必要があります。リストに含まれていないメソッドは、Dying Gaspメッセージの送信には使用されません。

考えられるメソッドは、snmp-traps、syslog です。

デフォルト設定

デフォルトでは、Dying Gasp は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード。

hostname

デバイスのホスト名を指定または変更するには、**hostname** グローバル コンフィギュレーション モード コマンドを使用します。既存のホスト名を削除するには、このコマンドの **no** 形式を使用します。

構文

hostname *name*

no hostname

パラメータ

Name：デバイスのホスト名を指定します。（長さ：1ー58 文字）。ホスト名は文字で始まり、文字または数字で終わり、その間には文字、数字、またはハイフンしか使用できません。

デフォルト設定

ホスト名は定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、デバイスのホスト名を「enterprise」として指定しています。

```
switchxxxxxx(config)# hostname enterprise
enterprise(config)#
```

reload

ユーザ指定の時間にオペレーティング システムをリロードするには、**reload** 特権 EXEC モード コマンドを使用します。

構文

reload [**in** [hhh:mm | mmm] | **at** hh:mm [day month]] | **cancel**]

パラメータ

- **in** hhh:mm | mmm：（オプション）指定した分数、または時間および分数が経過したときにソフトウェアがリロードされるようにスケジューリングします。リロードは、約 24 日以内に実行する必要があります。
- **at** hh:mm：（オプション）ソフトウェアのリロードが（24 時間制で）指定された時刻に行われるようにスケジューリングします。月日を指定すると、指定された日時にリロードが行われるようにスケジュールが設定されます。月日を指定しなかった場合、リロードは当日の指定時刻に行われます（指定時刻が現時刻より後の場合）。または翌日の指定時刻に行われます（指定時刻が現在時刻よりも前の場合）。00:00 を指定すると、深夜 0 時のリロードが設定されます。リロードは、24 日以内に実行される必要があります。
- **day**：（オプション）1 ～ 31 の範囲で日付を指定します。
- **month**：（オプション）月。
- **cancel**：（オプション）スケジューリングされているリロードをキャンセルします。

デフォルトの使用

なし

コマンド モード

特権 EXEC モード

User Guidelines

at キーワードは、システム クロックがデバイスに設定されている場合にのみ使用できます。いくつかのデバイスで同時にリロードが発生するようにスケジューリングするには、各デバイスで時間を SNTP と同期します。

at キーワードを使用してリロード時刻を指定するときに月日を指定した場合は、指定された日時にリロードが実行されます。月日が指定されていない場合は、リロードが（指定された時間が現在の時間よりも遅い場合は）現在の日の指定された時間、または（指定された時間が現在の時間よりも早い場合は）翌日の指定された時間に行われます。00:00 を指定すると、深夜 0 時のリロードが設定されます。リロードは、24 日以内に実行される必要があります。

スケジューリングされたリロードの情報を表示するには、**show reload** コマンドを使用します。

例 1：次に、スタック システムのすべてのユニット、またはスタンドアロン システムの単一ユニットでオペレーティング システムをリロードする例を示します。

```
switchxxxxxx> reload
This command will reset the whole system and disconnect your current session. Do you
want to continue? (y/n) [Y]
```

例 2：次に、スタック システムのすべてのユニット、またはスタンドアロン システムの単一ユニットで10分後にオペレーティング システムをリロードする例を示します。

```
switchxxxxxx> reload in 10
This command will reset the whole system and disconnect your current session. Reload is
 scheduled for 11:57:08 UTC Fri Apr 21 2012 (in 10 minutes). Do you want to continue?
(y/n) [Y]
```

例 3：次に、スタックシステムのすべてのユニット、またはスタンドアロンシステムの単一ユニットで 13:00 にオペレーティングシステムをリロードする例を示します。

```
switchxxxxxx> reload at 13:00
This command will reset the whole system and disconnect your current session. Reload is
 scheduled for 13:00:00 UTC Fri Apr 21 2012 (in 1 hour and 3 minutes). Do you want to
continue? (y/n) [Y]
```

例 4：次の例では、リロードをキャンセルしています。

```
switchxxxxxx> reload cancel
Reload cancelled.
```

reload factory-default

スタックまたはスタック内の特定のユニットをリロードし、設定を工場出荷時のデフォルトに戻すには、reload factory-default 特権 EXEC モードコマンドを使用します。

構文

reload factory-default [unit unit-id]

パラメータ

- [**unit** unit-id]：（オプション）工場出荷時のデフォルトにリセットし、指定されたユニットのみをリロードします。スタック内の他のユニットはリセットまたはリロードされません。このパラメータが指定されていない場合、スタック内のすべてのユニットが工場出荷時のデフォルトにリセットされ、リロードされます。

デフォルトの使用

デフォルトでは、スタック内のすべてのユニットが工場出荷時のデフォルト設定にリセットされ、リロードされます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、スタック内のすべてのユニットを工場出荷時のデフォルト設定にリセットします。[unit unit-id] パラメータが指定されている場合、指定されたユニットのみが工場出荷時のデフォルトにリセットされます。このコマンドは、デバイスリセットボタンを押して工場出荷時のデフォルトへのリセットとデバイスのリロードを開始するのと同じ効果があります。スタック設定、設定ファイル、syslog ファイル、およびその他の設定関連ファイルは消去されます。工場出荷時のデフォルトにリセットされたユニットはスタックから切断され、スタックトポロジが変更されます。これにより、スタック内のユニット間で切断が発生する可能性があります。

コマンドの [unit unit-id] パラメータでアクティブユニットが指定されている場合、スタックは残りのユニットのいずれかがスタンバイユニットである場合にのみ稼働を継続します。

例

例 1：次の例では、工場出荷時のデフォルトにリセットし、スタック内のすべてのユニットをリロードします。

```
switchxxxxxx> reload factory-default
This command will reset to factory default and reload all of the units in the
stack. It is highly recommended to backup the stack configuration before
applying this command.
```

例 2：次の例では、工場出荷時のデフォルトにリセットし、ユニット番号 3 のみをリロードします。

```
switchxxxxxx> reload factory-default unit 3
This command will reset to factory default and reload the selected unit. The
unit will disconnect from the stack and will no longer be a member of the
stack. The disconnection of the unit will affect the stack topology and may
disconnect other units in the stack.
Do you want to continue? (y/n) [Y]
```

resume

別のオープンしている Telnet セッションへの切り替えを有効にするには、**resume** EXEC モード コマンドを使用します。

構文

resume [*connection*]

パラメータ

connection：（オプション）接続番号を指定します。（範囲：1 ～ 4 接続。）

デフォルト設定

デフォルトの接続番号は、最新接続の番号です。

コマンド モード

特権 EXEC モード

例

次のコマンドは、オープンしている Telnet セッション番号 1 に切り替えます。

```
switchxxxxxx> resume 1
```

service cpu-utilization

CPU 使用率の測定を有効にするには、**service cpu-utilization** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

service cpu-utilization

no service cpu-utilization

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

CPU 使用率の測定は有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

CPU 使用率の情報を測定するには、**service cpu utilization** コマンドを使用します。

例

次の例では、CPU 使用率の測定を有効にしています。

```
switchxxxxxx(config)# service cpu-utilization
```

show cpld version

デバイス CPLD コードのバージョンを表示するには、**show cpld version** ユーザ EXEC モードコマンドを使用します。

構文

show cpld version [**unit** *unit-id*]

パラメータ

unit [*unit-id*]：ユニット番号を指定します（範囲：1 ～ 4）。指定しない場合、このコマンドはスタック内のすべてのユニットの CPLD コードのバージョンを表示します。

コマンド モード

ユーザ EXEC モード

例 1：次に、スタック内のすべてのユニットの CPLD バージョンを表示する例を示します。

```
switchxxxxxx> show cpld version
Unit ID     Unit Type    CPLD code Version
----        -----------     -------------
1           CBS350-48P-4X      1.0.1
2                   CBS350-48P-4X      1.0.2
```

例 2：次に、スタック内のユニットに CPLD がない CPLD バージョンを表示する例を示します。

```
switchxxxxxx> show cpld version
Unit ID     Unit Type    CPLD code Version
----        -----------     -------------
1           CBS350-48P-4X      Not Supported
2                   CBS350-48P-4X      1.0.2
```

show cpu input rate

CPU への入力フレームのレートをパケット/秒（pps）で表示するには、**show cpu input rate** ユーザ EXEC モードコマンドを使用します。

構文

show cpu input rate

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

例

次に、CPU 入力レート情報を表示する例を示します。

```
switchxxxxxx> show cpu input rate
Input Rate to CPU is 1030 pps.
```

show cpu utilization

CPU 使用率に関する情報を表示するには、**show cpu utilization** 特権 EXEC モード コマンドを使用します。

構文

show cpu utilization

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルトの使用

なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

show cpu-utilization コマンドは、CPU 使用率の測定を有効にする場合に使用します。

例

次に、CPU 使用率情報を表示する例を示します。

```
switchxxxxxx> show cpu utilization
CPU utilization service is on.
CPU utilization
-------------------------------------------------
five seconds: 5%; one minute: 3%; five minutes: 3%
```

show dying-gasp packets

dying-gasp イベントの発生時に送信されるパケットに関する情報を表示するには、特権 EXEC モードで show dying-gasp packets コマンドを使用します。

構文

show dying-gasp packets

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、スイッチの電源が失われた場合に送信されるパケットに関する情報を表示し、dying gasp パケットを送信します。

dying gasp メッセージが送信される各 SYSLOG サーバーおよび SNMP トラップ受信者に関する情報が提供されます。次の情報が含まれます。

受信者 IP アドレス

アウトバウンド インターフェイス

ローカル IP アドレス

ローカル MAC アドレス

ネクストホップの IP アドレスと MAC アドレス。

コマンドで syslog または snmp-trap キーワードを使用して、1 つの方式のパケットだけを表示することができます。

例

例：次の例は、コマンドの出力を示しています。

```
switchxxxxxx# show dying-gasp packets
Syslog packet for server 8.1.154.22, link type IP
Via interface gigabitEthernet1/0/6, local IP address 8.1.154.98
Encap type is ARPA, local MAC address 00:50:43:8a:ce:19
Next hop IP address 8.1.154.192, next hop MAC address a2:43:41:44:8a:f2
SNMP trap packet for server 6.193.2.29, link type IP
Via interface gigabitEthernet1/0/3, local IP address 6.193.2.5
Encap type is ARPA, local MAC address 00:50:43:8a:ce:19
Next hop IP address 6.193.2.45, next hop MAC address 82:a3:9c:15:cb:3d
```

show dying-gasp status

このコマンドは、Dying Gasp 機能のグローバル設定を表示します。

例

次の例で、show-dying-gasp-status を設定する方法を示します。

```
Switch000000#show dying-gasp status
Dying Gasp Status: Enabled
Method 1: Syslog
Method 2: SNMP Traps
```

show environment

環境情報を表示するには、**show environment** ユーザ EXEC モードコマンドを使用します。

構文

show environment {all | fan | temperature {status} | *stack* *[switch-number]*}

パラメータ

- **all**：ファンと温度の一般的なステータスを表示します。このパラメータを使用した場合は、スタックユニットのいずれかに障害が発生している場合は、その障害状況を報告します。
- **fan**：ファンのステータスを表示します。
- **temperature {status}**：温度ステータスを表示します。
- **stack *[switch-number]***：（オプション）スタックの環境ステータスの詳細をスタックユニットごとに表示します。switch-numberが指定されている場合は、選択したデバイス番号の電話番号の環境ステータスが表示されます。（範囲：1 ～ 4）

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

fan status パラメータと **temperature status** パラメータは、ファンセンサーや温度センサーが設置されているデバイスでのみ使用できます。

ファン ステータスは、次のいずれかになります。

- **OK**：ファンは正しく機能しています。
- **Failure**：1 つ以上のファンに障害が発生しています。
- **Fan read fail**：1 つ以上のファンからの情報の読み取りに失敗しました。
- **NA**：ファンは設置されていません。

温度は、次のいずれかになります。

- **OK**：温度は、警告しきい値を下回っています。
- **Warning**：温度は警告しきい値とクリティカルなしきい値の間です。
- **Critical**：温度は、クリティカルしきい値を上回っています。

センサー ステータスは、次のいずれかになります。

- **OK**：デバイスのすべてのセンサーが正常に機能しています。
- **Failure**：1 つ以上のセンサーに障害が発生しています。
- **NA**：センサーは取り付けられていません。

例 1：次に、デバイスまたはスタックの一般的な環境ステータスを表示する例を示します。

```
switchxxxxxx> show environment all
```

内部電源装置がアクティブになっています。

```
fans OK
Sensor is OK
Temperature is OK
#EDITOR: The temperature status is OK if ALL the temperature sensors status in all the
stack members is OK, and if the temperature of all the stack members is below the lowest
 threshold (this is calculated per stack member, if one or more of the stack members
temperature is above its specific threshold, the temperature status is FAILURE)
#EDITOR: Likewise the fan status will be OK - only if status of fans on ALL stack members
 is OK (meaning no fan fail - or with redundant fan support - only 1 fan fail and redundant
 fan active
```

例 2：次に、デバイスまたはスタックの電源の状態を表示する例を示します。

```
switchxxxxxx> show environment power
```

内部電源装置がアクティブになっています。

例 3：次に、デバイスまたはスタックの一般的なファンステータスを表示する例を示します。

```
switchxxxxxx> show environment fan
fans OK
#EDITOR: The fan status is OK if the fan sensors status in ALL the stack members is OK
```

例 4：次に、デバイスまたはスタックの温度ステータスを表示する例を示します。

```
switchxxxxxx> show environment temperature status
TEMPERATURE level is Warning
```

例 5：次に、デバイスまたはスタックの一般的な環境ステータスの詳細を表示する例を示します。

```
switchxxxxxx> show environment stack
Unit           fan Status
---            ----------
1              OK
2              Failure
3              Read fan fail
4              NA
#EDITOR: * fan Direction column will be printed only in SKUs which support this feature,
 or in a stack when one of the units might support this feature.
Unit           Sensor      Temperature
               Status       Level
---            ----------   --------------
1              OK             warning
2              Failure        NA
3              NA             NA
4              OK             OK
```

show inventory

製品インベントリリストを表示するには、**show inventory** ユーザ EXEC モードコマンドを使用します。

構文

show inventory [*entity*]

パラメータ

entity：表示するエンティティを指定します。スタック内の特定のユニット番号の番号（1 ～ 4）またはインターフェイス（イーサネット）名を指定できます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

デバイス、スタック内のユニット、および接続されているエンティティ（SFPなど）に関するインベントリ情報を取得して表示するには、**show inventory** コマンドを使用します。

エンティティを指定していない場合、コマンドはスタック内のすべてのユニットと接続されているすべてのエンティティの情報を表示します。

指定したエンティティがインターフェイス（イーサネット）名で、SFPがポートに挿入されていない場合、NAME & DESCR フィールドのみが表示され、DESCR は「No SFP Inserted」になります。

例

例 1：次に、スタンドアロン システム内のすべてのエンティティを表示する例を示します。

```
switchxxxxxx>  show inventory
NAME: "1", DESCR: "48-Port Gigabit with 4-Port 10-Gigabit Managed Switch"
PID: xx350-4x-K9, VID: V01, SN: 123456789
```

例 2：次に、スタンドアロン システム内の特定のエンティティを表示する例を示します。

```
switchxxxxxx> show inventory gigabitethernet1/0/49
NAME: "GigabitEthernet1/0/49", DESCR: "1000M base-LX Mini-GBIC SFP Transceiver"
PID: MGBLX1,VID: V01, SN: AGC1525UR7G
```

例 3：次に、VID 情報を SFP から読み取ることができない特定のエンティティの情報を表示します。

```
switchxxxxxx> show inventory gi1/0/1
NAME: "gi1/0/1", DESCR: "SFP-1000Base-LX"
PID: SFP-1000-LX ,VID: Information Unavailable , SN: 613bbgr8
```

例 4：次に、SFP がインターフェイスに挿入されていない特定のインターフェイスの情報を表示します。

```
switchxxxxxx> show inventory gi1/0/2
NAME: "gi1/0/2", DESCR: "SFP not inserted"
```

例 5：次に、ユニットが 2 つのスタック構成システムのすべてのエンティティを表示する例を示します。

```
switchxxxxxx> show inventory
NAME: "2", DESCR: "48-Port Gigabit with 4-Port 10-Gigabit Managed Switch"
PID: xx350-4x-K9 , VID: V01, SN: 123456789
NAME: "GigabitEthernet2/0/49", DESCR: "1000M base-LX Mini-GBIC SFP Transceiver"
PID: MGBLX1,  VID: V01, SN: AGC1525UR7G
NAME: "4", DESCR: "48-Port Gigabit with 4-Port 10-Gigabit Managed Switch"
PID: xx350-4x-K9 , VID: V01, SN: 123456789
```

例 6：次に、スタックのユニット 1 の情報を表示する例を示します。

```
switchxxxxxx> show inventory 1
NAME: "1"  DESCR: "48-Port Gigabit with 4-Port 10-Gigabit Managed Switch"
PID: xx350-4x-K9  VID:  V02  SN: 402
```

show platform certificate

アクティブなユニットのSUDI証明書またはAIK証明書と、任意でその証明書の署名を表示するには、show platform certificate 特権 EXEC モード コマンドを使用します。

構文

show platform {sudi | attestation} certificate [sign [nonce <nonce value>]]

パラメータ

- {**sudi | attestation**}：SUDI または構成証明（AIK：構成証明アイデンティティキー）証明書を表示します。
- **sign**：（オプション）証明書の署名を表示します。
- [**nonce** <nonce value>]：（オプション）リプレイアタックから保護するために署名で使用するナンスを指定します。（範囲：0 ～ 4,294,967,295）

デフォルトの使用

証明書は署名なしで表示されます。signパラメータをナンス値なしで指定した場合、署名はナンスを使用せずに生成されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

show platform certificate コマンドは、デバイスのSUDIまたはAIK（構成証明アイデンティティキー）証明書を表示します。

コマンド出力には、PEM形式の証明書チェーンが含まれます。表示される最初の証明書はCisco Root CA で、2 番目はシスコが https://www.cisco.com/security/pki/ で公開する証明書です。3 番目の証明書は、SUDI または AIK リーフ証明書です。

オプションの sign パラメータを使用すると、SUDI（sudi キーワードが使用されている場合）またはAIK（構成証明キーワードが使用されている場合）の秘密キーを使用して、コマンド出力に証明書の署名が表示されます。

コマンドは、リプレイアタックを防ぐために書名入力の一部として使用されるオプションの [nonce <nonce value>] パラメータもサポートしています。[nonce <nonce value>] パラメータが指定されていない場合、署名されたデータにナンスは含まれません。

コマンド出力には、署名バージョンが含まれます。署名値 1 は、SUDI 秘密キーが署名に使用されたことを示し、署名値 2 は AIK 秘密キーが署名に使用されたことを示します。

例

例 1：次の例では、SUDI 証明書チェーンが書名なしで表示されます。

```
switchxxxxxx> show platform sudi certificate
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODA5
MjA1ODI4WhgPMjA5OTA4MDkyMDU4MjhaMC0xDjAMBgNVBAoTBUNpc2NvMRswGQYD
VQQDExJDaXNjbyBSb290IENBIDIwOTkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDTtuM1fg0+9Gflik4axlCK1I2fb3ESCL8+tk8kOXlhfrJ/zlfRbe60
xRP0iUGMKWKBj0IvvWFf4AW/nyzCR8ujTt4a11Eb55SAKXbXYQ7L4YMg+lmZmg/I
v3GJEc3HCYU0BsY8g9LuLMvqwiNmAwM2jWzNq0EPArt/F6RiQKq6Ta3e7VIfDZ7J
65OA2xASA2FrSe9Vj97KpQReDcm6G7cqFH5f+CrdQ4qwAa4zWNyM3kOpUb637DNd
9m+n6WECyc/IUD+2e+yp21kBZIKH7JvDpu2U7NBPfr52mFX8AfCZgkXV69bp+iYf
saH1DvXIfPpNp93zGKUSXxEj4w881t2zAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQ4lVcPNCNO86EmILoUkcdBiB2j
WzANBgkqhkiG9w0BAQsFAAOCAQEAjeKZo+4xd05TFtq99nKnWA0J+DmydBOnPMwY
lDrKfBKe2wVu5AJMvRjgJIoY/CHVPaCOWH58UTqfji95eUaryQ/s36RKrBgMMlwr
WNItxE625PHuaN6EjD1WdWiRMZ2hy8F4FCKz5hgUEvN+PUNZwsPnpU6q3Ay0+11T
4TriwCV8kJx3cWu0NvTypYCCXMscSfLFQR13bo+1z6XNm30SecmrxkmQBVMqjCZM
VvAxhxW1iGnYdPRQuNqt0xITzCSERqg3QVVqYnFJUkNVN6j0dmmMVKZh17HgqLnF
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEZzCCA0+gAwIBAgIJCmR1UkzYYXxiMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODEx
MjAyODA4WhgPMjA5OTA4MDkyMDU4MjdaMDExHzAdBgNVBAMTFkhpZ2ggQXNzdXJh
bmNlIFNVREkgQ0ExDjAMBgNVBAoTBUNpc2NvMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAvdzeSWdDI6lRZDYRvA6JqaRvQyy6Dx1WaqI82UeKR4ZRn0ef
xMGvp4c88/VMS8WSjQO1qolMfMxqHkcSiFBOULx6Trquw4TrEf9sIuzvgJvDaEa8
IllXPwtPtNqZEIWi8jlinz2uGam93KuGPcioHfruzbDKWHL/HWFGYMgz+OKwhD3J
4NRySknQvUovfV8eWLeVOqW8rbnG3TZxv5VexOiK4jL3ObvsQPuAWUwUoo7nuFlE
GTG/VCeyCe/H8+afIScbZOkI9xejtckflnBYFVCyFxzm2H3YZatb6ohbyRXLtOPj
T3SJ+OOoYMlSLd28z727LpRbFFLGYhyWxEXDuQIDAQABo4IBgjCCAX4wDgYDVR0P
AQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwfwYIKwYBBQUHAQEEczBxMEEG
CCsGAQUFBzAChjVodHRwczovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2Nl
cnRzL2NyY2EyMDk5LmNlcjAsBggrBgEFBQcwAYYgaHR0cDovL3BraWN2cy5jaXNj
by5jb20vcGtpL29jc3AwHwYDVR0jBBgwFoAUOJVXDzQjTvOhJiC6FJHHQYgdo1sw
UgYDVR0gBEswSTBHBgorBgEEAQkVAR4AMDkwNwYIKwYBBQUHAgEWK2h0dHA6Ly93
d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9wb2xpY2llcy8wQwYDVR0fBDwwOjA4
oDagNIYyaHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2NybC9jcmNh
MjA5OS5jcmwwHQYDVR0OBBYEFOpro7nBE5d+G/s6jWhgBzlfh0j6MA0GCSqGSIb3
DQEBCwUAA4IBAQBcqYEOgAHhGWKndwM901XX2Enh4hjXR5avDg7G/f6Tb9H509dt
QW+AeZGEghhwUrw1EeG79tHkncAe+m+64xMC1ttyI1RSyn8rBqQYkXnnCRbtF/Nw
pQe5fjvdeIFWJhUI16TOt/ZlkNnWnLsUU1alZmN+J/FhSr8VTJWGRM9gY8hefH8f
5U7LMiDXxsFVHB7R6KGNjvtawrl6W6RKp2dceGxEIIvMahgMWWHHiWOQAOtVrHuE
NEjYR/7klLLwdgQF/NNCA2z47pSfMFnBcr8779GqVIbBTpOP2E6+1pBrE2jBNNoc
uBG1fgvh1qtJUdBbTziAKNoCo4sted6PW2/U
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEITCCAwmgAwIBAgIKBgEgAwc2RDFGxTANBgkqhkiG9w0BAQsFADAxMR8wHQYD
VQQDExZIaWdoIEFzc3VyYW5jZSBTVURJIENBMQ4wDAYDVQQKEwVDaXNjbzAgFw0y
MjA4MDExMDEwMDhaGA8yMDk5MDgwOTIwNTgyNlowYjEoMCYGA1UEBRMfUElEOkMx
MjAwLTE2UC0yRyBTTjpEVFkyNjMxMDAxNTEOMAwGA1UEChMFQ2lzY28xETAPBgNV
BAsTCFRQTSBTVURJMRMwEQYDVQQDEwpMSUdIVFNBQkVSMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxHlUxYHK+BoQ3N7sL2u0Tgc3aJuJGnfJbrMHtow3
S8EmyyebeZpdWbfpn/zFH8TC3J9cr1NA4EvYi1Qli9ioSuBlLTjDujhAIPVqZnmy
cEDjDG0QI2xPYz+nL83ULkYWWTejarfz4jIPYb9po1veMavEqcEtBQHmPAlbzZyL
adRSrj32ph+XlnZ8BKU1BzXq52zcXsz2fICd0evw4O9f2LOMTvzMkn/i8dLx4gy1
oP95/EgJLgTydtpZyuA8TG9fy23qrWdJJzM+ZS+6cYrl20Eu7j5t5oN3IfAYxMwk
1MRaR+Ft5QWgK/ZBvAd3emelLB7K48h/nxKBLrtD6aobiQIDAQABo4IBBjCCAQIw
DgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgwFoAU6mujucET
l34b+zqNaGAHOV+HSPowgaEGA1UdEQSBmTCBlqBQBgorBgEEAQkVAwQCoEITQDFG
```

```
OTlBMDQ5Qzk1MjgxRjU1RjhBNjhBNzJFMjA0OURCQzgyOTAwNjREMjUzMjdEMUI3
RDkzQ0IxNDc3MzdBMTmgQgYJKwYBBAEJFQIDoDUTM0NoaXBJRD1Vd01DQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQkh3PTAdBgNVHQ4EFgQUDyWO
Gy2I7j1nREZxpDmwbA5+hcQwDQYJKoZIhvcNAQELBQADggEBAA2KBFfaQf5kFaMJ
DJtGTyMNfu0hYjELDCwMK04iepo1w8bg9Rlb25LXYX+Rkk1/ZlIo3wLmRYNIddow
NQbJwt8Ch27kYyjnHcBWgz/M/DWOfKgEpNlS/Lw3ssLiAN67Y4dqUycUq7QVwG/I
zHO8oMu4sWjarkpiMTibJbw6w5PbJhd8meHoaJA1AV0pNKASvsIKoCZI1cRP/RFZ
dnRMM9LQUqeVob9hn5WRQ5PrweuALXMkUpmqeHsxSxa0M9w2u7dDYq/oeGZuUk93
9JaBqW4nwZ50MkwK9qLzYFzR5HD+YfJup22DoSdXZhO+gz4MzVCqDp5zsEyDPZl6
XLN5ZZ4=
-----END CERTIFICATE-----
```

例 2：次の例では、SUDI 証明書チェーンが 12345 のナンスを使用して証明書の署名付きで表示されます。

```
switchxxxxxx> show platform sudi certificate sign nonce 12345
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODA5
MjA1ODI4WhgPMjA5OTA4MDkyMDU4MjhaMC0xDjAMBgNVBAoTBUNpc2NvMRswGQYD
VQQDExJDaXNjbyBSb290IENBIDIwOTkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDTtuM1fg0+9Gflik4axlCK1I2fb3ESCL8+tk8kOXlhfrJ/zlfRbe60
xRP0iUGMKWKBj0IvvWFf4AW/nyzCR8ujTt4a11Eb55SAKXbXYQ7L4YMg+lmZmg/I
v3GJEc3HCYU0BsY8g9LuLMvqwiNmAwM2jWzNq0EPArt/F6RiQKq6Ta3e7VIfDZ7J
65OA2xASA2FrSe9Vj97KpQReDcm6G7cqFH5f+CrdQ4qwAa4zWNyM3kOpUb637DNd
9m+n6WECyc/IUD+2e+yp21kBZIKH7JvDpu2U7NBPfr52mFX8AfCZgkXV69bp+iYf
saH1DvXIfPpNp93zGKUSXxEj4w881t2zAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQ4lVcPNCNO86EmILoUkcdBiB2j
WzANBgkqhkiG9w0BAQsFAAOCAQEAjeKZo+4xd05TFtq99nKnWA0J+DmydBOnPMwY
lDrKfBKe2wVu5AJMvRjgJIoY/CHVPaCOWH58UTqfji95eUaryQ/s36RKrBgMMlwr
WNItxE625PHuaN6EjD1WdWiRMZ2hy8F4FCKz5hgUEvN+PUNZwsPnpU6q3Ay0+11T
4TriwCV8kJx3cWu0NvTypYCCXMscSfLFQR13bo+1z6XNm30SecmrxkmQBVMqjCZM
VvAxhxW1iGnYdPRQuNqt0xITzCSERqg3QVVqYnFJUkNVN6j0dmmMVKZh17HgqLnF
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEZzCCA0+gAwIBAgIJCmR1UkzYYXxiMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODEx
MjAyODA4WhgPMjA5OTA4MDkyMDU4MjdaMDExHzAdBgNVBAMTFkhpZ2ggQXNzdXJh
bmNlIFNVREkgQ0ExDjAMBgNVBAoTBUNpc2NvMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAvdzeSWdDI6lRZDYRvA6JqaRvQyy6Dx1WaqI82UeKR4ZRn0ef
xMGvp4c88/VMS8WSjQO1qolMfMxqHkcSiFBOULx6Trquw4TrEf9sIuzvgJvDaEa8
IllXPwtPtNqZEIWi8jlinz2uGam93KuGPcioHfruzbDKWHL/HWFGYMgz+OKwhD3J
4NRySknQvUovfV8eWLeVOqW8rbnG3TZxv5VexOiK4jL3ObvsQPuAWUwUoo7nuFlE
GTG/VCeyCe/H8+afIScbZOkI9xejtckflnBYFVCyFxzm2H3YZatb6ohbyRXLtOPj
T3SJ+OOoYMlSLd28z727LpRbFFLGYhyWxEXDuQIDAQABo4IBgjCCAX4wDgYDVR0P
AQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwfwYIKwYBBQUHAQEEczBxMEEG
CCsGAQUFBzAChjVodHRwczovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2Nl
cnRzL2NyY2EyMDk5LmNlcjAsBggrBgEFBQcwAYYgaHR0cDovL3BraWN2cy5jaXNj
by5jb20vcGtpL29jc3AwHwYDVR0jBBgwFoAUOJVXDzQjTvOhJiC6FJHHQYgdo1sw
UgYDVR0gBEswSTBHBgorBgEEAQkVAR4AMDkwNwYIKwYBBQUHAgEWK2h0dHA6Ly93
d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9wb2xpY2llcy8wQwYDVR0fBDwwOjA4
oDagNIYyaHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2NybC9jcmNh
MjA5OS5jcmwwHQYDVR0OBBYEFOpro7nBE5d+G/s6jWhgBzlfh0j6MA0GCSqGSIb3
DQEBCwUAA4IBAQBcqYEOgAHhGWKndwM901XX2Enh4hjXR5avDg7G/f6Tb9H509dt
QW+AeZGEghhwUrw1EeG79tHkncAe+m+64xMC1ttyI1RSyn8rBqQYkXnnCRbtF/Nw
pQe5fjvdeIFWJhUI16TOt/ZlkNnWnLsUU1alZmN+J/FhSr8VTJWGRM9gY8hefH8f
5U7LMiDXxsFVHB7R6KGNjvtawrl6W6RKp2dceGxEIIvMahgMWWHHiWOQAOtVrHuE
NEjYR/7klLLwdgQF/NNCA2z47pSfMFnBcr8779GqVIbBTpOP2E6+1pBrE2jBNNoc
uBG1fgvh1qtJUdBbTziAKNoCo4sted6PW2/U
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEITCCAwmgAwIBAgIKBgEgAwc2RDFGxTANBgkqhkiG9w0BAQsFADAxMR8wHQYD
VQQDExZIaWdoIEFzc3VyYW5jZSBTVURJIENBMQ4wDAYDVQQKEwVDaXNjbzAgFw0y
```

```
MjA4MDExMDEwMDhaGA8yMDk5MDgwOTIwNTgyNlowYjEoMCYGA1UEBRMfUElEOkMx
MjAwLTE2UC0yRyBTTjpEVFkyNjMxMDAxNTEOMAwGA1UEChMFQ2lzY28xETAPBgNV
BAsTCFRQTSBTVURJMRMwEQYDVQQDEwpMSUdIVFNBQkVSMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxHlUxYHK+BoQ3N7sL2u0Tgc3aJuJGnfJbrMHtow3
S8EmyyebeZpdWbfpn/zFH8TC3J9cr1NA4EvYi1Qli9ioSuBlLTjDujhAIPVqZnmy
cEDjDG0QI2xPYz+nL83ULkYWWTejarfz4jIPYb9po1veMavEqcEtBQHmPAlbzZyL
adRSrj32ph+XlnZ8BKU1BzXq52zcXsz2fICd0evw4O9f2LOMTvzMkn/i8dLx4gy1
oP95/EgJLgTydtpZyuA8TG9fy23qrWdJJzM+ZS+6cYrl20Eu7j5t5oN3IfAYxMwk
1MRaR+Ft5QWgK/ZBvAd3emelLB7K48h/nxKBLrtD6aobiQIDAQABo4IBBjCCAQIw
DgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgwFoAU6mujucET
l34b+zqNaGAHOV+HSPowgaEGA1UdEQSBmTCBlqBQBgorBgEEAQkVAwQCoEITQDFG
OTlBMDQ5Qzk1MjgxRjU1RjhBNjhBNzJFMjA0OURCQzgyOTAwNjREMjUzMjdEMUI3
RDkzQ0IxNDc3MzdBMTmgQgYJKwYBBAEJFQIDoDUTM0NoaXBJRD1Vd0lDQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQkh3PTAdBgNVHQ4EFgQUDyWO
Gy2I7j1nREZxpDmwbA5+hcQwDQYJKoZIhvcNAQELBQADggEBAA2KBFfaQf5kFaMJ
DJtGTyMNfu0hYjELDCwMK04iepo1w8bg9Rlb25LXYX+Rkk1/ZlIo3wLmRYNIddow
NQbJwt8Ch27kYyjnHcBWgz/M/DWOfKgEpNlS/Lw3ssLiAN67Y4dqUycUq7QVwG/I
zHO8oMu4sWjarkpiMTibJbw6w5PbJhd8meHoaJA1AV0pNKASvsIKoCZI1cRP/RFZ
dnRMM9LQUqeVob9hn5WRQ5PrweuALXMkUpmqeHsxSxa0M9w2u7dDYq/oeGZuUk93
9JaBqW4nwZ50MkwK9qLzYFzR5HD+YfJup22DoSdXZhO+gz4MzVCqDp5zsEyDPZl6
XLN5ZZ4=
-----END CERTIFICATE-----
Signature version: 1
Signature:
6ca45d415eace3b6cc09d84026dfcb4d1fbf614c319d3d28a3b924f6f432b26254aeca9c22aa150c
cfadd78bf2c4326d89f863eb52893e2cf3b9ddcd6d1f8ff00ea5830eec1281446c5ab5c92eee0030
6d25a1c75a6b0deaf9fee88b2b62d5e341bbe2fdbfb4cf4b5720d74f4e63f16c2012baadb5251a9d
bc871c4977335b8152715a95b48003d139e9e7e19fb7aa84f62e1a8c0e007a15f2a312c839b96170
e05e58a0e0f9ee78a28ffc9ddeb73fc7fdde0cbb556fa17aeb0d984bb4afa435fe40599de1c222bd
d132112ecb23ea1ca7ea78b40b2fb39d04867c05b0a7965e2180ba79688da06864be541f4956db96
3e48ad26f817bb56465f11e5ff89e128
```

例 3：次の例では、構成証明（AIK）証明書チェーンが 67890 のナンスを使用して証明書の署名付きで表示されます。

```
switchxxxxxx> show platform attestation certificate sign nonce 67890
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODA5
MjA1ODI4WhgPMjA5OTA4MDkyMDU4MjhaMC0xDjAMBgNVBAoTBUNpc2NvMRswGQYD
VQQDExJDaXNjbyBSb290IENBIDIwOTkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDTtuM1fg0+9Gflik4axlCK1I2fb3ESCL8+tk8kOXlhfrJ/zlfRbe60
xRP0iUGMKWKBj0IvvWFf4AW/nyzCR8ujTt4a11Eb55SAKXbXYQ7L4YMg+lmZmg/I
v3GJEc3HCYU0BsY8g9LuLMvqwiNmAwM2jWzNq0EPArt/F6RiQKq6Ta3e7VIfDZ7J
65OA2xASA2FrSe9Vj97KpQReDcm6G7cqFH5f+CrdQ4qwAa4zWNyM3kOpUb637DNd
9m+n6WECyc/IUD+2e+yp21kBZIKH7JvDpu2U7NBPfr52mFX8AfCZgkXV69bp+iYf
saH1DvXIfPpNp93zGKUSXxEj4w881t2zAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQ4lVcPNCNO86EmILoUkcdBiB2j
WzANBgkqhkiG9w0BAQsFAAOCAQEAjeKZo+4xd05TFtq99nKnWA0J+DmydBOnPMwY
lDrKfBKe2wVu5AJMvRjgJIoY/CHVPaCOWH58UTqfji95eUaryQ/s36RKrBgMMlwr
WNItxE625PHuaN6EjD1WdWiRMZ2hy8F4FCKz5hgUEvN+PUNZwsPnpU6q3Ay0+11T
4TriwCV8kJx3cWu0NvTypYCCXMscSfLFQR13bo+1z6XNm30Secmrxkm QBVMqjCZM
VvAxhxW1iGnYdPRQuNqt0xITzCSERqg3QVVqYnFJUkNVN6j0dmmMVKZh17HgqLnF
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEXzCCA0egAwIBAgIJCsCKA1bCuHJDMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODEx
MjAzMjQyWhgPMjA5OTA4MDkyMDU4MjdaMCkxFzAVBgNVBAMTDkF0dGVzdGF0aW9u
IENBMQ4wDAYDVQQKEwVDaXNjbzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAPH9/H1Cno5OxJ7xqpZZmnnfuuHKhhXQTjz6dUkjmbJmUXsFHMCNikbkLgTj
qgsbSfeOG0kVFAJCC2XkMsWgjuLV8laHXAY/tRWrgyHJ7RkqqUTh7ZLmhNFPxQaj
DdaqaPDNyKplgl8KhXwF+n1n4PQuH45dUE3Tp4P80AVZ4fNmow5n409ZIpcjOYfS
iLiQ8fID9hhY3GAVh5ugfLbLKhojCojCNgT+gzR4IM6amzHku1Ysuf7mUFd8vJtd
```

```
AWekGtr1XUB2gJ72vXwqV0lf4uFw7GHO+hREqogRLhtF/7uH6CoVO/fmcUFYIT+C
MSKzxJAbeITSd13WCNzSXYiXrTMCAwEAAaOCAYIwggF+MA4GA1UdDwEB/wQEAwIB
BjASBgNVHRMBAf8ECDAGAQH/AgEAMH8GCCsGAQUFBwEBBHMwcTBBBggrBgEFBQcw
AoY1aHR0cHM6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9jcmNh
MjA5OS5jZXIwLAYIKwYBBQUHMAGGIGh0dHA6Ly9wa2ljdnMuY2lzY28uY29tL3Br
aS9vY3NwMB8GA1UdIwQYMBaAFDiVVw80I07zoSYguhSRx0GIHaNbMFIGA1UdIARL
MEkwRwYKKwYBBAEJFQEcADA5MDcGCCsGAQUFBwIBFitodHRwOi8vd3d3LmNpc2Nv
LmNvbS9zZWN1cml0eS9wa2kvcG9saWNpZXMvMEMGA1UdHwQ8MDowOKA2oDSGMmh0
dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jcmwvY3JjYTIwOTkuY3Js
MB0GA1UdDgQWBBQAHroP19nnPZCyDOSo7cfzLETspjANBgkqhkiG9w0BAQsFAAOC
AQEAhyXlbLYZRW6CxRvVobb4Gvt8HFHKCaqx0yPbnDAjktzq3/yrb6TevdITFt2U
VZjO78/yJRACGffz8dlaBnVp8LEMcBZTzs2tvP6gkjgptqC+FFV0+8lCdxzoeRx6
vaVgpd9CPbpfLRp4wewp/phXonRshNxWXdVgk2lK/o3njguc/5jI5SPzejFMMJOF
ZgrExhmcKRDVap9fJi/JOizO+1Qwp9hPEthBElv9UksA4NKEdiwNjTOhPB6GU7wU
XrSFE5Svf5YVAPxKl0Gkw5ulSTiWM7UsnS1RaXfBPqrsR1SlzIQQlr4B85EzTBuK
HvlCRCEPQZcg3CItn3b8UtPLLQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEGTCCAwGgAwIBAgIKA4Nld5RVSDU2ozANBgkqhkiG9w0BAQsFADApMRcwFQYD
VQQDEw5BdHRlc3RhdGlvbiBDQTEOMAwGA1UEChMFQ2lzY28wIBcNMjIwODAxMTAx
MDA4WhgPMjA5OTA4MDkyMDU4MjZaMGIxKDAmBgNVBAUTH1BJRDpDMTIwMC0xNlAt
MkcgU046RFRZMjYzMTAwMTUxDjAMBgNVBAoTBUNpc2NvMREwDwYDVQQLEwhUUE0g
U1VESTETMBEGA1UEAxMKTElHSFRTQUJFUjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAJtUHXzPGFhzrlJ251GUrGuL8Ek3axTdrurLqzNslvkx5Ystp2VM
Q5qDua2ovRcESrSxTfNMwUDm9+FX8EipsxgIRX5+oZZ8ka8oNVEKyTPyB5upl7Xi
9G15wvVBUHceVERCX33LqV2wHiA2hMdsgDsSeGlJteQi3zjeokXeojW9MDyJsMTp
CBQHCGNS+GgKXSqMt3k54K8S3RSi/P/R/oPKoA0z2ZUsu9/bOHTAwX/ZGMJ8U48X
C93adaOef1J0grt5scL073jZ1SbI4NS2ind8DGS2f059pdKHZvCetNJMcGugnapx
S6jOkf4qiTVSpbuEos8VDMgubaWf7KUUSB8CAwEAAaOCAQYwggECMA4GA1UdDwEB
/wQEAwIF4DAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFAAeug/X2ec9kLIM5Kjt
x/MsROymMIGhBgNVHREEgZkwgZagUAYKKwYBBAEJFQMEAqBCE0AxRjk5QTA0OUM5
NTI4MUY1NUY4QTY4QTcyRTIwNDlEQkM4MjkwMDY0RDI1MzI3RDFCN0Q5M0NCMTQ3
NzM3QTE5oEIGCSsGAQQBCRUCA6A1EzNDaGlwSUQ9VXdJQ0FBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUJIdz0wHQYDVR0OBBYEFC2RwVIJl3l6EDvF
+2jc19Vq6mIdMA0GCSqGSIb3DQEBCwUAA4IBAQB0U1fS7UQaHdkhB/X44U+fOt0U
1wW/L5yPuDc7zWGHcxFkdZBP+4e4M491dKI8B0ULdFhZThHNf/WeQ2c9TftPc0kI
f3gqo9ez7oBlM/2Y1luG0D3WigAyZjonqmW3/tikYiVKGs7eGGylO22S9y5jXxjz
qqtz5LU+S9d18NGtKD1rYhA12ZZ9ikUhBUPDpbG0JanGaYOLpwVl7wkynYnI5bhn
gjAylgV5RqBRN6luvDWTN02LvXCKYChSMJxH8VN8d75D68qg/XcL0zcTUVViENsi
grZkZxpqU3cRJqSUVBsPXSSKhgryuVv0wcZcMAU1Bg7elM67bTzet+d1YvWH
-----END CERTIFICATE-----
Signature version: 2
Signature:
33bf4ff78bf66930494bc2376244e9b022931b7c0519a5d123e5571287a5b1ddcc4b90a80870d263
ec9f5a38b9f4c44973527b4ddcb6c8d515e64c9862362884671fff7e1e279fa6d1d8b3d81604930a
0a94b6ba8f6224ce6b60172b105ced211120528af39362269f0b4bbf7adcc9532e108b4035d2d139
62ffd5792ac1565f7e04932938b942e90ca9aefb8bf4a3cd0f804494486e1b579934aac8f42a57e9
40069463151d5e01c1d5e8b8e66b4f300c05e01aadcfaf3dc0588b6e699f1367af4fcfe19bc58a21
55d02592a7fbe158558937b9c642d90c39ce9f7a8f759cc8ec230443410dd668f3a9383bc89cc546
650902fbc637f921b4a3d17007ee98bb
```

show platform hardware integrity

アクティブユニットの PCR-15（PCR：プラットフォーム コンフィギュレーション レジスタ）の内容を含むチップ保護情報を表示し、オプションで、コマンド出力表示に含まれる PCR または PCR Quote の署名を表示するには、show platform hardware integrity 特権 EXEC モードコマンドを使用します。

構文

show platform hardware integrity [[attestation] [sign [nonce <nonce>]]]

パラメータ

- **sign**：（オプション）PCR-15 または PCR-15 Quote の署名を表示します。
- **attestation**：（オプション）構成証明（AIK）秘密キーを使用して PCR-15 Quote に署名します。attestation が指定されていない場合は、SUDI 秘密キーを使用して PCR-15 に署名します。
- [**nonce** <nonce value>]：（オプション）リプレイアタックから保護するために署名で使用するナンスを指定します。（範囲：0 ～ 4,294,967,295）

デフォルトの使用

PCR 情報は署名なしで表示されます。sign キーワードをナンス値なしで指定した場合、署名はナンスを使用せずに生成されます。attestation キーワードが指定されていない場合は、SUDI 秘密キーが PCR の署名に使用されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

show platform hardware Integrity コマンドは、オンデマンドのチップ保護構成証明を提供します。このコマンドは、アクティブユニット PCR（プラットフォーム コンフィギュレーション レジスタ）15 の内容を表示します。PCR-15 は、デバイス固有のチップ ID の拡張です。**sign** キーワードを使用した場合、コマンド出力で PCR-15 の署名が表示されます。**attestation** キーワードを使用した場合、コマンド出力には PCR Quote も含まれ、署名は見積に表示されます。

コマンドは、リプレイアタックを防ぐために書名入力の一部として使用されるオプションの [**nonce** <nonce value>] パラメータもサポートしています。[**nonce** <nonce value>] パラメータが指定されていない場合、署名されたデータにナンスは含まれません。

コマンド出力には、署名バージョンが含まれます。署名値 1 は、SUDI 秘密キーが PCR-15 の署名に使用されたことを示します。署名値 2 は、構成証明（AIK）秘密キーが PCR Quote の署名に使用されたことを示します。

例

例 1：次の例では、署名なしで PCR-15 の内容を表示します。

```
switchxxxxxx> show platform hardware integrity
PCR15: b45f34da34c6b142569f2c4f36264f3d0dfadde33f7721ed4bfd7b329ec71e6c
```

例 2：次の例では、ナンスなしの SUDI 秘密キーを使用して PCR-15 の署名付きで PCR-15 を表示します。

```
switchxxxxxx> show platform hardware integrity sign
PCR15: b45f34da34c6b142569f2c4f36264f3d0dfadde33f7721ed4bfd7b329ec71e6c
Signature Version: 1
Signature:
aba857b3c4a00191d6bc01617b5e73755810f0f4f67230e96de7a305f6882d94da9bdd2df3f12472
33f42fe0137b11971c128252e3a9813ec78d8640d87f284fc427db96b3412a07c24c78cda2242bd5
96c69ea06beb28feabfa014c48b96f420d65ffa725221319791e1f7c094acf743bbd48b7aafe088b
147894de42ca0e0634155432d8092b0ca82eb246ddb2de9a0bbd9a7914fdd7a1628dd5a29bbc4d02
9ddf846938e0b47f63bc488cf3dd2f439e684989ff39e834ac7534f5bc2187b293cfc5445af9a905
c8a3a5366fbc2cd74868912105ef4880a203772946ffae2de126cd769d111b362210bb9ce7a2af7b
f423360a90ac8dde4aacc2b47a7cc923
```

例 3：次の例では、ナンス 613 の構成証明（AIK）キーを使用して PCR-15、PCR-15 Quote、および見積の署名を表示します。

```
switchxxxxxx> show platform hardware integrity sign attestation nonce 613
PCR15: b45f34da34c6b142569f2c4f36264f3d0dfadde33f7721ed4bfd7b329ec71e6c
Signature Version: 2
Quote:
ff54434780180022000b9f2c580f14cf6f157964c1dc9fb17f8a9504b50976a120fb870831db9242
e5ac00207e5fab8920a8bbcd214d7ade666c74fc07f2aa41298ac81177dc9ba7f5af978100000000
002be9b5000000240000000001000201100000000000000001000b030080000020f508f73aab654d
716ae4a511616843ca53bdef8bb7959a26226dd4d477e7170b
Signature:
36e4f4d5fecaa820cd9dfb879b170007e35eeb2edb1ddb9736580c3bd7aefc1312e6bb946573b8ef
45b9f97084b1648c704d4e54ff6aa854e2ebd4389c880b2c060be391e14d14a411cc675fe6cde688
cf3d688570eaf5bd08b69185f7dfcbbe2a5329939096aa47b0bea5fc0f1907029789f67fbb187d88
2dc69bf24dda351fc55846be38d233d40a164f30a82482f72733c9c33decb06376527034ab19490b
fccbd8f4e108910fa0a923047f98e8c45ba9d9d8e28d134662c52d6ed5616d6fc33e40985b6c3921
644d3e53570c5bc17a7f4289cd46fb3f72a7e440720751889a2552395e9ef66ba9a6d8fe9b9a6aeb
a74e43129fa5447ad9b7158401cd9174
```

show platform integrity

アクティブユニットのブート完全性の可視性（BIV）情報を表示し、オプションで、コマンド出力表示に含まれる PCR または PCR Quote の署名を表示するには、show platform Integrity 特権 EXEC モードコマンドを使用します。

構文

show platform integrity [sign [attestation] [nonce <nonce>]]

パラメータ

- **sign**：（オプション）コマンド出力に表示される PCR または PCR Quote の署名を表示します。
- **attestation**：（オプション）構成証明（AIK）秘密キーを使用して PCR Quote に署名します。**attestation** が指定されていない場合は、SUDI 秘密キーを使用して PCR に署名します。
- [**nonce** <nonce value>]：（オプション）リプレイアタックから保護するために署名で使用するナンスを指定します。（範囲：0 ～ 4,294,967,295）

デフォルトの使用

PCR 情報は署名なしで表示されます。sign キーワードをナンス値なしで指定した場合、署名はナンスを使用せずに生成されます。attestation キーワードが指定されていない場合は、SUDI 秘密キーが PCR の署名に使用されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

show platform Integrity コマンドは、オンデマンドのブート整合性の可視性（BIV）構成証明を提供します。このコマンドは、アクティブユニットのブートローダーイメージと OS イメージのブートアップ測定値を表示します。測定値はハッシュ値として表示されます。また、コマンド出力には PCR-0 および PCR-8 の内容が表示されます。PCR-0 はブートローダー イメージ ハッシュの拡張で、PCR-8 は OS イメージハッシュの拡張です。**sign** キーワードを使用した場合、コマンド出力で PCR-0 および PCR-8 の署名が表示されます。**attestation** キーワードを使用した場合、コマンド出力には PCR Quote も含まれ、署名は見積に表示されます。

コマンドは、リプレイアタックを防ぐために書名入力の一部として使用されるオプションの [**nonce** <*nonce value*>] パラメータもサポートしています。[**nonce** <*nonce value*>] パラメータが指定されていない場合、署名されたデータにナンスは含まれません。

コマンド出力には、署名バージョンが含まれます。署名値 1 は、SUDI 秘密キーが PCR-0 および PCR-8 の署名に使用されたことを示し、署名値 2 は、構成証明（AIK）秘密キーが PCR Quote の署名に使用されたことを示します。

例

例 1：次の例では、イメージの測定値と PCR-0 および PCR-8 の内容を署名なしで表示します。

```
switchxxxxxx> show platform integrity
Platform: C1300-48P-4X
Boot Loader Version: 1.0.74
Boot Loader Hash:
810ca3abed75aec7fe3aeb5baa452e7577d2cd15970dae948368f23ee17575b2ae47701e5
OS Version: 4.0.0.76
OS Hash: 26F68EE9341A4CBB552D1A3D9B02920DF126287F12EEEADFC47BD0A8EE8B7D04
PCR0: ca153e2fddadb6af4b08721421c336d874f0a950c7f9699c1509a5fcb86017d6
PCR8: 9c26a9a7ca8033bb050df2b6974cbe0d3f17d65302feb637b40a37aff976e8b9
```

例 2：次の例では、SUDI 秘密キーとナンス値 248 を使用して、PCR-0 および PCR-8 の署名付きで、PCR-0 および PCR-8 のイメージの測定値と内容を表示します。

```
switchxxxxxx> show platform integrity sign nonce 248
Platform: C1300-48P-4X
Boot Loader Version: 1.0.74
Boot Loader Hash:
810ca3abed75aec7fe3aeb5baa452e7577d2cd15970dae948368f23ee17575b2ae47701e5
OS Version: 4.0.0.76
OS Hash: 26F68EE9341A4CBB552D1A3D9B02920DF126287F12EEEADFC47BD0A8EE8B7D04
PCR0: ca153e2fddadb6af4b08721421c336d874f0a950c7f9699c1509a5fcb86017d6
PCR8: 9c26a9a7ca8033bb050df2b6974cbe0d3f17d65302feb637b40a37aff976e8b9
Signature Version: 1
Signature:
74c2795731dad3fd9cb35310e3d3070dc666ec0ced60ad1b4586f08c18a7d6f5c82db6ac755794ca
810ca3abed75aec7fe3aeb5baa452e7577d2cd15970dae948368f23ee17575b2ae47701e5cac3d89
838696745bfbc620a95523574c6cc6128fbfcbaf86df88d5f56bda32d9f82f3b10ca8d170eac17f0
526194afd80c7880f8074de85eb81777bc94a6ef748f04737bb1ed29debb2d1c0a71074e8e4513b6
ba9253460c205cdd641bfe7976d16d13857db0115a9efd427ce0ccd86c1832b6ad3408640fec4a6f
ca40baebca3a0e2ab395774223776ebebc279e7ec7c759e949fee756f47cb6ca6c326edf68a35444
33f3ef8befcaac78b631188204191745
```

例 3：次の例では、構成証明（AIK）キーとナンス値 365 を使用して、イメージの測定値、PCR-0 と PCR-8 の内容、PCR Quote、および見積の署名を表示します。

```
switchxxxxxx> show platform integrity sign attestation nonce 365
Platform: C1300-48P-4X
Boot Loader Version: 1.0.74
Boot Loader Hash:
810ca3abed75aec7fe3aeb5baa452e7577d2cd15970dae948368f23ee17575b2ae47701e5
OS Version: 4.0.0.76
OS Hash: 26F68EE9341A4CBB552D1A3D9B02920DF126287F12EEEADFC47BD0A8EE8B7D04
PCR0: ca153e2fddadb6af4b08721421c336d874f0a950c7f9699c1509a5fcb86017d6
PCR8: 9c26a9a7ca8033bb050df2b6974cbe0d3f17d65302feb637b40a37aff976e8b9
Signature Version: 2
Quote:
ff54434780180022000b9f2c580f14cf6f157964c1dc9fb17f8a9504b50976a120fb870831db9242
e5ac000800000000000016d00000000002d085b0000002400000000010002011000000000000000
01000b0301010000200bf8a79c7d864c5556976737edc9a8e870e767d371cf6239892401f76e377e
64
Signature:
14d9b51c83185e790d6485ca76d58bfaab925ba0bc1f1a5ea4590d244b5206c69f53c84d8fc6d715
3af67ab747c7aebd3ba81bf36fbb11e45097adbcd6ec2d924496165505c52dc6a77c386156188e9e
0ce03d58cdbe1babe45141760a8b965440a82af1d3751e9f0b8e8570564c416a407fee901c175594
b7b2a556985c8df924b576f9d898e84db344af19aa724b20f5832d18c1ba2b0c501ef57670dfa643
31970179ea8415aaf2424abdf197386a8b6018c75f2346b930c982eba309aef350075812b894c2ac
36af9594d0d27b0c9aab0e6be17575ba1fc90d898cf70ed6e0a1ccdb15592b9ba8f08d6fb98f70a2
33905b820c64c08247e5ea2a81849b11
```

show reload

デバイスのステータスについて保留中のリロードがあるかどうかを表示するには、**show reload** 特権 EXEC モード コマンドを使用します。

構文

show reload

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドを使用して、保留中のソフトウェアのリロードを表示できます。保留中のリロードをキャンセルするには、このコマンドに **cancel** パラメータを指定します。

例

次の例では、リロードが 4 月 20 日土曜日 00:00 にスケジューリングされていることを表示しています。

```
switchxxxxxx> show reload
Reload scheduled for 00:00:00 UTC Sat April 20 (in 3 hours and 12 minutes)
```

show sessions

オープンしている Telnet セッションを表示するには、**show sessions** ユーザ EXEC モード コマンドを使用します。

構文

show sessions

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルトの使用

なし

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

show sessions コマンドは、ローカル デバイスへの現在の Telnet セッションによってオープンされたリモート ホストへの Telnet セッションを表示します。ローカルデバイスへの他の Telnet セッションによってオープンされたリモート ホストへの Telnet セッションは表示しません。

例

次に、オープンしている Telnet セッションを表示する例を示します。

```
switchxxxxxx> show sessions

Connection     Host              Address          Port     Byte
----------     -------------     ----------       -----    ----
1              Remote router     172.16.1.1       23       89
2              172.16.1.2        172.16.1.2       23       8
```

次の表では、上記の重要なフィールドについて説明します。

フィールド	説明
Connection	接続番号。
Host	Telnet セッションを介してデバイスが接続されるリモート ホスト。
Address	リモート ホストの IP アドレス。
Port	Telnet TCP ポート番号。

フィールド	説明
Byte	この接続でユーザに表示されるバイトのうち未読のバイトの数。

show software versions

システム ソフトウェア バージョン情報を表示するには、**show software versions** 特権 EXEC モードコマンドを使用します。

構文

show software versions [unit *unit-id***] [detailed]**

パラメータ

- **Detailed**：（オプション）BootRom ブートオン、CPLD、PoE コントローラ、OpenSSH、および OpenSSL に関連する追加のソフトウェアバージョンも表示します。

デフォルト

次のソフトウェアバージョン情報（イメージ、ブートローダー、およびカーネル）を表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

show software versions コマンドは、デバイスのイメージ、BootRom、ブートオン、ブートローダー、カーネル、および関連するソフトウェアモジュールのバージョン情報を表示します。

例

例 1：次の例では、基本的なデバイス ソフトウェア バージョン情報を表示します。

```
switchxxxxxx# show software versions
```

アクティブイメージのバージョン：	1.2.3.4
非アクティブイメージのバージョン：	5.6.7.8（再起動後にアクティブ）
カーネルのバージョン：	Linux 3.10.70
ユニット 1 のブートローダーのバージョン：	U-Boot 2013.01（2018 年 9 月 2 日 - 00:32:52）

例 2：次の例では、詳細なデバイス ソフトウェア バージョン情報を表示します。

```
switchxxxxxx# show software versions detailed
```

アクティブイメージのバージョン：	1.2.3.4
非アクティブイメージのバージョン：	5.6.7.8（再起動後にアクティブ）

カーネルのバージョン：	Linux 3.10.70
OpenSSL のバージョン：	1.1.0b
OpenSSH のバージョン：	7.3p1
BootRom のバージョン：	1.20
ブートオンのバージョン：	6.13
ブートローダーのバージョン：	U-Boot 2013.01（2018 年 9 月 2 日 - 00:32:52）
CPLD のバージョン：	9.29
PoE コントローラのバージョン：	21.190.18.3

show system

システム情報を表示するには、**show system** ユーザ EXEC モードコマンドを使用します。

構文

show system [**unit** *unit-id*]

パラメータ

unit-id：ユニット番号を指定します。（範囲：1 ～ 4）

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

システム情報を表示するには、**show system** コマンドを使用します。

システム MAC アドレスの出力には、デバイスのベース MAC アドレスが表示されます（ユーザが設定することはできません）。

システムオブジェクト ID の出力には、一意のシステムオブジェクト ID が表示されます（ユーザは設定できません）。

The *fan* output displays, per each unit, the device fan(s) status summary. The value of fail indicates that one or more of the fans is not functioning properly. To view specific status per each fan in device use the command show system fans （1468 ページ）.
The *sensor* and *temperature* output displays, per each unit, the temperature level and general status of all sensors. The value of fail for sensors indicates one ore more sensors are not functioning propery. To view per sensor status, temperature read and threshold levels, use command show system sensors （1471 ページ）.

例 1：次に、スタックのシステム情報を表示する例を示します。

```
switchxxxxxx# show system
System Description:                     C1300-48P-4X
System Up Time (days,hour:min:sec):     03,02:27:46
System Contact:
System Name:                            switch151400
System Location:
System MAC Address:                     00:24:ab:15:14:00
System Object ID:                          1.3.6.1.4.1.9.6.1.1006.48.5
Unit        Type
---- -----------------
1          C1300-48P-4X
2          C1300-48P-4X
Unit Fans Status
---- -----------
1        OK
2        fail
Unit     Sensor Status             Temperature Level
---- -------------------- -------------------------
1             OK                    Warning
2             Fail                  Warning
```

例 2：次に、スタック内のユニット 2 のシステム情報を表示する例を示します。

```
switchxxxxxx# show system unit 2
System Description:                          xxxx
System Up Time (days,hour:min:sec):  08,23:03:46
System Contact:
System Name:
System Location:
System MAC Address:                  00:99:88:66:33:33
System Object ID:                    1.3.6.1.4.1.674.10895.3031
Fans Status:                           OK
#Editor: For systems with no temperature sensors, the temperature in the following line
 will be blank and the Status will be N/A
Unit    Sensor Status              Temperature Level
----   ---------------------    -------------------------
2             Fail                    Critical
```

show system languages

サポートされている言語のリストを表示するには、**show system languages** ユーザ EXEC モードコマンドを使用します。

構文

show system languages

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルトの使用

なし

コマンド モード

ユーザ EXEC モード

例

次に、デバイスに設定された言語を表示する例を示します。Number of Sections は、デバイスで許可されている言語の数を示します。

```
switchxxxxxx> show system languages
 Language Name   Unicode Name   Code
--------------- -------------- ------
    English         English     en-US
   Japanese       µùÑµ£¼F¬P    ja-JP
```

show system tcam utilization

TCAM（Ternary Content Addressable Memory）使用率を表示するには、**show system tcam utilization** EXEC モード コマンドを使用します。

構文

show system tcam utilization[***unit*** *unit-id*]

パラメータ

unit-id：（オプション）ユニット番号を指定します。（範囲：1 ～ **4**）

デフォルトの使用

なし

コマンド モード

ユーザ EXEC モード

例

次の例では、TCAM 使用率情報が表示されています。

switchxxxxxx> **show system tcam utilization**

```
System: 75%
```

Unit	TCAM utilization [%]
----	--------------------
1	58
2	57

show services tcp-udp

アクティブな TCP サービスおよび UDP サービスに関する情報を表示するには、**show services tcp-udp** 特権 EXEC モード コマンドを使用します。

構文

show services tcp-udp

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

出力には、デバイスが TCP/UDP クライアントであるセッションは表示されません。

例

```
switchxxxxxx> show services tcp-udp
Type  Local IP Address     Remote IP address        Service Name      State
----- ----------------- -------------------  ------------ - -----------
TCP  All:22             SSH        LISTEN
TCP  All:23             Telnet        LISTEN
TCP  All:80             HTTP        LISTEN
TCP  All:443             HTTPS        LISTEN
TCP  172.16.1.1:23    172.16.1.18:8789         Telnet        ESTABLISHED
TCP6  All-23             Telnet        LISTEN
TCP6  fe80::200:b0ff:fe00:0-23              Telnet
  fe80::200:b0ff:fe00:0-8999                 ESTABLISHED
UDP  All:161             SNMP
UDP6 A ll-161             SNMP
```

show tech-support

問題の報告時にテクニカル アシスタンス センターに提供できるシステムと設定の情報を表示するには、**show tech-support** ユーザ EXEC モードコマンドを使用します。

構文

show tech-support [***config*** | ***memory***]

パラメータ

- **memory**：（オプション）メモリおよびプロセッサの状態データを表示します。
- **config**：（オプション）デバイスでサポートされている CLI コマンド内のスイッチの設定を表示します。

デフォルト設定

デフォルトでは、このコマンドによって、テクニカルサポートに関連する show コマンドの出力が表示されます。表示する情報のタイプを指定するには、キーワードを使用します。パラメータを指定しない場合は、すべての設定およびメモリのデータが表示されます。

コマンド タイプ

スイッチ コマンド。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

警告：ネットワーク セグメント上の単一または複数のスイッチで、複数の **show tech-support** コマンドを実行しないでください。これを行うと、STP など一部の時間依存プロトコルのスタベーションが発生する可能性があります。

コンフィギュレーション ファイルの出力の表示にかかる時間が、設定されたセッション タイムアウト時間よりも長い場合、**show tech-support** コマンドはタイムアウトすることがあります。その場合、**set logout timeout** 値に **0** を入力してアイドル セッションの自動切断を無効にするか、より長いタイムアウト値を入力します。

show tech-support コマンド出力は連続表示されるので、1 画面ずつ表示されることはありません。出力を中断するには、Esc を押します。

ユーザが **memory** キーワードを指定した場合、**show tech-support** コマンドは次の出力を表示します。

- フラッシュ情報（ディレクトリ（存在する場合）またはフラッシュ マッピング）
- コマンド **show bootvar** の出力

- バッファ情報（**print os buff** など）
- メモリ情報（**print os mem** など）
- プロセス情報（print OS tasks など）
- ソフトウェア コンポーネントのバージョン
- コマンド **show cpu utilization** の出力

show system fans

デバイスのファンのステータスを表示するには、**show system fans** ユーザ EXEC モードコマンドを使用します。

構文

show system fans [*unit-id*]

パラメータ

unit-id：（オプション）リロードするユニット番号を指定します。（範囲：1～4）。指定しない場合、すべてのユニットの情報が表示されます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

ファンごとの詳細情報を表示するには、**show system fan** コマンドを使用します。次の情報が表示されます。

- ファンごとの実際の RPM。
- ファンごとのステータス：使用可能な値は、OK、fail、read fail;

例

ハードウェアが可変ファン速度をサポートしているユニットに表示されます。

```
switchxxxxxx> show system fans
```

ユニット ID：1		
ユニット/ファン ID =========	ファンの実際の速度（RPM）=====	ファンステータス=======
1/1	6000	OK
1/2	NA	Fail
1/3	NA	Read fail
1/4	4000	OK

ユニット ID：2		
ユニット/ファン ID =========	ファンの実際の速度（RPM）=====	ファンステータス=======

2/1	8000	OK
2/2	8000	OK
2/3	8000	OK

ユニット ID：3		
ユニット/ファン ID =========	ファンの実際の速度（RPM）=====	ファンステータス=======
3/1	5000	OK
3/2	4500	OK
3/3	5000	OK

ファン速度の表示をサポートしていないデバイスの表示：

```
switchxxxxxx> show system fans
```

ユニット ID：1	
ユニット/ファン ID =========	ファンステータス=======
1/1	OK
1/2	Fail
1/3	Read fail
1/4	OK

ユニット ID：2	
ユニット/ファン ID =========	ファンステータス=======
2/1	OK
2/2	OK
2/3	OK

ユニット ID：3	
ユニット/ファン ID =========	ファンステータス=======
3/1	OK

3/2	OK
3/3	OK

show system sensors

温度センサーのステータスを表示するには、**show system sensors** ユーザ EXEC モードコマンドを使用します。

構文

show system sensors

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルトの使用

なし

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

各デバイスセンサーごとに詳細なセンサー情報を表示するには、**show systemensors** コマンドを使用します。スタック内のユニットごとに情報を表示します。

次の情報が表示されます。

- センサーステータス
- センサー温度の読み取り値
- 警告およびクリティカルなアラームしきい値（摂氏温度）
- 特定のセンサーの位置。使用可能な位置は、PP（パケットプロセッサセンサー）、PCB（プリント基板回路上にあるセンサー）、PHY（PHY センサー）、POE（Poe チップセンサー）。

例

複数のセンサーステータスを伴うスタックシステムの表示

```
switchxxxxxx> show system sensors
```

ユニット/センサー ======	センサーのステータス ======	温度（C） ==========	警告アラーム温度（C） ==========	クリティカルアラーム温度（C）	センサーの位置 ======
1/1	OK	44	50	65	PCB
1/2	Failure	NA	65	75	PP

2/1	OK	65	60	70	PHY

show system id

システムアイデンティティ情報を表示するには、**show system id** ユーザ EXEC モードコマンドを使用します。

構文

show system id [***unit*** *unit-id]*

パラメータ

unit *unit-id*：（オプション）ユニット番号または all（すべて）。指定しない場合、デフォルトでは all です。（範囲：1 ～ 4）

コマンド モード

ユーザ EXEC モード

例

次の例では、システムの識別情報を表示します。

```
switchxxxxxx> show system id
serial number 114
```

show ports leds configuration

ポートの LED が有効か無効かを表示するには、**show port leds configuration** ユーザ EXEC モードを使用します。

コマンドを使用する必要があります。

構文

show ports leds configuration

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

例 1：次に、ポートの LED が有効になっている場合に、そのステータスを表示する例を示します。

```
switchxxxxxx> show ports leds configuration
Port leds are not disabled
x
```

例 2：次の例では、ポートの LED がオフになっているときの LED のステータスを表示します。

```
switchxxxxxx> show port leds configuration
Port leds are disabled
```

show users

アクティブなユーザに関する情報を表示するには、**show users** ユーザ EXEC モードコマンドを使用します。

構文

show users

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルトの使用

なし

コマンド モード

ユーザ EXEC モード

例

次の例では、アクティブなユーザに関する情報を表示しています。

```
switchxxxxxx> show users

Username          Protocol        Location
----------        -----------     ------------
Bob               Serial          172.16.0.1
John              SSH             172.16.0.8
Robert            HTTP            172.16.1.7
Betty             Telnet          172.16.1.6
Sam
```

show hardware version

ハードウェアバージョン情報を表示するには、**show hardware version** ユーザ EXEC モードコマンドを使用します。

構文

show hardware version [**unit** *unit-id*]

パラメータ

- ***unit***：（オプション）ユニット番号を指定します。（範囲：1 ～ 4）

デフォルトの使用

ユニットが指定されていない場合は、すべてのユニットのハードウェア バージョンを示します。

コマンド モード

ユーザ EXEC モード

例

次に、ハードウェア バージョン情報を表示する例を示します。

```
switchxxxxxx> show hardware version
Unit   HW Version
----   ------------
1       1.0.0
2       1.0.0.
```

show hardware components

デバイスのハードウェアコンポーネント情報を表示するには、**show hardware components** 特権 EXEC モードコマンドを使用します。

構文

show hardware components

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

show hardware components コマンドは、パケットプロセッサ、CPU、フラッシュ、PHY、およびその他のハードウェアコンポーネントなど、デバイスのコンポーネントの情報を表示します。

コンポーネントごとに表示される情報は、そのコンポーネントで使用可能な情報によって異なります。表示される情報の例：ベンダー名、製造部品番号（MPN）、およびHWのリバージョン。

例

例 1：次の例では、デバイス ハードウェア コンポーネントに関する情報を示します。

```
switchxxxxxx# show hardware components
```

```
MAC info:
```

ユニット ID/MAC ID ----------	ベンダー -------	MPN ----	改定 ---------
1	Marvell	98DX3236	A0
2	Marvell	98DX3336	A0

```
CPU info:
```

ユニット ID --------	ベンダー --------	MPN ----
1	Marvell	88F6820（Armada ARMv7）
2	Marvell	MV78230

PHY info:			
ユニット ID/PHY ID ----------	ベンダー -------	MPN ----	改定 ---------
1	Marvell	88E1680	A0
2	Marvell	88E3222	NS
2/1	Marvell	88E3680	A0

Flash info:		
ユニット ID -------	ベンダー ------	MPN ----
1	Micron	JS28F640J3D-75（65536 キロバイト）
2	MXIC Macronix	MX30LF2G18AC-TI（65536 キロバイト）

system light

デバイスまたはスタック内の特定のユニットのネットワークポートのLEDを点灯させるには、**system light** EXEC モードコマンドを使用します。

構文

system light [***unit*** *unit-id] [**duration** seconds*]

system light stop

パラメータ

- **unit-id**：ユニット番号を指定します。または、空白のままにすると、すべての LED が点灯します。
- **duration** *seconds*：LED を点灯させる秒数。指定しない場合は、デフォルトで 60 秒に設定されます。（範囲：5 ～ 3600）
- **stop**：LED の点灯を停止します。

コマンド モード

ユーザ EXEC モード

例

次に、システム LED を 6 秒間点灯させる例を示します。

```
switchxxxxxx> system light duration 65
```

system recovery

クリティカルなしきい値に達した温度から自動的に回復するようにシステムを設定するには、**system recovery** グローバル コンフィギュレーション モード コマンドを使用します。

自動回復を無効に戻すには、このコマンドの **no** 形式を使用します。

構文

system recovery

no system recovery

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

システム回復は、デフォルトで有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# no system recovery
```

system reset-button disable

デバイスのリセットボタンのリセット機能を無効にするには、system reset-button disable グローバル コンフィギュレーション モード コマンドを使用します。リセットボタンの機能を再度有効にするには、このコマンドの no 形式を使用します。

構文

system reset-button disable

no system reset-button disable

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

デフォルトでは、デバイスのリセットボタンの機能は有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

デバイスのリセットボタンのリセット機能を無効にするには、system reset-button disable コマンドを使用します。このコマンドを適用すると、リセットボタンを押しても、デバイスがリロードを行ったり、工場出荷時のデフォルトにリセットされたりすることはありません。これは、誤ってボタンを押したためにデバイスが不要なリロードを行ったり、工場出荷時のデフォルトに設定されたりするのを防ぐのに役立ちます。このコマンドは、スタック内のすべてのユニットのリセットボタンの機能を無効にします。

リセットボタンにリロードや工場出荷時のデフォルトへのリセット以外の機能がある場合、それらの機能はこの設定の影響を受けません。

リセットボタンを再度アクティブにし、ボタンを押すことでデバイスのリロードや工場出荷時のデフォルトへのリセットができるようにするには、コマンドの no 形式を使用します。

例

```
switchxxxxxx(config)# system reset-button disable
```

TACACS+ コマンド

この章は、次の項で構成されています。

- tacacs-server host （1484 ページ）
- tacacs-server host source-interface （1486 ページ）
- tacacs-server host source-interface-ipv6 （1487 ページ）
- tacacs-server key （1488 ページ）
- tacacs-server timeout （1489 ページ）
- show tacacs （1490 ページ）
- show tacacs key （1491 ページ）

tacacs-server host

TACACS+ ホストを指定するには、**tacacs-server host** グローバル コンフィギュレーション モード コマンドを使用します。指定した TACACS+ ホストを削除するには、このコマンドの **no** 形式を使用します。

構文

tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *key-string*] [**priority** *priority*]

encrypted tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *encrypted-key-string*] [**priority** *priority*]

no tacacs-server host {*ip-address* | *hostname*}

パラメータ

- **host** ip-address：TACACS+ サーバホストの IP アドレスを指定します。IP アドレスは、IPv4、IPv6、または IPv6z アドレスを使用できます。
- **host** hostname：TACACS+ サーバホスト名を指定します。（長さ：1 ～ 158 文字、ホスト名の各部分の最大ラベル長：63 文字）。
- **single-connection**：（オプション）デバイスが通信のたびにデーモンへの TCP 接続をオープンおよびクローズするのではなく、デバイスとデーモンの間で単一のオープンされた接続を維持することを指定します。
- **port** *port-number*：（オプション）TACACS サーバの TCP ポート番号を指定します。ポート番号を 0 にすると、そのホストは認証に使用されません。（範囲：0 ～ 65535）
- **timeout** *timeout*：（オプション）タイムアウト値を秒単位で指定します。（範囲：1 ～ 30）
- **key** *key-string*：（オプション）デバイスと TACACS+ サーバ間のすべての TACACS+ 通信用の認証および暗号キーを指定します。キーは TACACS+ デーモンで使用する暗号に一致している必要があります。空の文字列を指定するには、"" と入力します。（長さ：0 ～ 128 文字）。このパラメータを省略した場合は、グローバルに定義されたキーが使用されます。
- **key** *encrypted-key-string*：（オプション）key-string と同じですが、キーは暗号化形式です。
- **priority** *priority*：（オプション）TACACS+ サーバを使用する順序を指定します。0 が最も高い優先順位になります。（範囲：0 ～ 65535）

デフォルト設定

TACACS+ ホストは指定されません。

デフォルトの **port-number** は 1812 です。

timeout を指定しないと、グローバル値（**tacacs-server timeout** コマンドで設定）が使用されます。

key-string を指定しないと、グローバル値（**tacacs-server key** コマンドで設定）が使用されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

複数の **tacacs-server host** コマンドを使用して、複数のホストを指定できます。

例

次の例では、TACACS+ ホストを指定しています。

```
switchxxxxxx(config)# tacacs-server host 172.16.1.1
```

tacacs-server host source-interface

IPv4 TACACS+ サーバとの通信に IPv4 アドレスを送信元 IPv4 アドレスとして使用する送信元インターフェイスを指定するには、**tacacs-server host source-interface** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

tacacs-server host source-interface *interface-id*

no tacacs-server host source-interface

パラメータ

- ***interface-id***：送信元インターフェイスを指定します。

デフォルト設定

送信元 IPv4 アドレスは、発信インターフェイスで定義され、ネクスト ホップ IPv4 サブネットに属する IPv4 アドレスです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスの場合は、ネクスト ホップ IPv4 サブネットに属するインターフェイス IP アドレスが適用されます。

送信元インターフェイスが発信インターフェイスでない場合は、送信元インターフェイスで定義された最小 IPv4 アドレスが適用されます。

使用可能な IPv4 送信元アドレスがない場合は、IPv4 TACACS+ サーバと通信しようとすると、SYSLOG メッセージが発行されます。

送信元インターフェイスとして OOB は定義できません。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# tacacs-server host source-interface vlan 100
```

tacacs-server host source-interface-ipv6

IPv6 TACACS+ サーバとの通信に IPv6 アドレスを送信元 IPv6 アドレスとして使用する送信元インターフェイスを指定するには、**tacacs-server host source-interface-ipv6** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

tacacs-server host source-interface-ipv6 *interface-id*

no tacacs-server host source-interface-ipv6

パラメータ

- ***interface-id***：送信元インターフェイスを指定します。

デフォルト設定

IPv6 送信元アドレスは、発信インターフェイスで定義された IPv6 アドレスであり、RFC6724 に従って選択されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

送信元インターフェイスが発信インターフェイスである場合は、送信元 IPv6 アドレスはインターフェイスで定義され、RFC 6724 に従って選択された IPv6 アドレスです。

送信元インターフェイスが発信インターフェイスでない場合は、送信元 IPv6 アドレスは送信元インターフェイス上で定義され、宛先 IPv6 アドレスの範囲と一致します。

使用できる IPv6 送信元アドレスがない場合は、IPv6 TACACS+ サーバとの通信を試行する際に SYSLOG メッセージが発行されます。

例

次の例では、VLAN 10 を 送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# tacacs-server host source-interface-ipv6 vlan 100
```

tacacs-server key

デバイスと TACACS+ デーモン間のすべての TACACS+ 通信に使用する認証暗号キーを設定するには、**tacacs-server key** グローバル コンフィギュレーション モード コマンドを使用します。キーを無効にするには、このコマンドの **no** 形式を使用します。

構文

tacacs-server key *key-string*

encrypted tacacs-server key *encrypted-key-string*

no tacacs-server key

パラメータ

- ***key-string***：デバイスと TACACS+ サーバ間のすべての TACACS+ 通信に認証および暗号キーを指定します。キーは TACACS+ デーモンで使用する暗号に一致している必要があります。（長さ：0 ～ 128 文字）
- ***encrypted-key-string***：key-string と同じですが、キーは暗号化形式です。

デフォルト設定

デフォルトのキーは空の文字列です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、すべての TACACS+ サーバの認証キーとして Enterprise を設定しています。

```
switchxxxxxx(config)# tacacs-server key enterprise
```

tacacs-server timeout

デバイスが TACACS+ サーバの応答を待機する間隔を設定するには、**tacacs-server timeout** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

tacacs-server timeout *timeout*

no tacacs-server timeout

パラメータ

- ***timeout***：タイムアウト値を秒単位で指定します。（範囲：1 ～ 30）。

デフォルト設定

デフォルトのタイムアウト値は 5 秒です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、すべての TACACS+ サーバに対してタイムアウト値を 30 に設定しています。

```
switchxxxxxx(config)# tacacs-server timeout 30
```

show tacacs

TACACS+ サーバの設定および統計情報を表示するには、**show tacacs** 特権 EXEC モード コマンドを使用します。

構文

show tacacs [*ip-address*]

パラメータ

- ***ip-address***：TACACS+ サーバ名、IPv4 アドレス、または IPv6 アドレスを指定します。

デフォルト設定

ip-address を指定しない場合は、すべての TACACS+ サーバの情報が表示されます。

コマンド モード

特権 EXEC モード

例

次に、すべての TACACS+ サーバの設定および統計情報を表示する例を示します。

```
switchxxxxxx# show tacacs
```

IP address Status Port Single Time Priority

Connection Out

--- --- --- --- --- ---

172.16.1.1 Connected 49 No Global 1

```
Global values
-------------
Time Out: 3
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10
```

show tacacs key

TACACS+ サーバの設定されたキーを表示するには、**show tacacs key** 特権 EXEC モード コマンドを使用します。

構文

show tacacs key [*ip-address*]

パラメータ

- ***ip-address***：TACACS+ サーバの名前または IP アドレスを指定します。

デフォルト設定

ip-address を指定しない場合は、すべての TACACS+ サーバの情報が表示されます。

コマンド モード

特権 EXEC モード

例

次の例では、すべての TACACS+ サーバの設定と統計情報を表示します。

```
switchxxxxxx# show tacacs key

IP address                              Key (Encrypted)
----------                              ---------------
172.16.1.1                              1238af77aaca17568f1298cced165fec
172.16.1.2                              1238af77aaca17568f12988601fcabed

Global key (Encrypted)
----------------------
1238af77aaca17568f1298bc5476ddad
```

Telnet コマンド、SSH コマンド、および Slogin コマンド

この章は、次の項で構成されています。

- ip telnet server （1494 ページ）
- ip SSH logging （1495 ページ）
- ip ssh server （1496 ページ）
- ip ssh port （1497 ページ）
- ip ssh password-auth （1498 ページ）
- ip ssh pubkey-auth （1499 ページ）
- crypto key pubkey-chain ssh （1501 ページ）
- user-key （1502 ページ）
- key-string （1503 ページ）
- show ip ssh （1505 ページ）
- show crypto key pubkey-chain ssh （1506 ページ）

ip telnet server

リモート Telnet クライアントからの接続要求を受け入れる Telnet サーバとしてデバイスを有効にするには、**ip telnet server** グローバル コンフィギュレーション モード コマンドを使用します。リモート Telnet クライアントでは、Telnet 接続を介してデバイスを設定できます。

デバイス上の Telnet サーバ機能を無効にするには、このコマンドの no 形式を使用します。

構文

ip telnet server

no ip telnet server

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

デバイスでリモート SSH クライアントとリモート Telnet クライアントの両方からの接続要求を受け入れるようにすることができます。リモート クライアントからデバイスへの接続には（Telnet ではなく）SSH を使用することを推奨します。SSH はセキュア プロトコルですが、Telnet はそうではないからです。デバイスを SSH サーバとして有効にするには、**ip ssh server** コマンドを使用します。

例

次の例では、Telnet サーバからデバイスを設定できるようにしています。

```
switchxxxxxx(config)# ip telnet server
```

ip SSH logging

SSHセッションのセットアップとシャットダウンに関連するトラップの送信を有効または無効にするには、グローバル コンフィギュレーション モードでip ssh loggingを使用します。デフォルト設定に戻すには、このコマンドのno形式を使用します。

構文

ip ssh logging [enable | disable]

no ip ssh logging

パラメータ

- **enable** ：デバイスで SSH ロギングを有効にします。
- **disable** ：デバイスで SSH ロギングを無効にします。

デフォルト設定

デフォルトでは、SSH セッションロギングは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、デバイスで SSH ロギングを有効にします。SSH ロギングは、SSH セッションのセットアップと切断の進行状況を追跡する手段です。SSHセッションのセットアップと切断の進行状況は、プロセスの一部として生成される SYSLOG メッセージを使用して追跡されます。SSH ロギングが無効になっている場合、SSHのセットアップまたは切断プロセスの一部として SYSLOG メッセージは生成されません。

例

次に、デバイスで SSH ロギングを有効にする例を示します。

```
switchxxxxxx(config)# ip ssh logging enable
```

ip ssh server

ip ssh server グローバル コンフィギュレーション モード コマンドは、デバイスを SSH サーバとして有効にし、リモート SSH クライアントからの接続要求を受け入れることができるようにします。リモート SSH クライアントでは、SSH 接続を介してデバイスを管理できます。

デバイスで SSH サーバ機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip ssh server

no ip ssh server

デフォルト設定

SSH サーバ機能はデフォルトでは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

デバイスは、SSH サーバとして、暗号キーを自動的に生成します。

新しい SSH サーバ キーを生成するには、**crypto key generate dsa** コマンドおよび **crypto key generate rsa** コマンドを使用します。

例

次の例では、デバイスを SSH サーバとして設定しています。

```
switchxxxxxx(config)# ip ssh server
```

ip ssh port

ip ssh port グローバル コンフィギュレーション モード コマンドは、SSH サーバで使用する TCP ポートを指定します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ip ssh port *port-number*

no ip ssh port

パラメータ

- ***port-number***：SSH サーバで使用する TCP ポート番号を指定します。（範囲：1ー59999）。

デフォルト設定

デフォルトの TCP ポート番号は 22 です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、TCP ポート番号 808 を SSH サーバで使用することを指定しています。

```
switchxxxxxx(config)# ip ssh port 808
```

ip ssh password-auth

受信 SSH セッションのパスワード認証を有効にするには、**ip ssh password-auth** グローバル コンフィギュレーション モード コマンドを使用します。

この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip ssh password-auth

no ip ssh password-auth

デフォルト設定

受信 SSH セッションのパスワード認証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、リモート SSH クライアントのローカル SSH サーバによるパスワード キー認証が有効になります。

ローカル SSH サーバは有効になっているすべての SSH 認証方式をアドバタイズし、リモート SSH クライアントがそれらのいずれかを選択します。

リモート SSH クライアントが公開キーによって正常に認証された後も、クライアントがデバイスへの管理アクセスを取得するためには、クライアントを引き続き AAA 認証する必要があります。

SSH 認証方式が有効でない場合、リモート SSH クライアントはデバイスに対する管理アクセスを取得する前に AAA 認証される必要があります。

例

次の例では、SSH クライアントのパスワード認証を有効にしています。

```
switchxxxxxx(config)# ip ssh password-auth
```

ip ssh pubkey-auth

受信 SSH セッションの公開キー認証を有効にするには、**ip ssh pubkey-auth** グローバル コンフィギュレーション モード コマンドを使用します。

この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip ssh pubkey-auth [**auto-login**]

no ip ssh pubkey-auth

パラメータ

- **auto-login**：デバイス管理の AAA 認証（CLI ログイン）が必要ないことを指定します。デフォルトでは、SSH 認証後、ログインが必要です。

デフォルト設定

受信 SSH セッションの公開キー認証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、リモート SSH クライアントのローカル SSH サーバによる公開キー認証が有効になります。

ローカル SSH サーバは有効になっているすべての SSH 認証方式をアドバタイズし、リモート SSH クライアントがそれらのいずれかを選択します。

リモート SSH クライアントが公開キーによって正常に認証された後も、クライアントがデバイスへの管理アクセスを取得するためには、クライアントを引き続き AAA 認証する必要があります。ただし、auto-login パラメータを指定した場合を除きます。

SSH 認証方式が有効でない場合、リモート SSH クライアントはデバイスに対する管理アクセスを取得する前に AAA 認証される必要があります。

公開キーによる SSH 認証に **auto-login** キーワードを指定した場合、SSH 認証が正常に完了し、使用された SSH の名前がローカル ユーザ データベースで検出されると、管理アクセスが付与されます。デバイス管理の AAA 認証は、ユーザに対して透過的です。ユーザ名がローカル ユーザ データベース内にない場合、ユーザは警告メッセージを受信し、SSH 認証とは関係なくデバイス管理の AAA 認証を通過する必要があります。

auto-login キーワードを指定しないと、管理アクセスは、ユーザが SSH 認証とデバイス管理の AAA 認証の両方を個別に受けて通過した場合にのみ付与されます。有効な SSH 認証方式がない場合、管理アクセスは、ユーザがデバイス管理によって AAA 認証された場合にのみ付与さ

れます。SSH 認証方式がないというのは、SSH は有効になっているものの、公開キーによる SSH 認証もパスワードも有効になっていないということです。

例

次の例では、SSH クライアントの認証を有効にしています。

```
switchxxxxxx(config)# ip ssh pubkey-auth
```

crypto key pubkey-chain ssh

crypto key pubkey-chain ssh グローバル コンフィギュレーション モード コマンドは、SSH 公開キー チェーン コンフィギュレーション モードを開始します。このモードは、SSH クライアント公開キーなどデバイスの公開キーを手動で指定する場合に使用します。

構文

crypto key pubkey-chain ssh

デフォルト設定

キーが存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、SSH クライアント公開キーを手動で指定する場合に使用します。

例

次の例では、SSH 公開キー チェーン コンフィギュレーション モードを開始して、ユーザ 'bob' に対して SSH 公開キー チェーンの RSA キー ペアを手動で設定しています。

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

user-key

user-key SSH 公開キー文字列コンフィギュレーション モード コマンドは、ユーザ名と手動で設定した SSH 公開キーを関連付けます。

SSH ユーザと関連する公開キーを削除するには、**no user-key** コマンドを使用します。

構文

user-key *username* {**rsa** | **dsa**}

no user-key *username*

パラメータ

- ***username***：リモート SSH クライアントのユーザ名を指定します。（長さ：1 ～ 48 文字）
- **rsa**：RSA キー ペアを手動で設定することを指定します。
- **dsa**：DSA キー ペアを手動で設定することを指定します。

デフォルト設定

SSH 公開キーは存在しません。

コマンド モード

SSH 公開キー文字列コンフィギュレーション モード

使用上のガイドライン

このコマンドを入力すると、ユーザに関連付けられた既存のキー（ある場合）は削除されます。このキーをユーザに設定するには、このコマンドの後に key-string コマンドを入力する必要があります。

例

次の例では、SSH 公開キー チェーン bob の SSH 公開キーを手動で設定しています。

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
```

key-string

key-string SSH 公開キーストリング コンフィギュレーション モード コマンドを使用して、SSH 公開キーを手動で指定します。

構文

key-string *[***row** key-string]

パラメータ

- **row**：SSH 公開キーを行ごとに指定します。行の最大長は、160 文字です。
- ***key-string***：UU でエンコードされた DER 形式のキーを指定します。UU エンコードされた DER 形式は、OpenSSH で使用される authorized_keys ファイルと同じ形式です。

デフォルト設定

キーが存在しません。

コマンド モード

SSH 公開キー文字列コンフィギュレーション モード

使用上のガイドライン

row パラメータを指定しない **key-string** SSH 公開キー文字列コンフィギュレーション モード コマンドは、次にどの SSH 公開キーを対話式に設定するかを指定する場合に使用します。文字を含めずに行を入力してコマンドを完了します。

key-string row SSH 公開キー文字列コンフィギュレーション モード コマンドは、SSH 公開キーを行ごとに指定する場合に使用します。各行は、**key-string row** コマンドで始める必要があります。

UU エンコードされた DER 形式は、OpenSSH で使用される authorized_keys ファイルと同じ形式です。

例

次の例では、SSH 公開キー クライアント 'bob' の公開キー文字列を入力しています。

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
```

```
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string row AAAAB3Nza
switchxxxxxx(config-keychain-key)# key-string row C1yc2
```

show ip ssh

show ip ssh 特権 EXEC モード コマンドは、SSH サーバ設定を表示します。

構文

show ip ssh

コマンド モード

特権 EXEC モード

例

次に、SSH サーバの設定を表示する例を示します。

```
switchxxxxxx# show ip ssh
SSH server enabled. Port: 22
SSH session logging is disabled
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled with auto-login.
SSH Password Authentication is enabled.
Active incoming sessions:
```

IP Address	SSH Username	Version	Cipher	Auth Code
---	---	---	---	---
172.16.0.1	John Brown	1.5	3DES	HMAC-SHA1
182.20.2.1	Bob Smith	1.5	3DES	Password

次の表に、この出力で表示される重要なフィールドの説明を示します。

フィールド	説明
IP Address	クライアント アドレス
SSH Username	ユーザ名
Version	SSH バージョン番号
Cipher	暗号化タイプ（3DES、Blowfish、RC4）
Auth Code	認証コード（HMAC MD5、HMAC SHA1）またはパスワード

show crypto key pubkey-chain ssh

show crypto key pubkey-chain ssh 特権 EXEC モード コマンドを使用すると、デバイスに保存されている SSH 公開キーが表示されます。

構文

show crypto key pubkey-chain ssh [**username** *username*] [**fingerprint** {**bubble-babble** | **hex**}]

パラメータ

- **username** *username*：リモート SSH クライアントのユーザ名を指定します。（長さ：1 ～ 48 文字）
- **fingerprint** {**bubble-babble** | **hex**}：フィンガープリントの表示形式を指定します。次の値が可能です。

  bubble-babble：フィンガープリントが Bubble Babble 形式で表示されることを指定します。

  hex：フィンガープリントを 16 進形式で表示することを指定します。

デフォルト設定

デフォルトのフィンガープリント形式は 16 進数です。

コマンド モード

特権 EXEC モード

例

次の例では、デバイスに保存されている SSH 公開キーを表示します。

```
switchxxxxxx# show crypto key pubkey-chain ssh
Username       Fingerprint
-----------    -----------------------------------------------------------
bob            9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
john           98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8
switchxxxxxx# show crypto key pubkey-chain ssh username bob
Username       Fingerprint
-----------    -----------------------------------------------------------
bob            9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
```

UDLD コマンド

この章は、次の項で構成されています。

- show udld （1508 ページ）
- udld （1511 ページ）
- udld message time （1513 ページ）
- udld port （1514 ページ）

show udld

管理および動作上の単一方向リンク検出プロトコル（UDLD）ステータスを表示するには、特権 EXEC モードで **show udld** コマンドを使用します。

構文

show udld [*interface-id*] [**neighbors**]

パラメータ

- ***interface-id***：イーサネット ポートのインターフェイス識別子。
- **neighbors**：ネイバー情報のみを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

インターフェイスID値を入力しない場合は、UDLDが有効になっているすべてのインターフェイスの管理および動作上の UDLD ステータスが表示されます。

例 1：次に、すべてのインターフェイスの UDLD 状態を表示する例を示します。出力に表示されるフィールドのほとんどは説明がなくてもわかるようになっています。説明がなくてもわからないフィールドについては、以下で定義しています。

```
switchxxxxxx# show udld
Global UDLD mode: normal
Message Time: 15 sec(default)
Interface gi1/0/1
  Port UDLD mode: aggressive
  Port Current state: Bidirectional
  Number of detected neighbors: 1
  Port Neighbor Table
    Neighbor Device ID: 1234567893
      Neighbor MAC: 00:00:01:22:33:dd
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 20 sec
      Neighbor Current State: Bidirectional
      Neighbor Expiration Time: 7 sec
    Neighbor Device ID: 1234544893
      Neighbor MAC: 00:00:01:22:33:ff
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 15 sec
      Neighbor Current State: Undetermined
      Neighbor Expiration Time: 17 sec
Interface gi1/0/2
  Port UDLD mode: normal (default)
  Port Current state: Undetermined
  Number of detected neighbors: 1
```

```
    Neighbor Device ID: 1234567753
      Neighbor MAC: 00:00:01:22:33:fe
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 15 sec
      Neighbor Current State: Undetermined
      Neighbor Expiration Time: 11 sec
Interface gi1/0/3
  Port UDLD mode: disabled
Interface gi1/0/4
  Port UDLD mode: normal (default)
  Port Current state: shutdown
Field Descriptions:
```

- **Global UDLD mode**：**udld** コマンドによって設定されたグローバル UDLD モード（通常またはアグレッシブ）。
- **Message Time**：**udld message time** コマンドによって設定されたメッセージ時間。
- **Port UDLD mode**：インターフェイス UDLD モード（通常またはアグレッシブ）。
- **Port Current state**：UDLD 動作状態：インターフェイス UDLD モード（通常またはアグレッシブ）。
  - **Disabled**：UDLD は、**udld port disable** コマンドによってポートで無効になっています。
  - **Shutdown**：UDLD はポートで有効であり、ポートの動作状態は DOWN です。
  - **Detection**：UDLD がリンクの状況を検出しています。
  - **Bidirectional**：リンクは双方向です。
  - **Undetermined**：リンク ステートは不確定です。UDLD メッセージはポートで受信されていません。
- **Neighbor Device ID**：ネイバーのデバイス ID。
- **Neighbor MAC**：ネイバーの MAC アドレス。
- **Neighbor Device Name**：ネイバーのデバイス名。
- **Neighbor Port ID**：最新の UDLD メッセージを送信したネイバーのデバイスポート ID。
- **Neighbor Message Time**：ネイバーのメッセージ時間。
- **Neighbor Current State**：ネイバーの現在の状態。

  Bidirectional：ネイバーから受信した UDLD メッセージでは、Echo TLV にスイッチのデバイス ID およびポート ID が含まれています。

  Undetermined：ネイバーから受信した UDLD メッセージでは、Echo TLV にスイッチのデバイス ID およびポート ID が含まれていません。
- **Neighbor Expiration Time**：現在のネイバー状態が期限切れになるまでの残り時間（秒単位）。

例 2：次に、ある特定のインターフェイスのUDLDステートを表示する例を示します。

```
switchxxxxxx# show udld gi1/0/1
Global UDLD mode: normal
Message Time: 15 sec(default)
Interface gi1/0/1
  Port UDLD mode: aggressive
  Port Current state: Bidirectional
  Number of detected neighbors: 1
  Port Neighbor Table
    Neighbor Device ID: 1234567893
      Neighbor MAC: 00:00:01:22:33:dd
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 20 sec
      Neighbor Current State: Bidirectional
      Neighbor Expiration Time: 7 sec
    Neighbor Device ID: 1234544893
      Neighbor MAC: 00:00:01:22:33:ff
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 15 sec
      Neighbor Current State: Undetermined
      Neighbor Expiration Time: 17 sec
```

例 3：次に、ネイバー情報のみを表示する例を示します。

```
switchxxxxxx# show udld neighbors
Port      Device ID     Port-ID   Device Name     Message    Neighbor     Expiration
                                                 Time(sec) State       Time (sec)
--------- ------------- --------- --------------- ---------  ----------   ---------
gi1/0/1  1234567893     gi1/0/1   SAL0734K5R2        15      Bidirect          11
gi1/0/2  3456750193     gi1/0/2   SAL0734K5R3        20      Undetermined      5
```

例 4：次に、単一のインターフェイスのネイバー情報だけを表示する例を示します。

```
switchxxxxxx# show udld gi1/0/1 neighbors
Port      Device ID     Port-ID   Device Name     Message    Neighbor     Expiration
                                                 Time(sec) State       Time (sec)
--------- ------------- --------- --------------- ---------  ----------   ---------
gi1/0/1  1234567893    gi1/0/1   SAL0734K5R2        15      Bidirect          11
```

udld

単方向リンク検出（UDLD）プロトコルをグローバルに有効にするには、グローバル コンフィギュレーション モードで **udld** コマンドを使用します。UDLD を無効にするには、このコマンドの **no** 形式を使用します。

構文

udld aggressive | **normal**

no udld

パラメータ

- **aggressive**：すべての光ファイバ インターフェイス上で、アグレッシブ モード UDLD をデフォルトで有効にします。
- **normal**：すべての光ファイバ インターフェイス上で、標準モード UDLD をデフォルトで有効にします。

デフォルト設定

UDLD はすべての光ファイバ インターフェイスで無効です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、光ファイバ インターフェイスにだけ作用します。他のインターフェイス タイプで UDLD を有効にする場合は、**udld port** コマンドをインターフェイス コンフィギュレーション モードで使用します。

すべての光ファイバ ポートで UDLD を無効にするには、このコマンドの **no** 形式を使用します。

デバイスは、RFC 5171 で指定されている UDLD プロトコルをサポートしています。

UDLD は、通常とアグレッシブの 2 つの動作モードをサポートしています。アグレッシブ モードでは、デバイスはリンクが双方向であることを明示的に検出できない場合にはポートをシャットダウンします。通常モードでは、デバイスはリンクが単方向であることを明示的に検出した場合にはインターフェイスをシャットダウンします。ローカルデバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカルデバイスが受信しない場合に、単一方向リンクが発生します。

UDLD によってシャットダウンされたインターフェイスをリセットするのに、次のコマンドを使用します。

- **interface** *interface-id* パラメータを指定した **errdisable recover reset** コマンド。特定のインターフェイスをリセットします。
- **udld** パラメータを指定した **errdisable recover reset** コマンド。UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **udld** パラメータを指定した **errdisable recover cause** コマンド。UDLD error-disabled ステートから自動的に回復します。

例

次に、すべての光ファイバ インターフェイスで UDLD を有効にする例を示します。

```
switchxxxxxx(config)# udld normal
```

udld message time

2 つのプローブ メッセージを送信する際の間隔のグローバル値を設定するには、グローバル コンフィギュレーション モードで **udld message time** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

udld message time *seconds*

no udld message time

パラメータ

seconds：2 つのプローブ メッセージを送信する際の間隔。有効な値は 1 ～ 90 秒です。

デフォルト設定

15 秒

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、メッセージ間隔（2 つのプローブ メッセージを連続して送信する際の間隔）のデフォルト値を変更する場合に使用します。

例

次の例では、間隔を 40 秒にグローバルに設定する方法を示します。

```
switchxxxxxx(config)# udld message time 40
```

udld port

イーサネット ポートで UDLD プロトコルを有効にするには、インターフェイス コンフィギュレーション モードで **udld port** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

udld port [**aggressive** | **normal** | **disable**]

no udld port

パラメータ

- **aggressive**：このインターフェイスで UDLD をアグレッシブ モードで有効にします。
- **normal**：このインターフェイスで UDLD を通常モードで有効にします。いずれのキーワードも指定しない場合、normal キーワードが適用されます。
- **disable**：このインターフェイスで UDLD を無効にします。

デフォルト設定

デフォルトの設定は次のとおりです。

- 光ファイバ インターフェイスは、**udld** コマンドによって設定された状態にあります。
- 光ファイバ以外のインターフェイスは、Disable 状態にあります。

コマンド モード

インターフェイス（イーサネット）コンフィギュレーション モード

使用上のガイドライン

このコマンドは、光ファイバ ポートでグローバル **udld** コマンドの設定をオーバーライドする場合に使用します。

ポートが光ファイバポートから光ファイバ以外のポートに、またはその逆に変更された場合でも、プラットフォーム ソフトウェアによってモジュールまたはギガビット インターフェイス コンバータ（GBIC）の変更が検出されるため、すべての設定が維持されます。

例 1：この例では、現在のグローバル **udld** 設定に関係なく、イーサネット ポートで UDLD を通常モードで有効にする方法を示しています。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# udld port normal
switchxxxxxx(config-if)# exit
```

例 2：この例では、デフォルト設定に戻す方法を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no udld port
switchxxxxxx(config-if)# exit
```

例 3：この例では、現在のグローバル **udld** 設定に関係なく、イーサネット ポートで UDLD を無効にする方法を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# udld port disable
switchxxxxxx(config-if)# exit
```

ユーザ インターフェイス コマンド

この章は、次の項で構成されています。

- configure （1518 ページ）
- disable （1519 ページ）
- do （1520 ページ）
- enable （1521 ページ）
- end （1522 ページ）
- exit (Configuration) （1523 ページ）
- exit（EXEC） （1524 ページ）
- help （1525 ページ）
- history （1526 ページ）
- history size （1527 ページ）
- login （1528 ページ）
- terminal datadump （1529 ページ）
- terminal history （1530 ページ）
- terminal history size （1531 ページ）
- terminal prompt （1532 ページ）
- terminal width （1533 ページ）
- show banner （1534 ページ）
- show history （1535 ページ）
- show privilege （1536 ページ）

configure

グローバル コンフィギュレーション モードを開始するには、**configure** 特権 EXEC モード コマンドを使用します。

構文

configure [***terminal***]

パラメータ

terminal：（オプション）terminal キーワードの有無にかかわらず、グローバル コンフィギュレーション モードを開始します。

コマンド モード

特権 EXEC モード

例

次に、グローバル 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。

```
switchxxxxxx# configure
switchxxxxxx(config)#
```

disable

特権 EXEC モードを終了し、ユーザ EXEC モードに戻るには、**disable** 特権 EXEC モード コマンドを使用します。

構文

disable [*privilege-level*]

パラメータ

privilege-level：（オプション）特権レベルを指定した特権レベルに下げます。特権レベルを空白のままにすると、レベルは最小の特権レベルに下げられます。

デフォルト設定

デフォルトの特権レベルは 15 です。

コマンド モード

特権 EXEC モード

例

次の例では、ユーザをユーザ レベル 1 に戻しています。

```
switchxxxxxx# disable 1
switchxxxxxx#
```

do

グローバル コンフィギュレーション モードまたは任意のコンフィギュレーション サブモードから EXEC レベル コマンドを実行するには、**do** コマンドを使用します。

構文

do *command*

パラメータ

command：実行する EXEC レベル コマンドを指定します。

コマンド モード

すべてのコンフィギュレーション モード

例

次の例では、グローバル コンフィギュレーション モードから **show vlan** 特権 EXEC モード コマンドを実行しています。

```
switchxxxxxx(config)# do show vlan
```

Vlan	Name	Ports	Type	Authorization
----	----	-----	----	----------
1	1	gi1/0/1-4、Po1、Po2	other	必須
2	2	gi1/0/1	dynamicGvrp	必須
10	v0010	gi1/0/1	permanent	不要
11	V0011	gi1/0/1、gi1/0/3	permanent	必須
20	20	gi1/0/1	permanent	必須
30	30	gi1/0/1、gi1/0/3	permanent	必須
31	31	gi1/0/1	permanent	必須
91	91	gi1/0/1、gi1/0/4	permanent	必須
4093	guest-vlan	gi1/0/1、gi1/0/3	permanent	ゲスト

```
switchxxxxxx(config)#
```

enable

特権 EXEC モードを開始するには、**enable** ユーザ EXEC モード コマンドを使用します。

構文

enable [*privilege-level*]

パラメータ

privilege-level：（オプション）システムを開始する特権レベルを指定します（範囲：1、7、15）。

デフォルト設定

デフォルトの特権レベルは 15 です。

コマンド モード

ユーザ EXEC モード

例

次に、特権レベル 7 に入る例を示します。

```
switchxxxxxx#  enable 7
enter password:**********
switchxxxxxx# Accepted
```

次に、特権レベル 15 に入る例を示します。

```
switchxxxxxx#  enable
enter password:**********
switchxxxxxx# Accepted
```

end

現在のコンフィギュレーションセッションを終了して、特権EXECモードに戻るには、**end**コマンドを使用します。

構文

end

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

すべてのコンフィギュレーション モード

例

次の例では、グローバル コンフィギュレーション モード セッションを終了し、特権 EXEC モードに戻っています。

```
switchxxxxxx(config)# end
switchxxxxxx#
```

exit (Configuration)

任意のモードを終了し、ユーザを CLI モード階層内の次に高いモードにするには、**exit** コマンドを使用します。

構文

exit

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

すべてのコンフィギュレーション モード

例

次の例では、コンフィギュレーションモードをインターフェイス コンフィギュレーションモードから特権 EXEC モードに変更しています。

```
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# exit
```

exit（EXEC）

デバイスからログオフしてアクティブなターミナル セッションを終了するには、**exit** ユーザ EXEC モード コマンドを使用します。

構文

exit

パラメータ

このコマンドには、引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

例

次の例では、アクティブなターミナル セッションを終了しています。

```
switchxxxxxx#  exit
```

help

ヘルプ システムの簡単な説明を表示するには、**help** コマンドを使用します。

構文

help

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

すべてのコンフィギュレーション モード

例

次の例では、ヘルプ システムの説明を表示しています。

```
switchxxxxxx# help
Help may be requested at any point in a command by entering a question mark '?'. If
nothing matches the currently entered incomplete command, the help list is empty. This
indicates that there is no command matching the input as it currently appears. If the
request is within a command, press the Backspace key and erase the entered characters
to a point where the request results in a match.
Help is provided when:
1. There is a valid command and a help request is made for entering a parameter or
argument (e.g. 'show ?'). All possible parameters or arguments for the entered command
are then displayed.
2. An abbreviated argument is entered and a help request is made for arguments matching
 the input (e.g. 'show pr?').
```

history

入力したコマンドの保存を有効にするには、**history** ライン コンフィギュレーション モード コマンドを使用します。このコマンドを無効にするには、このコマンドの **no** 形式を使用します。

構文

history

no history

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

有効

コマンド モード

ライン コンフィギュレーション モード

使用上のガイドライン

このコマンドにより、ユーザが指定された行に入力したコマンドを保存できるようになります。以前の行に戻るには、上向き矢印または下向き矢印を使用します。

コンソール、Telnet、または SSH を介してユーザが次回ログインするときから有効になります。

次に、関連するコマンドを示します。

- terminal history size （1531 ページ） ユーザ EXEC モード コマンドは、現在のターミナル セッションの間このコマンドを有効または無効にする場合に使用します。

  history size （1527 ページ） ライン コンフィギュレーション モード コマンドは、コマンド履歴バッファのサイズを設定する場合に使用します。

例

次の例では、Telnet に対してコマンドを有効にしています。

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# history
```

history size

特定の行について履歴バッファに保存されるユーザ コマンドの最大数を変更するには、**history size** ライン コンフィギュレーション モード コマンドを使用します。コマンド履歴バッファ サイズをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

構文

history size *number-of-commands*

no history size

パラメータ

number-of-commands：システムの履歴バッファに記録されるコマンドの数を指定します。

デフォルト設定

デフォルトのコマンド履歴バッファ サイズは、コマンド 10 個です。

コマンド モード

ライン コンフィギュレーション モード

使用上のガイドライン

このコマンドは、特定の行に対してコマンド履歴バッファ サイズを設定します。コンソール、Telnet、または SSH を介してユーザが次回ログインするときから有効になります。

terminal history size ユーザ EXEC モード コマンドは、現在のターミナル セッションのコマンド履歴バッファ サイズを設定する場合に使用します。

割り当てたコマンド履歴バッファは、端末ユーザ別に用意され、共有バッファから取得されます。共有バッファに使用できる十分な領域がない場合は、コマンド履歴バッファ サイズをデフォルトのサイズよりも大きくすることはできません。

例

次の例では、Telnet のコマンド履歴バッファ サイズをエントリ 100 個に変更しています。

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# history size 100
```

login

ログインするユーザの変更を有効にするには、**login** ユーザ EXEC モード コマンドを使用します。このコマンドでログインした場合、ユーザはユーザ名/パスワードの入力を求められます。

構文

login

パラメータ

このコマンドには、引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

例

次の例では、特権 EXEC モードを開始し、必要なユーザ名 'bob' でログインしています。

```
switchxxxxxx#  login
User Name:bob
Password:*****
switchxxxxxx#
```

terminal datadump

ユーザに入力を求めずにshowコマンドのすべての出力をダンプできるようにするには、**terminal datadump** ユーザ EXEC モード コマンドを使用します。ダンプを無効にするには、このコマンドの **no** 形式を使用します。

構文

terminal datadump

terminal no datadump

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

出力時に、ダンプは無効になり、出力は 24 行ごとに一時停止します。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

デフォルトでは、出力に含まれる行が24行を超える場合、**More**プロンプトが表示されます。Enter キーを押すと次の行が表示され、**スペースキー**を押すと次の出力画面が表示されます。

terminal datadump コマンドにより、一時停止をなくして、show コマンドを入力した直後にすべての出力をダンプできます。

幅に制限はなく、端末に出力される行の幅は端末自体に基づきます。

このコマンドは、現在のセッションのみを対象とします。

例

次の例では、show コマンドを入力した直後にすべての出力をダンプしています。

```
switchxxxxxx#  terminal datadump
```

terminal history

現在のターミナルセッションの間コマンド履歴機能を有効にするには（つまり、実行コンフィギュレーション ファイルに保存されません）、**terminal history** ユーザ EXEC モード コマンドを使用します。このコマンドを無効にするには、このコマンドの **no** 形式を使用します。

構文

terminal history

terminal no history

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

すべての端末セッションのデフォルト設定は、history（1526 ページ）ライン コンフィギュレーション モード コマンドによって定義されます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

このコマンドは、現在のセッションの間コマンド履歴を有効にします。デフォルトは、history（1526 ページ） ライン コンフィギュレーション モード コマンドによって決まります。

このコマンドはすぐに有効になります。

例

次の例では、現在のターミナル セッションの間コマンド履歴機能を無効にしています。

```
switchxxxxxx#  terminal no history
```

terminal history size

現在のターミナルセッションのコマンド履歴バッファサイズを変更するには（つまり、実行コンフィギュレーションファイルに保存されない）、**terminal history size** ユーザ EXEC モードコマンドを使用します。また、コマンド履歴バッファサイズをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

構文

terminal history size *number-of-commands*

terminal no history size

パラメータ

number-of-commands：システムの履歴バッファに保持されるコマンドの数を指定します。（範囲：10 ー 206）

デフォルト設定

すべての端末セッションのデフォルト設定は、history size （1527ページ） ライン コンフィギュレーション モード コマンドによって定義されます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

terminal history size EXEC コマンドは、現在のターミナル セッションのコマンド履歴バッファサイズを変更する場合に使用します。history （1526 ページ） ライン コンフィギュレーション モード コマンドは、デフォルトの履歴バッファ サイズを変更する場合に使用します。

すべてのバッファにおけるコマンドの最大数は 207 です。

例

次の例では、現在のターミナル セッションのコマンド履歴バッファ サイズをコマンド 20 個に設定しています。

```
switchxxxxxx# terminal history size 20
```

terminal prompt

端末プロンプトを有効にするには、**terminal prompt** ユーザ EXEC モード コマンドを使用します。端末プロンプトを無効にするには、**terminal no prompt** コマンドを使用します。

コマンドは、セッションごとであり、設定データベースには保存されません。

構文

terminal prompt

terminal no prompt

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

デフォルト設定はプロンプト有効です。

コマンド モード

特権 EXEC モード

例

次の例では、端末プロンプトを無効にしています。

```
switchxxxxxx# terminal no prompt
```

terminal width

CLI セッションへの echo 入力の出力幅を決定するには、**terminal width** ユーザ EXEC モード コマンドを使用します。デフォルトに戻すには、**terminal no width** を使用します。

コマンドは、セッションごとであり、設定データベースには保存されません。

構文

terminal width *number-of-characters*

terminal no width

パラメータ

number-of-characters：CLI コマンドの echo 出力およびコンフィギュレーション ファイルに表示する文字の数を指定します。'0' を指定すると、画面の行の文字数が無限になります。（範囲：0、70 ～ 512）

デフォルト設定

デフォルトの文字数は 77 です。

コマンド モード

特権 EXEC モード

例

次の例では、端末幅を 100 文字に設定しています。

```
switchxxxxxx# terminal width 100
```

show banner

定義されているバナーを表示するには、ユーザ EXEC モードで **show banner** コマンドを使用します。

構文

show banner login

show banner exec

パラメータ

このコマンドには、引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

例

```
switchxxxxxx# show banner login
------------------------------------------------------------

Banner: Login
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
switchxxxxxx# show banner exec
Banner: EXEC
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
You have logged on
```

show history

現在のセッションで入力されたコマンドをリストするには、**show history** ユーザ EXEC モード コマンドを使用します。

構文

show history

パラメータ

このコマンドには、引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

バッファには、実行されたコマンドと実行されていないコマンドが含まれています。

コマンドは、最初のコマンドから最新のコマンドまでリストされます。

コンフィギュレーション モードを開始する場合やコンフィギュレーション モードから戻る場合、バッファはそのままの状態を保ちます。

例

次に、現在の特権EXECモードの間に入力されたすべてのコマンドを表示する例を示します。

```
switchxxxxxx# show version
SW version 3.131 (date 23-Jul-2005 time 17:34:19)
HW version 1.0.0
switchxxxxxx# show clock
15:29:03 Jun 17 2005
switchxxxxxx# show history
show version
show clock
show history
3 commands were logged (buffer size is 10)
```

show privilege

現在の特権レベルを表示するには、**show privilege** ユーザ EXEC モード コマンドを使用します。

構文

show privilege

パラメータ

このコマンドには、引数またはキーワードはありません。

コマンド モード

ユーザ EXEC モード

例

次に、ログオン中のユーザの特権レベルを表示する例を示します。

```
switchxxxxxx# show privilege
Current privilege level is 15
```

VLAN コマンド

この章は、次の項で構成されています。

- vlan database （1539 ページ）
- vlan （1540 ページ）
- show vlan （1541 ページ）
- interface vlan （1542 ページ）
- interface range vlan （1543 ページ）
- name （1544 ページ）
- switchport protected-port （1545 ページ）
- show interfaces protected-ports （1546 ページ）
- switchport （1547 ページ）
- switchport mode （1548 ページ）
- switchport access vlan （1551 ページ）
- switchport trunk allowed vlan （1552 ページ）
- switchport trunk native vlan （1554 ページ）
- switchport general allowed vlan （1555 ページ）
- switchport general pvid （1557 ページ）
- switchport general ingress-filtering disable （1558 ページ）
- switchport general acceptable-frame-type （1559 ページ）
- switchport general forbidden vlan （1560 ページ）
- switchport customer vlan （1561 ページ）
- ethtype （1562 ページ）
- switchport nni ethtype （1564 ページ）
- switchport vlan-mapping tunnel （1566 ページ）
- switchport vlan-mapping tunnel l2protocol vlan （1568 ページ）
- switchport vlan-mapping tunnel l2protocol cos （1569 ページ）
- switchport vlan-mapping tunnel l2protocol cos interface （1570 ページ）
- switchport vlan-mapping tunnel l2protocol drop-threshold （1571 ページ）
- switchport vlan-mapping tunnel l2protocol forward （1572 ページ）
- switchport vlan-mapping one-to-one （1574 ページ）

- map protocol protocols-group （1576 ページ）
- switchport general map protocols-group vlan （1578 ページ）
- show vlan protocols-groups （1579 ページ）
- map mac macs-group （1580 ページ）
- switchport general map macs-group vlan （1581 ページ）
- show vlan macs-groups （1583 ページ）
- map subnet subnets-group （1584 ページ）
- switchport general map subnets-group vlan （1585 ページ）
- show vlan subnets-groups （1586 ページ）
- show interfaces switchport （1587 ページ）
- private-vlan （1589 ページ）
- private-vlan association （1590 ページ）
- switchport private-vlan mapping （1592 ページ）
- switchport private-vlan host-association （1593 ページ）
- show vlan private-vlan （1595 ページ）
- switchport access multicast-tv vlan （1596 ページ）
- switchport customer multicast-tv vlan （1597 ページ）
- show vlan multicast-tv （1598 ページ）
- vlan prohibit-internal-usage （1599 ページ）
- show vlan internal usage （1601 ページ）

vlan database

VLAN コンフィギュレーション モードを開始するには、**vlan database** グローバル コンフィギュレーション モード コマンドを使用します。このモードは、VLAN を作成し、デフォルトの VLAN を定義するために使用します。

グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

構文

vlan database

デフォルト設定

VLAN 1 はデフォルトで存在します。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、VLAN コンフィギュレーション モードを開始し、VLAN 1972 を作成し、VLAN コンフィギュレーション モードを終了しています。

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# vlan 1972
switchxxxxxx(config-vlan)# exit
```

vlan

VLAN を作成し、（単一の VLAN を作成している場合のみ）名前を割り当てるには、**vlan** VLAN コンフィギュレーション モードまたはグローバル コンフィギュレーション モード コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

構文

vlan *vlan-range* | {*vlan-id* [**name** *vlan-name*]} [**media ethernet**] [**state active**]

no vlan *vlan-range*

パラメータ

- ***vlan-range***：VLAN ID を指定します。連続していない VLAN ID はカンマ（スペースなし）で区切ります。ID の範囲（範囲：2 ～ 4094）を指定するには、ハイフンを使用します。
- ***vlan-id***：VLAN ID を指定します。（範囲：2 ～ 4094）。
- ***vlan-name***：VLAN 名を指定します。（範囲：1 ～ 32 文字）。
- **media**：VLAN のメディア タイプを設定します。有効な値は、**ethernet** です。
- **state**：VLAN の状態を指定します。有効な値は、**active** です。

デフォルト設定

VLAN 1 はデフォルトで存在します。

コマンド モード

グローバル コンフィギュレーション モード

VLAN データベース コンフィギュレーション モード

使用上のガイドライン

VLANが存在しない場合は、作成されます。VLANを作成できない場合、エラーでコマンドが終了し、現在のコンテキストは変更されません。

例

次に、いくつかの VLAN を作成する例を示します。VLAN 1972 に「Marketing」の名前が割り当てられます。

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# vlan 19-23
switchxxxxxx(config-vlan)# vlan 100
switchxxxxxx(config-vlan)# vlan 1972 name Marketing
switchxxxxxx(config-vlan)# exit
```

show vlan

次の VLAN 情報を表示するには、**show vlan** 特権 EXEC モード コマンドを使用します。

構文

show vlan [**tag** vlan-id | **name** vlan-name]

パラメータ

- **tag** vlan-id：VLAN ID を指定します。
- **name** *vlan-name*：VLAN 名の文字列（長さ：1 ～ 32 文字）を指定します。

デフォルト設定

すべての VLAN が表示されます。

コマンド モード

特権 EXEC モード

例 1：次に、すべての VLAN の情報を表示する例を示します。

```
switchxxxxxx# show vlanCreated by: S-Static, G-GVRP, R-Radius Assigned VLAN, V-Voice
VLAN
```

VLAN	Name	Tagged Ports	UnTagged Ports	Created by
-----	----------	----------	----------	----------
1	デフォルト		gi1/0/1	S
10	Marketing	gi1/0/2	gi1/0/2	S
91	11	gi1/0/2 ～ 4	gi1/0/2	SGR
92	11	gi1/0/3 ～ 4		G
93	11	gi1/0/3 ～ 4		GR

interface vlan

特定のVLANのインターフェイス コンフィギュレーション（VLAN）モードを開始するには、**interface vlan** グローバル コンフィギュレーション モード コマンドを使用します。このコマンドを入力した後、すべてのコマンドがこの VLAN を設定します。

構文

interface vlan *vlan-id*

パラメータ

- ***vlan-id***：設定する VLAN を指定します。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

VLANは、存在しなければ作成されます。VLANを作成できない場合、このコマンドはエラーで終了し、現在のコンテキストは変更されません。

例

次の例では、IP アドレス 131.108.1.27 とサブネットマスク 255.255.255.0 で VLAN 1 を設定します。

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 131.108.1.27 255.255.255.0
```

interface range vlan

複数の VLAN を同時に設定するには、**interface range vlan** グローバル コンフィギュレーション モード コマンドを使用します。

構文

interface range vlan *vlan-range*

パラメータ

- ***vlan-range***：VLAN のリストを指定します。連続していない VLAN はカンマ（スペースなし）で区切ります。VLAN の範囲を指定するには、ハイフンを使用します。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

インターフェイス VLAN 範囲コンテキスト下のコマンドは、範囲内の各 VLAN で個別に実行されます。いずれかの VLAN でコマンドがエラーを返した場合は、エラー メッセージが表示され、残りの VLAN の設定が試みられます。

例

次の例では、VLAN 221 ～ 228 と 889 が同じコマンドを受信するようにグループ化しています。

```
switchxxxxxx(config)# interface range vlan 221-228, vlan 889
```

name

VLAN に名前を付けるには、**name** インターフェイス コンフィギュレーション（VLAN）モード コマンドを使用します。VLAN 名を削除するには、コマンドの **no** 形式を使用します。

構文

name *string*

no name

パラメータ

- ***string***：この VLAN に関連付けられる一意の名前を指定します。（長さ：1 ～ 32 文字）。

デフォルト設定

名前は定義されていません。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

VLAN 名は一意である必要があります。

例

次の例では、VLAN 19 に Marketing という名前を割り当てています。

```
switchxxxxxx(config)# interface vlan 19
switchxxxxxx(config-if)# name Marketing
```

switchport protected-port

同じスイッチ上の他の保護ポートから、レイヤ2のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを分離するには、**switchport protected-port** インターフェイス コンフィギュレーション モード コマンドを使用します。ポートで保護を無効にするには、このコマンドの **no** 形式を使用します。

構文

switchport protected-port

no switchport protected-port

デフォルト設定

保護されていない

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

パケットは、すべてのフィルタリング ルールおよびフィルタリング データベース（FDB）決定の対象になることに注意してください。

このコマンドは、同じスイッチ上の（入力インターフェイスと同じコミュニティに関連付けられていない）他の保護ポートからレイヤ2のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを分離する場合に使用します。パケットは引き続き FDB の決定とすべてのフィルタリング ルールに従うことに注意してください。

例

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport protected-port
```

show interfaces protected-ports

保護ポートの設定を表示するには、**show interfaces protected-ports** EXEC モード コマンドを使用します。

構文

show interfaces protected-ports [*interface-id* | **detailed**]

パラメータ

- ***interface-id***：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。
- **detailed**：現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

保護されているすべてのインターフェイスを表示します。detailed を使用しないと、提供ポートについてのみ表示されます。

コマンド モード

ユーザ EXEC モード

例

```
switchxxxxxx# show interfaces protected-ports
```

Interface	State
---	---
gi1/0/1	Protected
gi1/0/2	Protected
gi1/0/3	Unprotected
gi1/0/4	Unprotected

switchport

レイヤ 3 モードのインターフェイスをレイヤ 2 モードにするには、**switchport** インターフェイス コンフィギュレーション モード コマンドを使用します。レイヤ 3 モードにインターフェイスを戻す場合は、このコマンドの **no** 形式を使用します。

構文

switchport

no switchport

デフォルト設定

レイヤ 2 モード

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

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するには、**no switchport** コマンドを使用します。

802x.1 がインターフェイスで有効になっていて、次の条件のいずれかが当てはまる場合、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できません。

- ホスト モードが multi-host ではない。
- MAC ベースまたは Web ベースの認証が有効になっている。
- Radius VLAN 割り当てが有効になっている。

例

例 1：次に、ポート gi1/0/1 をレイヤ 2 モードにする例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport
```

例 2：次に、ポート gi1/0/1 をレイヤ 3 モードにする例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no switchport
```

switchport mode

VLAN メンバーシップ モードを設定するには、**switchport mode** インターフェイス コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport mode access | **trunk** | **general** | **private-vlan** {**promiscuous** | **host**} | **customer** | **vlan-mapping** {**tunnel** | **one-to-one** }

no switchport mode

パラメータ

- **access**：タグなしレイヤ 2 VLAN ポートを指定します。
- **trunk**：トランキング レイヤ 2 VLAN ポートを指定します。
- **general**：802-1q フルサポートの VLAN ポートを指定します。
- **customer**：エッジポートを顧客の装置に接続するように指定します。このポートから受信したトラフィックは、追加の 8 02.1q VLAN タグでトンネリングされます（Q-in-Q VLAN トンネリング）。
- **private-vlan promiscuous**：プライベート VLAN 無差別ポート。
- **private-vlan host**：プライベート VLAN ホスト ポート。
- **vlan-mapping tunnel**：VLAN マッピング トンネル エッジ ポート。
- **vlan-mapping one-to-one**：VLAN マッピング 1 対 1 エッジポート。

デフォルト設定

アクセス モード.

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

ポートのモードが変更されると、ポートはそのモードに対応する構成を受信します。

ポート モードが access に変更され、アクセス VLAN が存在しない場合、そのポートはどの VLAN にも属しません。

プロバイダーエッジスイッチのエッジインターフェイスの VLAN マッピングモードを設定するには、**switchport mode vlan-mapping** {**tunnel** | **one-to-one**} コマンドを使用します。エッジインターフェイスは、カスタマーネットワークがプロバイダーエッジスイッチに接続されている

インターフェイスです。スイッチが属するネットワークはプロバイダーネットワークです。これらのネットワーク（カスタマーネットワークとプロバイダーネットワーク）は同じ VLAN IDを使用でき、エッジインターフェイスはカスタマーVLAN（C-VLAN）とプロバイダーVLAN（S-VLAN）の間で VLAN マッピングを実行する必要があります。

エッジインターフェイスでは、C-VLAN が S-VLAN にマッピングされ、元の C-VLAN タグはペイロードの一部として保持されます。非エッジのタグ付きインターフェイスでフレームが送信される場合、元の C-VLAN-ID がマッピングされている S-VLAN の別のレイヤを使用して、フレームがカプセル化されます。したがって、フレームが非エッジ インターフェイス フレームで送信されると、外部S-VLANタグと内部C-VLANタグで二重にタグ付けされます。フレームがエッジインターフェイスで送信されると、S-VLAN タグが除去されます。

エッジインターフェイスでは、C-VLAN は S-VLAN にマッピングされ、入力フレームの元の C-VLAN-ID はマッピング先の S-VLAN ID に置き換えられます。タグなしフレームはドロップされます。対称変換でエッジインターフェイスに戻ります。

次の機能は、VLAN マッピングが許可されている場合は有効にできません。

- IPv4 ルーティング
- IPv6 ルーティング
- 自動スマートポート
- 音声 VLAN

switchport vlan-mapping コマンドでは、S-VLAN にポートを追加できません。

エッジインターフェイスを含む VLAN では、IPv4 と IPv6 のインターフェイスを定義することができません。

次のレイヤ 2 機能はエッジインターフェイスを含む VLAN ではサポートされません。

- IGMP スヌーピング
- MLD スヌーピング
- DHCP スヌーピング
- IPv6 ファースト ホップ セキュリティ

次のプロトコルはエッジインターフェイスでは有効にできません。

- STP
- GVRP

次の機能はエッジインターフェイスではサポートされません。

- RADIUS VLAN 割り当て
- 802.1x ゲスト VLAN

出力 ACL は 1 対 1 の VLAN マッピングエッジポートではサポートされません。

network キーワードまたはリフレクタポートを持つ宛先ポートは、エッジポートでは設定できません。

注。上記で指定したエッジポートのすべての制限は、**switchport vlan-mapping** コマンドと、これらの機能を設定するコマンドによってチェックされます。

デフォルトでは、スイッチは次の宛先 MAC アドレスを持つエッジポートで受信したフレームを転送しません。

- 01:80:C2:00:00:00-01:80:C2:00:00:FF
- 01:00:0C:00:00:00-01:00:0C:FF:FF:FF
- 01:00:0C:CD:CD:D0

注。これらの MAC アドレスを使用する次のプロトコルは、エッジポートで有効にすることができます。

- LACP：01:80:C2:00:00:02
- LLDP：01:80:C2:00:00:0E
- UDLD：01:00:0C:CC:CC:CC
- CDP：01:00:0C:CC:CC:CC

例

例 1：次に、gi1/0/1 をアクセスポート（タグなしレイヤ 2）VLAN ポートとして設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

例 2：次に、ポート gi1/0/2 をプライベート VLAN ホストモードにする例を示します。

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# switchport mode private-vlan host
```

switchport access vlan

アクセス モードのポートは、1 つまでの VLAN のタグなしメンバーにすることができます。**switchport access vlan** インターフェイス コンフィギュレーション コマンドは、インターフェイスを現在属している VLAN とは別の VLAN に再割り当てするか、**none** に割り当てます（この場合、どの VLAN のメンバーでもありません）。

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport access vlan {*vlan-id* | **none**}

no switchport access vlan

パラメータ

- ***vlan-id***：ポートを設定する VLAN を指定します。
- **none**：アクセス ポートが任意の VLAN に属することができないことを指定します。

デフォルト設定

インターフェイスは、デフォルト VLAN に属します。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

ポートが異なる VLAN に割り当てられると、以前の VLAN から自動的に削除され、新しい VLAN に追加されます。ポートに **none** が割り当てられている場合、以前の VLAN から削除され、その他の VLAN に割り当てられません。

例

次に、アクセスポート gi1/0/1 を VLAN 2 に割り当てる（さらに、それを以前の VLAN から削除する）例を示します。

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

switchport trunk allowed vlan

トランク インターフェイスは、単一の VLAN のタグなしのメンバーであり、さらに、1 つ以上の VLAN のタグ付きのメンバーである可能性があります。トランク ポートの VLAN の追加/削除を行うには、**switchport trunk allowed vlan** インターフェイス コンフィギュレーション モード コマンドを使用します。デフォルト値に戻すには、このコマンドの no 形式を使用します。

構文

switchport trunk allowed vlan {**all** | **none** | *vlan-list* | **add** vlan-list | **remove** vlan-list | **except** vlan-list}

no switchport trunk allowed vlan

パラメータ

- **all**：1 ～ 4094 のすべての VLAN を指定します。いつでも、ポートは、その時点で存在するすべての VLAN に属します。（範囲：1 ～ 4094）。
- **none**：空の VLAN リストを指定します。ポートはどの VLAN にも属しません。
- ***vlan-list***：インターフェイスがメンバーになっている VLAN ID のリストを指定します。このコマンドに指定する VLAN は、ポートがメンバーになる唯一の VLAN です（トランク VLAN メンバーシップに関連する以前のすべての設定が破棄されます）。ID の範囲を指定するには、ハイフンを使用します。連続していない VLAN ID はカンマ（スペースなし）で区切ります（範囲：1 ～ 4094）。
- **add** vlan-list：ポートに追加する VLAN ID のリスト。連続していない VLAN ID はカンマ（スペースなし）で区切ります。ID の範囲を指定するには、ハイフンを使用します。
- **remove** vlan-list：ポートから削除する VLAN ID のリスト。連続していない VLAN ID はカンマ（スペースなし）で区切ります。ID の範囲を指定するには、ハイフンを使用します。
- **except** vlan-list：*vlan-list* に属する VLAN を除き、1 ～ 4094 の範囲のすべての VLAN を含めた VLAN ID のリスト。

デフォルト設定

デフォルトでは、トランク ポートは作成されたすべての VLAN に属します。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

モードがトランクとして設定されているときにポートが属する VLAN を指定するには、**switchport trunk allowed vlan** コマンドを使用します。

存在していなかったVLANを設定できます。存在していなかったVLANが作成されると、ポートが自動的に追加されます。

禁止 VLAN を設定できます。

例

トランク ポート 1 ～ 13 に VLAN 2、3、および 100 を追加するには

```
switchxxxxxx(config)# interface range gi1/0/1-3
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2-3,100
switchxxxxxx(config-if)
```

switchport trunk native vlan

トランク ポートにタグなしのパケットが到達すると、ポートのネイティブ VLAN に送られます。トランク インターフェイスのネイティブ VLAN を定義するには、**switchport trunk native vlan** インターフェイス コンフィギュレーション モード コマンドを使用します。デフォルトのネイティブ VLAN に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport trunk native vlan {*vlan-id* | **none**}

no switchport trunk native vlan

パラメータ

- ***vlan-id***：ネイティブ VLAN ID を指定します。
- **none**：アクセス ポートが任意の VLAN に属することができないことを指定します。

デフォルト設定

デフォルトのネイティブ VLAN は Default VLAN です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

インターフェイスPVIDの値は、このVLANIDに設定されます。インターフェイスがネイティブ VLAN に属する場合は、VLAN タグなし出力インターフェイスとして設定されます。

ポート モードが trunk のときにのみ設定が適用されます。

例

次に、VLAN 2 をポート gi1/0/1 のネイティブ VLAN として定義する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport trunk native vlan 2
switchxxxxxx(config-if)# exit
```

switchport general allowed vlan

一般ポートは、タグ付きパケットまたはタグなしパケットを受信できます。一般ポートに対してVLANを追加/削除し、出力上のパケットがタグ付きかタグなしかを設定するには、**switchport general allowed vlan** インターフェイス コンフィギュレーション モード コマンドを使用します。このコマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

構文

switchport general allowed vlan add vlan-list [**tagged** | **untagged**]

switchport general allowed vlan remove vlan-list

no switchport general allowed vlan

パラメータ

- **add** vlan-list：追加する VLAN ID のリスト。連続していない VLAN ID はカンマ（スペースなし）で区切ります。ID の範囲はハイフンで指定します。（範囲：1 ～ 4094）
- **remove** vlan-list：削除する VLAN ID のリスト。連続していない VLAN ID はカンマ（スペースなし）で区切ります。ID の範囲を指定するには、ハイフンを使用します。
- **tagged**：設定されている VLAN にタグ付きでパケットが送信されることを指定します
- **untagged**：設定されている VLAN にタグなしでパケットが送信されることを指定します（これがデフォルトです）

デフォルト設定

ポートは、VLAN のメンバーではありません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

インターフェイスが追加された VLAN の禁止メンバーである場合は、インターフェイスはこの特定のVLANのメンバーになりません。この場合、エラー メッセージ（「An interface cannot become a member of a forbidden VLAN. This message will only be displayed once.」）が表示され、vlan-list にさらに VLAN がある場合、コマンドは実行を続行します。

存在していなかった VLAN は設定できません。VLAN が削除されると、vlan-list から削除されます。

ポート モードが general のときにのみ設定が適用されます。

例

この例では、gi1/0/1 を追加し、さらに VLAN 2 および 3 を追加します。パケットは、出力でタグ付きになります。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport general allowed vlan add 2-3 tagged
```

switchport general pvid

インターフェイスが一般モードの場合にインターフェイスのポート VLAN ID（PVID）を設定するには、**switchport general pvid** インターフェイス コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport general pvid *vlan-id*

no switchport general pvid

パラメータ

- ***vlan-id***：ポート VLAN ID（PVID）を指定します。

デフォルト設定

PVID は、デフォルトの VLAN PVID です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

例 1：次に、gi1/0/2 PVID を 234 に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# switchport general pvid 234
```

例 2：次に、以下を実行する例を示します。

- VLAN 2 と 3 をタグ付きとして、VLAN 100 をタグなしとして gi1/0/4 に追加する
- VID 100 を PVID として定義する

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)#  switchport general allowed vlan add 2-3 tagged
switchxxxxxx(config-if)# switchport general allowed vlan add 100 untagged
switchxxxxxx(config-if)# switchport general pvid 100
switchxxxxxx(config-if)# exit
```

switchport general ingress-filtering disable

一般ポートでポート入力フィルタリングを無効にするには（パケットは入力で破棄されません）、**switchport general ingress-filtering disable** インターフェイス コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

デフォルト設定

入力フィルタリングが有効になっています。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、gi1/0/1 のポート入力フィルタ処理を無効にする例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general ingress-filtering disable
```

switchport general acceptable-frame-type

switchport general acceptable-frame-type インターフェイス コンフィギュレーション モード コマンドでは、インターフェイスでフィルタリング（破棄）するパケットのタイプ（タグ付き/タグなし）を設定します。入力フィルタリングをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

switchport general acceptable-frame-type {**tagged-only** | **untagged-only** | **all**}

no switchport general acceptable-frame-type

パラメータ

- **tagged-only**：タグなしパケットおよび優先順位タグ付きパケットを無視（破棄）します。
- **untagged-only**：VLAN タグ付きパケット（優先順位タグ付きパケットは含まない）を無視（破棄）します。
- **all**：タグなしパケットや優先順位タグ付きパケットを破棄しません。

デフォルト設定

すべてのフレーム タイプが入力時に受け入れられます（**all**）。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

例

次に、ポート gi1/0/3 を一般モードに設定して、入力でタグなしのフレームを破棄する例を示します。

```
switchxxxxxx(config)# interface gi1/0/3
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general acceptable-frame-type tagged-only
```

switchport general forbidden vlan

ポートの特定の VLAN の追加/削除を禁止するには、**switchport general forbidden vlan** インターフェイス コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport general forbidden vlan {**add** *vlan-list* | **remove** vlan-list}

no switchport general forbidden vlan

パラメータ

- **add** *vlan-list*：インターフェイスに追加する VLAN ID のリストを指定します。連続していない VLAN ID はカンマ（スペースなし）で区切ります。ID の範囲を指定するには、ハイフンを使用します。
- **remove** vlan-list：インターフェイスから削除する VLAN ID のリストを指定します。連続していない VLAN ID は、カンマ（スペースなし）で区切ります。ID の範囲はハイフンで指定します。

デフォルト設定

すべての VLAN が許可されています。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

禁止 VLAN を、システム上に存在しない VLAN か、ポートですでに定義されている VLAN にすることはできません。

例

次に、VLAN 5 ～ 7 で禁止されているメンバーシップとして gi1/0/4 を定義する例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport general forbidden vlan add 5-7
switchxxxxxx(config-if)# exit
```

switchport customer vlan

インターフェイスが顧客モード（**switchport mode** コマンドによって設定）の場合にポートの VLAN を設定するには、**switchport customer vlan** インターフェイス コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport customer vlan *vlan-id*

no switchport customer vlan

パラメータ

- ***vlan-id***：顧客 VLAN を指定します。

デフォルト設定

VLAN は、顧客として設定されません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

ポートは、顧客モードの場合、QinQ モードになります。これにより、ユーザはプロバイダー ネットワーク全体で自身の VLAN 配置（PVID）を使用できます。スイッチは、1 つ以上の顧客ポートが含まれる場合、QinQ モードになります。

例

次に、gi1/0/4 をカスタマー VLAN 5 のメンバーとして定義する例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport mode customer
switchxxxxxx(config-if)# switchport customer vlan 5
```

ethtype

S-VLAN タグに使用するイーサネットタイプをグローバルに定義するには、グローバル コンフィギュレーション モードで **ethtype** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ethtype dot1q | **dot1ad** | **9100** | **9200**

no ethtype

パラメータ

- **dot1q**：値 0x8100（802.1q VLAN タグ）が VLAN タグのイーサネットタグとして使用されます。
- **dot1ad**：値 0x88a8（802.1ad VLAN タグ）が VLAN タグのイーサネットタグとして使用されます。
- **9100**：値 0x9100 が VLAN タグのイーサネットタグとして使用されます。
- **9200**：値 0x9200 が VLAN タグのイーサネットタグとして使用されます。

デフォルト設定

dot1q

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

S-VLAN タグに使用するイーサネットタイプをグローバルに定義するには、**ethtype** コマンドを使用します。設定はすべての NNI インターフェイスに適用されます。すべての非エッジインターフェイスは NNI インターフェイスと見なされます。エッジインターフェイスは、次のいずれかのモードを持つインターフェイスです。

- customer
- vlan-mapping tunnel
- vlan-mapping one-to-one

デフォルト設定を復元するには、**no ethtype** コマンドを使用します。

例

次に、イーサネットタイプを VLAN タグで dot1ad（0x88a8）に設定する例を示します。

```
switchxxxxxx(config)# ethtype dot1ad
```

switchport nni ethtype

NNIインターフェイスのS-VLANタグに使用されるイーサネットタイプを定義するには、インターフェイス（イーサネット、ポートチャネル）コンフィギュレーションモードで**switchport nni ethtype** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport nni ethtype dot1q | **dot1ad** | **9100** | **9200**

no switchport nni ethtype

パラメータ

- **dot1q**：値 0x8100（802.1q VLAN タグ）が VLAN タグのイーサネットタグとして使用されます。
- **dot1ad**：値 0x88a8（802.1ad VLAN タグ）が VLAN タグのイーサネットタグとして使用されます。
- **9100**：値 0x9100 が VLAN タグのイーサネットタグとして使用されます。
- **9200**：値 0x9200 が VLAN タグのイーサネットタグとして使用されます。

デフォルト設定

ethtype コマンドによって設定されます。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

NNIインターフェイスのS-VLANタグに使用するイーサネットタイプを定義するには、**switchport nni ethtype** コマンドを使用します。すべての非エッジインターフェイスは NNI インターフェイスと見なされます。エッジインターフェイスは、次のいずれかのモードを持つインターフェイスです。

- customer
- vlan-mapping tunnel
- vlan-mapping one-to-one

デフォルト設定を復元するには、**no switchport nni ethtype** コマンドを使用します。

例

次に、イーサネットタイプを VLAN タグで dot1ad（0x88a8）に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport nni ethtype dot1ad
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping tunnel

エッジインターフェイスで選択的トンネリングを設定するには、インターフェイス（イーサネット、ポートチャネル）コンフィギュレーション モードで **switchport vlan-mapping tunnel** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

構文

switchport vlan-mapping tunnel {*vlan-list* | **default**} {*outer-vlan-id* | **drop**}

no switchport vlan-mapping tunnel [*vlan-list* | **default**]

パラメータ

- ***vlan-list***：選択的トンネリングのカスタマー VLAN（C-VLAN）を指定します。リストの VLAN ID はカンマで区切るか、または一連の VLAN ID はハイフンで区切ります（例：1,2,3-5）。指定できる範囲は 1 ～ 4094 です。
- **default**：指定していない C-VLAN のリストを指定します。デフォルトアクションを指定しない場合、C-VLAN が指定されていない入力フレームはドロップされます。
- ***outer-vlan-id***：追加された外部 S-VLAN タグを指定します。S-VLAN タグの範囲は 1 ～ 4094 です。
- **drop**：指定した C-VLAN を持つフレームをドロップするように指定します。

デフォルト設定

VLAN マッピングは設定されません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

特定の C-VLAN に選択的トンネリングを設定するには、**switchport vlan-mapping tunnel** *vlan-list outer-vlan-id* コマンドを使用します。

このコマンドを設定する前に、*outer-vlan-id* 引数で指定した S-VLAN を作成する必要があります。この VLAN が存在しない場合、コマンドは失敗します。

特定の C-VLAN に選択的ドロップを設定するには、**switchport vlan-mapping tunnel** *vlan-list* **drop** コマンドを使用します。

指定していないものを除く C-VLAN にトンネリングを設定するには、**switchport vlan-mapping tunnel default** *external-vlan-id* コマンドを使用します。

指定していないものを除くドロップ C-VLAN を設定するには、**switchport vlan-mapping tunnel default drop** コマンドを使用します。

switchport vlan-mapping tunnel コマンドは次のアクションを実行します。

- *vlan-list* から *outer-vlan-id* に VLAN をマッピングする ACL を作成していない場合は、作成します。
- *vlan-list* から VLAN ごとに 1 つのルールを ACL に追加します。
- この ACL の位置を TTI に予約します。TTI に十分な空き領域がない場合、コマンドは失敗します。

注。ACL は switchport mode **vlan-mapping tunnel** コマンドを使用してインターフェイスにバインドできます。

- *outer-vlan-id* 引数で指定した VLAN にエッジインターフェイスを追加します。

ACL には V + 1 ルールが含まれます。ここでは、

- **V**：指定した C-VLAN の数。

vlan-list 引数に共通の VLAN-ID が含まれていない場合にのみ、いくつかの **switchport vlan-mapping tunnel** コマンドを同じインターフェイスで定義できます。

指定した C-VLAN のトンネリングを削除し、対応する S-VLAN からインターフェイスを削除するには、**no switchport vlan-mapping tunnel** *vlan-list* コマンドを使用します。

デフォルトのトンネリングを削除し、対応する S-VLAN からインターフェイスを削除するには、**no switchport vlan-mapping tunnel default** コマンドを使用します。

すべての C-VLAN のトンネリングを削除し、対応する S-VLAN からインターフェイスを削除するには、**no switchport vlan-mapping tunnel** コマンドを使用します。

例

例 1：次に、ポート上のすべてのトラフィックの従来のトンネリングを S-VLAN ID 10 に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel default 10
switchxxxxxx(config-if)# exit
```

例 2：次に、C-VLAN ID 5、7、または 8 のトラフィックを S-VLAN ID 100 でトンネリングするようにポート上の選択的トンネリングを設定する例を示します。他の C-VLAN ID のトラフィックはドロップされます。

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# switchport vlan-mapping tunnel 5,7-8 100
switchxxxxxx(config-if)# switchport vlan-mapping tunnel 12,27 5
switchxxxxxx(config-if)# switchport vlan-mapping tunnel default drop
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping tunnel l2protocol vlan

VLAN マッピング トンネル インターフェイスで受信した、タグなしの転送レイヤ 2 フレームのカプセル化に使用する S-VLAN-ID を指定するには、インターフェイス（イーサネット、ポートチャネル）コンフィギュレーション モードで **switchport vlan-mapping tunnel l2protocol vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport vlan-mapping tunnel l2protocol vlan *vlan-id*

no switchport vlan-mapping tunnel l2protocol vlan

パラメータ

- ***vlan-id***：タグなしの転送レイヤ 2 フレームのカプセル化に使用する S-VLAN-ID を指定します。

デフォルト設定

VLAN_ID が定義されていません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

VLAN マッピング トンネル インターフェイスで受信した、タグなしの転送レイヤ 2 フレームのカプセル化に使用する S-VLAN-ID を指定するには、**switchport vlan-mapping tunnel l2protocol vlan** コマンドを使用します。S-VLAN ID は、ポートですでに定義されている S-VLAN の ID にすることも、新しい ID にすることもできます。

コマンドが設定されていない場合は、許可されているタグなしレイヤ2フレームは転送されません。

例

次に、L2 フレームの転送に使用する S-VLAN を指定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol vlan 100
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping tunnel l2protocol cos

プロバイダーネットワークに転送されるレイヤ 2 フレームの S-VLAN タグにサービスクラス（CoS）値をグローバルに指定するには、グローバル コンフィギュレーション モードで **switchport vlan-mapping tunnel l2protocol cos** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport vlan-mapping tunnel l2protocol cos *cos-value*

no switchport vlan-mapping tunnel **l2protocol cos**

パラメータ

- ***cos-value***：CoS 値を 0 ～ 7 で指定します。

デフォルト設定

cos-value は 5 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

プロバイダーネットワークに転送されるレイヤ 2 フレームの S-VLAN タグにサービスクラス（CoS）値をグローバルに指定するには、**switchport vlan-mapping tunnel l2protocol cos** コマンドを使用します。

デフォルトの CoS に戻すには、**no switchport vlan-mapping tunnel l2protocol cos** コマンドを使用します。

例

次に、転送する L2 フレームの cos を指定する例を示します。

```
switchxxxxxx(config)# switchport vlan-mapping tunnel l2protocol cos 6
```

switchport vlan-mapping tunnel l2protocol cos interface

インターフェイスごとのサービスクラス（CoS）をプロバイダーネットワークに転送するレイヤ2フレームのS-VLANタグに指定するには、インターフェイス（イーサネット、ポートチャネル）コンフィギュレーション モードで **switchport vlan-mapping tunnel l2protocol cos interface** を使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport vlan-mapping tunnel l2protocol cos interface *cos-value*

vlan-mapping tunnel l2protocol cos interface

パラメータ

- ***cos-value***：CoS 値を 0 ～ 7 で指定します。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

特定の VLAN マッピング トンネル エッジ インターフェイスで受信してプロバイダーネットワークに送信する転送レイヤ 2 フレームの S-VLAN タグにサービスクラス（CoS）値をグローバルに指定するには、**switchport vlan-mapping tunnel l2protocol cos interface** コマンドを使用します。

特定のVLANマッピング トンネル エッジ インターフェイスのデフォルトのCoSに戻すには、**no switchport vlan-mapping tunnel l2protocol cos interface** コマンドを使用します。

例

次に、転送された L2 トンネル化フレームの CoS を指定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol cos interface 6
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping tunnel l2protocol drop-threshold

特定の VLAN マッピング トンネル エッジ インターフェイスで受信できる、転送された L2 パケットのドロップしきい値を指定するには（キロビット/秒単位）、インターフェイス（イーサネット、ポートチャネル）コンフィギュレーション モードで **switchport vlan-mapping tunnel l2protocol drop-threshold** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport vlan-mapping tunnel l2protocol drop-threshold [disable | enable *committed-rate-kbps***]**

no switchport vlan-mapping tunnel l2protocol drop-threshold

パラメータ

- **disable**：インターフェイスのドロップしきい値を無効にします。
- **enable**：インターフェイスのドロップしきい値を有効にします。
- ***committed-rate-kbps***：しきい値を指定します（キロビット/秒単位）。（範囲：8 ～ 256）

デフォルト設定

ドロップしきい値が有効になっており、レートは 32 キロビット/秒に設定されています。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

特定の VLAN マッピング トンネル エッジ インターフェイスで受信した転送済み L2 プロトコルフレームのドロップしきい値を有効または無効にしてドロップレートを設定するには、switchport vlan-mapping tunnel l2protocol drop-threshold コマンドを使用します。このしきい値を超えるフレームはドロップされます。

L2 プロトコルフレームは、switchport vlan-mapping tunnel l2protocol forward （1572 ページ） コマンドを使用してトンネリングされるプロトコルフレームです。

設定を 32 キロビット/秒のレートで有効になっているデフォルトのドロップしきい値に戻すには、**no switchport vlan-mapping tunnel l2protocol drop-threshold** コマンドを使用します。

例

次に、ドロップしきい値を 16 キロビット/秒に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol drop-threshold 16
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping tunnel l2protocol forward

VLAN マッピング トンネル インターフェイスで受信したプロバイダーネットワーク上のタグなしレイヤ 2 フレームを介した転送を有効にするには、インターフェイス（イーサネット、ポートチャネル）コンフィギュレーション モードで **switchport vlan-mapping tunnel l2protocol forward** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

switchport vlan-mapping tunnel l2protocol forward [*protocol*]

no switchport vlan-mapping tunnel l2protocol forward [*protocol*]

パラメータ

- ***protocol***：コマンドを適用するプロトコルを設定します。引数には次のいずれかの値を使用できます。
  - cdp
  - lldp
  - stp
  - vtp

protocol 引数を設定しない場合、コマンドはこれらすべてのプロトコルに適用されます。

デフォルト設定

レイヤ 2 フレームは転送されません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

デフォルトでは、スイッチは次の宛先 MAC アドレスを持つエッジポートで入力 L2 PDU をドロップします。

- 01:80:C2:00:00:00-01:80:C2:00:00:FF。ただし、エッジポートで処理される LACP フレーム（宛先 01:80:C2:00:00:02）は除きます。
- 01:00:0C:00:00:00-01:00:0C:FF:FF:FF
- 01:00:0C:CD:CD:D0

VLAN マッピング トンネル インターフェイスで受信する特定のレイヤ 2 プロトコルのプロバイダーネットワークを介してタグなしフレームの転送を有効にするには、**switchport vlan-mapping**

tunnel l2protocol forward コマンドを使用します。受信したタグ付きレイヤ 2 フレームは破棄されます。

L2プロトコルが転送されると、スイッチはカスタマーの宛先MACアドレスを「既知の」マルチキャストアドレス01:00:0C:CD:CD:D0で上書きしてから、非エッジポートでフレームを送信します。

この既知のマルチキャストアドレスに等しい宛先アドレスを持つフレームを非エッジポートで受信すると、スイッチはそれをS_VLANに属するすべての非エッジポートとS-VLANに属し、特定のプロトコルの転送オプションで設定されたすべてのエッジポートに転送します。

スイッチは、「既知の」宛先 MAC アドレスをそれぞれのレイヤ 2 プロトコル MAC アドレスに置き換えます。

CDPを同じインターフェイスで有効にすることも、トンネリングすることもできません。ポート チャネル インターフェイスで **CDP** トンネリングを有効にするには、まず、**CDP** をポートチャネル（アクティブと非アクティブ）の**すべての**メンバーで無効にする必要があります。同様に、CDP が有効になっているイーサネット インターフェイスは、CDP トンネリングが有効になっているポートチャネルに追加できません。

LLDP を同じインターフェイスで有効にすることも、トンネリングすることもできません。ポート チャネルイ ンターフェイスで **LLDP** トンネリングを有効にするには、まず、**LLDP** をポートチャネル（アクティブと非アクティブ）の**すべての**メンバーで無効にする必要があります。同様に、CDP が有効になっているイーサネット インターフェイスは、CDP トンネリングが有効になっているポートチャネルに追加できません。

トンネルが定義されている場合にすべてのレイヤ 2 BPDU のデフォルトの処理に戻すには、*protocol* 引数を指定せずに **no switchport vlan-mapping tunnel l2protocol forward** コマンドを使用します。

指定したプロトコル BPDU のデフォルトの処理に戻すには、*protocol* 引数を指定して **no switchport vlan-mapping tunnel l2protocol forward** コマンドを使用します。

例 1：次に、4 つのすべてのプロトコル（CDP、LLDP、VTP、および STP）フレームを転送するように指定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol forward
switchxxxxxx(config-if)# exit
```

例 2：次に、CDP プロトコルと LLDP プロトコルのフレームのみを転送するように指定する例を示します（他の STP と VTP の 2 つのプロトコルはドロップされます）。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol forward cdp
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol forward lldp
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping one-to-one

エッジインターフェイスで 1 対 1 の VLAN 変換を設定するには、インターフェイス（イーサネット、ポートチャネル）コンフィギュレーション モードで **switchport vlan-mapping one-to-one** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

構文

switchport vlan-mapping one-to-one *vlan-id translated-vlan-id*

no switchport vlan-mapping one-to-one [*vlan-id*]

パラメータ

- ***vlan-id***：1 対 1 の VLAN 変換の外部 VLAN（E-VLAN）を指定します。指定できる範囲は 1 ～ 4094 です。
- ***translated-vlan-id***：E-VLAN を置き換える B-VLAN を指定します。指定できる範囲は 1 ～ 4094 です。

デフォルト設定

VLAN マッピングは設定されません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

選択的な 1 対 1 の VLAN 変換を設定するには、**switchport vlan-mapping one-to-one** コマンドを使用します。

このコマンドを設定する前に、*translated-vlan-id* 引数で指定した S-VLAN を作成する必要があります。この VLAN が存在しない場合、コマンドは失敗します。

異なる引数を指定した複数の **switchport vlan-mapping one-to-one** コマンドを同じインターフェイス上で定義できます。

VLAN マッピング 1 対 1 モードでは、インターフェイスは、このインターフェイス上のマッピングが出力タグ付きインターフェイスとして定義されるすべての S-VLAN に属します。インターフェイス PVID は 4095 に設定されています。

VLAN マッピング 1 対 1 モードでは、インターフェイスは 1 つの入力 ACL と 1 つの出力 ACL を使用します。**switchport vlan-mapping one-to-one** コマンドはこの ACL にルールを追加します。これらは

ACL は次の目的で適用されます。

- 入力 ACL（TTI）：

- 指定した C-VLAN-ID を S-VLAN-ID に置き換えます。
- C-VLAN-ID が指定されていないフレームをドロップします。
- タグなし入力フレームをドロップします。

- 出力 ACL（TCAM 内）：
  - S-VLAN-ID を C-VLAN-ID に置き換えます。

switchport vlan-mapping one-to-one コマンドは、これらの ACL にルールを追加し、そのモードが vlan-mapping one-to-one の場合にのみインターフェイスにバインドされます。

入力 ACL には V + 1 ルールが含まれており、出力 ACL には V ルールが含まれています。

- **V**：指定した C-VLAN の数。

特定の E-VLAN に対する 1 対 1 の VLAN 変換設定を削除するには、**no switchport vlan-mapping one-to-one** *vlan-id* コマンドを使用します。

すべての VLAN 1 対 1 変換を削除するには、**no switchport vlan-mapping one-to-one** コマンドを使用します。

例

次に、ポートで 1 対 1 VLAN 変換を設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan mapping one-to-one 5 105
switchxxxxxx(config-if)# switchport vlan mapping one-to-one 15 5
switchxxxxxx(config-if)# switchport vlan mapping one-to-one 105 225
switchxxxxxx(config-if)# exit
```

map protocol protocols-group

プロトコルをプロトコルのグループにマッピングするには、**map protocol protocols-group** VLAN コンフィギュレーション モード コマンドを使用します。このプロトコル グループは、switchport general map protocols-group vlan で使用できます。グループからプロトコルを削除するには、このコマンドの **no** 形式を使用します。

構文

map protocol *protocol* [*encapsulation-value*] **protocols-group** *group*

no map protocol *protocol* [*encapsulation*]

パラメータ

- ***protocol***：16 ビット プロトコル番号または使用上のガイドラインに記載されている予約済みの名前のいずれかを指定します。（範囲：0x0600 ～ 0xFFFF）
- ***encapsulation-value***：Ethernet、rfc1042、llcOther のいずれかの値を指定します。
- **protocols-group** *group*：プロトコルのグループのグループ番号を指定します（範囲：1 ～ 2147483647）。

デフォルト設定

デフォルトのカプセル化の値は Ethernet です。

コマンド モード

VLAN データベース コンフィギュレーション モード

使用上のガイドライン

そのプロトコルに基づくパケットの転送には、プロトコルのグループを設定し、これらのグループを VLAN にマッピングする必要があります。

値 0x8100 は、イーサネット カプセル化のプロトコル番号として有効ではありません。

次のプロトコル名がイーサネット カプセル化用に予約されています。

- ip
- arp
- ipv6
- ipx

例

次に、IP プロトコルをプロトコル グループ番号 213 にマッピングする例を示します。

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map protocol ip protocols-group 213
```

switchport general map protocols-group vlan

プロトコルに基づいてパケットを転送する（つまり、分類ルールを設定する）には、**switchport general map protocols-group vlan** インターフェイス コンフィギュレーション モード コマンドを使用します。このコマンドは、特定のプロトコルが含まれているインターフェイスに到達したパケットを特定の VLAN に転送します。プロトコルに基づくパケットの転送を停止するには、このコマンドの **no** 形式を使用します。

構文

switchport general map protocols-group *group* **vlan** *vlan-id*

no switchport general map protocols-group *group*

パラメータ

- ***group***：**map protocol protocols-group** コマンドに定義したグループ番号を指定します（範囲：1 ～ 65535）。
- ***vlan-id***：分類ルールで VLAN ID を定義します。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

VLAN 分類ルールの優先順位は次のとおりです。

- MAC ベースの VLAN（ルール間での最適一致）
- サブネット ベースの VLAN（ルール間での最適一致）
- プロトコル ベースの VLAN
- PVID

例

次に、プロトコルグループ 1 に属するプロトコルのパケットを VLAN 8 に転送する例を示します。

```
switchxxxxxx(config-if)# switchport general map protocols-group 1 vlan 8
```

show vlan protocols-groups

定義済みのプロトコルグループに属しているプロトコルを表示するには、**show vlan protocols-groups** EXEC モード コマンドを使用します。

構文

show vlan protocols-groups

コマンド モード

ユーザ EXEC モード

例

次に、プロトコルグループ情報を表示する例を示します。

```
switchxxxxxx# show vlan protocols-groups

Encapsulation            Protocol              Group ID
-------------            --------------        --------
Ethernet                 0x800 (IP)            1
Ethernet                 0x806 (ARP)           1
Ethernet                 0x86dd (IPv6)         2
Ethernet                 0x8898                3
```

map mac macs-group

MAC アドレスまたは MAC アドレス範囲を MAC アドレスのグループにマップするには、**map mac macs-group** VLAN コンフィギュレーション モード コマンドを使用します。マッピングを削除するには、このコマンドの **no** 形式を使用します。

構文

map mac *mac-address* {*prefix-mask* | **host**} **macs-group** *group*

no map mac *mac-address* {*prefix-mask* | **host**}

パラメータ

- ***mac-address***：MAC アドレスのグループにマップする MAC アドレスを指定します。
- ***prefix-mask***：マスクの 1 の数を指定します。
- **host**：マスクがすべて 1 で構成されることを指定します。
- ***group***：グループ番号を指定します（範囲：1 ～ 2147483647）。

コマンド モード

VLAN データベース コンフィギュレーション モード

使用上のガイドライン

MACアドレスに基づいてパケットを転送するには、MACアドレスのグループを設定し、これらのグループを VLAN にマップする必要があります。

最大 256 個の MAC アドレス（ホストまたは範囲）を 1 つまたは多数の MAC ベースの VLAN グループにマップできます。

例

次に、MAC アドレスの 2 つの グループを作成し、一般モードにポートを設定し、MAC アドレスのグループを特定の VLAN にマッピングする例を示します。

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
switchxxxxxx(config-vlan)# map mac 0000.0000.2222 host macs-group 2
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general map macs-group 1 vlan 2
switchxxxxxx(config-if)# switchport general map macs-group 2 vlan 3
```

switchport general map macs-group vlan

MAC ベースの分類ルールを設定するには、**switchport general map macs-group vlan** インターフェイス コンフィギュレーション モード コマンドを使用します。分類ルールを削除するには、このコマンドの no 形式を使用します。

構文

switchport general map macs-group *group* **vlan** *vlan-id*

no switchport general map macs-group *group*

パラメータ

- **group**：グループ番号を指定します（範囲：1 ～ 2147483647）。
- ***vlan-id***：ルールに関連付けられた VLAN ID を定義します。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

MAC ベースの VLAN ルールでは、同じインターフェイス上で範囲を重複させることはできません。

VLAN 分類ルールの優先順位は次のとおりです。

- MAC ベースの VLAN（ルール間での最適一致）
- サブネット ベースの VLAN（ルール間での最適一致）
- プロトコル ベースの VLAN
- PVID

使用上のガイドライン

インターフェイスに割り当てられた MAC ベースのグループ内の各 MAC アドレス（ホストまたは範囲）は、それぞれ単一の TCAM エントリを消費します。

例

次に、MAC アドレスの 2 つの グループを作成し、一般モードにポートを設定し、MAC アドレスのグループを特定の VLAN にマッピングする例を示します。

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
switchxxxxxx(config-vlan)# map mac 0000.0000.2222 host macs-group 2
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface gi1/0/4
```

```
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general map macs-group 1 vlan 2
switchxxxxxx(config-if)# switchport general map macs-group 2 vlan 3
```

show vlan macs-groups

定義されている MAC ベースの分類ルールに属する MAC アドレスを表示するには、**show vlan macs-groups** EXEC モード コマンドを使用します。

構文

show vlan macs-groups

デフォルト設定

コマンド モード

ユーザ EXEC モード

例

次に、定義されている MAC ベースの分類ルールを表示する例を示します。

```
switchxxxxxx# show vlan macs-groups
     MAC Address              Mask               Group ID
-------------------- -------------------- --------------------
  00:12:34:56:78:90            20                   22
  00:60:70:4c:73:ff            40                   1
```

map subnet subnets-group

IP サブネットを IP サブネットのグループにマッピングするには、**map subnet subnets-group** VLAN コンフィギュレーション モード コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

構文

map subnet *ip-address prefix-mask* **subnets-group** *group*

no map subnet *ip-address prefix-mask*

パラメータ

- ***ip-address***：グループにマッピングするサブネットの IP アドレス プレフィックスを指定します。
- ***prefix-mask***：マスクの 1 の数を指定します。
- ***group***：グループ番号を指定します。（範囲：1 ～ 2147483647）

コマンド モード

VLAN データベース コンフィギュレーション モード

使用上のガイドライン

その IP サブネットに基づくパケットの転送には、IP サブネットのグループを設定し、これらのグループを VLAN にマッピングする必要があります。

例

次に、IP サブネットを IP サブネット 4 のグループにマッピングする例を示します。その後、この IP サブネットのグループを VLAN 8 にマッピングします

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map subnet 172.16.1.1 24 subnets-group 4
switchxxxxxx(config-vlan)# switchport general map subnets-group 4 vlan 8
```

switchport general map subnets-group vlan

サブネットベースの分類ルールを設定するには、**switchport general map subnets-group vlan** インターフェイス コンフィギュレーション モード コマンドを使用します。サブネットベースの分類ルールを削除するには、このコマンドの **no** 形式を使用します。

構文

switchport general map subnets-group *group* **vlan** *vlan-id*

no switchport general map subnets-group *group*

パラメータ

- ***group***：グループ番号を指定します。（範囲：1 ～ 2147483647）
- ***vlan-id***：ルールに関連付けられた VLAN ID を定義します。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

VLAN 分類ルールの優先順位は次のとおりです。

- MAC ベースの VLAN（ルール間の最適な一致）
- サブネットベースの VLAN（ルール間の最適な一致）
- プロトコル ベースの VLAN
- PVID

例

次に、IP サブネットを IP サブネット 4 のグループにマッピングする例を示します。その後、この IP サブネットのグループを VLAN 8 にマッピングします

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map subnet 172.16.1.1 24 subnets-group 4
switchxxxxxx(config-vlan)# switchport general map subnets-group 4 vlan 8
```

show vlan subnets-groups

サブネットグループ情報を表示するには、**show vlan subnets-groups** EXEC モード コマンドを使用します。

構文

show vlan subnets-groups

コマンド モード

ユーザ EXEC モード

例

次に、サブネットグループ情報を表示する例を示します。

```
switchxxxxxx# show vlan subnets-groups
IP Subnet Address    Mask        Group ID
---------------- ----------- --------------
     1.1.1.1          32            1
   172.16.2.0         24            2
```

show interfaces switchport

すべてのインターフェイスまたは特定のインターフェイスの管理ステータスと動作ステータスを表示するには、**show interfaces switchport** 特権 EXEC コマンドを使用します。

構文

show interfaces switchport [*interface-id*]

パラメータ

- ***Interface-id***：インターフェイス ID を指定します。インターフェイス ID には、イーサネット ポートまたはポート チャネルのいずれかのタイプを指定できます。

コマンド モード

特権 EXEC モード

デフォルト

すべてのインターフェイスのステータスが表示されます。

使用上のガイドライン

各ポート モードには独自のプライベート設定があります。**show interfaces switchport** コマンドはすべての設定を表示しますが、[Administrative Mode] に表示される現在のポート モードに対応するポート モード設定のみがアクティブです。

例

```
switchxxxxxx# show interfaces switchport gi1/0/1
Gathering information...
S-VLAN Ethernet Type: 0x88a8 (802.1ad)
VLAN Mapping Tunnel L2 protocols Global CoS: 6
Name: gi1/0/1
Switchport: enable
Administrative Mode: access
Operational Mode: down
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs: 1
                2-4094 (Inactive)
General PVID: 1
General VLANs: none
General Egress Tagged VLANs: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: Enabled
General GVRP VLANs: none
Customer Mode VLAN: none
VLAN Mapping Tunnel:
S-VLAN Ethernet Type: 0x8100 (802.1q)
```

```
C-VLANs                 Outer S-VLAN
---------------------   ------------
2                       12
12,16-18                100
default                 1100
VLAN Mapping Tunnel L2 protocols S-VLAN: 100
VLAN Mapping Tunnel L2 protocols Interface CoS: 6 (global)
VLAN Mapping Tunnel L2 protocols forward enabled: cdp,stp
Drop Threshold: 4 kbps (default)
VLAN Mapping One-to-one:
C-VLANs                 Translated S-VLAN
---------------------   ----------------------
2                       102
12                      112
100                     10
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN: none
Protected: Enabled, Uplink is gi1/0/1
Classification rules:
Classification Type   Group ID   VLAN ID
-------------------   --------   -------
Protocol                   1        19
Protocol                   1        20
Protocol                   2        72
Subnet                     1        15
MAC                        1        77
```

private-vlan

プライベート VLAN を設定するには、**private-vlan** インターフェイス VLAN コンフィギュレーション モード コマンドを使用します。通常の VLAN 設定に VLAN を戻すには、このコマンドの **no** 形式を使用します。

構文

private-vlan {**primary** | **community** | **isolated**}

no private-vlan

パラメータ

- **primary**：VLAN をプライマリ VLAN として指定します。
- **community**：VLAN をコミュニティ VLAN として指定します。
- **isolated**：VLAN を隔離 VLAN として指定します。

デフォルト設定

プライベート VLAN は設定されていません。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

- VLAN のメンバーであるプライベート VLAN ポートがある場合は、VLAN タイプを変更することはできません。
- 他のプライベート VLAN に関連付けられている VLAN タイプを変更することはできません。
- VLAN を削除すると、VLAN タイプは VLAN のプロパティとして保持されません。

例

次の例では、vlan 2 をプライマリ VLAN として設定しています。

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# private-vlan primary
```

private-vlan association

プライマリ VLAN とセカンダリ VLAN との関連付けを設定するには、**private-vlan association** インターフェイス VLAN コンフィギュレーション モード コマンドを使用します。関連付けを解除するには、コマンドの **no** 形式を入力します。

構文

private-vlan association [**add** | **remove**] *secondary-vlan-list*

no private-vlan association

パラメータ

- **add** *secondary-vlan-list*：プライマリ VLAN に追加するタイプ セカンダリの VLAN ID の一覧。連続していない VLAN ID はカンマ（スペースなし）で区切ります。ある範囲の ID を指定するには、ハイフンを使用します。これは、デフォルトのアクションです。
- **remove** secondary-vlan-list：プライマリ VLAN から関連付けを解除するタイプがセカンダリの VLAN ID のリスト。連続していない VLAN ID はカンマ（スペースなし）で区切ります。ID の範囲を指定するには、ハイフンを使用します。

デフォルト設定

プライベート VLAN は設定されていません。

コマンド モード

インターフェイス（VLAN）コンフィギュレーション モード

使用上のガイドライン

- このコマンドは、プライマリ VLAN のコンテキストでのみ実行できます。
- 他のプライベート VLAN に関連付けられているプライベート VLAN を削除したり、そのタイプを変更したりすることはできません。
- プライマリ VLAN は、1 つの隔離 VLAN にのみ関連付けることができます。
- セカンダリ VLAN は、1 つのプライマリ VLAN にのみ関連付けることができます。
- セカンダリ VLAN のメンバーであるプライベート VLAN ポートがある場合は、セカンダリ VLAN とプライマリ VLAN との関連付けを削除することはできません。
- MSTP モードでは、プライベート VLAN に関連付けられているすべての VLAN を同じインスタンスにマップする必要があります。

例

次の例では、セカンダリ VLAN 20、21、22 および 24 をプライマリ VLAN 2 に関連付けています。

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# private-vlan association add 20-22,24
```

switchport private-vlan mapping

プライベート VLAN 無差別ポートの VLAN を設定するには、**switchport private-vlan mapping** インターフェイス コンフィギュレーション モード コマンドを使用します。このコマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

構文

switchport private-vlan mapping *primary-vlan-id* [**add** | **remove**] *secondary-vlan-list*

no switchport private-vlan mapping

パラメータ

- ***primary-vlan-id***：プライマリ VLAN の VLAN ID。
- **add** secondary-vlan-list：ポートに追加するセカンダリ VLAN を 1 つ以上指定します。
- **remove** secondary-vlan-list：ポートから削除するセカンダリ VLAN を 1 つ以上指定します。

デフォルト設定

VLAN は設定されません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

セカンダリ VLAN は、プライマリ VLAN に関連付ける必要があります。それ以外の場合、設定は受け入れられません。

例

次の例では、無差別ポート gi1/0/4 をプライマリ VLAN 10 とセカンダリ VLAN 20 に追加しています。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport private-vlan mapping 10 add 20
```

switchport private-vlan host-association

プライベート VLAN のプライマリ VLAN およびセカンダリ VLAN とホスト ポートとの関連付けを設定するには、**switchport private-vlan host-association** インターフェイス コンフィギュレーション モード コマンドを使用します。このコマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

構文

switchport private-vlan host-association *primary-vlan-id secondary-vlan-id*

no switchport private-vlan host-association

パラメータ

- ***primary-vlan-id***：プライマリ VLAN の VLAN ID。
- ***secondary-vlan-id***：セカンダリ VLAN を指定します。

デフォルト設定

関連付けはありません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

セカンダリ VLAN は、プライマリ VLAN に関連付ける必要があります。それ以外の場合、設定は受け入れられません。**private-vlan association** コマンドを参照してください。

ポート関連付け設定は、セカンダリ VLAN のタイプによって異なります。

コミュニティ セカンダリ VLAN のポート関連付け設定は、次のようになっています。

- ポートは、タグなしとしてプライマリ VLAN およびセカンダリ VLAN に追加されます。
- PVID は、セカンダリ VLAN の VLAN ID に設定されます。
- ポート入力フィルタリングは有効になっています。

隔離セカンダリ VLAN のポート関連付け設定は、次のようになっています。

- ポートは、タグなしとしてプライマリ VLAN にのみ追加され、セカンダリ VLAN には追加されません。
- PVID は、セカンダリ VLAN の VLAN ID に設定されます。
- ポート入力フィルタリングは無効になっています。

例

次に、ポート gi1/0/4 をプライマリ VLAN 10 のセカンダリ VLAN 20 に設定する例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport private-vlan host-association 10 20
```

show vlan private-vlan

プライベート VLAN 情報を表示するには、**show vlan private-vlan** EXEC モード コマンドを使用します。

構文

show vlan private-vlan [**tag** *vlan-id*]

パラメータ

- **tag** vlan-id：表示するプライベート VLAN を表すプライマリ VLAN。

デフォルト設定

すべてのプライベート VLAN が表示されます。

コマンド モード

ユーザ EXEC モード

使用上のガイドライン

show vlan private-vlan コマンドは、プライベート VLAN のメンバーであるプライベート VLAN 以外のポートを対象としません。プライマリ VLAN 以外のタグ パラメータを指定すると、show 出力が空になります。

例

```
switchxxxxxx# show vlan private-vlan
  Primary    Secondary     Type             Ports
---------- ----------- ----------- ----------------------
    150                  primary           gi1/0/1
    150         151      isolated          gi1/0/2
    160                  primary           gi1/0/3
    160         161      community         gi1/0/4
switchxxxxxx# show vlan private-vlan 150
  Primary    Secondary     Type             Ports
---------- ----------- ----------- ----------------------
    150                  primary           gi1/0/1
    150         151      isolated          gi1/0/4
```

switchport access multicast-tv vlan

アクセス ポートにマルチキャスト TV VLAN を割り当てるには、インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モードで **switchport access multicast-tv vlan** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

switchport access multicast-tv vlan *vlan-id*

no switchport access multicast-tv vlan

パラメータ

- ***vlan-id***：マルチキャスト TV VLAN ID を指定します。

デフォルト設定

マルチキャスト伝送の受信は無効です。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

ポートを別のマルチキャスト TV VLAN に割り当てると、ポートは以前の VLAN から自動的に削除され、その新しいマルチキャスト TV VLAN に追加されます。

既存のマルチキャスト TV VLAN をアクセス ポートに割り当てると、マルチキャスト TV VLAN のメンバーシップで受信したマルチキャスト メッセージはアクセス ポートに転送されます。アクセス ポートで受信したすべてのメッセージは、そのアクセス VLAN にのみブリッジされます。

例

次に、VLAN 11 からマルチキャスト伝送を受信するように gi1/0/4 を有効にする例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport access multicast-tv vlan 11
```

switchport customer multicast-tv vlan

顧客ポートにマルチキャスト TV VLAN を割り当てるには、インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モードで **switchport customer multicast-tv vlan** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

switchport customer multicast-tv vlan {**add** *vlan-list* | **remove** vlan-list}

パラメータ

- **add** *vlan-list*：インターフェイスに追加するマルチキャスト TV VLAN の一覧を指定します。
- **remove** *vlan-list*：インターフェイスから削除するマルチキャスト TV VLAN の一覧を指定します。

デフォルト設定

ポートはどの マルチキャスト TV VLAN のメンバーでもありません。

コマンド モード

インターフェイス（イーサネット、ポート チャネル）コンフィギュレーション モード

使用上のガイドライン

既存のマルチキャスト TV VLAN がカスタマー ポートに割り当てられると、マルチキャスト TV VLAN のメンバーシップで受信されたマルチキャスト メッセージはカスタマー ポートに転送されます。カスタマー ポートで受信されたすべてのメッセージは、マルチキャスト TV VLAN のみにブリッジされません。

例

次に、VLAN 5、6、7 からマルチキャスト伝送を受信するように gi1/0/4 を有効にする例を示します。

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport customer multicast-tv vlan add 5-7
```

show vlan multicast-tv

マルチキャスト TV VLAN の送信元ポートおよび受信側ポートを表示するには、**show vlan Multicast-tv** EXEC モード コマンドを使用します。送信元ポートは VLAN に対してトラフィックを送受信できますが、受信側ポートは VLAN からトラフィックを受信することだけができます。

構文

show vlan Multicast-tv vlan *vlan-id*

パラメータ

- ***vlan-id***：VLAN ID を指定します。

コマンド モード

ユーザ EXEC モード

例

次に、マルチキャスト TV VLAN 1000 の送信元ポートおよび受信側ポートに関する情報を表示する例を示します。

```
switchxxxxxx# show vlan multicast-tv vlan 1000
```

Source Ports	Receiver Ports
------------	----------------------
gi1/0/3, gi1/0/4	gi1/0/1-2

vlan prohibit-internal-usage

スイッチによって内部 VLAN として使用できない VLAN を指定するには、グローバル コンフィギュレーション モードで **vlan prohibit-internal-usage** コマンドを使用します。

構文

vlan prohibit-internal-usage none | {add | except | remove} *vlan-list*

パラメータ

- **none**：[Prohibit Internal Usage VLAN] 一覧を空にします。スイッチでは、どの VLAN も内部 VLAN として使用できます。
- **except**：[Prohibit Internal Usage VLAN] 一覧に、*vlan-list* 引数で指定されている VLAN を除くすべての VLAN を含めます。*vlan-list* 引数で指定されている VLAN のみをスイッチが内部 VLAN として使用できます。
- **add**：指定した VLAN を [Prohibit Internal Usage VLAN] 一覧に追加します。
- **remove**：指定した VLAN を [Prohibit Internal Usage VLAN] 一覧から削除します。
- ***vlan-list***：VLAN の一覧。連続していない VLAN ID はカンマ（スペースなし）で区切ります。ID の範囲を指定するには、ハイフンを使用します。使用できる VLAN ID は、1 ～ 4094 までです。

デフォルト設定

[Prohibit Internal Usage VLAN] 一覧は空になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

スイッチで内部 VLAN が必要になるのは次の場合です。

- IP インターフェイスごとに 1 つの VLAN がイーサネット ポートまたはポート チャネルに直接定義されている。
- IPv6 トンネルごとに 1 つの VLAN。
- 802.1x 用に 1 つの VLAN。

スイッチは、内部 VLAN が必要になると、VLAN ID が最も大きいフリー VLAN を取得します。

vlan prohibit-internal-usage コマンドは、リロード後に内部 VLAN として使用できない VLAN の一覧を定義する場合に使用します。

内部使用目的でソフトウェアによって VLAN が選択されている場合に、その VLAN をスタティック VLAN またはダイナミック VLAN に使用するには、次のいずれかの操作を行います。

- [Prohibited User Reserved VLAN] 一覧に VLAN を追加します。
- スタートアップ コンフィギュレーション ファイルに実行コンフィギュレーション ファイルをコピーします。
- スイッチをリロードします。
- VLAN を作成します。

例 1：次の例では、VLAN 4010、4012、および 4090 ～ 4094 を内部 VLAN として使用できないことを指定しています。

```
vlan prohibit-internal-usage add 4010,4012,4090-4094
```

例 2：次に、4000 ～ 4107 を除くすべての VLAN を内部 VLAN として使用できないことを指定する例を示します。

```
vlan prohibit-internal-usage all
vlan prohibit-internal-usage remove 4000-4107
```

例 3：次の例では、4000 ～ 4107 を除くすべての VLAN を内部 VLAN として使用できないように指定しています。

```
vlan prohibit-internal-usage 4000-4107
```

show vlan internal usage

デバイスによって内部で使用されている（ユーザによる定義）VLANの一覧を表示するには、**show vlan internal usage** 特権 EXEC モード コマンドを使用します。

構文

show vlan internal usage

コマンド モード

特権 EXEC モード

例

次に、スイッチによって内部で使用されている VLAN を表示する例を示します。

show vlan internal usage

```
User Reserved VLAN list after reset: 4010,4012,4080-4094
Current User Reserved VLAN list: 4010,4012,4090-4094
VLAN   Usage
----   --------
4089   gi1/0/2
4088   gi1/0/3
4087   tunnel 1
4086   802.1x
```

Voice VLAN コマンド

この章は、次の項で構成されています。

- show voice vlan （1604 ページ）
- show voice vlan local （1607 ページ）
- voice vlan state （1609 ページ）
- voice vlan refresh （1611 ページ）
- voice vlan id （1612 ページ）
- voice vlan vpt （1613 ページ）
- voice vlan dscp （1614 ページ）
- voice vlan oui-table （1615 ページ）
- voice vlan cos mode （1617 ページ）
- voice vlan cos （1618 ページ）
- voice vlan aging-timeout （1619 ページ）
- voice vlan enable （1620 ページ）

show voice vlan

音声 VLAN タイプが OUI の場合に、すべてのインターフェイスまたは特定のインターフェイスの音声 VLAN ステータスを表示するには、**show voice vlan** 特権 EXEC モード コマンドを使用します。

構文

show voice vlan [**type** {***oui*** [{*interface-id* | **detailed**}] | *auto*}]

パラメータ

- **type oui**：（オプション）よく使用される OUI 音声 VLAN 固有のパラメータを表示します。
- **type auto**：（オプション）よく使用される自動音声 VLAN 固有のパラメータを表示します。
- **interface-id**：（オプション）イーサネット ポート ID を指定します。
- **detailed**：（オプション）現在のポートに加えて、現在のポート以外のポートの情報を表示します。

デフォルト設定

type パラメータを省略した場合は、現在の音声 VLAN タイプが使用されます。

interface-id パラメータを省略した場合は、現在のすべてのインターフェイスに関する情報が表示されます。detailed を使用した場合は、現在のポート以外のポートも表示されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

パラメータを指定しないでこのコマンドを使用すると、現在の音声 VLAN タイプ パラメータ、ローカルの音声 VLAN 設定、および合意済みの音声 VLAN 設定が表示されます。

type パラメータを指定してこのコマンドを使用すると、選択したタイプに関連する音声 VLAN パラメータが表示されます。ローカルの音声 VLAN 設定および合意済みの音声 VLAN 設定は、これが現在の音声 VLAN ステータスである場合にのみ表示されます。

interface-id パラメータは、OUI VLAN タイプに対してのみ意味を持ちます。

例

次に、さまざまな設定でこのコマンドの出力を表示する例を示します。

例 1：**auto** 音声 VLAN パラメータを表示します（これは、実際に有効になっている音声 VLAN ステータスから独立しています）。

```
switch>show voice vlan type auto
switchxxxxxx# show voice vlan type auto
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 15:52:51
switchxxxxxx#
```

例 2：音声 VLAN ステータスが自動有効になっている場合に、現在の音声 VLAN パラメータを表示します。

```
switch>show voice vlan
Administrate Voice VLAN state is auto-enabled on IPv4
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 16:48:13
switchxxxxxx#
```

例 3：管理音声 VLAN ステータスが自動トリガーになっているものの、音声 VLAN がトリガーされていない場合に、現在の音声 VLAN パラメータを表示します。

```
switch>show voice vlan
Administrate Voice VLAN state is auto-triggered on ipv6
Operational Voice VLAN state is disabled
VSDP Authentication is disabled
```

例 4：管理音声 VLAN ステータスが自動トリガーで、音声 VLAN がトリガーされている場合に、現在の音声 VLAN パラメータを表示します。

```
switchxxxxxx(config)# voice vlan state auto-triggered
switchxxxxxx(config)# voice vlan state auto-triggered
operational voice vlan state is auto
admin state is auto triggered
switchxxxxxx# show voice vlan
Administrate Voice VLAN state is auto-triggered on ipv6
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 15:52:51
```

例 5：自動音声 VLAN と OUI の両方が無効になっている場合に、現在の音声 VLAN パラメータを表示します。

```
switch>show voice vlan
switchxxxxxx# show voice vlan
Administrate Voice VLAN state is disabled
Operational Voice VLAN state is disabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Aging timeout: 1440 minutes
```

例 6：音声 VLAN 動作状態が OUI である場合に、音声 VLAN パラメータを表示します。

```
switch>show voice vlan
Administrate Voice VLAN state is oui-enabled
Operational Voice VLAN state is oui-enabled
Best Local Voice VLAN-ID is 1 (default)
Best Local VPT is 4
Best Local DSCP is 1
Aging timeout: 1440 minutes
CoS: 6
Remark: Yes
OUI table
MAC Address - Prefix   Description
--------------------   ------------------
00:E0:BB               3COM
00:03:6B               Cisco
00:E0:75               Veritel
00:D0:1E               Pingtel
00:01:E3               Simens
00:60:B9               NEC/Philips
00:0F:E2               Huawei-3COM
00:09:6E               Avaya
Interface        Enabled    Secure    Activated  CoS Mode
-------------    -------    -------   ---------  --------
gi1/0/1              Yes        Yes         Yes      all
gi1/0/2              Yes        Yes         No       src
gi1/0/3              No         No
...
```

show voice vlan local

show voice vlan local 特権 EXEC モード コマンドは、最適なローカル音声 VLAN など、自動音声 VLAN ローカル設定に関する情報を表示します。

構文

show voice vlan local

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

例 1：CDP デバイスがインターフェイスに接続され、競合が検出されています。

```
30-Apr-2011 00:39:24 %VLAN-W-ConflictingCDPDetected: conflict detected between operational
 VLAN and new CDP device 00:1e:13:73:3d:62 on interface gi7. Platform TLV is -4FXO-K9,
Voice VLAN-ID is 100...
switchxxxxxx# show voice vlan local
Administrate Voice VLAN state is auto-triggered on IPv6
Operational Voice VLAN state is auto-enabled
VSDP Authentication is enabled, key string name is alpha
The character '*; marks the best local Voice VLAN
VLAN-ID  VPT    DSCP   Source        MAC Address         Interface
-------- -----  -----  ---------     -----------         ------------
   1       5     46    default       ---                 ---
  *104     7     63    static        ---                 ---
   100                 CDP           00:1e:13:73:3d:62   gi1/0/4
```

例 2：音声 VLAN ステータスが自動トリガーされる場合に、ローカル音声 VLAN 設定を表示します。

```
switchxxxxxx# show voice vlan local
Administrate Voice VLAN state is auto-triggered on IPv4
Operational Voice VLAN state is auto-enabled
 VLAN-ID   VPT   DSCP    Source        MAC Address       Interface
--------- ----- ------ ---------- -------------------- -----------
    1       5     46    default            ---             ---
  *100                    CDP       00:23:56:1a:dc:68     gi1/0/4   100
    CDP       00:44:55:44:55:4d     gi1/0/4
The character "*" marks the best local voice VLAN.
```

例 3：音声 VLAN ステータスが OUI である場合に、ローカル音声 VLAN 設定を表示します。

```
switchxxxxxx# show voice vlan local
Administrate Voice VLAN state is auto-OUI
Operational Voice VLAN state is OUI
The character '*; marks the best local Voice VLAN
VLAN-ID    VPT   DSCP   Source      MAC Address      Interface
---------  ----  -----  ---------   ------------     -------------------
       1    0     0     default        ---               ---
     *10    1     27    static         ---               ---
```

```
10                CDP           00:00:12:ea:87:dc    gi1/0/1
10                CDP           00:00:aa:aa:89:dc    po1
```

voice vlan state

デバイスで機能している音声 VLAN のタイプを設定したり、音声 VLAN を完全に無効にしたりするには、**voice vlan state** グローバル コンフィギュレーション モード コマンドを使用します。

デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

voice vlan state {***auto-enabled*** **|** ***auto-triggeredoui-enabled*** | ***disabled***}

no voice vlan state

パラメータ

- **auto-enabled**：自動音声 VLAN を有効にします。
- **auto-triggered**：音声 VLAN をアドバタイズする CDP デバイスをスイッチが検出した場合や、スイッチで音声 VLAN ID を手動で設定した場合に、スイッチ上の自動音声 VLAN をスタンバイにして稼働させます。
- **oui-enabled**：音声 VLAN のタイプを OUI にします。
- **disabled**：音声 VLAN を無効にします。

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

工場出荷時のデフォルトでは、CDP、LLDP、およびLLDP-MEDがスイッチで有効になっています。また、手動 Smartport モードおよび Basic QoS with trusted DSCP が有効になっています。

すべてのポートが、デフォルトの音声VLANでもあるデフォルトのVLAN 1のメンバーです。

状態がダイナミック音声 VLAN（**auto-triggered**）モードに設定されている場合、音声 VLAN はトリガー（ポートに接続された音声デバイスで受信するアドバタイズメント）によって有効になります。

管理状態は次の状態になる場合があります。

- **disabled**：動作状態は**無効**です。
- **oui-enabled**：動作状態は **oui-enabled** です。
- **auto-enabled**：動作状態は **auto-enabled** です。

- **auto-triggered**：次のいずれかが行われた場合にのみ、動作状態は **auto-triggered** です。
  - 工場出荷時のデフォルトではなく、ローカルで静的に音声 VLAN ID や CoS/802.1p や DSCP を設定する。
  - 現在のデバイスと同じファミリのデバイスでない隣接する CDP デバイスから CDP 音声 VLAN アドバタイズメントを受信する。
  - Voice Service Discovery Protocol（VSDP）メッセージをネイバー スイッチから受信した。VSDP は、SF および SG シリーズ マネージド スイッチ向けの Cisco Small Business 独自プロトコルです。
  - それ以外の場合、動作状態は **disabled** です。

注：

- 管理状態を **oui-enabled** から **auto-enabled**（または **auto-triggered**）に変更するか、その逆の変更を行うには、まず管理状態を **disabled** に設定する必要があります。
- Auto SmartPort 管理状態が**有効**である場合に、管理状態を **oui-enabled** に設定することはできません。
- 音声 VLAN がデフォルトの VLAN（VLAN 1）である場合に、管理状態を **oui-enabled** に設定することはできません。**oui-enabled** モードの場合、音声 VLAN を 1 にすることはできません。

例

例 1：次の例では、音声 VLAN の OUI モードを有効にしています。最初の試行は機能しませんでした。最初に音声 VLAN を無効にする必要があります。

```
switchxxxxxx(config)# voice vlan state oui-enabled
Disable the voice VLAN before changing the voice VLAN trigger.
switchxxxxxx(config)# voice vlan state disabled
switchxxxxxx(config)# voice vlan state oui-enabled
<CR>
```

例 2：次の例では、音声 VLAN 状態を無効にします。ポート上のすべての Auto Smartport 設定が削除されます。

```
switchxxxxxx(config)# voice vlan state disabled
All interfaces with Auto Smartport dynamic type will be set to default.
Are you sure you want to continue? (Y/N)[Y] Y
switchxxxxxx(config)# 30-Apr-2011 00:04:41 %LINK-W-Down:  Vlan 5
30-Apr-2011 00:04:41 %LINK-W-Down:  Vlan 8
30-Apr-2011 00:04:41 %LINK-W-Down:  Vlan 9
30-Apr-2011 00:04:41 %LINK-W-Down:  Vlan 100
```

例 3：次の例では、音声 VLAN 状態を auto-triggered に設定します。VLAN は、Auto Smartport 状態が適用された後に再アクティブ化されます。

```
switchxxxxxx(config)# voice vlan state auto-triggered
switchxxxxxx(config)# 30-Apr-2011 00:13:52 %LINK-I-Up:  Vlan 5
30-Apr-2011 00:13:52 %LINK-I-Up:  Vlan 8
30-Apr-2011 00:13:52 %LINK-I-Up:  Vlan 9
30-Apr-2011 00:13:52 %LINK-I-Up:  Vlan 100
```

voice vlan refresh

外部から学習したすべての音声 VLAN 属性を削除し、音声 VLAN をデフォルトの音声 VLAN にリセットすることで、VLAN 内のすべての自動音声 VLAN 対応スイッチで音声 VLAN 検出プロセスを再開するには、**voice vlan refresh** グローバル コンフィギュレーション モード コマンドを使用します。

構文

voice vlan refresh

パラメータ

このコマンドには、引数またはキーワードはありません。

デフォルト設定

なし

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# voice vlan refresh
switchxxxxxx(config)#
30-Apr-2011 02:01:02 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by VSDP. Voice VLAN-ID
 100, VPT 5, DSCP 46 (Notification that Agreed Voice VLAN is updated)
(Auto Smartport configuration is changed)
30-Apr-2011 02:01:05 %LINK-W-Down:  Vlan 50
30-Apr-2011 02:01:05 %LINK-W-Down:  Vlan 100
30-Apr-2011 02:01:06 %LINK-I-Up:  Vlan 50
30-Apr-2011 02:01:06 %LINK-I-Up:  Vlan 100
switchxxxxxx# show voice vlan
Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 100
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
(Following is the new active source)
Agreed Voice VLAN is received from switch b0:c6:9a:c1:da:00
Agreed Voice VLAN priority is  2 (active CDP device)
Agreed Voice VLAN-ID is 100
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Apr-30 02:01:02
```

voice vlan id

音声 VLAN の VLAN 識別子を静的に設定するには、**voice vlan id** グローバル コンフィギュレーション モード コマンドを使用します。音声 VLAN をデフォルトの VLAN（1）に戻すには、このコマンドの **no** 形式を使用します。

構文

voice vlan id *vlan-id*

no voice vlan id

パラメータ

vlan id *vlan-id*：音声 VLAN（範囲 1 ～ 4094）を指定します。

デフォルト設定

VLAN ID 1 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

音声 VLAN は、存在しなければ自動的に作成されます。このコマンドの **no** 形式によって、これが自動的に削除されることはありません。

例

次の例では、デバイス上の音声 VLAN として VLAN 35 を有効にします。

```
switchxxxxxx(config)# voice vlan id 35
For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCP will cause
the switch to advertise the administrative voice VLAN as static voice VLAN which has
higher priority than voice VLAN learnt from external sources.
Are you sure you want to continue? (Y/N)[Y] Y
30-Apr-2011 00:19:36 %VLAN-I-VoiceVlanCreated: Voice Vlan ID 35 was created.
switchxxxxxx(config)# 30-Apr-2011 00:19:51 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated
 by VSDP. Voice VLAN-ID 35, VPT 5, DSCP 46
```

voice vlan vpt

ネットワーク ポリシー TLV の LLDP によってアドバタイズされる VPT（802.1p VLAN プライオリティ タグ）の値を指定するには、**voice vlan vpt** グローバル コンフィギュレーション モード コマンドを使用します。この値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

voice vlan vpt *vpt-value*

no voice vlan vpt

パラメータ

vpt *vpt-value*：アドバタイズする VPT 値（範囲 0 ～ 7）。

デフォルト設定

5

コマンド モード

グローバル コンフィギュレーション モード

例

次に、音声 VLAN VPT として 7 を設定する例を示します。新しい設定が古い設定とは異なるという通知が表示されます。

```
switchxxxxxx(config)# voice vlan vpt 7
For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCPwill cause the
 switch to advertise the administrative voice VLAN as static voice VLANwhich has higher
 priority than voice VLAN learnt from external sources.
Are you sure you want to continue? (Y/N)[Y] Y
30-Apr-2011 00:24:52 %VLAN-W-BestLocal!=Oper: inconsistency detected, VSDP voice VLAN
configuration differs from best local. Best local is Voice VLAN-ID 104, VPT 5, DSCP 46
switchxxxxxx(config)# 30-Apr-2011 00:25:07 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated
 by VSDP. Voice VLAN-ID 104, VPT 7, DSCP 46
```

voice vlan dscp

ネットワーク ポリシーTLVのLLDPによってアドバタイズされるDSCPの値を指定するには、**voice vlan dscp** グローバル コンフィギュレーション モード コマンドを使用します。この値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

voice vlan dscp *dscp-value*

no voice vlan dscp

パラメータ

dscp *dscp-value*：DSCP 値（範囲 0 ～ 63）。

デフォルト設定

46

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、音声 VLAN DSCP として 63 が設定されています。

```
switchxxxxxx(config)# voice vlan dscp 63
For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCPwill cause the
 switch to advertise the administrative voice VLAN as static voice VLANwhich has higher
 priority than voice VLAN learnt from external sources.
Are you sure you want to continue? (Y/N)[Y] Y
30-Apr-2011 00:31:07 %VLAN-W-BestLocal!=Oper: inconsistency detected, VSDP voice VLAN
configuration differs from best local. Best local is Voice VLAN-ID 104, VPT 7, DSCP 46
switchxxxxxx(config)# 30-Apr-2011 00:31:22 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated
 by VSDP. Voice VLAN-ID 104, VPT 7, DSCP 63
```

voice vlan oui-table

音声 OUI テーブルを設定するには、**voice vlan oui-table** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

voice vlan oui-table *{**add** mac-address-prefix | **remove** mac-address-prefix}* [*text*]

no voice vlan oui-table

パラメータ

- **add** *mac-address-prefix*：指定した MAC アドレス プレフィックスを音声 VLAN OUI テーブルに追加します（長さ：3 バイト）。
- **remove** *mac-address-prefix*：指定した MAC アドレス プレフィックスを音声 VLAN OUI テーブルから削除します（長さ：3 バイト）。
- **text**：（オプション）指定したテキストを指定した MAC アドレスの説明として音声 VLAN OUI テーブルに追加します（長さ：1 ～ 32 文字）。

デフォルト設定

デフォルトの音声 VLAN OUI テーブルは次のとおりです。

OUI	説明
00:01:e3	Siemens AG の電話機
00:03:6b	Cisco の電話機
00:09:6e	Avaya の電話機
00:0f:e2	Huawei-3COM の電話機
00:60:b9	NEC/Philips の電話機
00:d0:1e	Pingtel の電話機
75:e0:00	Veritel Polycom の電話機
00:e0:bb	3COM の電話機

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

VoIP 設備/電話機からのパケットの分類は、送信元 MAC アドレスにおけるパケットの OUI に基づいています。OUI は、IEEE によってグローバルに割り当てられます（管理されます）。

MAC アドレスの場合、最初の 3 バイトには製造者 ID（組織固有識別子（OUI））が含まれ、最後の 3 バイトには一意のステーション ID が含まれています。

市場で優位に立つ IP フォン メーカーは数が限られ、名前もよく知られているため、既知の OUI 値がデフォルトで設定されており、ユーザは必要に応じて OUI を追加/削除できます。

例

次の例では、音声 VLAN OUI テーブルにエントリを追加しています。

```
switchxxxxxx(config)# voice vlan oui-table add 00:AA:BB experimental
```

voice vlan cos mode

サービス（CoS）モードの OUI 音声 VLAN クラスを選択するには、**voice vlan cos mode** インターフェイス コンフィギュレーション モード コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

構文

voice vlan cos mode {*src* | **all** }

no voice vlan cos mode

パラメータ

- **src**：QoS 属性は、送信元 MAC アドレスに OUI があるパケットに適用されます。
- **all**：QoS 属性は、音声 VLAN に分類されるパケットに適用されます。

デフォルト設定

デフォルト モードは **src** です。

コマンド モード

インターフェイス コンフィギュレーション モード

例

次の例では、音声パケットに QoS 属性を適用しています。

```
switchxxxxxx(config-if)# voice vlan cos mode all
```

voice vlan cos

OUI 音声 VLAN サービス クラス（CoS）を設定するには、**voice vlan cos** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

voice vlan *cos cos* [*remark*]

no voice vlan cos

パラメータ

- **cos** *cos*：音声 VLAN サービス クラスの値を指定します。（範囲：0 ～ 7）
- **remark**：（オプション）L2 ユーザ優先順位を CoS 値で再マークすることを指定します。

デフォルト設定

デフォルトの CoS 値は、6 です。

L2 ユーザ優先順位は、デフォルトでは再マークされません。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、OUI 音声 VLAN CoS を 7 に設定し、再マークを行わないようにしています。

```
switchxxxxxx(config)# voice vlan cos 7
```

voice vlan aging-timeout

OUI 音声 VLAN エージング タイムアウト間隔を設定するには、**voice vlan aging-timeout** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

voice vlan aging-timeout *minutes*

no voice vlan aging-timeout

パラメータ

aging-timeout *minutes*：音声 VLAN エージング タイムアウト間隔を分単位で指定します。（範囲：1 ～ 43200）。

デフォルト設定

1440 分

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、OUI 音声 VLAN エージング タイムアウト間隔を 12 時間に設定しています。

```
switchxxxxxx(config)# voice vlan aging-timeout 720
```

voice vlan enable

インターフェイスで OUI 音声 VLAN 設定を有効にするには、**voice vlan enable** インターフェイス コンフィギュレーション モード コマンドを使用します。インターフェイスで OUI 音声 VLAN 設定を無効にするには、このコマンドの **no** 形式を使用します。

構文

voice vlan enable

no voice vlan enable

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

無効

コマンド モード

インターフェイス コンフィギュレーション モード

使用上のガイドライン

このコマンドは、音声 VLAN 状態が（show voice vlan （1604 ページ） を使用して）OUI 音声 VLAN としてグローバルに設定されている場合にのみ適用できます。

ポートは、PVID/ネイティブ VLAN ID のメンバーである場合にのみ音声 VLAN に参加できます。

送信元 MAC アドレス OUI アドレス（voice vlan oui-table （1615 ページ） によって定義）があるパケットがポートでトラップされると、ポートが音声 VLAN に追加されます。注：パケット VLAN ID は、音声 VLAN である必要はありません。任意の VLAN にすることができます。

ポートは、タグ付きポートとして音声 VLAN に参加します。

送信元 MAC アドレス OUI アドレスのある最後の MAC アドレスをインターフェイスで受信してからの時間がタイムアウト リミット（voice vlan aging-timeout （1619 ページ） によって設定）を超えた場合、インターフェイスは音声 VLAN から削除されます。

例

次に、gi1/0/2 で OUI 音声 VLAN 設定を有効にする例を示します。

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# voice vlan enable
```

Web サーバ コマンド

この章は、次の項で構成されています。

- ip https certificate （1622 ページ）
- ip https logging （1623 ページ）
- ip http port （1624 ページ）
- ip http server （1625 ページ）
- ip http secure-server （1626 ページ）
- ip http timeout-policy （1627 ページ）
- show ip http （1628 ページ）
- show ip https （1629 ページ）

ip https certificate

HTTPS のアクティブな証明書を設定するには、**ip https certificate** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ip https certificate *number*

no ip https certificate

パラメータ

number：証明書番号を指定します。(範囲：1 ～ 2)

デフォルト設定

デフォルトの証明書番号は 1 です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、HTTPS のアクティブな証明書を設定しています。

```
switchxxxxxx(config)# ip https certificate 2
```

ip https logging

HTTPS セッションのセットアップと切断のロギングを有効または無効にするには、グローバル コンフィギュレーション モードで ip https logging コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

構文

ip https logging {enable| disable}

no ip https logging

パラメータ

- **enable**：デバイスで HTTPS ロギングを有効にします
- **disable**：デバイスで HTTPS ロギングを無効にします。

デフォルト設定

デフォルトでは、HTTPS セッションロギングは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード。

使用上のガイドライン

このコマンドは、デバイスで HTTPS ロギングを有効にします。HTTPS ロギングは、HTTPS セッションのセットアップと切断の進行状況を追跡する手段です。HTTPS セッションのセットアップと切断の進行状況は、プロセスの一部として生成される SYSLOG メッセージを使用して追跡されます。HTTPS ロギングが無効になっている場合、SSH のセットアップまたは切断プロセスの一部として SYSLOG メッセージは生成されません。

例

次に、デバイスで HTTPS ロギングを有効にする例を示します。

```
switchxxxxxx(config)# ip https logging enable
```

ip http port

Web ブラウザ インターフェイスで使用する TCP ポートを指定するには、**ip http port** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ip http port *port-number*

no ip http port

パラメータ

port *port-number*：HTTP サーバで使用するためのものです。（範囲：1 ー 59999）

デフォルト設定

デフォルトのポート番号は 80 です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、http ポート番号を 100 に設定しています。

```
switchxxxxxx(config)# ip http port 100
```

ip http server

Web ブラウザからデバイスを設定およびモニタできるようにするには、**ip http server** グローバル コンフィギュレーション モード コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip http server

no ip http server

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

HTTP サーバが有効です。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、Web ブラウザからデバイスを設定できるようにしています。

```
switchxxxxxx(config)# ip http server
```

ip http secure-server

ブラウザからデバイスを安全に設定またはモニタできるようにするには、**ip http secure-server** グローバル コンフィギュレーション モード コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip http secure-server

no ip http secure-server

パラメータ

このコマンドには引数またはキーワードはありません。

デフォルト設定

有効

コマンド モード

グローバル コンフィギュレーション モード

例

```
switchxxxxxx(config)# ip http secure-server
```

ip http timeout-policy

http/https セッションでシステムがユーザ入力を待機する間隔を設定するには（これを過ぎるとシステムは自動的にログオフします）、**ip http timeout-policy** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

構文

ip http timeout-policy *idle-seconds* [{**http-only** | **https-only**}]

no ip http timeout-policy

パラメータ

- ***idle-seconds***：データの受信がない場合や、応答データを送信できない場合に、接続をオープンしたままにしておく最大秒数を指定します。（範囲：0 ～ 86400）
- **http-only**：（オプション）http に対してのみタイムアウトを指定します。
- **https-only**：（オプション）https に対してのみタイムアウトを指定します。

デフォルト設定

600 秒。設定は HTTP と HTTPS の両方に適用されます。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

タイムアウトを指定しないようにするには、**ip http timeout-policy 0** コマンドを入力します。

例

次の例では、http タイムアウトを 1000 秒に設定しています。

```
switchxxxxxx(config)# ip http timeout-policy 1000
```

show ip http

HTTP サーバ設定を表示するには、**show ip http** 特権 EXEC モード コマンドを使用します。

構文

show ip http

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

次の例では、HTTP サーバの構成が表示されています。

```
switchxxxxxx# show ip http
HTTP server enabled
Port: 80
Interactive timeout: 10 minutes, 0 seconds
```

show ip https

HTTPS サーバー設定を表示するには、**show ip https** 特権 EXEC モードコマンドを使用します。

構文

show ip https

パラメータ

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC モード

例

次の例では、HTTPS サーバの構成が表示されています。

```
switchxxxxxx# show ip https
HTTPS server enabled
Port: 443
Interactive timeout: Follows the HTTP interactive timeout (10 minutes, 0 seconds)
https session logging is disabled
Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```

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。