Catalyst 2960-XR スイッチ セキュリティ コマンド リファレンス、Cisco IOS Release 15.0(2)EX1

初版：2013 年 08 月 08 日

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

Text Part Number: OL-29433-01-J

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

目 次

はじめに

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。 たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します （ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
bold フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
Italic フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*italic* フォントで示しています。
`courier` フォント	システムが表示するターミナルセッションおよび情報は、`courier` フォントで示しています。
`太字の courier フォント`	太字の courier フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。

表記法	説明
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。 stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

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

ヒント 「問題解決に役立つ情報」です。

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

ワンポイント アドバイス　時間を節約する方法です。 ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　**「警告」の意味です。 人身事故を予防するための注意事項が記述されています。**

関連資料

（注）　スイッチをインストールまたはアップグレードする前に、スイッチのリリース ノートを参照してください。

- 次の URL にある Catalyst 2960-XR スイッチのマニュアル：
  http://www.cisco.com/go/cat2960xr_docs
- 次の URL にある Cisco SFP および SFP+ モジュールのマニュアル（互換性マトリクスを含む）：
  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- 次の URL にある Cisco Validated Design （CVD）のマニュアル：
  http://www.cisco.com/go/designzone

マニュアルの入手方法およびテクニカル サポート

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

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

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

コマンドライン インターフェイスの使用

コマンドライン インターフェイスの使用に関する情報

コマンド モード

Cisco IOS ユーザ インターフェイスは、いくつかのモードに分かれています。 使用できるコマンドの種類は、現在のモードによって異なります。 システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。

CLI セッションはコンソール接続、Telnet、SSH、またはブラウザを使用することによって開始できます。

セッションを開始すると、ユーザ モード（別名ユーザ EXEC モード）から始まります。 ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。 たとえばユーザ EXEC コマンドの大部分は、**show** コマンド（現在のコンフィギュレーション ステータスを表示する）、**clear** コマンド（カウンタまたはインターフェイスをクリアする）などのように、1 回限りのコマンドです。 ユーザ EXEC コマンドは、スイッチをリブートするときには保存されません。

すべてのコマンドにアクセスするには、特権EXECモードを開始する必要があります。 特権EXECモードを開始するには、通常、パスワードが必要です。 このモードでは、任意の特権 EXEC コマンドを入力でき、また、グローバル コンフィギュレーション モードを開始することもできます。

コンフィギュレーション モード（グローバル、インターフェイス、およびライン）を使用して、実行コンフィギュレーションを変更できます。 設定を保存した場合はこれらのコマンドが保存され、スイッチをリブートするときに使用されます。 各種のコンフィギュレーション モードにアクセスするには、まずグローバル コンフィギュレーション モードを開始する必要があります。 グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードに移行できます。

次の表に、主要なコマンド モード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。

表 *1*：コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	Telnet、SSH、またはコンソールを使用してセッションを開始します。	`Switch>`	**logout** または **quit** を入力します。	このモードを使用して次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`Switch#`	**disable** を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`Switch(config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。	このモードは、スイッチ全体に適用するパラメータを設定する場合に使用します。
VLAN コンフィギュレーション	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`Switch(config-vlan)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	

モード	アクセス方法	プロンプト	終了方法	モードの用途
				このモードを使用して、VLAN（仮想LAN）パラメータを設定します。VTPモードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が1006以上）を作成してスイッチのスタートアップ コンフィギュレーション ファイルに設定を保存できます。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを入力し、インターフェイスを指定します。	`Switch(config-if)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権EXECモードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、イーサネット ポートのパラメータを設定します。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで、**line vty** または **line console** コマンドを使用して回線を指定します。	`Switch(config-line)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権EXECモードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、端末回線のパラメータを設定します。

ヘルプ システムの使用

システム プロンプトで疑問符（?）を入力すると、各コマンド モードに使用できるコマンドのリストが表示されます。 また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。

手順の概要

1. **help**
2. *abbreviated-command-entry* **?**
3. *abbreviated-command-entry* <Tab>
4. **?**
5. *command* **?**
6. *command keyword* **?**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**help** 例： `Switch# help`	コマンド モードのヘルプ システムの簡単な説明を表示します。

ステップ 2	*abbreviated-command-entry* **?**
	
	例：
	`Switch# di?`
	`dir disable disconnect`
		特定のストリングで始まるコマンドのリストを表示します。

ステップ 3	*abbreviated-command-entry* <Tab>
	
	例：
	`Switch# sh conf<tab>`
	`Switch# show configuration`
		特定のコマンド名を補完します。

ステップ 4	**?** 例： `Switch> ?`	特定のコマンド モードで使用可能なすべてのコマンドをリストします。
ステップ 5	*command* **?** 例： `Switch> show ?`	コマンドに関連するキーワードを一覧表示します。

	コマンドまたはアクション	目的

ステップ 6	*command keyword* **?**
	
	例：
	`Switch(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`
		キーワードに関連する引数を一覧表示します。

コマンドの省略形

スイッチでコマンドが一意に認識される長さまでコマンドを入力します。

show configuration 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
Switch# show conf
```

コマンドの no 形式および default 形式

大部分のコンフィギュレーション コマンドに、**no** 形式があります。 **no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、**no shutdown** 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、インターフェイスのシャットダウンが取り消されます。 **no** キーワードなしでコマンドを使用すると、ディセーブルにされた機能を再度イネーブルにしたり、デフォルトでディセーブルになっている機能をイネーブルにすることができます。

コンフィギュレーション コマンドには、**default** 形式もあります。 コマンドの **default** 形式は、コマンドの設定値をデフォルトに戻します。 大部分のコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じになります。 ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。 これらのコマンドについては、**default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI のエラー メッセージ

次の表に、CLI を使用してスイッチを設定するときに表示される可能性のあるエラー メッセージの一部を紹介します。

表 *2* : *CLI* の代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	スイッチがコマンドとして認識できるだけの文字数が入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Incomplete command.`	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。 間違っている箇所をキャレット（^）記号で示しています。	疑問符（?）を入力すると、そのコマンド モードで使用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギング

スイッチの設定変更を記録して表示させることができます。 Configuration Change Logging and Notification 機能を使用することで、セッションまたはユーザ ベースごとに変更内容をトラッキングできます。 ログに記録されるのは、適用された各コンフィギュレーション コマンド、コマンドを入力したユーザ、コマンドの入力時間、コマンドに対するパーサからのリターン コードです。この機能には、登録しているアプリケーションの設定が変更されるときに通知される非同期通知方式もあります。 Syslog へこの通知を送信することも選択できます。

（注） CLI または HTTP の変更のみがログとして記録されます。

CLI を使用して機能を設定する方法

コマンド履歴の設定

入力したコマンドは、ソフトウェア側にコマンド履歴として残されます。 コマンド履歴機能は、アクセスコントロールリストの設定時など、長い複雑なコマンドまたはエントリを何度も入力しなければならない場合、特に便利です。 必要に応じて、この機能をカスタマイズできます。

コマンド履歴バッファ サイズの変更

デフォルトでは、スイッチは履歴バッファにコマンドライン10行を記録します。 現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。 この手順は任意です。

手順の概要

1. **terminal history** [**size** *number-of-lines*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal history** [**size** *number-of-lines*] 例： `Switch# terminal history size 200`	特権 EXEC モードで現在のターミナル セッション中にスイッチが記録するコマンドラインの数を変更します。 サイズは 0 から 256 までの間で設定できます。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、次の表に示すいずれかの操作を行います。 これらの操作は任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

手順の概要

1. **Ctrl+P** または**上矢印**キー
2. **Ctrl+N** または**下矢印**キー
3. **show history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**Ctrl+P** または上矢印キー	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。
ステップ 2	**Ctrl+N** または下矢印キー	**Ctrl+P** または上矢印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。
ステップ 3	**show history** 例： `Switch# show history`	特権 EXEC モードで、直前に入力したコマンドをいくつか表示します。 表示されるコマンドの数は、**terminal history** グローバル コンフィギュレーション コマンドおよび **history** ライン コンフィギュレーション コマンドの設定値によって指定されます。

コマンド履歴機能のディセーブル化

コマンド履歴機能は、自動的にイネーブルになっています。 現在の端末セッションまたはコマンドラインでディセーブルにできます。 この手順は任意です。

手順の概要

1. **terminal no history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal no history** 例： `Switch# terminal no history`	特権 EXEC モードで現在のターミナル セッションにおけるこの機能をディセーブルにします。

編集機能のイネーブル化およびディセーブル化

拡張編集モードは自動的にイネーブルになりますが、ディセーブルにして再度イネーブルにすることができます。

手順の概要

1. **terminal editing**
2. **terminal no editing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal editing** 例： `Switch# terminal editing`	特権 EXEC モードで現在のターミナル セッションにおける拡張編集モードを再びイネーブルにします。
ステップ 2	**terminal no editing** 例： `Switch# terminal no editing`	特権 EXEC モードで現在のターミナル セッションにおける拡張編集モードをディセーブルにします。

キーストロークによるコマンドの編集

キーストロークは、コマンドラインの編集に役立ちます。 これらのキーストロークは任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 *3*：編集コマンド

編集コマンド	説明
Ctrl-B または**左矢印**キー	カーソルを 1 文字後退させます。
Ctrl-F または**右矢印**キー	カーソルを 1 文字前進させます。
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。
Esc B	カーソルを 1 単語後退させます。
Esc F	カーソルを 1 単語前進させます。
Ctrl+T	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
Delete キーまたは **Backspace** キー	カーソルの左にある文字を消去します。
Ctrl+D	カーソル位置にある文字を削除します。
Ctrl+K	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
Ctrl+U または Ctrl+X	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
Ctrl+W	カーソルの左にある単語を削除します。
Esc D	カーソルの位置から単語の末尾までを削除します。
Esc C	カーソル位置のワードを大文字にします。

Esc L	カーソルの場所にある単語を小文字にします。
Esc U	カーソルの位置から単語の末尾までを大文字にします。
Ctrl+V または Esc Q	特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。
Return キー	1 行または 1 画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 （注） **show** コマンドの出力など、端末画面に一度に表示できない長い出力では、More プロンプトが使用されます。More プロンプトが表示された場合は、Return キーおよびスペース キーを使用してスクロールできます。
スペース バー	1 画面分下にスクロールします。
Ctrl+L または Ctrl+R	スイッチから画面に突然メッセージが出力された場合に、現在のコマンドラインを再表示します。

画面幅よりも長いコマンドラインの編集

画面上で 1 行分を超える長いコマンドラインについては、コマンドのラップアラウンド機能を使用できます。 カーソルが右マージンに達すると、そのコマンドラインは 10 文字分だけ左へシフトされます。 コマンドラインの先頭から 10 文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。 これらのキー操作は任意です。

コマンドの先頭にスクロールして入力内容をチェックするには、Ctrl+B キーまたは←キーを繰り返し押します。 コマンドラインの先頭に直接移動するには、Ctrl+A を押します。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次に、画面上で 1 行分を超える長いコマンドラインを折り返す例を示します。

手順の概要

1. **access-list**
2. **Ctrl+A**
3. **Return** キー

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**access-list**
	
	例：
	`Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		1 行分を超えるグローバル コンフィギュレーション コマンド入力を表示します。
		最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。 ドル記号（$）は、その行が左へスクロールされたことを表します。 カーソルが行末に達するたびに、その行は再び10 文字分だけ左へシフトされます。

ステップ 2	**Ctrl+A** 例： `Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	完全な構文をチェックします。 行末に表示されるドル記号（$）は、その行が右へスクロールされたことを表します。
ステップ 3	**Return** キー	コマンドを実行します。 ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。 画面の幅が異なる場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。 ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンドエントリを呼び出して変更できます。

show および more コマンド出力の検索およびフィルタリング

show および **more** コマンドの出力を検索およびフィルタリングできます。 この機能は、大量の出力をソートする場合や、出力から不要な情報を除外する場合に役立ちます。 これらのコマンドの使用は任意です。

手順の概要

1. {**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	{**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*
	
	例：
	`Switch# show interfaces | include protocol`
	`Vlan1 is up, line protocol is up`
	`Vlan10 is up, line protocol is down`
	`GigabitEthernet1/0/1 is up, line protocol is down`
	`GigabitEthernet1/0/2 is up, line protocol is up`
		出力を検索およびフィルタリングします。
		文字列では、大文字と小文字が区別されます。 たとえば、**| exclude output** と入力した場合、**output** を含む行は表示されませんが、**Output** を含む行は表示されます。

コンソール接続または Telnet による CLI アクセス

CLI にアクセスするには、スイッチのハードウェア インストレーション ガイドに記載されている手順で、スイッチのコンソール ポートに端末または PC を接続するか、または PC をイーサネット管理ポートに接続して、スイッチの電源をオンにする必要があります。

スイッチがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッションによって CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にスイッチを設定しておく必要があります。

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチ コンソール ポートに管理ステーションまたはダイヤルアップ モデムを接続するか、またはイーサネット管理ポートに PC を接続します。 コンソール ポートまたはイーサネット管理ポートへの接続については、スイッチのハードウェア インストレーション ガイドを参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化 Secure Shell（SSH; セキュア シェル）パッケージを使用します。 スイッチは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、スイッチにイネーブル シークレット パスワードを設定しておくことも必要です。
  - スイッチは同時に最大 16 の Telnet セッションをサポートします。 1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。
  - スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

コンソール ポート、イーサネット管理ポート、Telnet セッション、または SSH セッションを通じて接続すると、管理ステーション上にユーザ EXEC プロンプトが表示されます。

セキュリティ コマンド

aaa accounting dot1x

認証、許可、アカウンティング（AAA）アカウンティングをイネーブルにして、IEEE 802.1x セッションの特定のアカウンティング方式を、回線単位またはインターフェイス単位で定義する方式リストを作成するには **aaa accounting dot1x** 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。 IEEE 802.1x アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting dot1x {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ...] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}...]}

no aaa accounting dot1x {*name* | **default** }

構文の説明

name	サーバ グループ名。 これは、**broadcast group** および **group** キーワードの後に入力する場合に使用するオプションです。
default	デフォルト リストにあるアカウンティング方式を、アカウンティング サービス用に指定します。
start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。 start アカウンティング レコードはバックグラウンドで送信されます。 アカウンティング サーバが start accounting 通知を受け取ったかどうかには関係なく、要求されたユーザ プロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウンティング レコードをイネーブルにして、アカウンティング レコードを各グループの最初のサーバに送信します。 最初のサーバが利用できない場合、スイッチはバックアップ サーバのリストを使用して最初のサーバを識別します。
group	アカウンティング サービスに使用するサーバ グループを指定します。 有効なサーバ グループ名は次のとおりです。 • *name*：サーバ グループ名 • **radius**：すべての RADIUS ホストのリスト • **tacacs+**：全 TACACS+ ホストのリスト **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。 オプションの **group** キーワードより多くのキーワードを入力できます。
radius	（任意）RADIUS アカウンティングをイネーブルにします。
tacacs+	（任意）TACACS+ アカウンティングをイネーブルにします。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、RADIUS サーバへのアクセスが必要です。

インターフェイスに IEEE 802.1x RADIUS アカウンティングを設定する前に、**dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを入力することを推奨します。

例

次の例では、IEEE 802.1x アカウンティングを設定する方法を示します。

```
Switch(config)# aaa new-model
Switch(config)# aaa accounting dot1x default start-stop group radius
```

aaa accounting identity

IEEE 802.1x、MAC 認証バイパス（MAB）および Web 認証セッションの認証、許可、およびアカウンティング（AAA）アカウンティングをイネーブルにするには、**aaa accounting identity** 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。 IEEE 802.1x アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting identity {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ...] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}...]}

no aaa accounting identity {*name* | **default** }

構文の説明

name	サーバ グループ名。 これは、**broadcast group** および **group** キーワードの後に入力する場合に使用するオプションです。
default	デフォルト リストにあるアカウンティング方式を、アカウンティング サービス用に使用します。
start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。 start アカウンティング レコードはバックグラウンドで送信されます。 アカウンティング サーバが start アカウンティング通知を受け取ったかどうかには関係なく、要求されたユーザプロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウンティング レコードをイネーブルにして、アカウンティング レコードを各グループの最初のサーバに送信します。 最初のサーバが利用できない場合、スイッチはバックアップ サーバのリストを使用して最初のサーバを識別します。
group	アカウンティング サービスに使用するサーバ グループを指定します。 有効なサーバ グループ名は次のとおりです。 • *name*：サーバ グループ名 • **radius**：すべての RADIUS ホストのリスト • **tacacs+**：全 TACACS+ ホストのリスト **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。 オプションの **group** キーワードより多くのキーワードを入力できます。
radius	（任意）RADIUS 認証をイネーブルにします。
tacacs+	（任意）TACACS+ アカウンティングをイネーブルにします。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

AAA アカウンティング アイデンティティをイネーブルにするには、ポリシー モードをイネーブルにする必要があります。 ポリシー モードをイネーブルにするには、特権 EXEC モードで **authentication display new-style** コマンドを入力します。

例

次の例では、IEEE 802.1x アカウンティング アイデンティティを設定する方法を示します。

```
Switch# authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.

(1) If you save the config in this mode, it will be written
    to NVRAM in NEW-style config, and if you subsequently
    reload the router without reverting to legacy config and
    saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
    will only become IPv6-capable once you have entered new-
    style config manually, or have reloaded with config saved
    in 'authentication display new' mode.

Switch# configure terminal
Switch(config)# aaa accounting identity default start-stop group radius
```

aaa authentication dot1x

IEEE 802.1x 認証に準拠するポートで認証、許可、アカウンティング（AAA）方式を使用するように指定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **aaa authentication dot1x** 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。 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication dot1x {**default**} *method1*

no aaa authentication dot1x {**default**} *method1*

構文の説明

default	ユーザがログインするときのデフォルトの方式。 この引数の後に続く、リストされた認証方式を使用します。
method1	サーバ認証を指定します。 認証用にすべての RADIUS サーバのリストを使用するには、**group radius** キーワードを入力します。 （注） 他のキーワードがコマンドラインのヘルプ ストリングに表示されますが、サポートされているのは **default** および **group radius** キーワードだけです。

コマンド デフォルト

認証は実行されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために特定の順序で試みる方式を指定します。 実際に 802.1x に準拠している唯一の方式は、クライアント データが RADIUS 認証サーバに対して確認される **group radius** 方式です。

group radius を指定した場合、**radius-server host** グローバル コンフィギュレーション コマンドを使用して RADIUS サーバを設定する必要があります。

設定された認証方式のリストを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

例

次の例では AAA をイネーブルにして IEEE 802.1x 準拠の認証リストを作成する方法を示します。この認証は、最初に RADIUS サーバとの交信を試みます。 この動作でエラーが返信された場合、ユーザはネットワークへのアクセスが許可されません。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
```

aaa authorization network

IEEE 802.1x VLAN割り当てなどのすべてのネットワーク関連サービス要求に対してユーザRADIUS認証を使用するようにスイッチを設定するには、**aaa authorization network** 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。 RADIUSユーザ認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization network default group radius

no aaa authorization network default

構文の説明

default group radius	デフォルトの認証リストとして、サーバ グループ内のすべてのRADIUS ホストのリストを使用します。

コマンド デフォルト

認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

スイッチが、デフォルトの認証リスト内にある RADIUS サーバから IEEE 802.1x 認証パラメータをダウンロードできるようにするには、**aaa authorization network default group radius** 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。 認証パラメータは、VLAN 割り当てなど、RADIUS サーバからパラメータを取得する機能で使用されます。

設定された認証方式リストを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

例

この例では、すべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を行うようスイッチを設定する方法を示します。

```
Switch(config)# aaa authorization network default group radius
```

authentication host-mode

ポートで認証マネージャ モードを設定するには、**authentication host-mode** 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。 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。

authentication host-mode {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}

no authentication host-mode

構文の説明

multi-auth	ポートのマルチ認証モード（multi-auth モード）をイネーブルにします。
multi-domain	ポートのマルチドメイン モードをイネーブルにします。
multi-host	ポートのマルチホスト モードをイネーブルにします。
single-host	ポートのシングルホスト モードをイネーブルにします。

コマンド デフォルト

シングルホスト モードがイネーブルにされています。

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

接続されているデータ ホストが 1 つだけの場合は、シングルホスト モードを設定する必要があります。 シングルホスト ポートでの認証のために音声デバイスを接続しないでください。 ポートで音声 VLAN が設定されていないと、音声デバイスの許可が失敗します。

データ ホストが IP フォン経由でポートに接続されている場合は、マルチドメイン モードを設定する必要があります。 音声デバイスを認証する必要がある場合は、マルチドメイン モードを設定する必要があります。

ハブの背後にデバイスを配置し、それぞれを認証してポート アクセスのセキュリティを確保できるようにするには、マルチ認証モードに設定する必要があります。 音声 VLAN が設定されている場合は、このモードで認証できる音声デバイスは 1 つだけです。

マルチホストモードでも、ハブ越しの複数ホストのためのポートアクセスが提供されますが、マルチホストモードでは、最初のユーザが認証された後でデバイスに対して無制限のポートアクセスが与えられます。

例

次の例では、ポートのマルチ認証モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode multi-auth
```

次の例では、ポートのマルチドメイン モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode multi-domain
```

次の例では、ポートのマルチホスト モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode multi-host
```

次の例では、ポートのシングルホスト モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode single-host
```

設定を確認するには、**show authentication sessions interface** *interface* **details** 特権 EXEC コマンドを入力します。

authentication mac-move permit

スイッチ上での MAC 移動をイネーブルにするには、**authentication mac-move permit** 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。 MAC 移動をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication mac-move permit

no authentication mac-move permit

構文の説明

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 デフォルト

MAC 移動はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、スイッチ上のポート間で認証ホストを移動できます。たとえば、認証されたホストとポートの間にデバイスがあり、そのホストが別のポートに移動した場合、認証セッションは最初のポートから削除され、ホストは新しいポート上で再認証されます。

MAC移動がディセーブルで、認証されたホストが別のポートに移動した場合、そのホストは再認証されず、違反エラーが発生します。

例

次の例では、スイッチ上で MAC 移動をイネーブルにする方法を示します。

```
Switch(config)# authentication mac-move permit
```

authentication priority

プライオリティ リストに認証方式を追加するには、インターフェイス コンフィギュレーション モードで **authentication priority** 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。

authentication priority [**dot1x** | **mab**] {**webauth**}

no authentication priority [**dot1x** | **mab**] {**webauth**}

構文の説明

dot1x	（任意）認証方式の順序に 802.1x を追加します。
mab	（任意）認証方式の順序に MAC 認証バイパス（MAB）を追加します。
webauth	認証方式の順序に Web 認証を追加します。

コマンド デフォルト

デフォルトのプライオリティは、802.1x 認証、MAC 認証バイパス、Web 認証の順です。

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

順序付けでは、スイッチがポートに接続された新しいデバイスを認証しようとするときに試行する方式の順序を設定します。

ポートにフォールバック方式を複数設定するときは、Web 認証（webauth）を最後に設定してください。

異なる認証方式にプライオリティを割り当てることにより、プライオリティの高い方式を、プライオリティの低い進行中の認証方式に割り込ませることができます。

（注） クライアントがすでに認証されている場合に、プライオリティの高い方式の割り込みが発生すると、再認証されることがあります。

認証方式のデフォルトのプライオリティは、実行リストの順序におけるその位置と同じで、802.1x認証、MAC認証バイパス（MAB）、Web認証の順です。 このデフォルトの順序を変更するには、キーワード **dot1x**、**mab**、および **webauth** を使用します。

例

次の例では、802.1x を最初の認証方式、Web 認証を 2 番めの認証方式として設定する方法を示します。

```
Switch(config-if)# authentication priority dotx webauth
```

次の例では、MAB を最初の認証方式、Web 認証を 2 番めの認証方式として設定する方法を示します。

```
Switch(config-if)# authentication priority mab webauth
```

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event fail	認証マネージャが認証エラーを認識されないユーザ クレデンシャルの結果として処理する方法を指定します。
authentication event no-response action	認証マネージャが認証エラーを応答のないホストの結果として処理する方法を指定します。
authentication event server alive action reinitialize	以前に到達不能であった認証、許可、アカウンティング サーバが使用可能になったときに認証マネージャ セッションを再初期化します。
authentication event server dead action authorize	認証、許可、アカウンティング サーバが到達不能になったときに認証マネージャ セッションを許可します。
authentication fallback	Web 認証のフォール バック方式をイネーブルにします。
authentication host-mode	ホストの制御ポートへのアクセスを許可します。
authentication open	ポートでオープン アクセスをイネーブルにします。

コマンド	説明
authentication order	認証マネージャがポート上のクライアントの認証を試みる順序を指定します。
authentication periodic	ポートの自動再認証をイネーブルにします。
authentication port-control	制御ポートの許可ステートを設定します。
authentication timer inactivity	機能しない認証マネージャ セッションを強制終了するまでの時間を設定します。
authentication timer reauthenticate	認証マネージャが許可ポートの再認証を試みる間隔を指定します。
authentication timer restart	認証マネージャが無許可ポートの認証を試みる間隔を指定します。
authentication violation	ポート上でセキュリティ違反が生じた場合に取るアクションを指定します。
mab	ポートの MAC 認証バイパスをイネーブルにします。
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication sessions	現在の認証マネージャ セッションに関する情報を表示します。
show authentication sessions interface	特定のインターフェイスの認証マネージャに関する情報を表示します。

authentication violation

新しいデバイスがポートに接続するとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続するときに発生する違反モードを設定するには、**authentication violation** 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。

authentication violation{ **protect**|**replace**|**restrict**|**shutdown** }

no authentication violation{ **protect**|**replace**|**restrict**|**shutdown** }

構文の説明

protect	予期しない着信 MAC アドレスをドロップします。 syslog エラーは生成されません。
replace	現在のセッションを削除し、新しいホストによる認証を開始します。
restrict	違反エラーの発生時に Syslog エラーを生成します。
shutdown	エラーによって、予期しないMACアドレスが発生するポートまたは仮想ポートがディセーブルになります。

コマンド デフォルト

authentication violation shutdown モードがイネーブルにされています。

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

ポート上でセキュリティ違反が発生したときに実行するアクションを指定するには、**authentication violation** コマンドを使用します。

例

次の例では、新しいデバイスがポートに接続する場合に、errdisable になり、シャットダウンするように IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation shutdown
```

次の例では、新しいデバイスがポートに接続する場合に、システム エラー メッセージを生成して、ポートを制限モードに変更するように 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation restrict
```

次の例では、新しいデバイスがポートに接続するときに、そのデバイスを無視するように 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation protect
```

次の例では、新しいデバイスがポートに接続するときに、現在のセッションを削除し、新しいデバイスによる認証を開始するように 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation replace
```

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

cisp enable

スイッチ上で Client Information Signalling Protocol（CISP）をイネーブルにして、サプリカント スイッチのオーセンティケータとして機能するようにするには、**cisp 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。

cisp enable

no cisp enable

構文の説明

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 デフォルト

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

オーセンティケータとサプリカント スイッチの間のリンクはトランクです。 両方のスイッチで VTP をイネーブルにする場合は、VTP ドメイン名が同一であり、VTP モードがサーバである必要があります。

VTP モードを設定する場合に MD5 チェックサムの不一致エラーにならないようにするために、次の点を確認してください。

- VLAN が異なる 2 台のスイッチに設定されていないこと。同じドメインに VTP サーバが 2 台存在することがこの状態の原因になることがあります。
- 両方のスイッチで、設定のリビジョン番号が異なっていること。

例

次の例では、CISP をイネーブルにする方法を示します。

```
Switch(config)# cisp enable
```

関連コマンド

コマンド	説明
dot1x credentials*profile*	プロファイルをサプリカント スイッチに設定します。
dot1x supplicant force-multicast	802.1Xサプリカントがマルチキャストパケットを送信するように強制します。
dot1x supplicant controlled transient	802.1X サプリカントによる制御アクセスを設定します。
show cisp	指定されたインターフェイスのCISP情報を表示します。

clear errdisable interface vlan

errdisable の VLAN を再びイネーブルにするには、スイッチ上で **clear errdisable interface** 特権 EXEC コマンドを使用します。

clear errdisable interface *interface-id* **vlan** [*vlan-list*]

構文の説明

interface-id	インターフェイスを指定します。
vlan list	（任意）再びイネーブルにする VLAN のリストを指定します。VLAN リストを指定しない場合は、すべての VLAN が再びイネーブルになります。

コマンド デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

shutdown および **no shutdown** のインターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにするか、**clear errdisable** インターフェイス コマンドを使用して VLAN の errdisable をクリアできます。

例

次の例では、ギガビット イーサネット ポート 4/0/2 で errdisable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet4/0/2 vlan
```

関連コマンド

コマンド	説明
errdisable detect cause	特定の原因、またはすべての原因に対して errdisable 検出をイネーブルにします。
errdisable recovery	回復メカニズム変数を設定します。
show errdisable detect	errdisable 検出ステータスを表示します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status err-disabled	errdisable ステートになっているインターフェイスのリストのインターフェイス ステータスを表示します。

clear mac address-table

特定のダイナミック アドレス、特定のインターフェイス上のすべてのダイナミック アドレス、スタック メンバ上のすべてのダイナミック アドレス、または特定の VLAN 上のすべてのダイナミック アドレスを MAC アドレス テーブルから削除するには、**clear mac-address-table** コマンドを特権 EXEC モードで使用します。 このコマンドはまた MAC アドレス通知グローバル カウンタもクリアします。

clear mac address-table {**dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification**}

構文の説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
address *mac-addr*	（任意）指定されたダイナミック MAC アドレスを削除します。
interface *interface-id*	（任意）指定された物理ポートまたはポート チャネル上のすべてのダイナミック MAC アドレスを削除します。
vlan *vlan-id*	（任意）指定された VLAN のすべてのダイナミック MAC アドレスを削除します。 指定できる範囲は 1 ～ 4094 です。
move update	MAC アドレス テーブルの move-update カウンタをクリアします。
notification	履歴テーブルの通知をクリアし、カウンタをリセットします。

コマンド デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

show mac address-table 特権 EXEC コマンドを入力することにより、情報が削除されたかどうかを確認できます。

例

次の例では、ダイナミック アドレス テーブルから特定の MAC アドレスを削除する方法を示します。

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

関連コマンド

コマンド	説明
mac address-table notification	MAC アドレス通知機能をイネーブルにします。
mac address-table move update {**receive** | **transmit**}	スイッチ上の MAC アドレス テーブル移行更新を設定します。
show mac address-table	MAC アドレス テーブルのスタティック エントリおよびダイナミック エントリを表示します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。
show mac address-table notification	**interface** キーワードが追加されると、すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
snmp trap mac-notification change	特定のインターフェイスの SNMP MAC アドレス通知トラップをイネーブルにします。

deny（MAC アクセス リスト コンフィギュレーション）

条件が一致した場合に非IPトラフィックが転送されるのを防止するには、スイッチスタックまたはスタンドアロン スイッチ上で **deny** MAC アクセスリスト コンフィギュレーション コマンドを使用します。 名前付き MAC アクセス リストから拒否条件を削除するには、このコマンドの **no** 形式を使用します。

deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos** *cos*]

no deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos** *cos*]

構文の説明

any	すべての送信元または宛先 MAC アドレスを拒否します。
host *src-MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非IPトラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非IPトラフィックは拒否されます。
type mask	（任意）パケットの Ethertype 番号と、Ethernet II または SNAP カプセル化を指定して、パケットのプロトコルを識別します。 type には、0 ～ 65535 の 16 進数を指定できます。 mask は、一致をテストする前に Ethertype に適用される don't care ビットのマスクです。
aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする Ethertype AppleTalk Address Resolution Protocol を指定します。
amber	（任意）EtherType DEC-Amber を指定します。
appletalk	（任意）EtherType AppleTalk/EtherTalk を指定します。

dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニングツリーを指定します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	（任意）EtherType DEC-Diagnostic を指定します。
dsm	（任意）EtherType DEC-DSM を指定します。
etype-6000	（任意）EtherType 0x6000 を指定します。
etype-8042	（任意）EtherType 0x8042 を指定します。
lat	（任意）EtherType DEC-LAT を指定します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を指定します。
lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。 *mask* は、一致をテストする前に LSAP 番号に適用される don’t care ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を指定します。
mop-dump	（任意）EtherType DEC-MOP Dump を指定します。
msdos	（任意）EtherType DEC-MSDOS を指定します。
mumps	（任意）EtherType DEC-MUMPS を指定します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NETBIOS）を指定します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を指定します。
vines-ip	（任意）EtherType VINES IP を指定します。
xns-idp	（任意）10 進数、16 進数、または 8 進数の任意の Ethertype である EtherType Xerox Network Systems（XNS）プロトコル スイート（0 ～ 65535）を指定します。

cos *cos*	（任意）プライオリティを設定するため、0 ～ 7 までのサービス クラス（CoS）値を指定します。 CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。 **cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。

コマンド デフォルト

このコマンドには、デフォルトはありません。 ただし、名前付き MAC ACL のデフォルト アクションは拒否です。

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

MAC 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、**mac access-list extended** 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。

host キーワードを使用した場合、アドレス マスクは入力できません。**host** キーワードを使用しない場合は、アドレス マスクを入力する必要があります。

アクセス コントロール エントリ（ACE）がアクセス コントロール リストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。 つまり、一致がない場合にはパケットは拒否されます。 ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。 Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を表に一覧表示します。

表 *4*：*IPX* フィルタ基準

IPX カプセル化タイプ		**フィルタ基準**
Cisco IOS 名	**Novel 名**	
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	Novel 名	
novell-ether	Ethernet 802.3	LSAP 0xFFFF

例

次の例では、すべての送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを拒否する名前付き MAC 拡張アクセス リストを定義する方法を示します。 このリストに一致するトラフィックは拒否されます。

```
Switch(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

次の例では、名前付き MAC 拡張アクセス リストから拒否条件を削除する方法を示します。

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

次の例では、Ethertype 0x4321 のすべてのパケットを拒否します。

```
Switch(config-ext-macl)# deny any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
permit	MAC アクセスリスト コンフィギュレーションから許可します。 条件が一致した場合に非 IP トラフィックが転送されるのを許可します。
show access-lists	スイッチに設定されたアクセス コントロール リストを表示します。

device-role（IPv6 スヌーピング）

ポートに接続されているデバイスのロールを指定するには、IPv6 スヌーピング コンフィギュレーション モードで **device-role** コマンドを使用します。

device-role {**node** | **switch**}

構文の説明

node	接続されたデバイスのロールをノードに設定します。
switch	接続されたデバイスのロールをスイッチに設定します。

コマンド デフォルト

デバイスのロールはノードです。

コマンド モード

IPv6 スヌーピング コンフィギュレーション（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

device-role コマンドは、ポートに接続されているデバイスのロールを指定します。 デフォルトでは、デバイスのロールはノードです。

switch キーワードは、リモート デバイスがスイッチであり、ローカル スイッチがマルチスイッチ モードで動作していることを示します。ポートで学習したバインディング エントリは、trunk_port プリファレンス レベルでマークされます。 ポートが trusted ポートに設定されている場合、バインディング エントリは trunk_trusted_port プリファレンス レベルでマークされます。

例

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、デバイスを IPv6 スヌーピング コンフィギュレーション モードにし、デバイスをノードとして設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# device-role node
```

device-role（IPv6 ND 検査）

ポートに接続されているデバイスのロールを指定するには、ネイバー探索（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 **device-role** コマンドを使用します。

device-role {**host** | **monitor** | **router** | **switch**}

構文の説明

host	接続されたデバイスのロールをホストに設定します。
monitor	接続されたデバイスのロールをモニタに設定します。
router	接続されたデバイスのロールをルータに設定します。
switch	接続されたデバイスのロールをスイッチに設定します。

コマンド デフォルト

デバイスのロールはホストです。

コマンド モード

ND 検査ポリシー コンフィギュレーション（config-nd-inspection）

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

device-role コマンドは、ポートに接続されているデバイスのロールを指定します。 デフォルトでは、デバイスのロールはホストであるため、すべての着信ルータ アドバタイズメントとリダイレクト メッセージはブロックされます。 デバイス ロールが **router** キーワードを使用してイネーブルになっている場合、このポートですべてのメッセージ（ルータ送信要求 [RS]、ルータ アドバタイズメント（RA）、またはリダイレクト）が許可されます。

router または **monitor** キーワードが使用されている場合、マルチキャストの RS メッセージは制限付きブロードキャストがイネーブルかどうかに関係なく、ポートでブリッジされます。 ただし、monitor キーワードは着信 RA またはリダイレクト メッセージを許可しません。 monitor キーワードを使用すると、これらのメッセージを必要とするデバイスがそれらを受け取ります。

switch キーワードは、リモート デバイスがスイッチであり、ローカル スイッチがマルチスイッチ モードで動作していることを示します。ポートで学習したバインディング エントリは、trunk_port

プリファレンス レベルでマークされます。 ポートが trusted ポートに設定されている場合、バインディング エントリは trunk_trusted_port プリファレンス レベルでマークされます。

例

次に、Neighbor Discovery Protocol（NDP）ポリシー名を policy1 と定義し、デバイスを ND インスペクション ポリシー コンフィギュレーション モードにして、デバイスをホストとして設定する例を示します。

```
Switch(config)#  ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# device-role host
```

dot1x critical（グローバル コンフィギュレーション）

IEEE 802.1X クリティカル認証パラメータを設定するには、グローバル コンフィギュレーション モードで **dot1x critical** コマンドを使用します。

dot1x critical eapol

構文の説明

eapol	スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。

コマンド デフォルト

eapol はディセーブルです

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

例

次に、スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するよう指定する例を示します。

```
Switch(config)# dot1x critical eapol
```

dot1x pae

Port Access Entity（PAE）タイプを設定するには、インターフェイス コンフィギュレーション モードで **dot1x pae** コマンドを使用します。 設定された PAE タイプをディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x pae {**supplicant** | **authenticator**}

no dot1x pae {**supplicant** | **authenticator**}

構文の説明

supplicant	インターフェイスはサプリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。
authenticator	インターフェイスはオーセンティケータとしてだけ動作し、サプリカント向けのメッセージに応答しません。

コマンド デフォルト

PAE タイプ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 コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

IEEE 802.1x 認証をポート上でディセーブルにする場合は、**no dot1x pae** 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。

dot1x port-control インターフェイス コンフィギュレーション コマンドを入力するなどしてポート上で IEEE 802.1x 認証を設定した場合、スイッチは自動的にポートを IEEE 802.1x オーセンティケータとして設定します。 オーセンティケータの PAE 動作は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを入力した後でディセーブルになります。

例

次に、インターフェイスがサプリカントとして動作するように設定されている例を示します。

```
Switch(config)# interface g1/0/3
Switch(config-if)# dot1x pae supplicant
```

dot1x supplicant controlled transient

認証中に802.1xサプリカントポートへのアクセスを制御するには、グローバル コンフィギュレーション モードで **dot1x supplicant controlled transient** コマンドを使用します。 認証中にサプリカントのポートを開くには、このコマンドの **no** 形式を使用します。

dot1x supplicant controlled transient

no dot1x supplicant controlled transient

構文の説明

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 デフォルト

認証中に 802.1x サプリカントのポートへのアクセスが許可されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、BPCU ガードがイネーブルにされたオーセンティケータ スイッチにサプリカントのスイッチを接続する場合、オーセンティケータのポートはサプリカント スイッチが認証する前にスパニングツリー プロトコル（STP）のブリッジ プロトコル データ ユニット（BPDU）を受信した場合、errdisable 状態になる可能性があります。 Cisco IOS Release 15.0(1) SE 以降では、認証中にサプリカントのポートから送信されるトラフィックを制御できます。 **dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証が完了する前にオーセンティケータ ポートがシャットダウンすることがないように、認証中に一時的にサプリカントのポートをブロックします。 認証に失敗すると、サプリカントのポートが開きます。 **no dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証期間中にサプリカント ポートが開きます。 これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドによりオーセンティケータのスイッチ ポートでイネーブルになっている場合、サプリカント スイッチで **dot1x supplicant controlled transient** コマンドを使用することを強く推奨します。

例

次に、認証の間にスイッチの 802.1x サプリカントのポートへのアクセスを制御する例を示します。

```
Switch(config)# dot1x supplicant controlled transient
```

dot1x supplicant force-multicast

マルチキャストまたはユニキャストの Extensible Authentication Protocol over LAN（EAPOL）パケットを受信した場合、常にサプリカント スイッチにマルチキャスト EAPOL だけを送信させるようにするには、**dot1x supplicant force-multicast** 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。

dot1x supplicant force-multicast

no dot1x supplicant force-multicast

構文の説明

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 デフォルト

サプリカント スイッチは、ユニキャスト EAPOL パケットを受信すると、ユニキャスト EAPOL パケットを送信します。 同様に、マルチキャスト EAPOL パケットを受信すると、EAPOL パケットを送信します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

Network Edge Access Topology（NEAT）がすべてのホスト モードで機能するようにするには、サプリカント スイッチ上でこのコマンドをイネーブルにします。

例

次の例では、サプリカント スイッチがオーセンティケータ スイッチにマルチキャスト EAPOL パケットを送信するように設定する方法を示します。

```
Switch(config)# dot1x supplicant force-multicast
```

関連コマンド

コマンド	説明
cisp enable	スイッチの Client Information Signalling Protocol（CISP）をイネーブルにすることで、スイッチがサプリカント スイッチに対するオーセンティケータとして動作するようにします。
dot1x credentials	ポートに 802.1x サプリカント資格情報を設定します。
dot1x pae supplicant	インターフェイスがサプリカントとしてだけ機能するように設定します。

dot1x test eapol-capable

すべてのスイッチ ポート上の IEEE 802.1x のアクティビティをモニタリングして、IEEE 802.1x をサポートするポートに接続しているデバイスの情報を表示するには、**dot1x test eapol-capable** 特権 EXEC コマンドを使用します。

dot1x test eapol-capable [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）クエリー対象のポートです。

コマンド デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

スイッチ上のすべてのポートまたは特定のポートに接続するデバイスの IEEE 802.1x 機能をテストするには、このコマンドを使用します。

このコマンドには、no 形式はありません。

例

次の例では、スイッチ上で IEEE 802.1x の準備チェックをイネーブルにして、ポートに対してクエリーを実行する方法を示します。 また、ポートに接続しているデバイスを確認するためのクエリーの実行対象ポートから受信した応答が IEEE 802.1x 対応であることを示します。

```
Switch# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
capable
```

関連コマンド

コマンド	説明
dot1x test timeout *timeout*	IEEE 802.1x 準備クエリーに対する EAPOL 応答を待機するために使用されるタイムアウトを設定します。

dot1x test timeout

EEE 802.1x 準備状態を照会しているポートからの EAPOL 応答の待機に使用されるタイムアウトを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で **dot1x test timeout** 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。

dot1x test timeout *timeout*

構文の説明

timeout	EAPOL 応答を待機する時間（秒）。 指定できる範囲は 1 ～ 65535 秒です。

コマンド デフォルト

デフォルト設定は 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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

EAPOL応答を待機するために使用されるタイムアウトを設定するには、このコマンドを使用します。

このコマンドには、no 形式はありません。

例

次の例では、EAPOL 応答を 27 秒間待機するようにスイッチを設定する方法を示します。

```
Switch# dot1x test timeout 27
```

タイムアウト設定のステータスを確認するには、**show run** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x test eapol-capable [**interface** *interface-id*]	すべての、または指定された IEEE 802.1x 対応ポートに接続するデバイスで IEEE 802.1x の準備が整っているかを確認します。

dot1x timeout

再試行タイムアウトの値を設定するには、グローバル コンフィギュレーション モードまた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** コマンドを使用します。 再試行タイムアウト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。

dot1x timeout {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

構文の説明

auth-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 指定できる範囲は 1 ～ 65535 です。 デフォルトは 30 です。
held-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 指定できる範囲は 1 ～ 65535 です。 デフォルト値は 60 です。
quiet-period *seconds*	認証情報の交換に失敗したあと、クライアントの再認証を試みるまでにオーセンティケータ（サーバ）が待機状態（HELD 状態）を続ける秒数を設定します。 指定できる範囲は 1 ～ 65535 です。 デフォルト値は 60 です。
ratelimit-period *seconds*	動作の不正なクライアント PC（たとえば、スイッチ処理電力の無駄につながる、EAP-START パケットを送信する PC）から送信される EAP-START パケットを抑制します。 • オーセンティケータはレート制限時間中、認証に成功したクライアントからの EAPOL-Start パケットを無視します。 • 指定できる範囲は 1 ～ 65535 です。 デフォルトでは、レート制限はディセーブルになっています。

server-timeout *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 • 指定できる範囲は 1 ～ 65535 です。 デフォルトは 30 です。 サーバが指定時間内に 802.1X パケットへの応答を送信しない場合、パケットは再度送信されます。
start-period *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 指定できる範囲は 1 ～ 65535 です。 デフォルトは 30 です。
supp-timeout *seconds*	EAP 要求 ID 以外のすべての EAP メッセージについて、オーセンティケータからホストへの再送信時間を設定します。 指定できる範囲は 1 ～ 65535 です。 デフォルトは 30 です。
tx-period *seconds*	クライアントに EAP 要求 ID パケットを再送信する間隔を（応答が受信されないものと仮定して）秒数で設定します。 • 指定できる範囲は 1 ～ 65535 です。 デフォルトは 30 です。 • 802.1X パケットがサプリカントに送信され、そのサプリカントが再試行期間後に応答しなかった場合、そのパケットは再度送信されます。

コマンド デフォルト

定期的な再認証と定期的なレート制限が行われます。

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

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、異常な状況に対する調整を行う必要があるときに限って変更してください。

dot1x reauthentication インターフェイス コンフィギュレーション コマンドを使用して定期的な再認証をイネーブルにしただけの場合、**dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドは、スイッチの動作に影響します。

待機時間の間、スイッチはどのような認証要求も受け付けず、開始もしません。 デフォルトよりも小さい数を入力することによって、ユーザへの応答時間を短縮できます。

ratelimit-period が 0（デフォルト）に設定された場合、スイッチは認証に成功したクライアントからの EAPOL パケットを無視し、それらを RADIUS サーバに転送します。

例

次に、さまざまな 802.1X 再送信およびタイムアウト時間が設定されている例を示します。

```
Switch(config)# configure terminal
Switch(config)# interface g1/0/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x timeout auth-period 2000
Switch(config-if)# dot1x timeout held-period 2400
Switch(config-if)# dot1x timeout quiet-period 600
Switch(config-if)# dot1x timeout start-period 90
Switch(config-if)# dot1x timeout supp-timeout 300
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout server-timeout 60
```

epm access-control open

アクセス コントロール リスト（ACL）が設定されていないポートにオープン ディレクティブを設定するには、グローバル コンフィギュレーション モードで **epm access-control open** コマンドを使用します。 オープン ディレクティブをディセーブルにするには、このコマンドの **no** 形式を使用します。

epm access-control open

no epm access-control open

構文の説明

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 デフォルト

デフォルトのディレクティブが適用されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

スタティック ACL が設定されたアクセス ポートに、認可ポリシーのないホストを許可するオープンディレクティブを設定するには、このコマンドを使用します。 このコマンドを設定しない場合、ポートは設定された ACL のポリシーをトラフィックに適用します。 ポートにスタティック ACL が設定されていない場合、デフォルトおよびオープンの両方のディレクティブがポートへのアクセスを許可します。

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

例

次の例では、オープン ディレクティブを設定する方法を示します。

```
Switch(config)# epm access-control open
```

関連コマンド

コマンド	説明
show running-config	現在実行されているコンフィギュレーション ファイルの内容を表示します

ip admission

Web 認証をイネーブルにするには、**ip admission** コンフィギュレーション コマンドを使用します。このコマンドは、fallback-profile モードでも使用できます。 Web 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip admission *rule*

no ip admission *rule*

構文の説明

rule	IP アドミッション ルールの名前。

コマンド デフォルト

Web 認証はディセーブルです。

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

フォールバック プロファイル モード

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

ip admission コマンドにより、スイッチ ポートに Web 認証ルールが適用されます。

例

次の例では、スイッチ ポートに Web 認証ルールを適用する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip admission rule1
```

次の例では、IEEE 802.1x 対応のスイッチ ポートで使用するフォールバック プロファイルに Web 認証ルールを適用する方法を示します。

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(config-fallback-profile)# ip admission rule1
```

ip admission name

Web 認証をイネーブルにするには、グローバル コンフィギュレーション モードで **ip admission name** コマンドを使用します。 Web 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip admission name *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

no ip admission name *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

構文の説明

name	ネットワーク アドミッション制御ルールの名前。
consent	*admission-name* 引数を使用して、認証プロキシ コンテンツの Web ページを指定された IP アドミッション ルールに関連付けます。
proxy http	Web 認証のカスタム ページを設定します。
absolute-timer *minutes*	（任意）外部サーバがタイム アウトするまでの経過時間（分）。
inactivity-time *minutes*	（任意）外部ファイル サーバが到達不能であると見なされるまでの経過時間（分）。
list	（任意）指定されたルールをアクセス コントロール リスト（ACL）に関連付けます。
acl	標準、拡張リストを指定のアドミッション制御ルールに適用します。 値の範囲は1～199、または拡張範囲で 1300 から 2699 です。
acl-name	名前付きのアクセス リストを指定のアドミッション制御ルールに適用します。
service-policy type tag	（任意）コントロール プレーン サービス ポリシーを設定できます。
service-policy-name	**policy-map type control tag***policyname* コマンド、キーワード、および引数を使用して設定されたコントロール プレーン タグのサービス ポリシー。 このポリシー マップは、タグを受信したときのホストでの処理を適用するために使用されます。

コマンド デフォルト

Web 認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

ip admission name コマンドにより、Web 認証がスイッチ上でグローバルにイネーブルになります。

スイッチ上で Web 認証をグローバルにイネーブルにしてから、**ip access-group in** および **ip admission web-rule** インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイス上で Web 認証をイネーブルにします。

例

次に、スイッチ ポートで Web 認証のみを設定する例を示します。

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 101 in
Switch(config-if)# ip admission rule
Switch(config-if)# end
```

次の例では、スイッチ ポートでのフォールバック メカニズムとして、Web 認証とともに IEEE 802.1x 認証を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip admission name rule2 proxy http
Switch(config)# fallback profile profile1
Switch(config)# ip access group 101 in
Switch(config)# ip admission name rule2
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

関連コマンド

コマンド	説明
dot1x fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
fallback profile	Web 認証のフォールバック プロファイルを作成します。
ip admission	ポートで Web 認証をイネーブルにします。
show authentication sessions interface *interface* **detail**	Web認証セッションのステータスに関する情報を表示します。
show ip admission	NAC のキャッシュされたエントリまたは NAC 設定についての情報を表示します。

ip device tracking maximum

レイヤ 2 ポートで IP ポート セキュリティ バインディングのトラッキングをイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip device tracking maximum** コマンドを使用します。 信頼できないレイヤ 2 インターフェイスで IP ポート セキュリティをディセーブルにするには、このコマンドの **no 形式**を使用します。

ip device tracking maximum *number*

no ip device tracking maximum *number*

構文の説明

number	ポートの IP デバイス トラッキング テーブルに作成するバインディングの数。 範囲は 1～10 です。

コマンド デフォルト

なし

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、レイヤ 2 アクセス ポートで IP-MAC フィルタを使用して IP ポート セキュリティをイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# end
```

ip device tracking probe

Address Resolution Protocol（ARP）プローブの IP デバイス トラッキング テーブルを設定するには、グローバル コンフィギュレーション モードで **ip device tracking probe** コマンドを使用します。 ARP インスペクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip device tracking probe {**count** *number*| **delay** *seconds*| **interval** *seconds*| **use-svi** *address*}

no ip device tracking probe {**count** *number*| **delay** *seconds*| **interval** *seconds*| **use-svi** *address*}

構文の説明

count *number*	が ARP プローブを送信する回数を設定します。 範囲は 1 ～ 255 です。
delay *seconds*	が ARP プローブを送信するまで待機する秒数を設定します。 範囲は 1 ～ 120 です。
interval*seconds*	が応答を待ち、ARP プローブを再送信するまでの秒数を設定します。指定できる範囲は 30 ～ 1814400 秒です。
use-svi	仮想インターフェイス（SVI）IP アドレスを ARP プローブのソースとして使用します。

コマンド デフォルト

カウント番号は 3 です。

遅延はありません。

30 秒間隔です。

ARP プローブのデフォルト ソース IP アドレスはレイヤ 3 インターフェイスで、スイッチポートでは 0.0.0.0 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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

スイッチ ポートのデフォルト ソース IP アドレス 0.0.0.0 が使用され、ARP プローブがドロップする場合に、IP デバイス トラッキング テーブルが SVI IP アドレスを ARP プローブに使用するように設定するには、**use-svi** キーワードを使用します。

例

次の例では、SVI を ARP プローブのソースとして設定する方法を示します。

```
Switch(config)# ip device tracking probe use-svi
```

ip dhcp snooping database

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）のスヌーピング データベースを設定するには、グローバル コンフィギュレーション モードで **ip dhcp snooping database** コマンドを使用します。 DHCP スヌーピング サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

no ip dhcp snooping database [**timeout** | **write-delay**]

構文の説明

flash:*url*	flash を使用して、エントリを格納するためのデータベースの URL を指定します。
ftp:*url*	FTP を使用して、エントリを格納するためのデータベースの URL を指定します。
http:*url*	HTTP を使用して、エントリを格納するためのデータベースの URL を指定します。
https:*url*	セキュア HTTP（HTTPS）を使用して、エントリを格納するためのデータベースの URL を指定します。
rcp:*url*	リモートコピー（RCP）を使用して、エントリを格納するためのデータベースの URL を指定します。
scp:*url*	セキュア コピー（SCP）を使用して、エントリを格納するためのデータベースの URL を指定します。
tftp:*url*	TFTP を使用して、エントリを格納するためのデータベースの URL を指定します。
timeout *seconds*	中断タイムアウト インターバルを指定します。有効値は 0 ～ 86,400 秒です。

write-delay *seconds*	ローカル DHCP スヌーピング データベースにデータが追加されてから、DHCP スヌーピング エントリを外部サーバに書き込みするまでの時間を指定します。有効値は 15 ～ 86,400 秒です。

コマンド デフォルト

DHCP スヌーピング データベース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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを入力する前に、インターフェイス上で DHCP スヌーピングをイネーブルにする必要があります。 DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping** コマンドを使用します。

例

次に、TFTP を使用してデータベースの URL を指定する例を示します。

```
Switch(config)#  ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

次に、DHCP スヌーピング エントリを外部サーバに書き込むまでの時間を指定する例を示します。

```
Switch(config)#  ip dhcp snooping database write-delay 15
```

ip dhcp snooping information option format remote-id

オプション 82 リモート ID サブオプションを設定するには、スイッチで **ip dhcp snooping information option format remote-id** 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。 デフォルトのリモート ID サブオプションを設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}

no ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}

構文の説明

hostname	スイッチのホスト名をリモート ID として指定します。
string *string*	1 ～ 63 の ASCII 文字（スペースなし）を使用して、リモート ID を指定します。

コマンド デフォルト

スイッチの MAC アドレスは、リモート ID 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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、**ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用して DHCP スヌーピングをグローバルにイネーブルにする必要があります。

オプション 82 機能がイネーブルの場合、デフォルトのリモート ID サブオプションはスイッチの MAC アドレスです。 このコマンドを使用すると、スイッチのホスト名または 63 個の ASCII 文字列（スペースなし）のいずれかをリモート ID として設定できます。

（注） ホスト名が 63 文字を超える場合、リモート ID 設定では 63 文字以降は省略されます。

例

次の例では、オプション 82 リモート ID サブオプションを設定する方法を示します。

```
Switch(config)# ip dhcp snooping information option format remote-id hostname
```

ip dhcp snooping verify no-relay-agent-address

DHCP クライアント メッセージのリレー エージェント アドレス（giaddr）が信頼できないポート上のクライアントのハードウェア アドレスに一致することを確認して、DHCP スヌーピング機能をディセーブルにするには、グローバル コンフィギュレーション モードで **ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。 検証をイネーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify no-relay-agent-address

no ip dhcp snooping verify no-relay-agent-address

構文の説明

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 デフォルト

DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアント メッセージのリレー エージェント IP アドレス（giaddr）フィールドが 0 であることを確認します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアント メッセージのリレー エージェントの IP アドレス（giaddr）フィールドが 0 であることを確認します。giaddr フィールドが 0 でない場合、メッセージはドロップされます。 検証をディセーブルにするには、**ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。 検証を再度イネーブルにするには、**no ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。

例

次に、DHCP クライアント メッセージの giaddr 検証をイネーブルにする例を示します。

```
Switch(config)# no ip dhcp snooping verify no-relay-agent-address
```

ip source binding

スタティック IP ソース バインディング エントリを追加するには、**ip source binding** コマンドを使用します。 スタティック IP ソース バインディング 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。

ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

no ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

構文の説明

mac-address	バインディング対象 MAC アドレスです。
vlan *vlan-id*	レイヤ 2 VLAN ID を指定します。有効な値は1～4094 です。
ip-address	バインディング対象 IP アドレスです。
interface *interface-id*	物理インターフェイスの ID です。

コマンド デフォルト

IP 送信元バインディング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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、スタティック IP ソース バインディング エントリだけを追加するために使用できます。

no 形式は、対応する IP ソース バインディング エントリを削除します。 削除が正常に実行されるためには、すべての必須パラメータが正確に一致しなければなりません。 各スタティック IP バインディング エントリは MAC アドレスと VLAN 番号がキーであることに注意してください。 コマ

ンドに既存の MAC アドレスと VLAN 番号が含まれる場合、別のバインディング エントリが作成される代わりに既存のバインディング エントリが新しいパラメータで更新されます。

例

次の例では、スタティック IP ソース バインディング エントリを追加する方法を示します。

```
Switch# configure terminal
Switchconfig) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1
```

ip verify source

インターフェイス上のIP ソース ガードをイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip verify source** コマンドを使用します。 IP ソース ガードをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip verify source [**port-security**][**smartlog**]

no ip verify source

構文の説明

port-security	（任意）IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにします。 **port-security** キーワードを入力しない場合、IP アドレス フィルタリングによる IP ソース ガードがイネーブルになります。
smartlog	（任意）インターフェイスの IP ソース ガード スマート ロギングをイネーブルにします。

コマンド デフォルト

IP 送信元ガードはディセーブルです。

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、**ip verify source** 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。

送信元IPおよびMACアドレス フィルタリングによるIP ソース ガードをイネーブルにするには、**ip verify source port-security** 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。

インターフェイス上で IP ソース ガード スマート ログインがイネーブルになっている場合、拒否されたパケットの内容が Flexible NetFlow コレクタに送られます。

例

次の例では、送信元 IP アドレス フィルタリングによる IP ソース ガードをインターフェイス上でイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source
```

次の例では、送信元 IP および MAC アドレス フィルタリングによる IP ソース ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source port-security
```

次に、インターフェイスの IP ソース ガード スマート ロギングをイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source smartlog
```

設定を確認するには、**show ip verify source** 特権 EXEC コマンドを入力します。

ipv6 snooping policy

IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング 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 **ipv6 snooping policy** コマンドを使用します。 IPv6 スヌーピング 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。

ipv6 snooping policy *snooping-policy*

no ipv6 snooping policy *snooping-policy*

構文の説明

snooping-policy	スヌーピング ポリシーのユーザ定義名。 ポリシー名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。

コマンド デフォルト

IPv6 スヌーピング 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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

IPv6 スヌーピング ポリシーを作成するには、**ipv6 snooping policy** コマンドを使用します。 **ipv6 snooping policy** コマンドがイネーブルの場合、コンフィギュレーション モードが IPv6 スヌーピング コンフィギュレーション モードに変更されます。 このモードでは、管理者が次の IPv6 ファーストホップ セキュリティ コマンドを設定できます。

- **device-role** コマンドは、ポートに接続されているデバイスのロールを指定します。
- **limit address-count** *maximum* コマンドはポートで使用できる IPv6 アドレスの数を制限します。
- **protocol** コマンドは、アドレスをダイナミック ホスト コンフィギュレーション プロトコル（DHCP）またはネイバー探索プロトコル（NDP）で収集する必要があることを指定します。
- **security-level** コマンドは適用されるセキュリティのレベルを指定します。
- **tracking** コマンドは、ポートのデフォルトのトラッキング ポリシーを上書きします。

- **trusted-port** コマンドは、あるポートを信頼できるポートとして設定します。つまり、メッセージが受信されると検証は限定的に実行されるか、まったく実行されません。

例

次に、IPv6 スヌーピング ポリシーを設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#
```

limit address-count

ポートで使用できるIPv6アドレスの数を制限するには、ネイバー探索プロトコル（NDP）インスペクション ポリシー コンフィギュレーション モードまたはIPv6 スヌーピング コンフィギュレーション モードで**limit address-count** 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。

limit address-count *maximum*

no limit address-count

構文の説明

maximum	ポートで許可されているアドレスの数。 範囲は 1 ～ 10000 です。

コマンド デフォルト

デフォルト設定は無制限です。

コマンド モード

ND 検査ポリシー コンフィギュレーション（config-nd-inspection）

IPv6 スヌーピング コンフィギュレーション（ipv6-snooping）

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

limit address-count コマンドは、ポリシーが適用されているポートで使用できる IPv6 アドレスの数を制限します。 ポート上の IPv6 アドレスの数を制限すると、バインディング テーブル サイズの制限に役立ちます。 範囲は 1 ～ 10000 です。

例

次に、NDP ポリシー名を policy1 と定義し、スイッチを NDP インスペクション ポリシー コンフィギュレーション モードにし、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# limit address-count 25
```

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# limit address-count 25
```

mab request format attribute 32

スイッチ上でVLAN IDベースのMAC認証をイネーブルにするには、**mab request format attribute 32 vlan access-vlan** 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。

mab request format attribute 32 vlan access-vlan

no mab request format attribute 32 vlan access-vlan

構文の説明

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 デフォルト

VLAN-ID ベースの MAC 認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

RADIUS サーバがホスト MAC アドレスと VLAN に基づいて新しいユーザを認証できるようにするには、このコマンドを使用します。

Microsoft IAS RADIUS サーバを使用したネットワークでこの機能を使用します。 Cisco ACS はこのコマンドを無視します。

例

次の例では、スイッチで VLAN-ID ベースの MAC 認証をイネーブルにする方法を示します。

```
Switch(config)# mab request format attribute 32 vlan access-vlan
```

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。

コマンド	説明
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
mab	ポートの MAC-based 認証をイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するようポートを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

match（アクセス マップ コンフィギュレーション）

1 つまたは複数のアクセス リストとパケットと照合するように VLAN マップを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上でアクセスマップ コンフィギュレーション モードで **match** コマンドを使用します。 照合パラメータを削除するには、このコマンドの **no** 形式を使用します。

match {**ip address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** {*name*} [*name*] [*name*]...}

no match {**ip address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** {*name*} [*name*] [*name*]...}

構文の説明

ip address	パケットを IP アドレス アクセス リストと照合するようにアクセス マップを設定します。
mac address	パケットを MAC アドレス アクセス リストと照合するようにアクセス マップを設定します。
name	パケットを照合するアクセス リストの名前です。
number	パケットを照合するアクセス リストの番号です。 このオプションは、MAC アクセス リストに対しては無効です。

コマンド デフォルト

デフォルトのアクションでは、一致パラメータは VLAN マップに適用されません。

コマンド モード

アクセス マップ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

vlan access-map グローバル コンフィギュレーション コマンドを使用して、アクセス マップ コンフィギュレーション モードを開始します。

1 つのアクセス リストの名前または番号を入力する必要があります。その他は任意です。 パケットは、1 つまたは複数のアクセス リストに対して照合できます。 いずれかのリストに一致すると、エントリの一致としてカウントされます。

アクセス マップ コンフィギュレーション モードでは、**match** コマンドを使用して、VLAN に適用される VLAN マップの一致条件を定義できます。 **action** コマンドを使用すると、パケットが条件に一致したときに実行するアクションを設定できます。

パケットは、同じプロトコル タイプのアクセス リストに対してだけ照合されます。IP パケットは、IP アクセス リストに対して照合され、その他のパケットはすべて MAC アクセス リストに対して照合されます。

同じマップ エントリに、IP アドレスと MAC アドレスの両方を指定できます。

例

次の例では、VLAN アクセス マップ vmap4 を定義して VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップでは、パケットがアクセス リスト al2 に定義された条件に一致すると、インターフェイスは IP パケットをドロップします。

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

設定を確認するには、**show vlan access-map** 特権 EXEC コマンドを入力します。

no authentication logging verbose

認証システム メッセージから詳細情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で **no authentication logging verbose** 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。

no authentication logging verbose

構文の説明

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 デフォルト

すべての詳細情報はシステム メッセージに表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、認証システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。 失敗メッセージはフィルタリングされません。

例

verbose 認証システム メッセージをフィルタリングするには、次の手順に従います。

```
Switch(config)# no authentication logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。

コマンド	説明
no mab logging verbose	MAC 認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

no dot1x logging verbose

802.1x システム メッセージから詳細情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で **no dot1x logging verbose** 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。

no dot1x logging verbose

構文の説明

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 デフォルト

すべての詳細情報はシステム メッセージに表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、802.1x システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。 失敗メッセージはフィルタリングされません。

例

verbose 802.1x システム メッセージをフィルタリングするには、次の手順に従います。

```
Switch(config)# no dot1x logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。

コマンド	説明
no mab logging verbose	MAC 認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

no mab logging verbose

MAC 認証バイパス（MAB）のシステム メッセージから詳細情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で **no mab logging verbose** 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。

no mab logging verbose

構文の説明

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 デフォルト

すべての詳細情報はシステム メッセージに表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、MAC 認証バイパス（MAB）システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。 失敗メッセージはフィルタリングされません。

例

verbose MAB システム メッセージをフィルタリングするには、次の手順に従います。

```
Switch(config)# no mab logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。

コマンド	説明
no mab logging verbose	MAC認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

permit（MACアクセス リストコンフィギュレーション）

条件が一致した場合に非IPトラフィックが転送されるのを許可するには、スイッチスタックまたはスタンドアロン スイッチ上で **permit** MAC アクセスリスト コンフィギュレーション コマンドを使用します。 拡張 MAC アクセス リストから許可条件を削除するには、このコマンドの **no** 形式を使用します。

{**permit** {**any** | **host***src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap***lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos***cos*]

nopermit {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos***cos*]

構文の説明

any	すべての送信元または宛先 MAC アドレスを拒否します。
host *src-MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを指定します。 パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非IP トラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを指定します。 パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非IP トラフィックは拒否されます。
type mask	（任意）パケットの Ethertype 番号と、Ethernet II または SNAP カプセル化を指定して、パケットのプロトコルを識別します。 • *type* には、0 ～ 65535 の 16 進数を指定できます。 • *mask* は、一致をテストする前に Ethertype に適用される don’t care ビットのマスクです。
aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする Ethertype AppleTalk Address Resolution Protocol を指定します。
amber	（任意）EtherType DEC-Amber を指定します。
appletalk	（任意）EtherType AppleTalk/EtherTalk を指定します。

dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニングツリーを指定します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	（任意）EtherType DEC-Diagnostic を指定します。
dsm	（任意）EtherType DEC-DSM を指定します。
etype-6000	（任意）EtherType 0x6000 を指定します。
etype-8042	（任意）EtherType 0x8042 を指定します。
lat	（任意）EtherType DEC-LAT を指定します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を指定します。
lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。 *mask* は、一致をテストする前に LSAP 番号に適用される don't care ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を指定します。
mop-dump	（任意）EtherType DEC-MOP Dump を指定します。
msdos	（任意）EtherType DEC-MSDOS を指定します。
mumps	（任意）EtherType DEC-MUMPS を指定します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NETBIOS）を指定します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を指定します。
vines-ip	（任意）EtherType VINES IP を指定します。
xns-idp	（任意）EtherType Xerox Network Systems（XNS）プロトコル スイートを指定します。
cos *cos*	（任意）プライオリティを設定するため、0 ～ 7 までの任意の Class of Service（CoS）値を指定します。 CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。 **cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。

コマンド デフォルト

このコマンドには、デフォルトはありません。 ただし、名前付き MAC ACL のデフォルト アクションは拒否です。

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

appletalk は、コマンドラインのヘルプ ストリングには表示されますが、一致条件としてはサポートされていません。

MAC 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、**mac access-list extended** 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。

host キーワードを使用した場合、アドレス マスクは入力できません。**any** キーワードまたは **host** キーワードを使用しない場合は、アドレス マスクを入力する必要があります。

アクセス コントロール エントリ（ACE）がアクセス コントロール リストに追加されると、リストの最後には暗黙の **deny-any-any** 条件が存在します。 つまり、一致がない場合にはパケットは拒否されます。 ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。 Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を、次の表に一覧表示します。

表 *5* : ***IPX*** **フィルタ基準**

IPX カプセル化タイプ		**フィルタ基準**
Cisco IOS 名	**Novell 名**	
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

例

次の例では、あらゆる送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを許可する名前付き MAC 拡張アクセス リストを定義する方法を示します。 このリストに一致するトラフィックは許可されます。

```
Switch(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

次の例では、名前付き MAC 拡張アクセス リストから許可条件を削除する方法を示します。

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

次の例では、Ethertype 0x4321 のすべてのパケットを許可します。

```
Switch(config-ext-macl)# permit any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
deny	MACアクセスリストコンフィギュレーションを拒否します。 条件が一致した場合に非 IP トラフィックが転送されるのを拒否します。
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
show access-lists	スイッチに設定されたアクセス コントロール リストを表示します。

protocol（IPv6 スヌーピング）

アドレスをダイナミック ホスト コンフィギュレーション プロトコル（DHCP）またはネイバー探索プロトコル（NDP）で収集する必要があることを指定するか、プロトコルを IPv6 プレフィックス リストに関連付けるには、**protocol** コマンドを使用します。 DHCP または NDP によるアドレス収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

protocol {**dhcp** | **ndp**}

no protocol {**dhcp** | **ndp**}

構文の説明

dhcp	アドレスをダイナミック ホスト コンフィギュレーション プロトコル（DHCP）パケットで収集する必要があることを指定します。
ndp	アドレスをネイバー探索プロトコル（NDP）パケットで収集する必要があることを指定します。

コマンド デフォルト

スヌーピングとリカバリは DHCP および NDP の両方を使用して試行します。

コマンド モード

IPv6 スヌーピング コンフィギュレーション モード（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

アドレスが DHCP または NDP に関連付けられたプレフィックス リストと一致しない場合は、制御パケットがドロップされ、バインディング テーブル エントリのリカバリはそのプロトコルに対しては試行されません。

- **no protocol** {**dhcp** | **ndp**} コマンドを使用すると、プロトコルはスヌーピングまたはグリーニングに使用されません。
- **no protocol dhcp** コマンドを使用すると、DHCP は依然としてバインディング テーブルのリカバリに使用できます。
- データ収集は DHCP および NDP でリカバリできますが、宛先ガードは DHCP によってのみリカバリできます。

例

次に、IPv6 スヌーピングポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、アドレスの収集に DHCP を使用するようにポートを設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# protocol dhcp
```

security level（IPv6 スヌーピング）

適用されるセキュリティのレベルを指定するには、IPv6スヌーピングポリシーコンフィギュレーション モードで **security-level** コマンドを使用します。

security level {**glean** | **guard** | **inspect**}

構文の説明

glean	アドレスをメッセージから抽出し、検証を行わずにそれらをバインディング テーブルにインストールします。
guard	収集と検査の両方を実行します。 さらに、信頼できるポートで受信されていない場合、または別のポリシーによって許可されていない場合、RA メッセージおよび DHCP サーバ メッセージは拒否されます。
inspect	メッセージの一貫性と準拠度を検証します。特に、アドレス所有権が強制されます。 無効なメッセージはドロップされます。

コマンド デフォルト

デフォルトのセキュリティ レベルは guard です。

コマンド モード

IPv6 スヌーピング コンフィギュレーション（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、デバイスを IPv6 スヌーピング コンフィギュレーション モードにし、セキュリティ レベルを inspect として設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# security-level inspect
```

show aaa acct-stop-cache

改竄されたセッションのアカウンティング セッション ID を表示するには、**show aaa acct-stop-cache** コマンドを使用します。

構文の説明

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

改竄されたセッションのアカウンティング終了レコードはスタンバイ スイッチにのみキャッシュされます。

例

次の例では、**show aaa acct-stop-cache** コマンドの出力を示します。

```
Switch# show aaa acct-stop-cache
```

show aaa clients

AAA クライアントの統計情報を表示するには、**show aaa clients** コマンドを使用します。

show aaa clients [**detailed**]

構文の説明

detailed	（任意）詳細な AAA クライアントの統計情報を示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、**show aaa clients** コマンドの出力を示します。

```
Switch# show aaa clients
Dropped request packets: 0
```

show aaa command handler

コマンド ハンドラの統計情報を表示するには、**show aaa command handler** コマンドを使用します。

show aaa command handler

構文の説明

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、**show aaa command handler** コマンドの出力を示します。

```
Switch# show aaa command handler

AAA Command Handler Statistics:
    account-logon: 0, account-logoff: 0
    account-query: 0, pod: 0
    service-logon: 0, service-logoff: 0
    user-profile-push: 0, session-state-log: 0
    reauthenticate: 0, bounce-host-port: 0
    disable-host-port: 0, update-rbacl: 0
    update-sgt: 0, update-cts-policies: 0
    invalid commands: 0
    async message not sent: 0
```

show aaa local

AAA ローカル方式オプションを表示するには、**show aaa local** コマンドを使用します。

show aaa local {**netuser** {*name* | **all** } | **statistics** | **user lockout**}

構文の説明

netuser	AAA ローカル ネットワークまたはゲスト ユーザ データベースを指定します。
name	ネットワーク ユーザ名。
all	ネットワークおよびゲスト ユーザ情報を指定します。
statistics	ローカル認証の統計情報を表示します。
user lockout	AAA ローカルのロックアウトされたユーザを指定します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、**show aaa local statistics** コマンドの出力を示します。

```
Switch# show aaa local statistics

Local EAP statistics

EAP Method         Success       Fail
---------------------------------------
Unknown                  0          0
EAP-MD5                  0          0
EAP-GTC                  0          0
LEAP                     0          0
PEAP                     0          0
EAP-TLS                  0          0
EAP-MSCHAPV2             0          0
EAP-FAST                 0          0

Requests received from AAA:                  0
Responses returned from EAP:                 0
Requests dropped (no EAP AVP):               0
Requests dropped (other reasons):            0
```

```
Authentication timeouts from EAP:           0

Credential request statistics
Requests sent to backend:                   0
Requests failed (unable to send):           0
Authorization results received

  Success:                                  0
  Fail:                                     0
```

show aaa servers

AAA サーバの MIB によって認識されるすべての AAA サーバを表示するには、**show aaa servers** コマンドを使用します。

show aaa servers [private|public|[detailed]]

構文の説明

detailed	（任意）AAA サーバの MIB によって認識されるプライベート AAA サーバを表示します。
public	（任意）AAA サーバの MIB によって認識されるパブリック AAA サーバを表示します。
detailed	（任意）詳細な AAA サーバの統計情報を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、**show aaa servers** コマンドの出力を示します。

```
Switch# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
```

```
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

show aaa sessions

AAA セッション MIB によって認識される AAA セッションを表示するには、**show aaa sessions** コマンドを使用します。

show aaa sessions

構文の説明

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、**show aaa sessions** コマンドの出力を示します。

```
Switch# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
   Unique Id: 4025
   User Name: *not available*
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
```

show authentication sessions

現在の認証マネージャ セッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。

show authentication sessions [**database**][**handle** *handle-id* [**details**]][**interface** *type number* [**details**][**mac** *mac-address* [**interface** *type number*][**method** *method-name* [**interface** *type number* [**details**] [**session-id** *session-id* [**details**]]

構文の説明

database	（任意）セッションデータベースに格納されているデータだけを示します。
handle *handle-id*	（任意）認証マネージャ情報を表示する特定のハンドルを指定します。
details	（任意）詳細情報を表示します。
interface *type number*	（任意）認証マネージャ情報を表示する特定のインターフェイスのタイプと番号を指定します。
mac *mac-address*	（任意）情報を表示する特定の MAC アドレスを指定します。
method *method-name*	（任意）認証マネージャ情報を表示する特定の認証方法を指定します。 方式を指定する場合（**dot1x**、**mab**、または **webauth**）、インターフェイスも指定できます。
session-id *session-id*	（任意）認証マネージャ情報を表示する特定のセッションを指定します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

現在のすべての認証マネージャ セッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。 特定の認証マネージャ セッションに関する情報を表示するには、1 つ以上のキーワードを使用します。

このテーブルは、報告された認証セッションで想定される動作状態を示します。

表 *6*：認証方式のステート

状態	説明
Not run	このセッションの方式は実行されていません。
Running	このセッションの方式が実行中です。
Failed over	この方式は失敗しました。次の方式が結果を出すことが予期されています。
Success	この方式は、セッションの成功した認証結果を提供しました。
Authc Failed	この方式は、セッションの失敗した認証結果を提供しました。

次の表に、使用できる認証方式を示します。

表 *7*：認証方式のステート

状態	説明
dot1x	802.1X
mab	MAC 認証バイパス
webauth	Web 認証

例

次に、スイッチ上のすべての認証セッションを表示する例を示します。

```
Switch# show authentication sessions
Interface    MAC Address     Method   Domain   Status         Session ID
Gi1/0/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/0/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/0/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

```
Switch# show authentication sessions interface gigabitethernet2/0/47
            Interface:  GigabitEthernet2/0/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000000002763C
      Acct Session ID:  0x00000002
               Handle:  0x25000000
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
----------------------------------------
            Interface:  GigabitEthernet2/0/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

show cisp

指定されたインターフェイスの CISP 情報を表示するには、**show cisp** 特権 EXEC コマンドを使用します。

show cisp {[**clients** | **interface** *interface-id*] | **registrations** | **summary**}

構文の説明

clients	（任意）CISP クライアントの詳細を表示します。
interface *interface-id*	（任意）指定されたインターフェイスの CISP 情報を表示します。有効なインターフェイスには、物理ポートとポートチャネルが含まれます。
registrations	CISP の登録情報を表示します。
summary	（任意）CISP のサマリー情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、**show cisp interface** コマンドの出力を示します。

```
Switch# show cisp interface fast 0
CISP not enabled on specified interface
```

次の例では、**show cisp registration** コマンドの出力を示します。

```
Switch# show cisp registrations
Interface(s) with CISP registered user(s):
-------------------------------------------
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
```

```
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
Gi3/0/23
```

関連コマンド

コマンド	説明
cisp enable	Client Information Signalling Protocol（CISP）をイネーブルにします。
dot1x credentials *profile*	サプリカント スイッチでプロファイルを設定します。

show dot1x

スイッチまたは指定されたポートのIEEE 802.1x統計情報、管理ステータス、および動作ステータスを表示するには、**show dot1x** ユーザ EXEC コマンドを使用します。

show dot1x [**all** [**count** | **details** | **statistics** | **summary**]] [**interface** *type number* [**details** | **statistics**]] [**statistics**]

構文の説明

all	（任意）すべてのインターフェイスのIEEE 802.1x情報を表示します。
count	（任意）許可されたクライアントと無許可のクライアントの総数を表示します。
details	（任意）IEEE 802.1xインターフェイスの詳細を表示します。
statistics	（任意）すべてのインターフェイスのIEEE 802.1x統計情報を表示します。
summary	（任意）すべてのインターフェイスの IEEE 802.1x サマリー情報を表示します。
interface *type number*	（任意）指定したポートの IEEE 802.1X ステータスを表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、**show dot1x all** コマンドの出力を示します。

```
Switch# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3
```

次の例では、**show dot1x all count** コマンドの出力を示します。

```
Switch# show dot1x all count
Number of Dot1x sessions
------------------------------
Authorized Clients        = 0
UnAuthorized Clients      = 0
Total No of Client        = 0
```

次の例では、**show dot1x all statistics** コマンドの出力を示します。

```
Switch# show dot1x statistics
Dot1x Global Statistics for
-------------------------------------------
RxStart = 0     RxLogoff = 0    RxResp = 0      RxRespID = 0
RxReq = 0       RxInvalid = 0   RxLenErr = 0
RxTotal = 0

TxStart = 0     TxLogoff = 0    TxResp = 0
TxReq = 0       ReTxReq = 0     ReTxReqFail = 0
TxReqID = 0     ReTxReqID = 0   ReTxReqIDFail = 0
TxTotal = 0
```

show eap pac peer

拡張認証プロトコル（EAP）のセキュア トンネリングを介したフレキシブル認証（FAST）ピアの格納済み Protected Access Credential（PAC）を表示するには、**show eap pac peer** 特権 EXEC コマンドを使用します。

show eap pac peer

構文の説明

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、**show eap pac peers** 特権 EXEC コマンドの出力を示します。

```
Switch> show eap pac peers
No PACs stored
```

関連コマンド

コマンド	説明
clear eap sessions	スイッチまたは指定されたポートの EAP のセッション情報をクリアします。

show ip dhcp snooping statistics

DHCP スヌーピング統計情報をサマリー形式または詳細形式で表示するには、**show ip dhcp snooping statistics** ユーザ EXEC コマンドを使用します。

show ip dhcp snooping statistics [**detail**]

構文の説明

detail	（任意）詳細な統計情報を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

スイッチ スタックでは、すべての統計情報がスタック マスターで生成されます。 新しいアクティブ スイッチが選定された場合、統計カウンタはリセットされます。

例

次の例では、**show ip dhcp snooping statistics** コマンドの出力を示します。

```
Switch> show ip dhcp snooping statistics

 Packets Forwarded                                = 0
 Packets Dropped                                  = 0
 Packets Dropped From untrusted ports             = 0
```

次の例では、**show ip dhcp snooping statistics detail** コマンドの出力を示します。

```
Switch> show ip dhcp snooping statistics detail

 Packets Processed by DHCP Snooping               = 0
 Packets Dropped Because
   IDB not known                                  = 0
   Queue full                                     = 0
   Interface is in errdisabled                    = 0
   Rate limit exceeded                            = 0
   Received on untrusted ports                    = 0
   Nonzero giaddr                                 = 0
   Source mac not equal to chaddr                 = 0
   Binding mismatch                               = 0
   Insertion of opt82 fail                        = 0
   Interface Down                                 = 0
   Unknown output interface                       = 0
```

```
Reply output port equal to input port               = 0
Packet denied by platform                           = 0
```

次の表に、DHCP スヌーピング統計情報およびその説明を示します。

表 *8*：*DHCP* スヌーピング統計情報

DHCP スヌーピング統計情報	説明
Packets Processed by DHCP Snooping	転送されたパケットおよびドロップされたパケットも含めて、DHCP スヌーピングによって処理されたパケットの合計数。
Packets Dropped Because IDB not known	パケットの入力インターフェイスを判断できないエラーの数。
Queue full	パケットの処理に使用される内部キューが満杯であるエラーの数。非常に高いレートでDHCPパケットを受信し、入力ポートでレート制限がイネーブルになっていない場合、このエラーが発生することがあります。
Interface is in errdisabled	errdisableとしてマークされたポートでパケットを受信した回数。 これが発生する可能性があるのは、ポートがerrdisableステートである場合にパケットが処理キューに入り、そのパケットが後で処理される場合です。
Rate limit exceeded	ポートで設定されているレート制限を超えて、インターフェイスが errdisable ステートになった回数。
Received on untrusted ports	信頼できないポートで DHCP サーバ パケット（OFFER、ACK、NAK、LEASEQUERY のいずれか）を受信してドロップした回数。
Nonzero giaddr	信頼できないポートで受信した DHCP パケットのリレーエージェントアドレスフィールド（giaddr）がゼロ以外だった回数。または **no ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを設定しておらず、信頼できないポートで受信したパケットにオプション 82 データが含まれていた回数。
Source mac not equal to chaddr	DHCP パケットのクライアント MAC アドレス フィールド（chaddr）がパケットの送信元MACアドレスと一致せず、**ip dhcp snooping verify mac-address** グローバル コンフィギュレーション コマンドが設定されている回数。

DHCP スヌーピング統計情報	説明
Binding mismatch	MAC アドレスと VLAN のペアのバインディングになっているポートとは異なるポートで、RELEASE パケットまたは DECLINE パケットを受信した回数。 これは、誰かが本来のクライアントをスプーフィングしようとしている可能性があることを示しますが、クライアントがスイッチの別のポートに移動して RELEASE または DECLINE を実行したことを表すこともあります。 MAC アドレスは、イーサネット ヘッダーの送信元 MAC アドレスではなく、DHCP パケットの chaddr フィールドから採用されます。
Insertion of opt82 fail	パケットへのオプション 82 挿入がエラーになった回数。オプション 82 データを含むパケットがインターネットの単一物理パケットのサイズを超えた場合、挿入はエラーになることがあります。
Interface Down	パケットが DHCP リレー エージェントへの応答であるが、リレー エージェントの SVI インターフェイスがダウンしている回数。 DHCP サーバへのクライアント要求の送信と応答の受信の間で SVI がダウンした場合に発生するエラーですが、めったに発生しません。
Unknown output interface	オプション 82 データまたは MAC アドレス テーブルのルックアップのいずれかで、DHCP応答パケットの出力インターフェイスを判断できなかった回数。パケットはドロップされます。 オプション 82 が使用されておらず、クライアント MAC アドレスが期限切れになった場合に発生することがあります。 ポートセキュリティ オプションで IPSG がイネーブルであり、オプション 82 がイネーブルでない場合、クライアントの MAC アドレスは学習されず、応答パケットはドロップされます。
Reply output port equal to input port	DHCP 応答パケットの出力ポートが入力ポートと同じであり、ループの可能性の原因となった回数。 ネットワークの設定の誤り、またはポートの信頼設定の誤用の可能性を示します。
Packet denied by platform	プラットフォーム固有のレジストリによってパケットが拒否された回数。

show radius server-group

RADIUS サーバ グループのプロパティを表示するには、**show radius server-group** コマンドを使用します。

show radius server-group {*name* | **all**}

構文の説明

name	サーバ グループの名前。 サーバ グループの名前の指定に使用する文字列は、**aaa group server radius** コマンドを使用して定義する必要があります。
all	すべてのサーバ グループのプロパティを表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

aaa group server radius コマンドで定義したサーバ 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

次の例では、**show radius server-group all** コマンドの出力を示します。

```
Switch# show radius server-group all
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *9*：*show radius server-groups* コマンドのフィールドの説明

フィールド	説明
Server group	サーバ グループの名前。

フィールド	説明
Sharecount	このサーバ グループを共有している方式リストの数。 たとえば、1 つの方式リストが特定のサーバ グループを使用する場合、sharecount は 1 です。 2 つの方式リストが同じサーバ グループを使用する場合、sharecount は 2 です。
sg_unconfigured	サーバ グループが設定解除されました。
Type	タイプは、standard または nonstandard のいずれかです。 タイプはグループ内のサーバが非標準の属性を受け入れるかどうかを示します。 グループ内のすべてのサーバに非標準のオプションが設定されている場合、タイプは「nonstandard」と表示されます。
Memlocks	メモリ内にあるサーバ グループ構造の内部参照の数。 この数は、このサーバ グループへの参照を保持している内部データ構造パケットまたはトランザクションがいくつあるかを表します。 Memlocks はメモリ管理のために内部的に使用されます。

show vlan access-map

特定の VLAN アクセスマップまたはすべての VLAN アクセスマップに関する情報を表示するには、特権 EXEC モードで **show vlan access-map** コマンドを使用します。

show vlan access-map [*map-name*]

構文の説明

map-name	（任意）特定の VLAN アクセス マップ名。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、**show vlan access-map** コマンドの出力を示します。

show vlan group

VLAN グループにマッピングされている VLAN を表示するには、特権 EXEC モードで **show vlan group** コマンドを使用します。

show vlan group [**group-name** *vlan-group-name* **[user_count]**]

構文の説明

group-name *vlan-group-name*	（任意）指定した VLAN グループにマッピングされている VLAN を表示します。
user_count	（任意）特定の VLAN グループにマッピングされている各 VLAN のユーザ数を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

show vlan group コマンドは既存の VLAN グループを表示し、各 VLAN グループのメンバである VLAN および VLAN の範囲を示します。 **group-name** キーワードを入力すると、指定した VLAN グループのメンバーのみが表示されます。

例

次の例では、特定の VLAN グループのメンバを表示する方法を示します。

switchport port-security aging static

設定されたセキュア アドレスに対してポート セキュリティ エージングをイネーブルにするには、インターフェイス コンフィギュレーション モードで **switchport port-security aging static** コマンドを使用します。 エージングをディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport port-security aging static

no switchport port-security aging static

構文の説明

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 デフォルト

ディセーブル

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

例

次の例では、設定されたセキュア アドレスに対してポート セキュリティ エージングをイネーブルにする方法を示します。

```
Switch(config-if)# switchport port-security aging static
```

tracking（IPv6 スヌーピング）

ポートのデフォルト トラッキング ポリシーを上書きするには、ipv6 スヌーピング ポリシー コンフィギュレーション モードで **tracking** コマンドを使用します。

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}

構文の説明

enable	トラッキングをイネーブルにします。
reachable-lifetime	（任意）到達可能という証明がない状態で、到達可能なエントリが直接的または間接的に到達可能であると判断される最大時間を指定します。 • **reachable-lifetime** キーワードは、**enable** キーワードがあるときのみ使用可能です。 • **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムがオーバーライドされます。
value	秒単位のライフタイム値。 指定できる範囲は 1 ～ 86400 で、デフォルトは 300 です。
infinite	エントリを無限に到達可能状態またはステイル状態に維持します。
disable	トラッキングをディセーブルにします。
stale-lifetime	（任意）時間エントリをステイル状態に維持します。これによりグローバルの stale-lifetime 設定が上書きされます。 • ステイル ライフタイムは 86,400 秒です。 • **stale-lifetime** キーワードは、**disable** キーワードがあるときのみ使用可能です。 • **stale-lifetime** キーワードを使用すると、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルなステイル ライフタイムがオーバーライドされます。

コマンド デフォルト

IPv6 のスヌーピングは到達可能な状態に維持されます。

コマンド モード

ipv6 snooping configuration（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

tracking コマンドはこのポリシーが適用されるポートの、**ipv6 neighbor tracking** コマンドで設定されたデフォルトのトラッキング ポリシーを上書きします。この機能は、たとえば、エントリを追跡しないが、バインディング テーブルにエントリを残して盗難を防止する場合などに、信頼できるポート上で有用です。

reachable-lifetime キーワードは、到達可能という証明がない状態で、あるエントリがトラッキングにより直接的に、またはIPv6 スヌーピングにより間接的に到達可能であると判断される最大時間を示します。**reachable-lifetime** 値に到達すると、エントリはステイル状態に移動します。tracking コマンドとともに **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムがオーバーライドされます。

stale-lifetime キーワードはエントリが削除されるか到達可能であると証明される前にテーブルに直接または間接的に保持される最大時間です。 **tracking** コマンドとともに **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルなステイル ライフタイムがオーバーライドされます。

例

次に、IPv6 スヌーピングポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、エントリを信頼できるポート上で無限にバインディング テーブルに保存するように設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

trusted-port

あるポートを信頼できるポートとして設定するには、IPv6 スヌーピング ポリシー モードまたは ND 検査ポリシー コンフィギュレーション モードで **trusted-port** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

trusted-port

no trusted-port

構文の説明

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 デフォルト

どのポートも信頼されていません。

コマンド モード

ND 検査ポリシー コンフィギュレーション（config-nd-inspection）

IPv6 スヌーピング コンフィギュレーション（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

trusted-port コマンドをイネーブルにすると、メッセージがこのポリシーを持つポートで受信された場合、限定的に実行されるか、まったく実行されません。ただし、アドレス スプーフィングから保護するために、メッセージは伝送するバインディング情報の使用によってバインディング テーブルを維持できるように分析されます。 これらのポートで検出されたバインディングは、信頼できるものとして設定されていないポートから受信したバインディングよりも信頼性が高いものと見なされます。

例

次に、NDP ポリシー名を policy1 と定義し、スイッチを NDP インスペクション ポリシー コンフィギュレーション モードにし、ポートを信頼するように設定する例を示します。

```
Switch(config)# ipv6  nd inspection  policy1
Switch(config-nd-inspection)# trusted-port
```

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートを信頼するように設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# trusted-port
```

vlan access-map

VLAN パケット フィルタリング用の VLAN マップ エントリを作成または修正し、VLAN アクセスマップ コンフィギュレーション モードに変更するには、スイッチ スタックまたはスタンドアロン スイッチ上で、グローバル コンフィギュレーション モードで **vlan access-map** コマンドを使用します。 VLAN マップ 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。

vlan access-map *name* [*number*]

no vlan access-map *name* [*number*]

（注） このコマンドは、LAN ベース フィーチャ セットを実行しているスイッチではサポートされません。

構文の説明

name	VLAN マップ名
number	（任意）作成または変更するマップ エントリのシーケンス番号（0 ～ 65535）。VLAN マップを作成する際にシーケンス番号を指定しない場合、番号は自動的に割り当てられ、10 から開始して 10 ずつ増加します。 この番号は、VLAN アクセス マップ エントリに挿入するか、または VLAN アクセス マップ エントリから削除する順番です。

コマンド デフォルト

VLAN に適用する VLAN マップ エントリまたは VLAN 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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードでは、このコマンドは VLAN マップを作成または修正します。 このエントリは、モードを VLAN アクセス マップ コンフィギュレーションに変更します。**match** アクセス マップ コンフィギュレーション コマンドを使用して、一致する IP または

非 IP トラフィック用にアクセス リストを指定します。**action** コマンドは、この一致によりパケットを転送またはドロップするかどうかを設定します。

VLAN アクセス マップ コンフィギュレーション モードでは、次のコマンドが利用できます。

- **action**：実行するアクションを設定します（転送またはドロップ）。
- **default**：コマンドをデフォルト値に設定します。
- **exit**：VLAN アクセスマップ コンフィギュレーション モードを終了します。
- **match**：一致する値を設定します（IP アドレスまたは MAC アドレス）。
- **no**：コマンドを無効にするか、そのデフォルトに設定します。

エントリ番号（シーケンス番号）を指定しない場合、マップの最後に追加されます。

VLAN ごとに VLAN マップは 1 つだけ設定できます。VLAN マップは、VLAN でパケットを受信すると適用されます。

シーケンス番号を指定して **no vlan access-map** *name* [*number*] コマンドを使用すると、エントリを 1 つ削除できます。

vlan filter インターフェイス コンフィギュレーション コマンドは、VLAN マップを 1 つまたは複数の VLAN に適用します。

VLAN マップ エントリの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、vac1 という名の VLAN マップを作成し、一致条件とアクションをその VLAN マップに適用する方法を示します。 他のエントリがマップに存在しない場合、これはエントリ 10 になります。

```
Switch(config)# vlan access-map vac1
Switch(config-access-map)# match ip address acl1
Switch(config-access-map)# action forward
```

次の例では、VLAN マップ vac1 を削除する方法を示します。

```
Switch(config)# no vlan access-map vac1
```

vlan filter

1 または複数の VLAN に VLAN マップを適用するには、スイッチ スタックまたはスタンドアロン スイッチ上で、グローバル コンフィギュレーション モードで **vlan filter** 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。

vlan filter *mapname* **vlan-list** {*list*| **all**}

no vlan filter *mapname* **vlan-list** {*list*| **all**}

（注） このコマンドは、LAN ベース フィーチャ セットを実行しているスイッチではサポートされません。

構文の説明

mapname	VLAN マップ エントリ名
vlan-list	マップを適用する VLAN を指定します。
list	tt、uu-vv、xx、および yy-zz 形式での 1 つまたは複数の VLAN リスト。カンマとダッシュの前後のスペースは任意です。 指定できる範囲は 1 ～ 4094 です。
all	マップをすべての VLAN に追加します。

コマンド デフォルト

VLAN フィルタはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

パケットを誤って過剰にドロップし、設定プロセスの途中で接続が無効になることがないように、VLAN アクセス マップを完全に定義してから VLAN に適用することを推奨します。

VLAN マップ エントリの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、VLAN マップ エントリ map1 を VLAN 20 および 30 に適用します。

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

次の例では、VLAN マップ エントリ map1 を VLAN 20 から削除する方法を示します。

```
Switch(config)# no vlan filter map1 vlan-list 20
```

設定を確認するには、**show vlan filter** 特権 EXEC コマンドを入力します。

vlan group

VLAN グループを作成または変更するには、グローバル コンフィギュレーション モードで **vlan group** コマンドを使用します。 VLAN グループから VLAN 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。

vlan group *group-name* **vlan-list** *vlan-list*

no vlan group *group-name* **vlan-list** *vlan-list*

構文の説明

group-name	VLAN グループの名前。 名前は最大 32 文字で、文字から始める必要があります。
vlan-list *vlan-list*	VLAN グループに追加される 1 つ以上の VLAN を指定します。 *vlan-list* 引数には単一の VLAN ID、VLAN ID リスト、または VLAN ID 範囲を指定できます。 複数のエントリはハイフン（-）またはカンマ（,）で区切ります。

コマンド デフォルト

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

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

指定された VLAN グループが存在しない場合、**vlan group** コマンドはグループを作成し、指定された VLAN リストをそのグループにマッピングします。 指定された VLAN グループが存在する場合は、指定された VLAN リストがそのグループにマッピングされます。

vlan group コマンドの **no** 形式を使用すると、指定された VLAN リストが VLAN グループから削除されます。 VLAN グループから最後の VLAN を削除すると、その VLAN グループは削除されます。

最大 100 の VLAN グループを設定でき、1 つの VLAN グループに最大 4094 の VLAN をマッピングできます。

例

次に、VLAN 7 ～ 9 と 11 を VLAN グループにマッピングする例を示します。

```
Switch(config)# vlan group group1 vlan-list 7-9,11
```

次の例では、VLAN グループから VLAN 7 を削除する方法を示します。

```
Switch(config)# no vlan group group1 vlan-list 7
```

索 引