



## セキュリティ

---

- [aaa accounting](#) (3 ページ)
- [aaa accounting dot1x](#) (7 ページ)
- [aaa accounting identity](#) (8 ページ)
- [aaa authentication dot1x](#) (10 ページ)
- [aaa new-model](#) (11 ページ)
- [authentication host-mode](#) (12 ページ)
- [authentication mac-move permit](#) (13 ページ)
- [authentication priority](#) (14 ページ)
- [authentication violation](#) (17 ページ)
- [cisp enable](#) (18 ページ)
- [clear errdisable interface vlan](#) (19 ページ)
- [clear mac address-table](#) (20 ページ)
- [confidentiality-offset](#) (22 ページ)
- [cts manual](#) (23 ページ)
- [cts role-based enforcement](#) (24 ページ)
- [cts role-based l2-vrf](#) (26 ページ)
- [cts role-based monitor](#) (27 ページ)
- [cts role-based permissions](#) (28 ページ)
- [delay-protection](#) (29 ページ)
- [deny \(MAC アクセス リスト コンフィギュレーション\)](#) (30 ページ)
- [device-role \(IPv6 スヌーピング\)](#) (34 ページ)
- [device-role \(IPv6 ND インспекション\)](#) (35 ページ)
- [device-tracking policy](#) (36 ページ)
- [dot1x critical \(グローバル コンフィギュレーション\)](#) (37 ページ)
- [dot1x pae](#) (38 ページ)
- [dot1x supplicant controlled transient](#) (39 ページ)
- [dot1x supplicant force-multicast](#) (40 ページ)
- [dot1x test eapol-capable](#) (41 ページ)
- [dot1x test timeout](#) (42 ページ)

- dot1x timeout (43 ページ)
- dtls (45 ページ)
- epm access-control open (46 ページ)
- include-icv-indicator (47 ページ)
- ip access-list role-based (48 ページ)
- ip admission (49 ページ)
- ip admission name (50 ページ)
- ip dhcp snooping database (52 ページ)
- ip dhcp snooping information option format remote-id (54 ページ)
- ip dhcp snooping verify no-relay-agent-address (55 ページ)
- ip http access-class (55 ページ)
- ip radius source-interface (57 ページ)
- ip source binding (58 ページ)
- ip verify source (59 ページ)
- ipv6 access-list (60 ページ)
- ipv6 snooping policy (62 ページ)
- key chain macsec (64 ページ)
- key-server (65 ページ)
- limit address-count (66 ページ)
- mab request format attribute 32 (67 ページ)
- macsec-cipher-suite (68 ページ)
- macsec network-link (70 ページ)
- match (アクセス マップ コンフィギュレーション) (70 ページ)
- mka pre-shared-key (72 ページ)
- mka suppress syslogs sak-rekey (72 ページ)
- authentication logging verbose (73 ページ)
- dot1x logging verbose (74 ページ)
- mab logging verbose (75 ページ)
- permit (MAC アクセス リスト コンフィギュレーション) (76 ページ)
- propagate sgt (cts manual) (80 ページ)
- protocol (IPv6 スヌーピング) (81 ページ)
- radius server (82 ページ)
- sak-rekey (84 ページ)
- sap mode-list (cts manual) (85 ページ)
- security level (IPv6 スヌーピング) (87 ページ)
- send-secure-announcements (88 ページ)
- server-private (RADIUS) (89 ページ)
- server-private (TACACS+) (91 ページ)
- show aaa clients (93 ページ)
- show aaa command handler (93 ページ)
- **show aaa local** (94 ページ)

- [show aaa servers](#) (95 ページ)
- [show aaa sessions](#) (96 ページ)
- [show authentication brief](#) (97 ページ)
- [show authentication sessions](#) (99 ページ)
- [show cts interface](#) (101 ページ)
- [show cts role-based permissions](#) (104 ページ)
- [show cisp](#) (105 ページ)
- [show dot1x](#) (106 ページ)
- [show eap pac peer](#) (108 ページ)
- [show ip dhcp snooping statistics](#) (108 ページ)
- [show radius server-group](#) (111 ページ)
- [show vlan access-map](#) (113 ページ)
- [show vlan filter](#) (113 ページ)
- [show vlan group](#) (114 ページ)
- [switchport port-security aging](#) (115 ページ)
- [switchport port-security mac-address](#) (116 ページ)
- [switchport port-security maximum](#) (119 ページ)
- [switchport port-security violation](#) (121 ページ)
- [tacacs server](#) (123 ページ)
- [tracking \(IPv6 スヌーピング\)](#) (124 ページ)
- [trusted-port](#) (125 ページ)
- [vlan access-map](#) (126 ページ)
- [vlan dot1Q tag native](#) (128 ページ)
- [vlan filter](#) (129 ページ)
- [vlan group](#) (130 ページ)

## aaa accounting

RADIUS または TACACS+ を使用する場合に、課金やセキュリティ目的で、要求されたサービスの認証、許可、およびアカウントिंग (AAA) アカウントिंग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 **aaa accounting** コマンドを使用します。AAA アカウントिंग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 {auth-proxy | system | network | exec | connections | commands level}
{default | list-name} {start-stop | stop-only | none} [broadcast] group group-name
no aaa accounting {auth-proxy | system | network | exec | connections | commands
level} {default | list-name} {start-stop | stop-only | none} [broadcast] group group-name
```

### 構文の説明

<b>auth-proxy</b>	すべての認証済みプロキシユーザイベントに関する情報を出力します。
<b>system</b>	リロードなどのユーザに関連付けられていないシステムレベルのすべてのイベントのアカウントングを実行します。

<b>network</b>	ネットワークに関連するあらゆるサービス要求にアカウントティングを実行します。
<b>exec</b>	EXEC シェルセッションのアカウントティングを実行します。このキーワードは、 <b>autocommand</b> コマンドによって生成される情報などのユーザプロフィール情報を返すことができます。
<b>connection</b>	ネットワーク アクセス サーバから確立されたすべてのアウトバウンド接続に関する情報を提供します。
<b>commands level</b>	指定した特権レベルですべてのコマンドのアカウントティングを実行します。有効な特権レベル エントリは 0 ~ 15 の整数です。
<b>default</b>	この引数のあとにリストされるアカウントティング方式を、アカウントティングサービスのデフォルトリストとして使用します。
<b>list-name</b>	次に記載されているアカウントティング方式のうち、少なくとも 1 つを含むリストの名前を付けるために使用する文字列です：
<b>start-stop</b>	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" アカウントティングレコードはバックグラウンドで送信されます。要求されたユーザプロセスは、"start" accounting 通知がアカウントティングサーバで受信されたかどうかに関係なく開始されません。
<b>stop-only</b>	要求されたユーザ プロセスの終了時に、"stop" アカウントティング通知を送信します。
<b>none</b>	この回線またはインターフェイスでアカウントティングサービスをディセーブルにします。
<b>broadcast</b>	(任意) 複数の AAA サーバへのアカウントティングレコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウントティングレコードを同時に送信します。最初のサーバが使用できない場合、そのグループ内で定義されたバックアップサーバを使用してフェールオーバーが発生します。
<b>group groupname</b>	次に記述されているキーワードの 1 つ以上を使用します： <a href="#">表 1: AAA アカウントティングの方式 (5 ページ)</a>

コマンド デフォルト AAA アカウントティング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 XE Everest 16.6.1	このコマンドが導入されました。

## 使用上のガイドライン

アカウントティングを有効にし、回線別またはインターフェイス別に特定のアカウントティング方式を定義する名前付き方法リストを作成するには、**aaa accounting** コマンドを使用します。

表 1: AAA アカウントティングの方式

キーワード	説明
<b>group radius</b>	<b>aaa group server radius</b> コマンドで定義されるすべての RADIUS サーバのリストを認証に使用します。
<b>group tacacs+</b>	<b>aaa group server tacacs+</b> コマンドで定義されるすべての TACACS+ サーバのリストを認証に使用します。
<b>group group-name</b>	<b>group-name</b> サーバグループで定義したように、アカウントティングのための RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

表 1: AAA アカウントティングの方式 (5 ページ) では、**group radius** 方式および **group tacacs+** 方式は、以前に定義した一連の RADIUS サーバまたは TACACS+ サーバを参照します。ホストサーバを設定するには、**radius server** および **tacacs server** コマンドを使用します。特定のサーバグループを作成するには、**aaa group server radius** および **aaa group server tacacs+** コマンドを使用します。

Cisco IOS ソフトウェアは次の 2 つのアカウントティング方式をサポートします。

- **RADIUS** : ネットワークアクセスサーバは、アカウントティングレコードの形式で RADIUS セキュリティサーバに対してユーザアクティビティを報告します。各アカウントティングレコードにはアカウントティングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティサーバに格納されます。
- **TACACS+** : ネットワークアクセスサーバは、アカウントティングレコードの形式で TACACS+ セキュリティサーバに対してユーザアクティビティを報告します。各アカウントティングレコードにはアカウントティングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティサーバに格納されます。

アカウントティングの方式リストは、アカウントティングの実行方法を定義します。名前付きアカウントティング方式リストにより、特定の回線またはインターフェイスで、特定の種類のアカウントティングサービスに使用する特定のセキュリティプロトコルを指定できます。**list-name** および **method** を入力してリストを作成します。**list-name** にはこのリストの名前として使用する任意の文字列 (**radius** や **tacacs+** などの方式名を除く) を指定し、**method** には指定されたシーケンスで試行する方式を指定します。

特定のアカウントティングの種類の **aaa accounting** コマンドを、名前付き方式リストを指定しないで発行した場合、名前付き方式リストが明示的に定義されているものを除いて、すべてのインターフェイスまたは回線 (このアカウントティングの種類が適用される) にデフォルトの方式リストが自動的に適用されます (定義済みの方式リストは、デフォルトの方式リストに優先し

ます)。デフォルトの方式リストが定義されていない場合、アカウントリングは実行されません。



(注) システムアカウントリングでは名前付きアカウントリングリストは使用されず、システムアカウントリングのためのデフォルトのリストだけを定義できます。

最小のアカウントリングの場合、**stop-only** キーワードを指定して、要求されたユーザプロセスの終了時に **stop** レコードアカウントリング通知を送信します。詳細なアカウントリングの場合、**start-stop** キーワードを指定することで、RADIUS または TACACS+ が要求されたプロセスの開始時に **start** アカウントリング通知を送信し、プロセスの終了時に **stop** アカウントリング通知を送信するようにできます。アカウントリングは RADIUS または TACACS+ サーバにだけ保存されます。**none** キーワードは、指定した回線またはインターフェイスのアカウントリングサービスをディセーブルにします。

AAA アカウントリングがアクティブにされると、ネットワークアクセスサーバは、ユーザが実装したセキュリティ方式に応じて、接続に関する RADIUS アカウントリング属性または TACACS+ AV ペアをモニタします。ネットワークアクセスサーバはこれらの属性をアカウントリングレコードとしてレポートし、アカウントリングレコードはその後セキュリティサーバのアカウントリングログに保存されます。サポートされる RADIUS アカウントリング属性の一覧については、『Cisco IOS Security Configuration Guide』の付録「RADIUS Attributes」を参照してください。サポートされる TACACS+ アカウントリングの AV ペアの一覧については、『Cisco IOS Security Configuration Guide』の付録「TACACS+ Attributes-Value Pairs」を参照してください。



(注) このコマンドは、TACACS または拡張 TACACS には使用できません。

次の例では、デフォルトのコマンドアカウントリング方式リストを定義しています。この例のアカウントリングサービスは TACACS+ セキュリティ サーバーによって提供され、**stop-only** 制限で特権レベル 15 コマンドに設定されています。

```
デバイス(config)# aaa accounting commands 15 default stop-only group TACACS+
```

次の例では、アカウントリングサービスが TACACS+ セキュリティ サーバーで提供され、**stop-only** 制限があるデフォルトの **auth-proxy** アカウントリング方式リストの定義を示します。**aaa accounting** コマンドは認証プロキシアカウントリングをアクティブにします。

```
デバイス(config)# aaa new model
デバイス(config)# aaa authentication login default group TACACS+
デバイス(config)# aaa authorization auth-proxy default group TACACS+
デバイス(config)# aaa accounting auth-proxy default start-stop group TACACS+
```

## aaa accounting dot1x

認証、認可、およびアカウントティング (AAA) アカウント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トティング方式を、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 アカウント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

<b>name</b>	サーバグループ名。これは、 <b>broadcast group</b> および <b>group</b> 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。
<b>default</b>	デフォルトリストにあるアカウントティング方式を、アカウントティングサービス用に指定します。
<b>start-stop</b>	プロセスの開始時に <b>start accounting</b> 通知を送信し、プロセスの終了時に <b>stop accounting</b> 通知を送信します。start アカウントティングレコードはバックグラウンドで送信されます。アカウントティングサーバが <b>start accounting</b> 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。
<b>broadcast</b>	複数の AAA サーバに送信されるアカウントティングレコードをイネーブルにして、アカウント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。
<b>group</b>	アカウント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。 <ul style="list-style-type: none"> <li>• <b>name</b> : サーバグループの名前。</li> <li>• <b>radius</b> : すべての RADIUS ホストのリスト。</li> <li>• <b>tacacs+</b> : すべての TACACS+ ホストのリスト。</li> </ul> <b>broadcast group</b> および <b>group</b> キーワードの後に入力する場合、 <b>group</b> キーワードはオプションです。オプションの <b>group</b> キーワードより多くの値を入力できます。
<b>radius</b>	(任意) RADIUS アカウントティングをイネーブルにします。
<b>tacacs+</b>	(任意) TACACS+ アカウントティングをイネーブルにします。

コマンドデフォルト AAA アカウントティング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 XE Everest 16.6.1	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。

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。

```
デバイス(config)# aaa new-model
デバイス(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、認可、およびアカウンティング (AAA) 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、**aaa accounting identity** 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	
<b>name</b>	サーバグループ名。これは、 <b>broadcast group</b> および <b>group</b> 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。
<b>default</b>	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。
<b>start-stop</b>	プロセスの開始時に <b>start accounting</b> 通知を送信し、プロセスの終了時に <b>stop accounting</b> 通知を送信します。 <b>start</b> 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 <b>start</b> 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。
<b>broadcast</b>	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。



<b>group</b>	<p>アカウント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。</p> <ul style="list-style-type: none"> <li>• <b>name</b> : サーバグループの名前。</li> <li>• <b>radius</b> : すべての RADIUS ホストのリスト。</li> <li>• <b>tacacs+</b> : すべての TACACS+ ホストのリスト。</li> </ul> <p><b>broadcast group</b> および <b>group</b> キーワードの後に入力する場合、<b>group</b> キーワードはオプションです。オプションの <b>group</b> キーワードより多くの値を入力できます。</p>
<b>radius</b>	(任意) RADIUS 認証をイネーブルにします。
<b>tacacs+</b>	(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 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 XE Everest 16.6.1	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 モードを有効にするには、特権 EXEC モードで **authentication display new-style** コマンドを入力します。

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。

```
デバイス# 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.

```
デバイス# configure terminal
```

```
デバイス(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使用する認証、認可、およびアカウントリング (AAA) 方式を指定するには、スタンドアロンスイッチ上のグローバル コンフィギュレーション モードで **aaa authentication dot1x** コマンドを使用します。認証を無効にするには、このコマンドの **no** 形式を使用します。

```
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法。この引数に続いてリストされた認証方式が使用されます。

**method1** サーバ認証を指定します。認証用にすべての RADIUS サーバの一覧を使用するには、**group radius** キーワードを入力します。

(注) コマンドラインのヘルプストリングには他のキーワードも表示されますが、サポートされるのは **default** および **group radius** キーワードのみです。

### 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 XE Everest 16.6.1	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。IEEE 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 コマンドを入力して 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一覧を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

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。

```
デバイス(config)# aaa new-model
デバイス(config)# aaa authentication dot1x default group radius
```

## aaa new-model

認証、認可、およびアカウントリング（AAA）アクセス制御モデルを有効にするには、グローバル コンフィギュレーションモードで **aaa new-model** コマンドを使用します。AAA アクセス制御モデルを無効にするには、このコマンドの **no** 形式を使用します。

**aaa new-model**  
**no aaa new-model**

### 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

AAA が有効になっていません。

### コマンド モード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	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、AAA アクセス制御システムが有効になります。

仮想端末回線（VTY）に関して **login local** コマンドが設定されている場合で、かつ **aaa new-model** コマンドが削除されている場合は、スイッチをリロードして、デフォルト設定または **login** コマンドを取得する必要があります。スイッチをリロードしない場合、スイッチは、VTY ではデフォルトで **login local** コマンドに設定されます。



(注) **aaa new-model** コマンドを削除することは推奨されません。

次に、この制限の例を示します。

```

デバイス(config)# aaa new-model
デバイス(config)# line vty 0 15
デバイス(config-line)# login local
デバイス(config-line)# exit
デバイス(config)# no aaa new-model
デバイス(config)# exit
デバイス# show running-config | b line vty

line vty 0 4
 login local !<=== Login local instead of "login"
line vty 5 15
 login local
!
```

### 例

次に、AAA を初期化する例を示します。

```
デバイス(config)# aaa new-model
```

```
デバイス(config)#
```

## 関連コマンド

Command	Description
<b>aaa accounting</b>	課金またはセキュリティ目的のために、要求されたサービスの AAA アカウンティングをイネーブルにします。
<b>aaa authentication arap</b>	TACACS+ を使用する ARAP の AAA 認証方式を有効にします。
<b>aaa authentication enable default</b>	ユーザが特権コマンドレベルにアクセスできるかどうかを決定する AAA 認証を有効にします。
<b>aaa authentication login</b>	ログイン時の AAA 認証を設定します。
<b>aaa authentication ppp</b>	PPP を実行しているシリアルインターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
<b>aaa authorization</b>	ネットワークへのユーザアクセスを制限するパラメータを設定します。

## 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 host-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
authentication host-mode {multi-auth | multi-domain | multi-host | single-host}
no authentication host-mode
```

## 構文の説明

<b>multi-auth</b>	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。
<b>multi-domain</b>	ポートのマルチドメインモードをイネーブルにします。
<b>multi-host</b>	ポートのマルチホストモードをイネーブルにします。
<b>single-host</b>	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 XE Everest 16.6.1	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。

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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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

device 上での MAC 移動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 **authentication mac-move permit** 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 移動は無効になっています。	
コマンド モード	グローバル コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	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、device 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。

次の例では、device 上で MAC 移動をイネーブルにする方法を示します。

```
デバイス(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。デフォルトに戻するには、**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	<b>dot1x</b>	(任意) 認証方式の順序に 802.1X を追加します。
	<b>mab</b>	(任意) 認証方式の順序に MAC 認証バイパス (MAB) を追加します。
	<b>webauth</b>	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 XE Everest 16.6.1

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。

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

```
デバイス(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 番目の認証方式として設定する方法を示します。

```
デバイス(config-if)# authentication priority mab webauth
```

関連コマンド

コマンド	説明
<b>authentication control-direction</b>	ポート モードを単一方向または双方向に設定します。
<b>authentication event fail</b>	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。
<b>authentication event no-response action</b>	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。

コマンド	説明
<b>authentication event server alive action reinitialize</b>	以前に到達不能であった認証、許可、アカウントिंग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。
<b>authentication event server dead action authorize</b>	認証、許可、アカウントिंग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。
<b>authentication fallback</b>	Web 認証のフォールバック方式をイネーブルにします。
<b>authentication host-mode</b>	ホストの制御ポートへのアクセスを許可します。
<b>authentication open</b>	ポートでオープンアクセスをイネーブルにします。
<b>authentication order</b>	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。
<b>authentication periodic</b>	ポートの自動再認証をイネーブルにします。
<b>authentication port-control</b>	制御ポートの許可ステータスを設定します。
<b>authentication timer inactivity</b>	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。
<b>authentication timer reauthenticate</b>	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。
<b>authentication timer restart</b>	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。
<b>authentication violation</b>	ポート上でセキュリティ違反が生じた場合に取りうるアクションを指定します。
<b>mab</b>	ポートのMAC認証バイパスをイネーブルにします。
<b>show authentication registrations</b>	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。
<b>show authentication sessions</b>	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。
<b>show authentication sessions interface</b>	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されたとき、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されたときに発生する違反モードを設定するには、インターフェイス コンフィギュレーションモードで **authentication violation** 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

<b>protect</b>	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。
<b>replace</b>	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。
<b>restrict</b>	違反エラーの発生時に Syslog エラーを生成します。
<b>shutdown</b>	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 XE Everest 16.6.1	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。

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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(config-if)# authentication violation replace
```

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

## cisp enable

スイッチ上で Client Information Signalling Protocol (CISP) を有効にして、サブリカントスイッチのオーセンティケータとして機能し、オーセンティケータスイッチのサブリカント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

デフォルトの動作や値はありません。

### 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 XE Everest 16.6.1	このコマンドが導入されました。
	このコマンドが再度導入されました。このコマンドはおよびではサポートされません。

### 使用上のガイドライン

オーセンティケータとサブ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 モードがサーバーである必要があります。

VTP モードを設定する場合に MD5 チェックサムの一貫性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 サーバーが 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。

次の例では、CISP をイネーブルにする方法を示します。

```
デバイス(config)# cisp enable
```

#### 関連コマンド

コマンド	説明
<b>dot1x credentials</b> プロファイル	プロファイルをサブリカント スイッチに設定します。
<b>dot1x supplicant force-multicast</b>	802.1X サブ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。
<b>dot1x supplicant controlled transient</b>	802.1X サブリカントによる制御アクセスを設定します。
<b>show cisp</b>	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

error-disabled 状態になっていた VLAN を再びイネーブルにするには、特権 EXEC モードで **clear errdisable interface** コマンドを使用します。

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

#### 構文の説明

<i>interface-id</i>	インターフェイスを指定します。
<i>vlan list</i>	(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

デフォルトの動作や値はありません。

#### コマンドモード

特権 EXEC

## clear mac address-table

コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	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 error-disabled をクリアできます。

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。

```
デバイス# clear errdisable interface gigabitethernet4/0/2 vlan
```

関連コマンド	コマンド	説明
	<b>errdisable detect cause</b>	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。
	<b>errdisable recovery</b>	回復メカニズム変数を設定します。
	<b>show errdisable detect</b>	errdisable 検出ステータスを表示します。
	<b>show errdisable recovery</b>	errdisable 回復タイマーの情報を表示します。
	<b>show interfaces status err-disabled</b>	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。

<b>address</b> <i>mac-addr</i>	(任意) 指定されたダイナミック MAC アドレスを削除します。
<b>interface</b> <i>interface-id</i>	(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。
<b>vlan</b> <i>vlan-id</i>	(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。
<b>move update</b>	MAC アドレステーブルの move-update カウンタをクリアします。
<b>notification</b>	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 デフォルトの動作や値はありません。

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 XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン 情報が削除されたことを確認するには、**show mac address-table** 特権 EXEC コマンドを入力します。

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。

```
デバイス# clear mac address-table dynamic address 0008.0070.0007
```

関連コマンド

コマンド	説明
<b>mac address-table notification</b>	MAC アドレス通知機能をイネーブルにします。
<b>mac address-table move update {receive   transmit}</b>	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。
<b>show mac address-table</b>	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。

コマンド	説明
<b>show mac address-table move update</b>	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。
<b>show mac address-table notification</b>	<b>interface</b> 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。
<b>snmp trap mac-notification change</b>	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。

## confidentiality-offset

MACsec Key Agreement (MKA) プロトコルを有効にして MACsec 動作の機密性オフセットを設定するには、MKA ポリシー コンフィギュレーションモードで **confidentiality-offset** コマンドを使用します。機密性オフセットを無効にするには、このコマンドの **no** 形式を使用します。

**confidentiality-offset**  
**no confidentiality-offset**

### 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

機密性オフセットが無効になっています。

### コマンド モード

MKA ポリシー コンフィギュレーション (config-mka-policy)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

### 例

次に、機密性オフセットを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# confidentiality-offset
```

### 関連コマンド

Command	Description
<b>mka policy</b>	MKA ポリシーを設定します。
<b>delay-protection</b>	MKPDU の送信で遅延保護を使用するように MKA を設定します。
<b>include-icv-indicator</b>	MKPDU に ICV インジケータを含めます。

Command	Description
<b>key-server</b>	MKA キーサーバオプションを設定します。
<b>macsec-cipher-suite</b>	SAK を取得するための暗号スイートを設定します。
<b>sak-rekey</b>	SAK キー再生成間隔を設定します。
<b>send-secure-announcements</b>	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。
<b>ssci-based-on-sci</b>	SCI に基づいて SSCI を計算します。
<b>use-updated-eth-header</b>	ICV 計算には更新されたイーサネットヘッダーを使用します。

## cts manual

Cisco TrustSec セキュリティのインターフェイスを手動で有効にするには、インターフェイス コンフィギュレーション モードで **cts manual** コマンドを使用します。

### cts manual

#### 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 (config-if)

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが変更され、いくつかのオプションが追加されました。
Cisco IOS XE 3.7E	このコマンドが導入されました。

#### 使用上のガイドライン

リンクにポリシーおよびセキュリティアソシエーションプロトコル (SAP) を設定する TrustSec 手動インターフェイス コンフィギュレーションを開始するには、**cts manual** コマンドを使用します。

**cts manual** コマンドが設定された場合、802.1X 認証はリンクで実行されません。ポリシーを定義し、リンクに適用するには、**policy** サブコマンドを使用します。デフォルトでは、ポリシーは適用されません。MACsec リンク間暗号化を設定するには、SAP ネゴシエーションパラメータを定義する必要があります。デフォルトでは、SAP は有効になっていません。同じ SAPPKM をリンクの両端で設定する必要があります (つまり、共有秘密)。

#### 例

次に、Cisco TrustSec 手動モードを開始する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# cts manual
Switch(config-if-cts-manual)#
```

次に、インターフェイスから Cisco TrustSec 手動設定を削除する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# no cts manual
```

## 関連コマンド

コマンド	説明
<b>propagate sgt (cts manual)</b>	Cisco TrustSec Security インターフェイスのレイヤ 2 での SGT の伝達を有効にします。
<b>sap mode-list (cts manual)</b>	PMK および SAP 認証モードと暗号化モードを手動で指定し、2 つのインターフェイス間で MACsec リンクの暗号化をネゴシエートします。
<b>show cts interface</b>	Cisco TrustSec インターフェイス設定の統計情報を表示します。

## cts role-based enforcement

Cisco TrustSec ロールベース (セキュリティグループ) アクセスコントロール適用を有効にするには、グローバル コンフィギュレーション モードで **cts role-based enforcement** コマンドを使用します。この設定を無効にするには、このコマンドの **no** 形式を使用します。

**cts role-based enforcement** [**logging-interval** 間隔 | **vlan-list** {**all** | *vlan-ID* [{,}] [{-}]}]

**no cts role-based enforcement** [**logging-interval** 間隔 | **vlan-list** {**all** | *vlan-ID* [{,}] [{-}]}]

## 構文の説明

<b>logging-interval</b> <i>interval</i>	(任意) セキュリティグループアクセスコントロールリスト (SGACL) のロギング間隔を設定します。 <i>interval</i> 引数の有効な値は 5 ~ 86400 秒です。デフォルトは 300 秒です。
<b>vlan-list</b>	(任意) ロールベース ACL が適用される VLAN を設定します。
<b>all</b>	(任意) すべての VLAN を指定します。
<i>vlan-ID</i>	(任意) VLAN ID。有効な値は 1 ~ 4094 です。
,	(任意) 別の VLAN をカンマで区切って指定します。
-	(任意) VLAN の範囲をハイフンで区切って指定します。

## コマンド デフォルト

ロールベース アクセス コントロールは適用されません。



コマンドモード      グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

## 使用上のガイドライン



(注) RBACL と SGACL は互換的に使用されます。

システムで Cisco TrustSec 対応インターフェイスの SGACL 適用をグローバルに有効または無効にするには、**cts role-based enforcement** コマンドを使用します。

特定のフローのログが出力されるデフォルトの間隔は300秒です。デフォルトの間隔を変更するには、**logging-interval** キーワードを使用します。ロギングは、Cisco ACE アプリケーションコントロールエンジンに **logging** キーワードがある場合にのみトリガーされます。

VLAN での SGACL 適用は、デフォルトでは有効になっていません。スイッチ仮想インターフェイス (SVI) でレイヤ2スイッチドパケットおよびレイヤ3スイッチドパケットの SGACL 適用を有効または無効にするには、**cts role-based enforcement vlan-list** コマンドを使用します。

*vlan-ID* 引数には単一の VLAN ID、VLAN ID のリスト、または VLAN ID の範囲を指定できます。

SGACL が適用される VLAN で SVI がアクティブである場合、SGACL はその VLAN 内のレイヤ2とレイヤ3の両方のスイッチドパケットに適用されます。レイヤ3スイッチングは SVI を使用しない VLAN 内では使用できないため、SVI を使用しない場合、SGACL はレイヤ2スイッチドパケットにのみ適用されます。

次に、SGACL ロギング間隔を設定する例を示します。

```
Switch(config)# cts role-based enforcement logging-interval 90
Switch(config)# logging rate-limit
```

```
May 27 10:19:21.509: %RBM-6-SGACLHIT:
ingress_interface='GigabitEthernet1/0/2' sgacl_name='sgacl2' action='Deny'
protocol='icmp' src-ip='16.16.1.3' src-port='8' dest-ip='17.17.1.2' dest-port='0'
sgt='101' dgt='202' logging_interval_hits='5'
```

## 関連コマンド

コマンド	説明
<b>logging rate-limit</b>	1秒間にログに記録されるメッセージの割合を制限します。
<b>show cts role-based permissions</b>	SGACL の権限リストを表示します。

## cts role-based l2-vrf

レイヤ 2 VLAN の Virtual Routing and Forwarding (VRF) インスタンスを選択するには、グローバル コンフィギュレーション モードで **cts role-based l2-vrf** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

```
cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{}-]
no cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{}-]
```

### 構文の説明

<i>vrf-name</i>	VRF インスタンスの名前。
<b>vlan-list</b>	VRF インスタンスに割り当てられる VLAN のリストを指定します。
<b>all</b>	すべての VLAN を指定します。
<i>vlan-ID</i>	VLAN ID。有効な値は 1 ~ 4094 です。
,	(任意) 別の VLAN をカンマで区切って指定します。
-	(任意) VLAN の範囲をハイフンで区切って指定します。

### コマンド デフォルト

VRF インスタンスは選択されていません。

### コマンド モード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	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-list* 引数には単一の VLAN ID、カンマで区切られた VLAN ID のリスト、またはハイフンで区切られた VLAN ID の範囲を指定できます。

**all** キーワードは、ネットワークデバイスによってサポートされている VLAN の全範囲と同等です。**all** キーワードは、不揮発性生成 (NVGEN) プロセスで保持されません。

**cts role-based l2-vrf** コマンドが同じ VRF に複数回実行される場合、入力される連続した各コマンドは、指定された VRF に VLAN ID を追加します。

**cts role-based l2-vrf** コマンドで設定された VRF 割り当ては、VLAN がレイヤ 2 VLAN として維持されている間はアクティブです。VRF の割り当てがアクティブな間に、学習した IP-SGT バインディングも VRF と IP プロトコルバージョンに関連付けられた転送情報ベース (FIB) テーブルに追加されます。VLAN のスイッチ仮想インターフェイス (SVI) がアクティブになると、VRF から VLAN への割り当てが非アクティブになり、VLAN で学習されたすべてのバインディングが SVI の VRF に関連付けられた FIB テーブルに移動されます。

SVI インターフェイスを設定するには **interface vlan** コマンドを使用し、VRF インスタンスをインターフェイスに関連付けるには **vrf forwarding** コマンドを使用します。

VRF から VLAN への割り当ては、割り当てが非アクティブになっても保持されます。SVI が削除された、または SVI の IP アドレスの変更された場合に再アクティブ化されます。再アクティブ化された場合、IP-SGT バインディングは、SVI の FIB に関連付けられた FIB テーブルから、**cts role-based l2-vrf** コマンドによって割り当てられた VRF に関連付けられた FIB テーブルに戻されます。

次に、VRF インスタンスに割り当てられる VLAN のリストを選択する例を示します。

```
Switch(config)# cts role-based l2-vrf vrf1 vlan-list 20
```

次に、SVI インターフェイスを設定し、VRF インスタンスを関連付ける例を示します。

```
Switch(config)# interface vlan 101
Switch(config-if)# vrf forwarding vrf1
```

#### 関連コマンド

コマンド	説明
<b>interface vlan</b>	VLAN インターフェイスを設定します。
<b>vrf forwarding</b>	VRF インスタンスまたは仮想ネットワークをインターフェイスまたはサブインターフェイスに関連付けます。
<b>show cts role-based permissions</b>	SGACL の権限リストを表示します。

## cts role-based monitor

ロールベース（セキュリティグループ）アクセスリストモニタリングを有効にするには、グローバル コンフィギュレーション モードで **cts role-based monitor** コマンドを使用します。ロールベース アクセス リスト モニタリングを削除するには、このコマンドの **no** 形式を使用します。

```
cts role-based monitor {all | permissions | {default | from {sgt | unknown}} to {sgt | unknown} [{ipv4}]}
```

```
no cts role-based monitor {all | permissions | {default | from {sgt | unknown}} to {sgt | unknown} [{ipv4}]}
```

#### 構文の説明

<b>all</b>	すべての宛先タグへのすべての送信元タグの権限をモニタします。
<b>permissions</b>	1 つの送信元タグから 1 つの宛先タグへの権限をモニタします。
<b>default</b>	デフォルトの権限リストをモニタします。
<b>from</b>	フィルタリングされるトラフィックの送信元グループタグを指定します。
<b>sgt</b>	セキュリティグループタグ（SGT）有効値は 2 ～ 65519 です。

**unknown** 未知の送信元または宛先グループタグ (DST) を指定します。

**ipv4** (任意) IPv4 プロトコルを指定します。

コマンドデフォルト      ロールベース アクセス コントロール モニタリングは有効になっていません。

コマンドモード          グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン      グローバルモニタモードを有効にするには、**cts role-based monitor all** コマンドを使用します。**cts role-based monitor all** コマンドが設定されている場合、**show cts role-based permissions** コマンドの出力には、設定されているすべてのポリシーのモニタモードが **true** と表示されます。

次に、送信元タグから宛先タグへの SGACL モニタを設定する例を示します。

```
Switch(config)# cts role-based monitor permissions from 10 to 11
```

関連コマンド	コマンド	説明
	<b>show cts role-based permissions</b>	SGACL の権限リストを表示します。

## cts role-based permissions

1 つの送信元グループから 1 つの宛先グループへの権限を有効にするには、グローバル コンフィギュレーションモードで **cts role-based permissions** コマンドを使用します。権限を削除するには、このコマンドの **no** 形式を使用します。

```
cts role-based permissions {default ipv4 | from {sgt | unknown} to {sgt | unknown} {ipv4}
{rbacl-name [{rbacl-name...}]}}
no cts role-based permissions {default [{ipv4}] | from {sgt | unknown} to
{sgt | unknown} [{ipv4}]}
```

構文の説明	default	説明
	<b>default</b>	デフォルトの権限リストを指定します。セキュリティ グループ アクセス コントロール リスト (SGACL) 権限が静的または動的に設定されていないすべてのセル (SGT ペア) は、デフォルトのカテゴリに属します。
	<b>ipv4</b>	IPv4 プロトコルを指定します。
	<b>from</b>	フィルタリングされるトラフィックの送信元グループ タグを指定します。
	<b>sgt</b>	セキュリティグループタグ (SGT) 有効値は 2 ~ 65519 です。

**unknown** 未知の送信元または宛先グループタグを指定します。

**rbacl-name** ロールベース アクセス コントロール リスト (RBACL) または SGACL の名前。  
この設定では最大 16 の SGACL を指定できます。

**コマンド デフォルト** 1 つの送信元グループから 1 つの宛先グループへの権限は有効になっていません。

**コマンド モード** グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

**使用上のガイドライン** 特定の送信元グループタグ (SGT)、宛先グループタグ (DGT) ペアの SGACL のリストを定義したり、置き換えたり、削除したりするには、**cts role-based permissions** コマンドを使用します。このポリシーは、同じ DGT または SGT に対するダイナミックなポリシーがないかぎり有効です。

**cts role-based permissions default** コマンドでは、同じ DGT に対するダイナミックなポリシーがないかぎり、デフォルトポリシーの SGACL のリストを定義したり、置き換えたり、削除したりすることができます。

次に、宛先グループの権限を有効にする例を示します。

```
Switch(config)# cts role-based permissions from 6 to 6 mon_2
```

**関連コマンド**

コマンド	説明
<b>show cts role-based permissions</b>	SGACL の権限リストを表示します。

## delay-protection

MACsec Key Agreement Protocol Data Unit (MKPDU) の送信に遅延保護を使用するように MKA を設定するには、MKA ポリシー コンフィギュレーション モードで **delay-protection** コマンドを使用します。遅延保護を無効にするには、このコマンドの **no** 形式を使用します。

**delay-protection**  
**no delay-protection**

**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** MKPDU の送信に対する遅延保護は無効になっています。

**コマンド モード** MKA ポリシー コンフィギュレーション (config-mka-policy)

## コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

## 例

次に、MKPDU の送信で遅延保護を使用するように MKA を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# delay-protection
```

## 関連コマンド

Command	Description
<b>mka policy</b>	MKA ポリシーを設定します。
<b>confidentiality-offset</b>	機密性オフセットを設定して MACsec を動作させます。
<b>include-icv-indicator</b>	MKPDU に ICV インジケータを含めます。
<b>key-server</b>	MKA キーサーバオプションを設定します。
<b>macsec-cipher-suite</b>	SAK を取得するための暗号スイートを設定します。
<b>sak-rekey</b>	SAK キー再生成間隔を設定します。
<b>send-secure-announcements</b>	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。
<b>ssci-based-on-sci</b>	SCI に基づいて SSCI を計算します。
<b>use-updated-eth-header</b>	ICV 計算には更新されたイーサネットヘッダーを使用します。

## 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 | larc-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 | larc-sca | lsap lsap mask |
```

**mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp** [**cos** *cos*]

## 構文の説明

<b>any</b>	すべての送信元または宛先 MAC アドレスを拒否します。
<b>host</b> <i>src-MAC-addr</i>   <i>src-MAC-addr mask</i>	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。
<b>host</b> <i>dst-MAC-addr</i>   <i>dst-MAC-addr mask</i>	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。
<i>type mask</i>	<p>(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。</p> <p><i>type</i> には、0 ~ 65535 の 16 進数を指定できます。</p> <p><i>mask</i> 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。</p>
<b>arp</b>	(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。
<b>amber</b>	(任意) EtherType DEC-Amber を指定します。
<b>appletalk</b>	(任意) EtherType AppleTalk/EtherTalk を指定します。
<b>dec-spanning</b>	(任意) EtherType Digital Equipment Corporation (DEC) スパニングツリーを指定します。
<b>decnet-iv</b>	(任意) EtherType DECnet Phase IV プロトコルを指定します。
<b>diagnostic</b>	(任意) EtherType DEC-Diagnostic を指定します。
<b>dsm</b>	(任意) EtherType DEC-DSM を指定します。
<b>etype-6000</b>	(任意) EtherType 0x6000 を指定します。

<b>etype-8042</b>	(任意) EtherType 0x8042 を指定します。
<b>lat</b>	(任意) EtherType DEC-LAT を指定します。
<b>lavc-sca</b>	(任意) EtherType DEC-LAVC-SCA を指定します。
<b>lsap</b> <i>lsap-number mask</i>	(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。  <i>mask</i> 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。
<b>mop-console</b>	(任意) EtherType DEC-MOP Remote Console を指定します。
<b>mop-dump</b>	(任意) EtherType DEC-MOP Dump を指定します。
<b>msdos</b>	(任意) EtherType DEC-MSDOS を指定します。
<b>mumps</b>	(任意) EtherType DEC-MUMPS を指定します。
<b>netbios</b>	(任意) EtherType DEC-Network Basic Input/Output System (NetBIOS) を指定します。
<b>vines-echo</b>	(任意) Banyan Systems による EtherType Virtual Integrated Network Service (VINES) Echo を指定します。
<b>vines-ip</b>	(任意) EtherType VINES IP を指定します。
<b>xns-idp</b>	(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。
<b>cos</b> <i>cos</i>	(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。 <b>cos</b> 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 XE Everest 16.6.1

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 access-list extended** グローバル コンフィギュレーション コマンドを使用して、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 2: 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
novell-ether	Ethernet 802.3	LSAP 0xFFFF

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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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
	<b>mac access-list extended</b>	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。
	<b>permit</b>	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。
	<b>show access-lists</b>	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

### コマンド履歴

リリース

変更内容

Cisco IOS XE Everest 16.6.1

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。

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。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# device-role node
```

## device-role (IPv6 ND インспекション)

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спек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 | switch}

### 構文の説明

<b>host</b>	接続されたデバイスのロールをホストに設定します。
<b>switch</b>	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 インспекション ポリシー 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 XE Everest 16.6.1	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。

**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。

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спек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。

```
デバイス(config)# ipv6 nd inspection policy policy1
```

```
デバイス (config-nd-inspection) # device-role host
```

## device-tracking policy

スイッチ統合型セキュリティ機能 (SISF) ベースの IP デバイス トラッキング ポリシーを設定するには、グローバル コンフィギュレーション モードで **device-tracking** コマンドを使用します。デバイス トラッキング 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。

```
device-tracking policy policy-name
no device-tracking policy policy-name
```

### 構文の説明

*policy-name* デバイス トラッキング 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

デバイス トラッキング 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
	このコマンドが導入されました。

### 使用上のガイドライン

デバイス トラッキング ポリシーを作成するには、SISF ベースの **device-tracking policy** コマンドを使用します。**device-tracking 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 モードがデバイス トラッキング 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。

- (任意) **device-role {node} | switch** : ポートに接続されたデバイスの役割を指定します。デフォルトは **node** です。
- (任意) **limit address-count value** : ターゲットごとに許可されるアドレス数を制限します。
- (任意) **no** : コマンドを無効にするか、またはそのデフォルトに設定します。
- (任意) **destination-glean {recovery| log-only} [dhcp]** : データ トラフィックの送信元アドレス グリーニングによるバインディング テーブルの回復をイネーブルにします。
- (任意) **data-glean {recovery| log-only} [dhcp | ndp]** : 送信元アドレスまたはデータ アドレスのグリーニングを使用したバインディング テーブルの回復をイネーブルにします。
- (任意) **security-level {glean|guard|inspect}** : この機能によって適用されるセキュリティのレベルを指定します。デフォルトは **guard** です。

**glean** : メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。

**guard** : アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバメッセージを拒否します。これがデフォルトのオプションです。

**inspect** : アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。

- (任意) **tracking {disable | enable}** : トラッキング オプションを指定します。
- (任意) **trusted-port** : 信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されません。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。

次に、デバイストラッキング ポリシーを設定する例を示します。

```
デバイス(config)# device-tracking policy policy1
```

```
デバイス(config-device-tracking)# trusted-port
```

## 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	<b>eapol</b> 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	<b>eapol</b> 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
	Cisco IOS XE Everest 16.6.1
	変更内容
	このコマンドが導入されました。

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。

```
デバイス(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、コマンドの **no** 形式を入力します。

```
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ブ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、サブ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 XE Everest 16.6.1	このコマンドが導入されました。
	このコマンドが再度導入されました。このコマンドは および ではサポートされません。

### 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。

次に、インターフェイスがサブ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。

```
デバイス(config)# interface g1/0/3
デバイス(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 XE Everest 16.6.1	このコマンドが導入されました。
	このコマンドが再度導入されました。このコマンドは および ではサポートされません。

### 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 Spanning Tree Protocol (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がブロックされます。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 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。

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。

```
デバイス(config)# dot1x supplicant controlled transient
```

## dot1x supplicant force-multicast

サブリカントスイッチで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に、常にマルチキャスト EAPOL パケットのみを送信するように強制するには、グローバルコンフィギュレーションモードで **dot1x supplicant force-multicast** 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

サブ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 XE Everest 16.6.1	このコマンドが導入されました。
	このコマンドが再度導入されました。このコマンドはおよびではサポートされません。

### 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、サブリカント スイッチ上でこのコマンドをイネーブルにします。

次の例では、サブ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。

```
デバイス(config)# dot1x supplicant force-multicast
```

### 関連コマンド

コマンド	説明
<b>cisp enable</b>	スイッチの Client Information Signalling Protocol (CISP) をイネーブルにすることで、スイッチがサブリカント 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。



コマンド	説明
<b>dot1x credentials</b>	ポートに 802.1x サブリカント資格情報を設定します。
<b>dot1x pae supplicant</b>	インターフェイスがサブ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、スイッチスタックまたはスタンドアロンスイッチ上で特権 EXEC モードで **dot1x test eapol-capable** 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 XE Everest 16.6.1	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。

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。

```
デバイス# 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
	<b>dot1x test timeout</b> <i>timeout</i>	IEEE 802.1X 準備クエリに対する 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

IEEE 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グローバルコンフィギュレーション モードで **dot1x test timeout** コマンドを使用します。

### dot1x test timeout *timeout*

構文の説明	<i>timeout</i>	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 XE Everest 16.6.1	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。

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。

```
デバイス# 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
	<b>dot1x test eapol-capable</b> [ <i>interface interface-id</i> ]	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をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
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

<b>auth-period seconds</b>	<p>サブリカントで保留ステートが維持される秒数（つまり、サブ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。</p> <p>有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。</p>
<b>held-period seconds</b>	<p>サブリカントで保留ステートが維持される秒数（つまり、サブ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。</p> <p>有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。</p>
<b>quiet-period seconds</b>	<p>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。</p> <p>有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。</p>
<b>ratelimit-period seconds</b>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 有効な範囲は 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。</li> </ul>
<b>server-timeout seconds</b>	<p>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。</p> <ul style="list-style-type: none"> <li>• 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。</li> </ul> <p>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。</p>

<b>start-period</b> <i>seconds</i>	<p>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。</p> <p>有効な範囲は1～65535です。デフォルトは30です。</p> <p>Cisco IOS リリース 15.2(5)E では、サブリカントモードでのみこのコマンドを使用できます。その他のモードでこのコマンドを適用すると、設定からそのコマンドが失われます。</p>
<b>supp-timeout</b> <i>seconds</i>	<p>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。</p> <p>有効な範囲は1～65535です。デフォルトは30です。</p>
<b>tx-period</b> <i>seconds</i>	<p>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。</p> <ul style="list-style-type: none"> <li>有効な範囲は1～65535です。デフォルトは30です。</li> <li>802.1Xパケットがサブリカントに送信され、そのサブ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。</li> </ul>

**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 XE Everest 16.6.1	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、ユーザー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 サーバーに転送します。

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。

```

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

```

## dtls

Datagram Transport Layer Security (DTLS) のパラメータを設定するには、RADIUS サーバコンフィギュレーションモードで **dtls** 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。

**dtls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* | **vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}]

**no dtls**

### 構文の説明

<b>connectiontimeout</b> <i>connection-timeout-value</i>	(任意) DTLS 接続タイムアウト値を設定します。
<b>idletimeout</b> <i>idle-timeout-value</i>	(任意) DTLS アイドルタイムアウト値を設定します。
<b>ip</b> { <b>radius source-interface</b> <i>interface-name</i>   <b>vrf forwarding</b> <i>forwarding-table-name</i> }	(任意) IP 送信元パラメータを設定します。
<b>port</b> <i>port-number</i>	(任意) DTLS ポート番号を設定します。
<b>retries</b> <i>number-of-connection-retries</i>	(任意) DTLS 接続再試行の回数を設定します。
<b>trustpoint</b> { <b>client</b> <i>trustpoint name</i>   <b>server</b> <i>trustpoint name</i> }	(任意) クライアントとサーバに DTLS トラストポイントを設定します。

### コマンド デフォルト

- DTLS 接続タイムアウトのデフォルト値は 5 秒です。
- DTLS アイドルタイムアウトのデフォルト値は 60 秒です。
- デフォルトの DTLS ポート番号は 2083 です。

- DTLS 接続再試行回数のデフォルト値は 5 です。

コマンドモード RADIUS サーバ コンフィギュレーション (config-radius-server)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン 認証、許可、およびアカウントिंग (AAA) サーバグループでは、すべてで同じサーバタイプを使用し、Transport Layer Security (TLS) のみか DTLS のみにすることを推奨します。

例 次に、DTLS 接続タイムアウト値を 10 秒に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# radius server R1
Device(config-radius-server)# dtls connectiontimeout 10
Device(config-radius-server)# end
```

関連コマンド

Command	Description
<b>show aaa servers</b>	DTLS サーバに関連する情報を表示します。
<b>clear aaa counters servers radius {server id   all}</b>	RADIUS DTLS 固有の統計情報をクリアします。
<b>debug radius dtls</b>	RADIUS DTLS 固有のデバッグを有効にします。

## 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 XE Everest 16.6.1	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。

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。

```
デバイス(config)# epm access-control open
```

関連コマンド	コマンド	説明
	<b>show running-config</b>	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

## include-icv-indicator

MKPDU に整合性チェック値 (ICV) インジケータを含めるには、MKA ポリシーコンフィギュレーションモードで **include-icv-indicator** コマンドを使用します。ICV インジケータを無効にするには、このコマンドの **no** 形式を使用します。

**include-icv-indicator**  
**no include-icv-indicator**

**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** ICV インジケータが含まれています。

**コマンドモード** MKA ポリシー コンフィギュレーション (config-mka-policy)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

**例** 次に、MKPDU に ICV インジケータを含める例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# include-icv-indicator
```

関連コマンド	Command	Description
	<b>mka policy</b>	MKA ポリシーを設定します。
	<b>confidentiality-offset</b>	機密性オフセットを設定して MACsec を動作させます。
	<b>delay-protection</b>	MKPDU の送信で遅延保護を使用するように MKA を設定します。
	<b>key-server</b>	MKA キーサーバオプションを設定します。
	<b>macsec-cipher-suite</b>	SAK を取得するための暗号スイートを設定します。
	<b>sak-rekey</b>	SAK キー再生成間隔を設定します。
	<b>send-secure-announcements</b>	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。
	<b>ssci-based-on-sci</b>	SCI に基づいて SSCI を計算します。
	<b>use-updated-eth-header</b>	ICV 計算には更新されたイーサネットヘッダーを使用します。

## ip access-list role-based

ロールベース（セキュリティグループ）アクセスコントロールリスト（RBACL）を作成して、ロールベース ACL 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 **ip access-list role-based** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

```
ip access-list role-based access-list-name
no ip access-list role-based access-list-name
```

### 構文の説明

*access-list-name* セキュリティグループアクセスコントロールリスト（SGACL）の名前。

### コマンド デフォルト

ロールベースの ACL 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 (config)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。



**使用上のガイドライン** SGACL ロギングの場合は、**permit ip log** コマンドを設定する必要があります。また、このコマンドは、ダイナミック SGACL のロギングを有効にするために、Cisco Identity Services Engine (ISE) でも設定する必要があります。

次に、IPv4トラフィックに適用できる SGACL を定義し、ロールベース アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
Switch(config)# ip access-list role-based rbacl1
Switch(config-rb-acl)# permit ip log
```

#### 関連コマンド

コマンド	説明
<b>permit ip log</b>	設定されたエントリに一致するロギングを許可します。
<b>show ip access-list</b>	現在のすべての IP アクセスリストの内容を表示します。

## ip admission

Web 認証を有効にするには、インターフェイス コンフィギュレーション モードで **ip admission** コマンドを使用します。このコマンドは、フォールバック プロファイル コンフィギュレーション 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 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 XE Everest 16.6.1	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** コマンドはスイッチポートに web 認証ルールを適用します。

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。

```
デバイス# configure terminal
```

```

デバイス(config)# interface gigabitethernet1/0/1
デバイス(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。

```

デバイス# configure terminal
デバイス(config)# fallback profile profile1
デバイス(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

<i>name</i>	ネットワークアドミッション制御ルールの名前。
<b>consent</b>	認証プロキシ同意 Web ページを <i>admission-name</i> 引数で指定された IP アドミッションルールに対応させます。
<b>proxy http</b>	Web 認証のカスタムページを設定します。
<b>absolute-timer</b> 分	(任意) 外部サーバがタイムアウトするまでの経過時間 (分)。
<b>inactivity-time</b> 分	(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)。
<b>list</b>	(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。
<i>acl</i>	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。
<i>acl-name</i>	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** *polycyname* 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 XE Everest 16.6.1	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、スイッチ上で Web 認証が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。

```

デバイス# configure terminal
デバイス(config) ip admission name http-rule proxy http
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 101 in
デバイス(config-if)# ip admission rule
デバイス(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。

```

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

```

```
デバイス(config-if)# end
```

関連コマンド	コマンド	説明
	<b>dot1x fallback</b>	IEEE802.1x 認証をサポートしてい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にポートを設定します。
	<b>fallback profile</b>	Web 認証のフォールバックプロファイルを作成します。
	<b>ip admission</b>	ポートで Web 認証をイネーブルにします。
	<b>show authentication sessions interface <i>interface</i> detail</b>	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。
	<b>show ip admission</b>	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 dhcp snooping database

Dynamic Host Configuration Protocol (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		
	<b>flash:<i>url</i></b>	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。
	<b>ftp:<i>url</i></b>	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。
	<b>http:<i>url</i></b>	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。

<b>https:url</b>	セキュアHTTP (HTTPS) を使用して、エント리를格納するためのデータベースのURLを指定します。
<b>rtp:url</b>	リモートコピー (RCP) を使用して、エント리를格納するためのデータベースのURLを指定します。
<b>scp:url</b>	セキュアコピー (SCP) を使用して、エント리를格納するためのデータベースのURLを指定します。
<b>tftp:url</b>	TFTPを使用して、エント리를格納するためのデータベースのURLを指定します。
<b>timeout seconds</b>	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。
<b>write-delay seconds</b>	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리를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 XE Everest 16.6.1	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。

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。

```
デバイス(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。

```
デバイス(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、スイッチのグローバル コンフィギュレーション モードで **ip dhcp snooping information option format remote-id** 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 XE Everest 16.6.1	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。

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。

```
デバイス(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 XE Everest 16.6.1	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。

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。

```
デバイス(config)# no ip dhcp snooping verify no-relay-agent-address
```

## ip http access-class

HTTP サーバへのアクセスを制限するために使用するアクセスリストを指定するには、グローバルコンフィギュレーションモードで **ip http access-class** コマンドを使用します。以前に設定したアクセスリストの関連付けを削除するには、このコマンドの **no** 形式を使用します。



- (注) 既存の **ip http access-class** *access-list-number* コマンドは、現在サポートされていますが、廃止される予定です。代わりに、**ip http access-class ipv4** {*access-list-number* | *access-list-name*} および **ip http access-class ipv6** *access-list-name* を使用してください。

```
ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name }
| ipv6 access-list-name }
no ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name
} | ipv6 access-list-name }
```

構文の説明		
	<b>ipv4</b>	セキュア HTTP サーバーへのアクセスを制限するように IPv4 アクセスリストを指定します。
	<b>ipv6</b>	セキュア HTTP サーバーへのアクセスを制限するように IPv6 アクセスリストを指定します。
	<i>access-list-number</i>	グローバル コンフィギュレーション コマンド <b>access-list</b> を使用して設定される、0～99 の標準 IP アクセスリスト番号。
	<i>access-list-name</i>	<b>ip access-list</b> コマンドで設定された標準 IPv4 アクセスリストの名前。

コマンド デフォルト      アクセス リストは、HTTP サーバには適用されません。

コマンド モード          グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが変更されました。 <b>ipv4</b> および <b>ipv6</b> キーワードが追加されました。
	Cisco IOS XE Release 3.3SE	このコマンドが導入されました。

使用上のガイドライン      このコマンドが設定されていると、指定されたアクセスリストは HTTP サーバに割り当てられます。HTTP サーバは、接続を受け入れる前にアクセスリストを確認します。確認に失敗すると、HTTP サーバは接続要求を承認しません。

#### 例

次に、アクセス リストを 20 に定義して、HTTP サーバに割り当てる例を示します。

```
Device(config)# ip access-list standard 20
Device(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Device(config-std-nacl)# permit 209.165.201.1 0.0.255.255
Device(config-std-nacl)# permit 209.165.200.225 0.255.255.255
Device(config-std-nacl)# exit
```



```
Device(config)# ip http access-class 20
```

次に、IPv4 の指定済みアクセス リストを定義して、HTTP サーバに割り当てる例を示します。

```
Device(config)# ip access-list standard Internet_filter
```

```
Device(config-std-nacl)# permit 1.2.3.4
```

```
Device(config-std-nacl)# exit
```

```
Device(config)# ip http access-class ipv4 Internet_filter
```

#### 関連コマンド

コマンド	説明
<b>ip access-list</b>	IDをアクセスリストに割り当て、アクセスリストのコンフィギュレーションモードを開始します。
<b>ip http server</b>	HTTP 1.1 サーバ (Cisco Web ブラウザ ユーザ インターフェイスを含む) をイネーブルにします。

## ip radius source-interface

すべての発信 RADIUS パケットに対して指定されたインターフェイスの IP アドレスを使用するように RADIUS 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 radius source-interface** コマンドを使用します。すべての発信 RADIUS パケットに対して指定されたインターフェイスの IP アドレスを使用しないように RADIUS を設定するには、このコマンドの **no** 形式を使用します。

**ip radius source-interface** *interface-name* [**vrf** *vrf-name* ]  
**no ip radius source-interface**

#### 構文の説明

<i>interface-name</i>	RADIUS がすべての発信パケットに使用するインターフェイスの名前です。
<b>vrf</b> <i>vrf-name</i>	(任意) Virtual Route Forwarding (VRF) 単位の設定です。

#### コマンド デフォルト

デフォルトの動作や値はありません。

#### コマンド モード

グローバル コンフィギュレーション (config)

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	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、すべての発信 RADIUS パケットの送信元アドレスとして使用するインターフェイスの IP アドレスを設定する場合に使用します。インターフェイスがアップ状態である限り、この IP アドレスが使用されます。RADIUS サーバでは、IP アドレスのリストを保持する代わりに、すべてのネットワーク アクセス クライアントに対して 1 つの IP アドレスエントリを使用できます。インターフェイスがアップ状態であるかダウン状態であるかに関係なく、関連付けられているインターフェイスの IP アドレスが使用されます。

特に、ルータに多数のインターフェイスがあり、特定のルータからのすべての RADIUS パケットに同一の IP アドレスが含まれるようにする場合は、**ip radius source-interface** コマンドが役立ちます。

指定されたインターフェイスに有効な IP アドレスがあり、アップ状態でないと、設定は有効になりません。指定されたインターフェイスに有効な IP アドレスがない場合やダウン状態である場合、RADIUS によって AAA サーバへの最適なルートに対応するローカル IP が選択されます。これを回避するには、インターフェイスに有効な IP アドレスを追加するか、そのインターフェイスをアップ状態にします。

このコマンドを VRF 単位で設定するには、**vrf vrf-name** キーワードと引数を使用します。これにより、ユーザのルートに別のユーザのルートとの相互関係がない複数のルーティングテーブルまたは転送テーブルを使用できます。

## 例

次に、すべての発信 RADIUS パケットに対してインターフェイス s2 の IP アドレスを使用するように RADIUS を設定する例を示します。

```
ip radius source-interface s2
```

次に、VRF の定義に対してインターフェイス Ethernet0 の IP アドレスを使用するように RADIUS を設定する例を示します。

```
ip radius source-interface Ethernet0 vrf vrf1
```

# 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

<i>mac-address</i>	バインディング対象 MAC アドレスです。
<b>vlan</b> <i>vlan-id</i>	レイヤ 2 VLAN ID を指定します。有効な値は 1~4094 です。

<i>ip-address</i>	バインディング対象 IP アドレスです。
<b>interface</b> <i>interface-id</i>	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 XE Everest 16.6.1	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せん。

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。

```

デバイス# configure terminal
デバイスconfig) 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 ガードを有効にするには、インターフェイス コンフィギュレーション モードで **ip verify source** コマンドを使用します。IP ソース ガードを無効にするには、このコマンドの **no** 形式を使用します。

**ip verify source** [**mac-check**][**tracking**]  
**no ip verify source**

<b>mac-check</b>	(任意) MAC アドレス検証による IP ソース ガードをイネーブルにします。
------------------	--

<b>tracking</b>	(任意) ポートで静的IPアドレスを学習するためにIPポートセキュリティ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 XE Everest 16.6.1	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 アドレス フィルタリングおよび MAC アドレス 検証による IP ソース ガードをイネーブルにするには、**ip verify source mac-check** 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。

## 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。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip verify source
```

次の例では、MAC アドレスの検証による IP ソース ガードをイネーブルにする方法を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip verify source mac-check
```

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 access-list

IPv6 アクセスリストを定義してデバイスを IPv6 アクセスリスト コンフィギュレーション モードに設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

```
ipv6 access-list access-list-name | match-local-traffic | log-update threshold threshold-in-msgs
| role-based list-name
noipv6 access-list access-list-name | client permit-control-packets | log-update threshold |
role-based list-name
```

構文の説明	<b>ipv6 access-list-name</b>	名前付き IPv6 ACL (最長 64 文字) を作成し、IPv6 ACL コンフィギュレーション モードを開始します。  <i>access-list-name</i> : IPv6 アクセス リストの名前。名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。
	<b>match-local-traffic</b>	ローカルで生成されたトラフィックに対する照合を有効にします。
	<b>log-update threshold threshold-in-msgs</b>	最初のパケットの一致後に、syslog メッセージを生成する方法を決定します。  <i>threshold-in-msgs</i> : 生成されるパケット数。
	<b>role-based list-name</b>	ロールベースの IPv6 ACL を作成します。

コマンドデフォルト IPv6 アクセス リストは定義されていません。

コマンドモード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
		このコマンドが再度導入されました。このコマンドは および ではサポートされません。

使用上のガイドライン IPv6 ACL は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用することで定義され、その許可と拒否の条件は IPv6 アクセス リスト コンフィギュレーション モードで **deny** コマンドおよび **permit** コマンドを使用することで設定されます。 **ipv6 access-list** コマンドを設定すると、デバイスは IPv6 アクセス リスト コンフィギュレーション モードになり、デバイス プロンプトは **Device(config-ipv6-acl)#** に変わります。 IPv6 アクセス リスト コンフィギュレーション モードから、定義済みの IPv6 ACL に許可および拒否の条件を設定できます。



(注) IPv6 ACL は一意な名前によって定義されます (IPv6 は番号付けされた ACL をサポートしません)。 IPv4 ACL と IPv6 ACL は同じ名前を共有できません。

IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permit any any** ステートメントおよび **deny any any** ステートメントでプロトコルタイプとして自動的に設定されます。

IPv6 ACL にはそれぞれ、最後に一致した条件として、暗黙の **permit icmp any any nd-na** ステートメント、 **permit icmp any any nd-ns** ステートメント、および **deny ipv6 any any** ステートメントがあります (前の 2 つの一致条件は、ICMPv6 ネイバー探索を許可します)。 1 つの IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれている必要があります。 IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク

層サービスを利用するため、デフォルトで、インターフェイス上でのIPv6ネイバー探索パケットの送受信がIPv6 ACLによって暗黙的に許可されます。IPv4の場合、IPv6ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータリンク層プロトコルを利用するため、デフォルトで、インターフェイス上でのARPパケットの送受信がIPv4 ACLによって暗黙的に許可されます。

IPv6 ACLをIPv6インターフェイスに適用するには、`access-list-name` 引数を指定して **ipv6 traffic-filter** 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。IPv6 ACLをデバイスとの着信および発信IPv6仮想端末接続に適用するには、`access-list-name` 引数を指定して、**ipv6 access-class** ラインコンフィギュレーションコマンドを使用します。

**ipv6 traffic-filter** コマンドでインターフェイスに適用されるIPv6 ACLは、デバイスによって発信されたトラフィックではなく、転送されたトラフィックをフィルタ処理します。

## 例

次に、`list1` という名前のIPv6 ACLを設定し、デバイスをIPv6アクセスリストコンフィギュレーションモードにする例を示します。

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

次に、`list2` という名前のIPv6 ACLを設定し、そのACLをイーサネットインターフェイス0上の発信トラフィックに適用する例を示します。特に、最初のACLエントリは、ネットワーク `FEC0:0:0:2::/64`（送信元IPv6アドレスの最初の64ビットとしてサイトローカルプレフィックス `FEC0:0:0:2` を持つパケット）がイーサネットインターフェイス0から出て行くことを拒否します。2番目のACLエントリは、その他のすべてのトラフィックがイーサネットインターフェイス0から出て行くことを許可します。2番目のエントリは、各IPv6 ACLの末尾に暗黙的な `deny all` 条件があるため、必要となります。

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

## ipv6 snooping policy



- (注) すべての既存のIPv6スヌーピングコマンド（より前）には、対応するSISFベースのデバイストラッキングコマンドが用意され、IPv4とIPv6の両方のアドレスファミリに設定を適用できるようになりました。詳細については、「**device-tracking** ポリシー」コマンドを参照してください。

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	<i>snooping-policy</i> 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 XE Everest 16.6.1	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 Dynamic Host Configuration Protocol (DHCP) または Neighbor Discovery Protocol (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、ポートを信頼できるポートとして設定します。つまり、メッセージを受信したときに検証が限定的に実行されるか、まったく実行されません。

次に、IPv6 スヌーピング ポリシーを設定する例を示します。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)#
```

## key chain macsec

事前共有キー（PSK）を取得するためにデバイスインターフェイスの MACsec キーチェーンの名前を設定するには、グローバル コンフィギュレーション モードで **key chain macsec** コマンドを使用します。CDP 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。

**key chain** *namemacsec* {**description** | **key** | **exit**}

### 構文の説明

<b>name</b>	キーを取得するために使用するキー チェーンの名前。
<b>description</b>	MACsec キー チェーンの説明を入力します。
<b>key</b>	MACsec キーを設定します。
<b>exit</b>	MACsec キーチェーン コンフィギュレーション モードを終了します。
<b>no</b>	コマンドを無効にするか、またはデフォルト値を設定します。

### コマンド デフォルト

key chain macsec は無効になっています。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、128 ビットの事前共有キー（PSK）を取得するために MACsec キー チェーンを設定する例を示します。

```
Switch#configure terminal
Switch(config)#key chain kcl macsec
Switch(config-keychain-macsec)#key 1000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-128-cmac
Switch(config-keychain-macsec-key)# key-string fb63e0269e2768c49bab8ee9a5c2258f
Switch(config-keychain-macsec-key)#end
Switch#
```

次に、256 ビットの事前共有キー（PSK）を取得するために MACsec キー チェーンを設定する例を示します。

```
Switch#configure terminal
Switch(config)#key chain kcl macsec
Switch(config-keychain-macsec)#key 2000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-256-cmac
Switch(config-keychain-macsec-key)# key-string
c865632acb269022447c417504a1bf5db1c296449b52627ba01f2ba2574c2878
```



```
Switch(config-keychain-macsec-key) #end
Switch#
```

## key-server

MKA キーサーバオプションを設定するには、MKA ポリシー コンフィギュレーション モードで **key-server** コマンドを使用します。MKA キーサーバオプションを無効にするには、コマンドの **no** 形式を使用します。

**key-server priority value**  
**no key-server priority**

### 構文の説明

**priority value** MKA キーサーバのプライオリティ値を指定します。

### コマンドデフォルト

MKA キーサーバは無効になっています。

### コマンドモード

MKA ポリシー コンフィギュレーション (config-mka-policy)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

### 例

次に、MKA キーサーバを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# key-server priority 33
```

### 関連コマンド

Command	Description
<b>mka policy</b>	MKA ポリシーを設定します。
<b>confidentiality-offset</b>	機密性オフセットを設定して MACsec を動作させます。
<b>delay-protection</b>	MKPDU の送信で遅延保護を使用するように MKA を設定します。
<b>include-icv-indicator</b>	MKPDU に ICV インジケータを含めます。
<b>macsec-cipher-suite</b>	SAK を取得するための暗号スイートを設定します。
<b>sak-rekey</b>	SAK キー再生成間隔を設定します。
<b>send-secure-announcements</b>	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。

Command	Description
<b>ssci-based-on-sci</b>	SCIに基づいてSSCIを計算します。
<b>use-updated-eth-header</b>	ICV計算には更新されたイーサネットヘッダーを使用します。

## 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、Neighbor Discovery Protocol (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 インスペクション ポリシーの設定  
 IPv6 スヌーピング 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 XE Everest 16.6.1	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。

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。

```
デバイス(config)# ipv6 nd inspection policy policy1
デバイス(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。

```

デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# limit address-count 25

```

## mab request format attribute 32

スイッチ上でVLANIDベースのMAC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 **mab request format attribute 32 vlan access-vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```

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 XE Everest 16.6.1	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。

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。

```

デバイス(config)# mab request format attribute 32 vlan access-vlan

```

### 関連コマンド

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

コマンド	説明
<b>authentication host-mode</b>	ポートで認証マネージャモードを設定します。
<b>authentication open</b>	ポートでオープンアクセスをイネーブまたはディセーブにします。
<b>authentication order</b>	ポートで使用する認証方式の順序を設定します。
<b>authentication periodic</b>	ポートで再認証をイネーブまたはディセーブにします。
<b>authentication port-control</b>	ポートの認証ステータスの手動制御をイネーブにします。
<b>authentication priority</b>	ポートプライオリティリストに認証方式を追加します。
<b>authentication timer</b>	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。
<b>authentication violation</b>	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。
<b>mab</b>	ポートの MAC-based 認証をイネーブにします。
<b>mab eap</b>	Extensible Authentication Protocol (EAP) を使用するようポートを設定します。
<b>show authentication</b>	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。

## macsec-cipher-suite

Security Association Key (SAK) を取得するための暗号スイートを設定するには、MKA ポリシー コンフィギュレーション モードで **macsec-cipher-suite** コマンドを使用します。SAK の暗号スイートを無効にするには、このコマンドの **no** 形式を使用します。

```
macsec-cipher-suite {gcm-aes-128 | gcm-aes-256 }
no macsec-cipher-suite {gcm-aes-128 | gcm-aes-256 }
```

### 構文の説明

**gcm-aes-128** 128 ビット暗号により SAK を取得するための暗号スイートを設定します。

**gcm-aes-256** 256ビット暗号によりSAKを取得するための暗号スイートを設定します。

コマンド デフォルト GCM-AES-128 暗号化は有効になっています。

コマンド モード MKA ポリシー コンフィギュレーション (config-mka-policy)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン デバイスがGCM-AES-128およびGCM-AES-256の両方の暗号方式をサポートしている場合は、ユーザ定義のMKAポリシーを定義して使用し、要件に基づいて、両方の暗号を含めるか、または256ビットのみの暗号を含めることを強くお勧めします。

### 例

次に、256ビット暗号化でSAKを取得するためのMACsec暗号スイートを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-256
```

### 関連コマンド

Command	Description
<b>mka policy</b>	MKA ポリシーを設定します。
<b>confidentiality-offset</b>	機密性オフセットを設定してMACsecを動作させます。
<b>delay-protection</b>	MKPDUの送信で遅延保護を使用するようにMKAを設定します。
<b>include-icv-indicator</b>	MKPDUにICVインジケータを含めます。
<b>key-server</b>	MKAキーサーバオプションを設定します。
<b>sak-rekey</b>	SAKキー再生成間隔を設定します。
<b>send-secure-announcements</b>	MKPDUの送信でセキュアなアナウンスを送信するようにMKAを設定します。
<b>ssci-based-on-sci</b>	SCIに基づいてSSCIを計算します。
<b>use-updated-eth-header</b>	ICV計算には更新されたイーサネットヘッダーを使用します。

## macsec network-link

アップリンク インターフェイスの MKA MACsec 設定を有効にするには、インターフェイスで **macsec network-link** コマンドを使用します。CDP 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。

### macsec network-link

構文の説明	<b>macsec network-link</b> EAP-TLS 認証プロトコルを使用してデバイス インターフェイスの MKA MACsec 設定を有効にします。	
コマンド デフォルト	macsec network-link は無効になっています。	
コマンド モード	インターフェイス コンフィギュレーション	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、EAP-TLS 認証プロトコルを使用して、インターフェイスに MACsec MKA を設定する例を示します。

```
Switch#configure terminal
Switch(config)# int G1/0/20
Switch(config-if)# macsec network-link
Switch(config-if)# end
Switch#
```

## 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を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 スイッチのアクセスマップ 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。一致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 {namenum} [{namenum}] [{namenum}]... | ipv6 address
{namenum} [{namenum}] [{namenum}]... | mac address {name} [{name}]
[{name}]...}
no match {ip address {namenum} [{namenum}] [{namenum}]... | ipv6 address
{namenum} [{namenum}] [{namenum}]... | mac address {name} [{name}]
[{name}]...}
```

構文の説明	<b>ip address</b> 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。
	<b>ipv6 address</b> パケットを IPv6 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。
	<b>mac address</b> 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。
	<b>name</b> パケットを照合するアクセス リストの名前です。
	<b>number</b> 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 XE Everest 16.6.1	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、IPv6 パケットは IPv6 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、IPv6 アドレスおよび MAC アドレスを指定できます。

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 `a12` 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。

```

デバイス (config) # vlan access-map vmap4
デバイス (config-access-map) # match ip address a12
デバイス (config-access-map) # action drop
デバイス (config-access-map) # exit

```

```
デバイス(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。

## mka pre-shared-key

事前共有キー（PSK）を使用してデバイスインターフェースのMKA MACsec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 **mka pre-shared-key key-chain key-chain name** コマンドを使用します。CDP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。

```
mka pre-shared-key key-chain key-chain-name
```

### 構文の説明

**mka pre-shared-key key-chain** PSK を使用してデバイス インターフェースの MACsec MKA 設定を有効にします。

### コマンド デフォルト

mka pre-shared-key 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 XE Denali 16.3.1

このコマンドが導入されました。

次に、PSK を使用して、インターフェースのMKA MACsecを設定する例を示します。

```
Switch#
Switch(config)# int G1/0/20
Switch(config-if)# mka pre-shared-key key-chain kcl
Switch(config-if)# end
Switch#
```

## mka suppress syslogs sak-rekey

ロギングにおいてMACsec Key Agreement (MKA) セキュアアソシエーションキー (SAK) のキー再生成メッセージを抑制するには、グローバル コンフィギュレーション モードで **mka suppress syslogs sak-rekey** コマンドを使用します。MKA SAK キー再生成メッセージのロギングを無効にするには、このコマンドの**no**形式を使用します。

```
mka suppress syslogs sak-rekey
no mka suppress syslogs sak-rekey
```

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 MKA SAK syslog メッセージがコンソールに表示されます。

**コマンドモード** グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.9.1	このコマンドが導入されました。

**使用上のガイドライン** MKA SAK syslog はすべてのキー再生成間隔で継続的に生成されるため、複数のインターフェイスで MKA が設定されている場合は生成される syslog の量が非常に多くなります。MKA SAK syslog を抑制するには、このコマンドを使用します。

### 例

次に、MKA SAK syslog ロギングを抑制する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka suppress syslogs sak-rekey
```

## 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 **authentication logging verbose** コマンドをグローバルコンフィギュレーションモードで使用します。

**authentication logging verbose**  
**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** システムメッセージの詳細ログは有効になっていません。

**コマンドモード** グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	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。

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。

```
デバイス(config)# 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
	<b>authentication logging verbose</b>	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。
	<b>dot1x logging verbose</b>	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。
	<b>mab logging verbose</b>	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。

## 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 **dot1x logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

```
dot1x logging verbose
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

システムメッセージの詳細ログは有効になっていません。

### コマンド モード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	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。

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。

```
デバイス(config)# 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
	<b>authentication logging verbose</b>	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。
	<b>dot1x logging verbose</b>	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。
	<b>mab logging verbose</b>	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。

## 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 **mab logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

**mab logging verbose**  
**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

システムメッセージの詳細ログは有効になっていません。

### コマンド モード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	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。

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。

```
デバイス(config)# 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
<b>authentication logging verbose</b>	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。

コマンド	説明
<b>dot1x logging verbose</b>	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。
<b>mab logging verbose</b>	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 トラフィックの転送を許可するには、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 | hostsrc-MAC-addr | src-MAC-addr mask} {any | hostdst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lvc-sca | lsaplsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]
```

```
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 | lvc-sca | lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]
```

### 構文の説明

<b>any</b>	すべての送信元または宛先 MAC アドレスを拒否します。
<b>host</b> <i>src-MAC-addr</i>   <i>src-MAC-addr mask</i>	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。
<b>host</b> <i>dst-MAC-addr</i>   <i>dst-MAC-addr mask</i>	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。

<i>type mask</i>	<p>(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。</p> <ul style="list-style-type: none"> <li>• <i>type</i> には、0 ~ 65535 の 16 進数を指定できます。</li> <li>• <i>mask</i> 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。</li> </ul>
<b>aarp</b>	(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。
<b>amber</b>	(任意) EtherType DEC-Amber を指定します。
<b>appletalk</b>	(任意) EtherType AppleTalk/EtherTalk を指定します。
<b>dec-spanning</b>	(任意) EtherType Digital Equipment Corporation (DEC) スパニングツリーを指定します。
<b>decnet-iv</b>	(任意) EtherType DECnet Phase IV プロトコルを指定します。
<b>diagnostic</b>	(任意) EtherType DEC-Diagnostic を指定します。
<b>dsm</b>	(任意) EtherType DEC-DSM を指定します。
<b>etype-6000</b>	(任意) EtherType 0x6000 を指定します。
<b>etype-8042</b>	(任意) EtherType 0x8042 を指定します。
<b>lat</b>	(任意) EtherType DEC-LAT を指定します。
<b>lave-sca</b>	(任意) EtherType DEC-LAVC-SCA を指定します。
<b>lsap</b> <i>lsap-number mask</i>	<p>(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。</p> <p><i>mask</i> 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。</p>
<b>mop-console</b>	(任意) EtherType DEC-MOP Remote Console を指定します。

<b>mop-dump</b>	(任意) EtherType DEC-MOP Dump を指定します。
<b>msdos</b>	(任意) EtherType DEC-MSDOS を指定します。
<b>mumps</b>	(任意) EtherType DEC-MUMPS を指定します。
<b>netbios</b>	(任意) EtherType DEC-Network Basic Input/Output System (NetBIOS) を指定します。
<b>vines-echo</b>	(任意) Banyan Systems による EtherType Virtual Integrated Network Service (VINES) Echo を指定します。
<b>vines-ip</b>	(任意) EtherType VINES IP を指定します。
<b>xns-idp</b>	(任意) EtherType Xerox Network Systems (XNS) プロトコルスイートを指定します。
<b>cos cos</b>	(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。 <b>cos</b> 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 XE Everest 16.6.1	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 access-list extended** グローバル コンフィギュレーション コマンドを使用して、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、次の表に一覧表示します。

表 3: 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

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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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
<b>deny</b>	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。

コマンド	説明
<b>mac access-list extended</b>	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。
<b>show access-lists</b>	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。

## propagate sgt (cts manual)

Cisco TrustSec Security (CTS) インターフェイスでレイヤ2のセキュリティグループタグ (SGT) 伝達を有効にするには、インターフェイス コンフィギュレーション モードで **propagate sgt** コマンドを使用します。SGT 伝達を無効にするには、このコマンドの **no** 形式を使用します。

### propagate sgt

#### 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

SGT 処理の伝達が有効になっています。

#### コマンド モード

CTS 手動インターフェイス コンフィギュレーション モード (config-if-cts-manual)

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

#### 使用上のガイドライン

SGT 処理の伝達によって、CTS 対応のインターフェイスは L2 SGT タグに基づいて CTS メタデータ (CMD) を受信および送信できます。ピアデバイスが SGT を受信できず、その結果、SGT タグを L2 ヘッダーに配置できない状況で、インターフェイスの SGT 伝達を無効にするには **no propagate sgt** コマンドを使用します。

#### 例

次に、手動で設定された TrustSec 対応のインターフェイスで SGT 伝達を無効にする例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# no propagate sgt
```

次に、ギガビットイーサネット インターフェイス 0 で SGT 伝達が無効になっている例を示します。

```
Switch#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
  CTS is enabled, mode:      MANUAL
  IFC state:                 OPEN
```



```

Authentication Status:  NOT APPLICABLE
Peer identity:          "unknown"
Peer's advertised capabilities: ""
Authorization Status:   NOT APPLICABLE
SAP Status:             NOT APPLICABLE
Propagate SGT:          Disabled
Cache Info:
Cache applied to link : NONE

```

関連コマンド	コマンド	説明
	<b>cts manual</b>	CTS のインターフェイスを有効にします。
	<b>show cts interface</b>	インターフェイスごとの Cisco TrustSec ステートおよび統計情報を表示します。

## protocol (IPv6 スヌーピング)

アドレスを Dynamic Host Configuration Protocol (DHCP) または Neighbor Discovery Protocol (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対応させるには、**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	dhc	ndp
	<b>dhc</b> 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。	<b>ndp</b> 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

コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	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 によるのみリカバリできます。

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。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# protocol dhcp
```

## radius server



- (注) Cisco IOS 15.2(5)E リリース以降では、Cisco IOS リリース 15.2(5)E より前のリリースで使用されていた **radius-server host** コマンドが **radius server** コマンドに置き換えられました。古いコマンドは廃止されました。

RADIUS アカウンティングと RADIUS 認証を含む RADIUS サーバーのパラメータを設定するには、スイッチスタックまたはスタンドアロンスイッチで **radius server** コンフィギュレーションサブモードコマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
radius server name
address {ipv4 | ipv6} ip{address / hostname} auth-port udp-port acct-port udp-port
key string
automate tester name | retransmit value | timeout seconds
no radius server name
```

### 構文の説明

<b>address {ipv4   ipv6}</b> <i>ip{address / hostname}</i>	RADIUS サーバの IP アドレスを指定します。
<b>auth-port</b> <i>udp-port</i>	(任意) RADIUS 認証サーバの UDP ポートを指定します。指定できる範囲は 0 ~ 65536 です。
<b>acct-port</b> <i>udp-port</i>	(任意) RADIUS アカウンティングサーバの UDP ポートを指定します。指定できる範囲は 0 ~ 65536 です。

<b>key string</b>	(任意) スイッチおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。  (注) キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。必ずこのコマンドの最終項目として <b>key</b> を設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 <b>key</b> にスペースが含まれる場合は、引用符が <b>key</b> の一部でない限り、 <b>key</b> を引用符で囲まないでください。
<b>automate tester name</b>	(任意) RADIUS サーバ ステータスの自動サーバ テストをイネーブルにし、使用されるユーザ名を指定します。
<b>retransmit value</b>	(任意) サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ~ 100 です。この設定は、 <b>radius-server retransmit</b> グローバル コンフィギュレーション コマンドによる設定を上書きします。
<b>timeout seconds</b>	(任意) スイッチが要求を再送信する前に RADIUS サーバからの応答を待機する時間間隔を指定します。指定できる範囲は 1 ~ 1000 です。この設定は、 <b>radius-server timeout</b> グローバル コンフィギュレーション コマンドによる設定を上書きします。
<b>no radius server name</b>	デフォルト設定に戻します。

#### コマンド デフォルト

- RADIUS アカウンティング サーバの UDP ポートは 1646 です。
- RADIUS 認証サーバの UDP ポートは 1645 です。
- 自動サーバ テストはディセーブルです。
- タイムアウトは 60 分 (1 時間) です。
- 自動テストがイネーブルの場合、UDP ポートのアカウンティングおよび認証時にテストが実行されます。
- 認証キーおよび暗号キー (string) は設定されていません。

#### コマンド モード

RADIUS サーバ サブモード 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 XE Everest 16.6.1	<b>radius-server host</b> コマンドを置き換える目的でこのコマンドが追加されました。

#### 使用上のガイドライン

- RADIUS アカウンティング サーバおよび RADIUS 認証サーバの UDP ポートをデフォルト以外の値に設定することを推奨します。

- **key string** サブモード コンフィギュレーション コマンドを使用すると、認証および暗号キーを設定できます。必ずこのコマンドの最終項目として **key** を設定してください。
- RADIUS サーバステータスの自動サーバテストをイネーブルにし、使用されるユーザ名を指定するには、**automate-tester name** キーワードを使用します。

次の例では、認証サーバの UDP ポートを 1645、アカウントサーバの UDP ポートを 1646 に設定し、文字列を設定する例を示します。

```
デバイス(config)# radius server ISE
デバイス(config-radius-server)# address ipv4 10.1.1 auth-port 1645 acct-port 1646
デバイス(config-radius-server)# key cisco123
```

## sak-rekey

定義された MKA ポリシーのセキュリティ アソシエーション キー (SAK) のキー再生成間隔を設定するには、MKA ポリシー コンフィギュレーション モードで **sak-rekey** コマンドを使用します。SAK キー再生成タイマーを無効にするには、このコマンドの **no** 形式を使用します。

```
sak-rekey {interval time-interval | on-live-peer-loss}
no sak-rekey {interval | on-live-peer-loss}
```

### 構文の説明

<b>interval</b> <i>time-interval</i>	SAK キー再生成間隔を秒単位で設定します。 範囲は 30 ~ 65535 で、デフォルトは 0 です。
<b>on-live-peer-loss</b>	ライブメンバーシップからのピア損失。

### コマンド デフォルト

SAK キー再生成タイマーは無効になっています。デフォルトは 0 です。

### コマンド モード

MKA ポリシー コンフィギュレーション (config-mka-policy)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.8.1a	このコマンドが導入されました。

### 例

次に、SAK キー再生成間隔を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# sak-rekey interval 300
```

## 関連コマンド

Command	Description
<b>mka policy</b>	MKA ポリシーを設定します。
<b>confidentiality-offset</b>	機密性オフセットを設定して MACsec を動作させます。
<b>delay-protection</b>	MKPDU の送信で遅延保護を使用するように MKA を設定します。
<b>include-icv-indicator</b>	MKPDU に ICV インジケータを含めます。
<b>key-server</b>	MKA キーサーバオプションを設定します。
<b>macsec-cipher-suite</b>	SAK を取得するための暗号スイートを設定します。
<b>send-secure-announcements</b>	MKPDU の送信でセキュアなアナウンスを送信するように MKA を設定します。
<b>ssci-based-on-sci</b>	SCI に基づいて SSCI を計算します。
<b>use-updated-eth-header</b>	ICV 計算には更新されたイーサネットヘッダーを使用します。

## sap mode-list (cts manual)

2 個のインターフェイスの間のリンク暗号化をネゴシエートするために使用される Security Association Protocol (SAP) の認証と暗号化モード（最高から最低に優先順位付けされた）を選択するには、Cisco TrustSec dot1x インターフェイス コンフィギュレーション モードで **sap mode-list** コマンドを使用します。モードリストを削除してデフォルトに戻すには、このコマンドの **no** 形式を使用します。

2 個のインターフェイス間で MACsec のリンク暗号化をネゴシエートするために、PMK と Security Association Protocol (SAP) の認証および暗号化モードを手動で指定するには、**sap mode-list** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

```
sap pmk mode-list {gcm-encrypt | gmac | no-encap | null} [gcm-encrypt | gmac | no-encap | null]
no sap pmk mode-list {gcm-encrypt | gmac | no-encap | null} [gcm-encrypt | gmac | no-encap | null]
```

## 構文の説明

<b>pmk</b> <i>hex_value</i>	16 進数データ PMK を指定します（先行する 0x なし。偶数の 16 進数文字を入力する。そうでない場合は、最後の文字に 0 のプレフィックスが付加される）。
-----------------------------	--

<b>mode-list</b>	アダプタイズされたモードのリストを指定します（最高から最低に優先順位付け）。
<b>gcm-encrypt</b>	GMAC 認証、GCM 暗号化を指定します。
<b>gmac</b>	GMAC 認証だけを指定し、暗号化を指定しません。
<b>no-encap</b>	カプセル化を指定しません。
<b>null</b>	カプセル化あり、認証なし、暗号化なしを指定します。

**コマンド デフォルト** デフォルトのカプセル化は **sap pmk mode-list gcm-encrypt null** です。ピア インターフェイスが 802.1AE MACsec または 802.REV レイヤ 2 リンク暗号化をサポートしない場合、デフォルトの暗号化は **null** です。

**コマンド モード** CTS 手動インターフェイス コンフィギュレーション (config-if-cts-manual)

**コマンド履歴**

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

**使用上のガイドライン** 認証と暗号化方式を指定するには、**sap pmk mode-list** コマンドを使用します。

セキュリティアソシエーションプロトコル (SAP) は 802.11i IEEE プロトコルのドラフトバージョンに基づいた暗号キーの取得および交換プロトコルです。SAP は MACsec をサポートするインターフェイス間の 802.1AE リンク間暗号化 (MACsec) を確立および管理するために使用します。

SAP および PMK は、**sap pmk mode-list** コマンドを使用して、2 個のインターフェイス間に手動で設定することもできます。802.1X 認証を使用する場合、両方 (サブリカントおよびオーセンティケーター) が Cisco Secure Access Control Server からピアのポートの PMK および MAC アドレスを受信します。

デバイスが Cisco TrustSec 対応ソフトウェアを実行していて、ハードウェアが Cisco TrustSec 非対応である場合は、**sap mode-list no-encap** コマンドを使用してカプセル化を拒否します。

例

次に、ギガビット イーサネット インターフェイスで SAP を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk FFEFE mode-list gcm-encrypt
```

関連コマンド	コマンド	説明
	<b>cts manual</b>	Cisco TrustSec のインターフェイスを有効にします。
	<b>propagate sgt (cts manual)</b>	Cisco TrustSec Security インターフェイスのレイヤ 2 での SGT の伝達を有効にします。
	<b>show cts interface</b>	Cisco TrustSec インターフェイス設定の統計情報を表示します。

## 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		
	<b>glean</b>	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。
	<b>guard</b>	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 サーバー メッセージは拒否されます。
	<b>inspect</b>	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

コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

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。

```
デバイス (config) # ipv6 snooping policy policy1
デバイス (config-ipv6-snooping) # security-level inspect
```

# send-secure-announcements

MKA が MACsec Key Agreement Protocol Data Unit (MKPDU) でセキュアな通知を送信できるようにするには、MKA ポリシー コンフィギュレーションモードで **send-secure-announcements** コマンドを使用します。このセキュアな通知の送信を無効にするには、このコマンドの **no** 形式を使用します。

**send-secure-announcements**  
**no send-secure-announcements**

## 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

MKPDU でのセキュアなアナウンスは無効になっています。

## コマンド モード

MKA ポリシー コンフィギュレーション (config-mka-policy)

## コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

## 使用上のガイドライン

セキュアなアナウンスは、以前はセキュアでないアナウンスで共有されていた MACsec 暗号スイート機能を再検証します。

## 例

次に、セキュアなアナウンスの送信を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy 2
Device(config-mka-policy)# send-secure-announcements
```

## 関連コマンド

Command	Description
<b>mka policy</b>	MKA ポリシーを設定します。
<b>confidentiality-offset</b>	機密性オフセットを設定して MACsec を動作させます。
<b>delay-protection</b>	MKPDU の送信で遅延保護を使用するように MKA を設定します。
<b>include-icv-indicator</b>	MKPDU に ICV インジケータを含めます。
<b>key-server</b>	MKA キーサーバオプションを設定します。
<b>macsec-cipher-suite</b>	SAK を取得するための暗号スイートを設定します。
<b>sak-rekey</b>	SAK キー再生成間隔を設定します。



Command	Description
<code>ssci-based-on-sci</code>	SCIに基づいてSSCIを計算します。
<code>use-updated-eth-header</code>	ICV計算には更新されたイーサネットヘッダーを使用します。

## server-private (RADIUS)

グループサーバに対して、プライベートRADIUSサーバのIPアドレスを設定するには、RADIUSサーバグループコンフィギュレーションモードで**server-private**コマンドを使用します。関連付けられたプライベートサーバを認証、許可、およびアカウントिंग(AAA)グループサーバから削除するには、このコマンドの**no**形式を使用します。

```
server-private ip-address [{auth-port port-number | acct-port port-number}] [non-standard]
[timeout seconds] [retransmit retries] [key string]
no server-private ip-address [{auth-port port-number | acct-port port-number}] [non-standard]
[timeout seconds] [retransmit retries] [key string]
```

### 構文の説明

<i>ip-address</i>	プライベートRADIUSサーバホストのIPアドレス。
<b>auth-port</b> <i>port-number</i>	(任意) 認証要求に対するユーザデータグラムプロトコル(UDP)宛先ポート。デフォルト値は1645です。
<b>acct-port</b> <i>port-number</i>	(任意) アカウントING要求に対するUDP宛先ポート。デフォルト値は1646です。
<b>non-standard</b>	(任意) RADIUSサーバでベンダー独自のRADIUS属性を使用。
<b>timeout</b> <i>seconds</i>	(オプション) デバイスがRADIUSサーバの応答を待機し、再送信するまでの時間間隔(秒単位)。この設定は <b>radius-server timeout</b> コマンドのグローバル値を上書きします。タイムアウト値が指定されていない場合は、グローバル値が使用されます。
<b>retransmit</b> <i>retries</i>	(任意) サーバが応答しない、または応答が遅い場合にRADIUS要求をサーバに再送信する回数。この設定は <b>radius-server retransmit</b> コマンドのグローバル設定を上書きします。
<b>key</b> <i>string</i>	(任意) デバイスとRADIUSサーバ上で稼働するRADIUSデーモン間で使用される認証および暗号キー。このキーは <b>radius-server key</b> コマンドのグローバル設定を上書きします。キー文字列を指定しない場合、グローバル値が使用されます。  <i>string</i> には、 <b>0</b> (暗号化されていないキーが続くことを指定)、 <b>6</b> (Advanced Encryption Scheme(AES)暗号化キーが続くことを指定) <b>7</b> (非公開のキーが続くことを指定)または暗号化されていない(クリアテキスト)サーバキーを指定する行を指定できます。

**コマンド デフォルト** server-private パラメータが指定されていない場合は、グローバルコンフィギュレーションが使用されます。グローバルコンフィギュレーションが指定されていない場合は、デフォルト値が使用されます。

**コマンド モード** RADIUS サーバグループ コンフィギュレーション (config-sg-radius)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

**使用上のガイドライン** **server-private** コマンドを使用して、特定のプライベートサーバと定義済みのサーバグループを関連付けます。Virtual Route Forwarding (VRF) インスタンス間でプライベートアドレスが重複する可能性を防ぐには、プライベートサーバ (プライベートアドレスを持つサーバ) をサーバグループ内で定義し、他のグループには示されないようにします。この場合も、グローバルプール (デフォルトの「radius」サーバグループなど) 内のサーバは、IP アドレスとポート番号を使って参照できます。このように、サーバグループ内のサーバのリストには、グローバルコンフィギュレーションにおけるホストの参照情報とプライベートサーバの定義が含まれます。



- (注)
- **radius-server directed-request** コマンドが設定されている場合、**server-private (RADIUS)** コマンドを設定してプライベート RADIUS サーバをグループサーバとして使用することはできません。
  - プライベート RADIUS サーバの AAA サーバ統計情報レコードの作成または更新はサポートされていません。プライベート RADIUS サーバが使用されている場合、エラーメッセージとトレースバックが発生しますが、これらのエラーメッセージやトレースバックは AAA RADIUS 機能には影響しません。これらのエラーメッセージとトレースバックを回避するには、プライベート RADIUS サーバの代わりにパブリック RADIUS サーバを設定します。

タイプ 6 AES 暗号化キーを設定するには、**password encryption aes** コマンドを使用します。

## 例

次に、sg\_water RADIUS グループサーバを定義してプライベートサーバを関連付ける例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius sg_water
Device(config-sg-radius)# server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# end
```

関連コマンド	コマンド	説明
	<b>aaa group server</b>	各種のサーバホストを別個のリストと別個の方式にグループ化します。
	<b>aaa new-model</b>	AAA アクセス コントロール モデルをイネーブルにします。
	<b>password encryption aes</b>	タイプ 6 の暗号化事前共有キーをイネーブルにします。
	<b>radius-server host</b>	RADIUS サーバホストを指定します。
	<b>radius-server directed-request</b>	ユーザが NAS にログインして認証用の RADIUS サーバを選択できるようにします。

## server-private (TACACS+)

グループサーバに対してプライベート TACACS+ サーバの IPv4 アドレスまたは IPv6 アドレスを設定するには、**server-private** コマンドをサーバグループ コンフィギュレーション モードで使用します。関連付けられたプライベートサーバを認証、許可、およびアカウントिंग (AAA) グループサーバから削除するには、このコマンドの **no** 形式を使用します。

```
server-private { ipv4-address | ipv6-address | fqdn } [ nat ] [ single-connection ] [ port port-number ] [ timeout seconds ] key [ { 0 | 7 } ] string
no server-private
```

構文の説明	説明
<i>ipv4-address</i>	プライベート TACACS+ サーバホストの IPv4 アドレスです。
<i>ipv6-address</i>	プライベート TACACS+ サーバホストの IPv6 アドレスです。
<b>fqdn</b>	ドメインネームサーバ (DNS) からのアドレス解決のためのプライベート TACACS+ サーバホストの完全修飾ドメイン名 (fqdn)。
<b>nat</b>	(任意) リモートデバイスのポートのネットワークアドレス変換 (NAT) アドレスを指定します。このアドレスは TACACS+ サーバに送信されます。
<b>single-connection</b>	(任意) ルータと TACACS+ サーバ間の単一の TCP 接続を維持します。
<b>timeoutseconds</b>	(任意) サーバ応答のタイムアウト値を指定します。この値を指定すると、このサーバに限り、 <b>tacacs-server timeout</b> コマンドで設定されたグローバルタイムアウト値が上書きされます。
<b>portport-number</b>	(任意) サーバのポート番号を指定します。この設定によって、デフォルトのポート 49 は上書きされます。

**key** [0|7] *string* (任意) 認証と暗号キーを指定します。このキーは TACACS+ デーモンで使用されるキーと一致する必要があります。このキーを指定すると、このサーバに対してグローバル `tacacs-server key` コマンドで設定されたキーのみが上書きされます。

数字を入力しないか、または 0 を入力した場合は、入力された文字列はプレーンテキストと見なされます。7 を入力すると、入力された文字列は暗号化されたテキストと見なされます。

#### コマンド デフォルト

`server-private` パラメータが指定されていない場合は、グローバルコンフィギュレーションが使用されます。グローバルコンフィギュレーションが指定されていない場合は、デフォルト値が使用されます。

#### コマンド モード

TACACS+ サーバグループ コンフィギュレーション (`config-sg-tacacs+`)

#### コマンド履歴

リリース

変更内容

Cisco IOS XE Everest 16.6.1 このコマンドが導入されました。

#### 使用上のガイドライン

`server-private` コマンドを使用して、特定のプライベートサーバと定義済みのサーバグループを関連付けます。Virtual Route Forwarding (VRF) 間でプライベートアドレスが重複する可能性を防ぐには、プライベートサーバ (プライベートアドレスを持つサーバ) をサーバグループ内で定義し、他のグループには示されないようにします。この場合も、グローバルプール (デフォルトの「TACACS+」サーバグループ) 内のサーバは、IP アドレスとポート番号を使用して参照できます。このように、サーバグループ内のサーバのリストには、グローバルコンフィギュレーションにおけるホストの参照情報とプライベートサーバの定義が含まれます。

次に、`tacacs1` TACACS+ グループサーバを定義してプライベートサーバを関連付ける例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa group server tacacs+ tacacs1
Device(config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco
Device(config-sg-tacacs+)# exit
Device(config)# ip vrf cisco
Device(config-vrf)# rd 100:1
Device(config-vrf)# exit
Device(config)# interface Loopback0
Device(config-if)# ip address 10.0.0.2 255.0.0.0
Device(config-if)# ip vrf forwarding cisco
```

#### 関連コマンド

コマンド	説明
<code>aaa group server</code>	各種のサーバホストを別個のリストと別個の方式にグループ化します。
<code>aaa new-model</code>	AAA アクセス コントロール モデルをイネーブルにします。

コマンド	説明
<b>ip tacacs source-interface</b>	すべての発信 TACACS+ パケットに対して、指定されたインターフェイスの IP アドレスを使用します。
<b>ip vrf forwarding (server-group)</b>	AAA TACACS+ サーバグループの VRF の参照を設定します。

## 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 XE Everest 16.6.1

このコマンドが導入されました。

次に、**show aaa clients** コマンドの出力例を示します。

```
デバイス# show aaa clients
Dropped request packets: 0
```

## show aaa command handler

AAA 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 XE Everest 16.6.1

このコマンドが導入されました。

次に、**show aaa command handler** コマンドの出力例を示します。

```

デバイス# 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

<b>netuser</b>	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。
<i>name</i>	ネットワーク ユーザ名。
<b>all</b>	ネットワークおよびゲスト ユーザ情報を指定します。
<b>statistics</b>	ローカル認証の統計情報を表示します。
<b>user lockout</b>	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 XE Everest 16.6.1	このコマンドが導入されました。

次に、**show aaa local statistics** コマンドの出力例を示します。

```

デバイス# 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

認証、許可、アカウントिंग（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	<b>detailed</b>	(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。
	<b>public</b>	(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。
	<b>detailed</b>	(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 (>)	
	特権 EXEC (>)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

### 例

次に、**show aaa servers** コマンドの出力例を示します。

```

Device# 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 XE Everest 16.6.1

このコマンドが導入されました。

次に、**show aaa sessions** コマンドの出力例を示します。

```

デバイス# 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 brief

特定のインターフェイスの認証セッションに関する概要情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show authentication brief** コマンドを使用します。

```
show authentication brief[switch{switch-number|active|standby}{R0}]
```

構文の説明	<i>switch-number</i>	<i>switch-number</i> 変数の有効な値は 1～9 です。
	<b>R0</b>	ルートプロセッサ (RP) スロット 0 に関する情報を表示します。
	<b>active</b>	アクティブ インスタンスを指定します。
	<b>standby</b>	スタンバイ インスタンスを指定します。
コマンドモード	特権 EXEC (#) ユーザ EXEC (>)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

次に、**show authentication brief** コマンドの出力例を示します。

```
Device# show authentication brief
```

Interface	MAC Address	AuthC	AuthZ	Fg	Uptime
Gi2/0/14	0002.0002.0001	m:NA d:OK	AZ: SA-	X	281s
Gi2/0/14	0002.0002.0002	m:NA d:OK	AZ: SA-	X	280s
Gi2/0/14	0002.0002.0003	m:NA d:OK	AZ: SA-	X	279s
Gi2/0/14	0002.0002.0004	m:NA d:OK	AZ: SA-	X	278s
Gi2/0/14	0002.0002.0005	m:NA d:OK	AZ: SA-	X	278s
Gi2/0/14	0002.0002.0006	m:NA d:OK	AZ: SA-	X	277s
Gi2/0/14	0002.0002.0007	m:NA d:OK	AZ: SA-	X	276s
Gi2/0/14	0002.0002.0008	m:NA d:OK	AZ: SA-	X	276s
Gi2/0/14	0002.0002.0009	m:NA d:OK	AZ: SA-	X	275s
Gi2/0/14	0002.0002.000a	m:NA d:OK	AZ: SA-	X	275s
Gi2/0/14	0002.0002.000b	m:NA d:OK	AZ: SA-	X	274s
Gi2/0/14	0002.0002.000c	m:NA d:OK	AZ: SA-	X	274s
Gi2/0/14	0002.0002.000d	m:NA d:OK	AZ: SA-	X	273s
Gi2/0/14	0002.0002.000e	m:NA d:OK	AZ: SA-	X	273s
Gi2/0/14	0002.0002.000f	m:NA d:OK	AZ: SA-	X	272s
Gi2/0/14	0002.0002.0010	m:NA d:OK	AZ: SA-	X	272s
Gi2/0/14	0002.0002.0011	m:NA d:OK	AZ: SA-	X	271s
Gi2/0/14	0002.0002.0012	m:NA d:OK	AZ: SA-	X	271s
Gi2/0/14	0002.0002.0013	m:NA d:OK	AZ: SA-	X	270s
Gi2/0/14	0002.0002.0014	m:NA d:OK	AZ: SA-	X	270s
Gi2/0/14	0002.0002.0015	m:NA d:OK	AZ: SA-	X	269s

次に、アクティブインスタンスに対する **show authentication brief** コマンドの出力例を示します。

```
Device# show authentication brief switch active R0
```

Interface	MAC Address	AuthC	AuthZ	Fg	Uptime
Gi2/0/14	0002.0002.0001	m:NA d:OK	AZ: SA-	X	1s
Gi2/0/14	0002.0002.0002	m:NA d:OK	AZ: SA-	X	0s
Gi2/0/14	0002.0002.0003	m:NA d:OK	AZ: SA-	X	299s
Gi2/0/14	0002.0002.0004	m:NA d:OK	AZ: SA-	X	298s
Gi2/0/14	0002.0002.0005	m:NA d:OK	AZ: SA-	X	298s
Gi2/0/14	0002.0002.0006	m:NA d:OK	AZ: SA-	X	297s
Gi2/0/14	0002.0002.0007	m:NA d:OK	AZ: SA-	X	296s
Gi2/0/14	0002.0002.0008	m:NA d:OK	AZ: SA-	X	296s
Gi2/0/14	0002.0002.0009	m:NA d:OK	AZ: SA-	X	295s
Gi2/0/14	0002.0002.000a	m:NA d:OK	AZ: SA-	X	295s
Gi2/0/14	0002.0002.000b	m:NA d:OK	AZ: SA-	X	294s
Gi2/0/14	0002.0002.000c	m:NA d:OK	AZ: SA-	X	294s
Gi2/0/14	0002.0002.000d	m:NA d:OK	AZ: SA-	X	293s
Gi2/0/14	0002.0002.000e	m:NA d:OK	AZ: SA-	X	293s
Gi2/0/14	0002.0002.000f	m:NA d:OK	AZ: SA-	X	292s
Gi2/0/14	0002.0002.0010	m:NA d:OK	AZ: SA-	X	292s
Gi2/0/14	0002.0002.0011	m:NA d:OK	AZ: SA-	X	291s
Gi2/0/14	0002.0002.0012	m:NA d:OK	AZ: SA-	X	291s
Gi2/0/14	0002.0002.0013	m:NA d:OK	AZ: SA-	X	290s
Gi2/0/14	0002.0002.0014	m:NA d:OK	AZ: SA-	X	290s
Gi2/0/14	0002.0002.0015	m:NA d:OK	AZ: SA-	X	289s
Gi2/0/14	0002.0002.0016	m:NA d:OK	AZ: SA-	X	289s

次に、スタンバイインスタンスに対する **show authentication brief** コマンドの出力例を示します。

```
Device# show authentication brief switch standby R0
```

```
No sessions currently exist
```

次の表で、この出力で表示される重要なフィールドについて説明します。

表 4: **show authentication brief** フィールドの説明

フィールド	説明
Interface	認証インターフェイスのタイプと番号。
MAC アドレス	クライアントの MAC アドレス。
AuthC	認証ステータス。
authz	承認ステータス。

フィールド	説明
FG	<p>現在のステータスを示すフラグ。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• A : ポリシーの適用中（詳細は複数行のステータスを参照）</li> <li>• D : 取り外し待ち</li> <li>• F : 最終の取り外しの進行中</li> <li>• I : IIF ID の割り当て待ち</li> <li>• P : セッションをプッシュ済み</li> <li>• R : ユーザプロファイルの削除中（詳細は複数行のステータスを参照）</li> <li>• U : ユーザプロファイルの適用中（詳細は複数行のステータスを参照）</li> <li>• X : 不明なブロック</li> </ul>
Uptime	セッションが起動してからの経過時間。

## 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

<b>database</b>	(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。
<b>handle handle-id</b>	(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。
<b>details</b>	(任意) 詳細情報を表示します。
<b>interface type number</b>	(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。
<b>mac mac-address</b>	(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 XE Everest 16.6.1

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 5: 認証方式の状態

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 6: 認証方式の状態

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

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。

```

デバイス# 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。

```

デバイス# 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 cts interface

インターフェイスの Cisco TrustSec (CTS) 設定の統計を表示するには、特権 EXEC モードで **show cts interface** コマンドを使用します。

```
show cts interface [{type slot/port | brief | summary}]
```

構文の説明	<b>type slot/port</b>	(任意) インターフェイス タイプおよびスロット番号またはポート番号を指定します。このインターフェイスの詳細な出力が返されます。
	<b>brief</b>	(任意) すべての CTS インターフェイスの短縮ステータスを表示します。
	<b>summary</b>	(任意) インターフェイスごとに、すべてのCTSインターフェイスのサマリーを、4個または5個のキーステータスフィールドを持つ表形式で表示します。

コマンド デフォルト なし

コマンド モード EXEC (>) 特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.3.1	このコマンドが変更され、いくつかのオプションが追加されました。
	Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン すべての CTS インターフェイスの冗長ステータスを表示するには、キーワードを使用せずに **show cts interface** コマンドを使用します。

#### 例

次に、キーワードを使用せずに出力を表示する例を示します (すべての CTS インターフェイスの冗長ステータス)。

```
Switch# show cts interface

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:00:18.232
  Authentication Status:  NOT APPLICABLE
    Peer identity:        "unknown"
    Peer's advertised capabilities: ""
  Authorization Status:   NOT APPLICABLE
  SAP Status:             NOT APPLICABLE
  Configured pairwise ciphers:
    gcm-encrypt
    null

  Replay protection:      enabled
  Replay protection mode: STRICT

  Selected cipher:

  Propagate SGT:          Enabled
  Cache Info:
    Cache applied to link : NONE

  Statistics:
    authc success:        0
    authc reject:         0
```

```

authc failure:          0
authc no response:     0
authc logoff:          0
sap success:           0
sap fail:              0
authz success:         0
authz fail:            0
port auth fail:       0
Ingress:
  control frame bypassed: 0
  sap frame bypassed:    0
  esp packets:          0
  unknown sa:           0
  invalid sa:           0
  inverse binding failed: 0
  auth failed:          0
  replay error:         0
Egress:
  control frame bypassed: 0
  esp packets:           0
  sgt filtered:          0
  sap frame bypassed:    0
  unknown sa dropped:    0
  unknown sa bypassed:   0
    
```

次に、**brief** キーワードを使用した出力例を示します。

```

Device# show cts interface brief

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:00:40.386
  Authentication Status:  NOT APPLICABLE
  Peer identity:          "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:   NOT APPLICABLE
  SAP Status:             NOT APPLICABLE
  Propagate SGT:          Enabled
  Cache Info:
    Cache applied to link : NONE
    
```

関連コマンド

コマンド	説明
<b>cts manual</b>	CTS のインターフェイスを有効にします。
<b>propagate sgt (cts manual)</b>	Cisco TrustSec Security (CTS) インターフェイスのレイヤ 2 でのセキュリティ グループ タグ (SGT) の伝達を有効にします。
<b>sap mode-list (cts manual)</b>	PMK および SAP 認証モードと暗号化モードを手動で指定し、2 つのインターフェイス間で MACsec リンクの暗号化をネゴシエートします。

## show cts role-based permissions

ロールベース（セキュリティグループ）アクセスコントロール権限リストを表示するには、特権 EXEC モードで **show cts role-based permissions** コマンドを使用します。

```
show cts role-based permissions [{default [{details | ipv4 [{details}]}] | from [{sgt [{ipv4 | to
[{sgt | unknown}] [{details | ipv4 [{details}]}]}] | unknown}] | ipv4 | to [{sgt | unknown}]
[{ipv4}]}]
```

### 構文の説明

<b>default</b>	（任意）デフォルトの権限リストに関する情報を表示します。
<b>details</b>	（任意）アタッチされたアクセスコントロールリスト（ACL）の詳細を表示します。
<b>ipv4</b>	（任意）IPv4 プロトコルに関する情報を表示します。
<b>from</b>	（任意）送信元グループに関する情報を表示します。
<i>sgt</i>	（任意）セキュリティグループタグ。有効値は 2 ～ 65519 です。
<b>to</b>	（任意）宛先グループに関する情報を表示します。
<b>unknown</b>	（任意）不明な送信元グループと宛先グループに関する情報を表示します。

### 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 XE Denali 16.3.1	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、SGACL 権限マトリックスのコンテンツを表示します。送信元セキュリティグループタグ（SGT）は **from** キーワードを使用して、宛先 SGT は **to** キーワードを使用して指定できます。両方のキーワードを指定すると、単一セルの RBACL が表示されます。列全体は、**to** キーワードを使用した場合にのみ表示されます。行全体は、**from** キーワードを使用した場合に表示されます。権限マトリックス全体は、**from** キーワードと **to** キーワードの両方を省略した場合に表示されます。

コマンド出力は、プライマリ キーの宛先 SGT およびセカンダリ キーの送信元 SGT でソートされます。各セルの SGACL は、設定で定義されているのと同じ順序で、または Cisco Identity Services Engine（ISE）から取得した順序で表示されます。

**details** キーワードは、**from** キーワードと **to** キーワードの両方を指定することで、単一のセルが選択された場合に表示されます。**details** キーワードが指定されている場合、単一セルの SGACL のアクセス制御エントリが表示されます。

次に、**show role-based permissions** コマンドの出力例を示します。



```
Switch# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
default_sgacl-02
Permit IP-00
IPv4 Role-based permissions from group 305:sgt to group 306:dgt (monitored):
test_reg_tcp_permit-02
RBACL Monitor All for Dynamic Policies : TRUE
RBACL Monitor All for Configured Policies : FALSE
IPv4 Role-based permissions from group 6:SGT_6 to group 6:SGT_6 (configured):
  mon_1
IPv4 Role-based permissions from group 10 to group 11 (configured):
  mon_2
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

## 関連コマンド

コマンド	説明
<b>cts role-based permissions</b>	送信元グループから宛先グループに対する権限を有効にします。
<b>cts role-based monitor</b>	ロールベースのアクセスリストのモニタリングを有効にします。

## show cisp

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

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

## 構文の説明

<b>clients</b>	(任意) CISP クライアントの詳細を表示します。
<b>interface interface-id</b>	(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。
<b>registrations</b>	CISP の登録情報を表示します。
<b>summary</b>	(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 XE Everest 16.6.1	このコマンドが導入されました。

リリース	変更内容
	このコマンドが再度導入されました。このコマンドはおよびではサポートされません。

次に、**show cisp interface** コマンドの出力例を示します。

```
デバイス# show cisp interface fast 0
CISP not enabled on specified interface
```

次に、**show cisp registration** コマンドの出力例を示します。

```
デバイス# 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
<b>cisp enable</b>	Client Information Signalling Protocol (CISP) をイネーブルにします。
<b>dot1x credentials profile</b>	サブリカント 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、ユーザー EXEC モードで **show dot1x** 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 XE Everest 16.6.1	このコマンドが導入されました。

次に、**show dot1x all** コマンドの出力例を示します。

```
デバイス# show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   3
```

次に、**show dot1x all count** コマンドの出力例を示します。

```
デバイス# show dot1x all count
Number of Dot1x sessions
-----
Authorized Clients       = 0
Unauthorized Clients     = 0
Total No of Client      = 0
```

次に、**show dot1x all statistics** コマンドの出力例を示します。

```
デバイス# 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

拡張可能認証プロトコル（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、特権 EXEC モードで **show eap pac peer** 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 XE Everest 16.6.1

このコマンドが導入されました。

次に、**show eap pac peers** 特権 EXEC コマンドの出力例を示します。

```

デバイス> show eap pac peers
No PACs stored

```

#### 関連コマンド

コマンド	説明
<b>clear eap sessions</b>	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概要形式または詳細形式で表示するには、ユーザー EXEC モードで **show ip dhcp snooping statistics** 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 XE Everest 16.6.1	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プライマリで生成されます。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。

次に、**show ip dhcp snooping statistics** コマンドの出力例を示します。

デバイス> **show ip dhcp snooping statistics**

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

次に、**show ip dhcp snooping statistics detail** コマンドの出力例を示します。

デバイス> **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 7: 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。

DHCP スヌーピング統計情報	説明
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 <b>no ip dhcp snooping information option allow-untrusted</b> 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、 <b>ip dhcp snooping verify mac-address</b> 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。
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。

DHCP スヌーピング統計情報	説明
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に 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、**the 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 XE Everest 16.6.1	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。

次に、`show radius server-group all` コマンドの出力例を示します。

```
デバイス# 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 8 : `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。
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、 <code>sharecount</code> 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、 <code>sharecount</code> 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、 <code>standard</code> または <code>nonstandard</code> 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「 <code>nonstandard</code> 」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。 <code>Memlocks</code> 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	<i>map-name</i> (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 XE Everest 16.6.1	このコマンドが導入されました。

次に、**show vlan access-map** コマンドの出力例を示します。

```

デバイス# show vlan access-map
Vlan access-map "vmap4" 10
  Match clauses:
    ip address: a12
  Action:
    forward
Vlan access-map "vmap4" 20
  Match clauses:
    ip address: a12
  Action:
    forward

```

## show vlan filter

すべての VLAN フィルタ、または特定の VLAN または 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 filter** コマンドを使用します。

**show vlan filter** {*access-map name* | *vlan vlan-id*}

構文の説明	<b>access-map</b> <i>name</i> (任意) 指定された VLAN アクセス マップのフィルタリング情報を表示します。
	<b>vlan</b> <i>vlan-id</i> (任意) 指定された VLAN のフィルタリング情報を表示します。指定できる範囲は 1 ~ 4094 です。
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 XE Everest 16.6.1	このコマンドが導入されました。

次に、**show vlan filter** コマンドの出力例を示します。

```
デバイス# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

## 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	
<b>group-name</b> <i>vlan-group-name</i>	(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。
<b>user_count</b>	(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 XE Everest 16.6.1	このコマンドが導入されました。

**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 グループのメンバのみが表示されます。

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

セキュアアドレスエントリのエージングタイムおよびタイプを設定する、または特定のポートのセキュアアドレスのエージング動作を変更するには、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** コマンドを使用します。ポートセキュリティエージングをディセーブルにする、またはパラメータをデフォルトの状態に設定するには、このコマンドの **no** 形式を使用します。

```
switchport port-security aging {static|time time|type {absolute|inactivity}}
no switchport port-security aging {static|time|type}
```

### 構文の説明

<b>static</b>	このポートに静的に設定されたセキュアアドレスのエージングをイネーブルにします。
<b>time</b> <i>time</i>	このポートのエージングタイムを指定します。指定できる範囲は0～1440分です。 <i>time</i> が 0 の場合、このポートのエージングはディセーブルです。
<b>type</b>	エージング タイプを設定します。
<b>absolute</b>	<b>absolute</b> エージングタイプを設定します。このポートのすべてのセキュアアドレスは、指定された時間（分）が経過した後に期限切れとなり、セキュアアドレスリストから削除されます。
<b>inactivity</b>	<b>inactivity</b> エージングタイプを設定します。指定された時間内にセキュア送信元アドレスからのデータトラフィックがない場合だけ、このポートのセキュアアドレスが期限切れになります。

### コマンド デフォルト

ポートセキュリティ エージング機能はディセーブルです。デフォルトの時間は 0 分です。  
デフォルトのエージング タイプは **absolute** です。  
デフォルトのスタティック エージング動作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 XE Everest 16.6.1	このコマンドが導入されました。

### 使用上のガイドライン

特定のポートのセキュアアドレス エージングをイネーブルにするには、ポート エージングタイムを 0 以外の値に設定します。

特定のセキュアアドレスに時間を限定してアクセスできるようにするには、エージングタイプを **absolute** に設定します。エージング タイムの期限が切れると、セキュアアドレスが削除されます。

継続的にアクセスできるセキュアアドレス数を制限するには、エージングタイプを **inactivity** に設定します。このようにすると、非アクティブになったセキュアアドレスが削除され、他のアドレスがセキュアになることができます。

セキュアアドレスへのアクセス制限を解除するには、セキュアアドレスとして設定し、**no switchport port-security aging static** 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、静的に設定されたセキュアアドレスのエージングをディセーブルにします。

次の例では、ポートのすべてのセキュア アドレスに対して、エージング タイプを **absolute**、エージング タイムを 2 時間に設定します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# switchport port-security aging time 120
```

次の例では、ポートに設定されたセキュア アドレスに対して、エージング タイプを **inactivity**、エージング タイムを 2 分に設定します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# switchport port-security aging time 2
デバイス(config-if)# switchport port-security aging type inactivity
デバイス(config-if)# switchport port-security aging static
```

次の例では、設定されたセキュアアドレスのエージングをディセーブルにする方法を示します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# no switchport port-security aging static
```

## switchport port-security mac-address

セキュア MAC アドレスまたはスティッキー MAC アドレスラーニングを設定するには、**switchport port-security mac-address** 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。

```
switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} | sticky
[{{mac-address | vlan {vlan-id {access | voice}}}}]}
no switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} |
sticky [{{mac-address | vlan {vlan-id {access | voice}}}}]}
```

### 構文の説明

**mac-address** 48 ビット MAC アドレスの入力によって指定するインターフェイスのセキュア MAC アドレス。設定された最大数まで、セキュア MAC アドレスを追加できます。

**vlan vlan-id** (任意) トランク ポート上でだけ、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しない場合は、ネイティブ VLAN が使用されます。

**vlan access** (任意) アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。

<b>vlan voice</b>	(任意) アクセスポートでだけ、VLAN を音声 VLAN として指定します。 (注) <b>voice</b> キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。
<b>sticky</b>	スティッキ ラーニングのインターフェイスをイネーブルにします。スティッキ ラーニングをイネーブルにすると、インターフェイスは動的に学習したすべてのセキュア MAC アドレスを実行コンフィギュレーションに追加して、これらのアドレスをスティッキ セキュア MAC アドレスに変換します。
<b>mac-address</b>	(任意) スティッキ セキュア MAC アドレスを指定する MAC アドレス。

**コマンドデフォルト** セキュア MAC アドレスは設定されていません。  
スティッキ ラーニング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 XE Everest 16.6.1	このコマンドが導入されました。

**使用上のガイドライン** セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることはできますが、ダイナミック アクセス ポートには設定できません。
- セキュア ポートはルーテッド ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートをスイッチド ポート アナライザ (SPAN) の宛先ポートにすることはできません。
- セキュア ポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。
- 音声 VLAN では、スタティック セキュアまたはスティッキ セキュア MAC アドレスを設定できません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュアアドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュアアドレスを設定する必要があります。

- 音声 VLAN はアクセス ポート上でだけサポートされます。トランク ポート上ではサポートされません。

スティッキ セキュア MAC アドレスには、次の特性があります。

- **switchport port-security mac-address sticky** 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、インターフェイス上でスティッキラーニングをイネーブルにした場合、インターフェイスはすべてのダイナミックセキュア MAC アドレス（スティッキラーニングがイネーブルになる前に動的に学習されたアドレスを含む）を、スティッキセキュア MAC アドレスに変換し、すべてのスティッキセキュア MAC アドレスを実行コンフィギュレーションに追加します。
- **no switchport port-security mac-address sticky** 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、スティッキラーニングをディセーブルする場合、または実行コンフィギュレーションを削除する場合は、スティッキセキュア MAC アドレスは実行コンフィギュレーションの一部に残りますが、アドレステーブルからは削除されます。削除されたアドレスはダイナミックに再設定することができ、ダイナミックアドレスとしてアドレス テーブルに追加されます。
- **switchport port-security mac-address sticky mac-address** 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、スティッキセキュア MAC アドレスを設定する場合、これらのアドレスはアドレステーブルおよび実行コンフィギュレーションに追加されます。ポートセキュリティがディセーブルの場合、スティッキセキュア MAC アドレスは実行コンフィギュレーションに残ります。
- スティッキセキュア MAC アドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時、またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくて済みます。スティッキセキュア アドレスを保存しない場合、アドレスは失われます。スティッキラーニングがディセーブルの場合、スティッキセキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。
- スティッキラーニングをディセーブルにして、**switchport port-security mac-address sticky mac-address** 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場合、エラーメッセージが表示され、スティッキセキュア MAC アドレスは実行コンフィギュレーションに追加されません。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、ポートでセキュア MAC アドレスと VLAN ID を設定する方法を示します。

```
デバイス(config)# interface gigabitethernet 2/0/2
デバイス(config-if)# switchport mode trunk
デバイス(config-if)# switchport port-security
デバイス(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

次の例では、スティッキラーニングをイネーブルにして、ポート上で2つのスティッキセキュア MAC アドレスを入力する方法を示します。

```

デバイス(config)# interface gigabitethernet 2/0/2
デバイス(config-if)# switchport port-security mac-address sticky
デバイス(config-if)# switchport port-security mac-address sticky 0000.0000.4141
デバイス(config-if)# switchport port-security mac-address sticky 0000.0000.000f

```

## switchport port-security maximum

セキュア MAC アドレスの最大数を設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security maximum** 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。

```

switchport port-security maximum value [vlan [{vlan-list} | [{access | voice}]]]
no switchport port-security maximum value [vlan [{vlan-list} | [{access | voice}]]]

```

### 構文の説明

**value** インターフェイスのセキュア MAC アドレスの最大数を設定します。

デフォルトの設定は 1 秒です。

**vlan** (任意) トランク ポートの場合、VLAN ごとまたは一定範囲の VLAN のセキュア MAC アドレスの最大数を設定します。**vlan** キーワードが入力されていない場合、デフォルト値が使用されます。

**vlan-list** (任意) カンマで区切られた VLAN の範囲またはハイフンで区切られた一連の VLAN。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。

**access** (任意) アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。

**voice** (任意) アクセス ポートでだけ、VLAN を音声 VLAN として指定します。

(注) **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

### コマンド デフォルト

ポートセキュリティをイネーブルにしてキーワードを入力しない場合、デフォルトのセキュア MAC アドレスの最大数は 1 です。

### コマンド モード

インターフェイス 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 XE Everest 16.6.1

このコマンドが導入されました。

### 使用上のガイドライン

スイッチまたはスイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この数字はアクティブな Switch Database Management (SDM) テンプレートによって決められます。**sdm prefer** コマンドを参照

してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることができますが、ダイナミック アクセス ポートには設定できません。
- セキュア ポートはルーテッド ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートをスイッチド ポート アナライザ (SPAN) の宛先ポートにすることはできません。
- セキュア ポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合は、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合は、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュア アドレスを設定する必要があります。

音声 VLAN はアクセス ポート上でだけサポートされます。トランク ポート上ではサポートされません。

- インターフェイスのセキュア アドレスの最大値を入力する場合、新しい値が前回の値より大きいと、新しい値によって前回の設定値が上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。

アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、確実にデバイスがポートの帯域幅を完全に使用できます。

インターフェイスのセキュア アドレスの最大値を入力すると、次の事象が発生します。

- 新しい値が前回の値より大きい場合、新しい値によって前回の設定値が上書きされます。
- 新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、ポートでポートセキュリティをイネーブルにし、セキュア アドレスの最大数を 5 に設定する方法を示します。違反モードはデフォルトで、セキュア MAC アドレスは設定されていません。

```
デバイス(config)# interface gigabitethernet 2/0/2
デバイス(config-if)# switchport mode access
```



```

デバイス(config-if)# switchport port-security
デバイス(config-if)# switchport port-security maximum 5

```

## switchport port-security violation

セキュア MAC アドレスの違反モード、またはポートセキュリティに違反した場合に実行するアクションを設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security violation** 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。

```

switchport port-security violation {protect|restrict|shutdown|shutdown vlan}
no switchport port-security violation {protect|restrict|shutdown|shutdown vlan}

```

### 構文の説明

<b>protect</b>	セキュリティ違反保護モードを設定します。
<b>restrict</b>	セキュリティ違反制限モードを設定します。
<b>shutdown</b>	セキュリティ違反シャットダウン モードを設定します。
<b>shutdown vlan</b>	VLAN ごとのシャットダウンにセキュリティ違反モードを設定します。

### コマンド デフォルト

デフォルトの違反モードは **shutdown** 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 XE Everest 16.6.1	このコマンドが導入されました。

### 使用上のガイドライン

セキュリティ違反保護モードでは、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスの packets はドロップされます。ドロップすることでセキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。



- (注) トランクポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

セキュリティ違反制限モードでは、セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスの packets はドロップされます。セキュア MAC ア

ドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。SNMPトラップが送信されます。Syslogメッセージがロギングされ、違反カウンタが増加します。

セキュリティ違反シャットダウンモードでは、違反が発生し、ポートのLEDがオフになると、インターフェイスが **errdisable** になります。SNMPトラップが送信されます。Syslogメッセージがロギングされ、違反カウンタが増加します。セキュアポートが **errdisable** ステートの場合には、**errdisable recovery cause psecure-violation** グローバルコンフィギュレーションコマンドを入力してこのステートを解除するか、**shutdown** および **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入力して手動で再びイネーブルにできます。

セキュリティ違反モードが VLAN ごとのシャットダウンに設定されると、違反が発生した VLAN のみが **errdisable** になります。

セキュアポートに関する制限事項は、次のとおりです。

- セキュアポートはアクセスポートまたはトランクポートにすることができますが、ダイナミックアクセスポートには設定できません。
- セキュアポートはルーテッドポートにはできません。
- セキュアポートは保護ポートにはできません。
- セキュアポートをスイッチドポートアナライザ (SPAN) の宛先ポートにすることはできません。
- セキュアポートをギガビットまたは 10 ギガビット EtherChannel ポートグループに含めることはできません。

セキュア MAC アドレスの最大値がアドレステーブルに存在し、アドレステーブルに存在しない MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合、または別のセキュアポートのセキュア MAC アドレスとして設定された MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合に、セキュリティ違反が起こります。

セキュアポートが **errdisable** ステートの場合には、**errdisable recovery cause psecure-violation** グローバルコンフィギュレーションコマンドを入力して、このステートから回復させることができます。**shutdown** および **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入力するか、**clear errdisable interface** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにすることができます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、MAC セキュリティ違反が発生した場合に VLAN のみをシャットダウンするようポートを設定する方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/2
デバイス(config)# switchport port-security violation shutdown vlan
```

## tacacs server

IPv6 または IPv4 用に TACACS+ サーバを設定し、TACACS+ サーバ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 **tacacs server** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

**tacacs server** *name*

**no tacacs server**

### 構文の説明

<b>name</b>	プライベート TACACS+サーバホストの名前。
-------------	--------------------------

### コマンドデフォルト

TACACS+ サーバは構成されていません。

### コマンドモード

グローバルコンフィギュレーション (config)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

### 使用上のガイドライン

**tacacs server** コマンドは、*name* 引数を使用して TACACS サーバを設定し、TACACS+ サーバコンフィギュレーションモードを開始します。設定が完了し、TACACS+サーバコンフィギュレーションモードを終了すると、設定が適用されます。

### 例

次の例は、名前 `server1` を使用して TACACS サーバを設定し、さらに設定を行うために TACACS+サーバコンフィギュレーションモードを開始する方法を示しています。

```
Device(config)# tacacs server server1
Device(config-server-tacacs)#
```

### 関連コマンド

Command	Description
<b>address ipv6 (TACACS+)</b>	TACACS+ サーバの IPv6 アドレスを設定します。
<b>key (TACACS+)</b>	TACACS+ サーバでサーバ単位の暗号キーを設定します。
<b>port (TACACS+)</b>	TACACS+ 接続に使用する TCP ポートを指定します。
<b>send-nat-address (TACACS+)</b>	クライアントの NAT 後のアドレスを TACACS+ サーバに送信します。
<b>single-connection (TACACS+)</b>	単一の TCP 接続を使用してすべての TACACS パケットを同じサーバーに送信できるようにします。
<b>timeout (TACACS+)</b>	指定された TACACS サーバからの応答を待機する時間を設定します。

## tracking (IPv6 スヌーピング)

ポートでデフォルトの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	
<b>enable</b>	トラッキングをイネーブルにします。
<b>reachable-lifetime</b>	<p>(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。</p> <ul style="list-style-type: none"> <li>• <b>reachable-lifetime</b> キーワードを使用できるのは、<b>enable</b> キーワードが指定されている場合のみです。</li> <li>• <b>reachable-lifetime</b> キーワードを使用すると、<b>ipv6 neighbor binding reachable-lifetime</b> 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上書きされます。</li> </ul>
<i>value</i>	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。
<b>infinite</b>	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。
<b>disable</b>	トラッキングをディセーブルにします。
<b>stale-lifetime</b>	<p>(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 <b>stale-lifetime</b> 設定が上書きされます。</p> <ul style="list-style-type: none"> <li>• ステイル ライフタイムは 86,400 秒です。</li> <li>• <b>stale-lifetime</b> キーワードを使用できるのは、<b>disable</b> キーワードが指定されている場合のみです。</li> <li>• <b>stale-lifetime</b> キーワードを使用すると、<b>ipv6 neighbor binding stale-lifetime</b> 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上書きされます。</li> </ul>
コマンド デフォルト	時間のエントリは到達可能な状態に維持されます。
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

コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.6.1	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上で **ipv6 neighbor tracking** コマンドによって設定されたデフォルトのトラッキングポリシーに優先します。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行します。**tracking** コマンドで **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上書きされません。

**stale-lifetime** キーワードは、エントリが削除されるか、直接または間接的に到達可能であると証明される前にテーブルに保持される最大時間です。**tracking** コマンドで **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上書きされます。

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。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(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 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 **trusted-port** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

**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 インスペクション ポリシーの設定 IPv6 スヌーピング 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 XE Everest 16.6.1	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。

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。

```
デバイス(config)# ipv6 nd inspection policy1
デバイス(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。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(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	<i>name</i>	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 XE Everest 16.6.1	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、照合する IP または非 IP トラフィックのアクセス リストを指定できます。また、**action** コマンドを使用して、この照合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** : 照合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、デフォルト値を設定します。

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、エントリを個別に削除できます。

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

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。

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。

```

デバイス(config)# vlan access-map vac1
デバイス(config-access-map)# match ip address acl1
デバイス(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。

```

デバイス(config)# no vlan access-map vac1

```

## vlan dot1Q tag native

トランクポートのネイティブ VLAN で dot1q (IEEE 802.1Q) のタグリングを有効にするには、グローバル コンフィギュレーション モードで **vlan dot1Q tag native** コマンドを使用します。

この機能を無効にするには、このコマンドの **no** 形式を使用します。

```

vlan dot1Q tag native
no vlan dot1Q tag native

```

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	グローバル コンフィギュレーション (config)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Everest 16.5.1a このコマンドが導入されました。	

**使用上のガイドライン** 通常は、ネイティブ VLAN ID で 802.1Q トランクを設定します。これによって、その VLAN 上のすべてのパケットからタグリングが取り除かれます。

ネイティブ VLAN でのタグリングを維持し、タグなしトラフィックをドロップするには、**vlan dot1q tag native** コマンドを使用します。デバイスによって、ネイティブ VLAN で受信したトラフィックがタグ付けされ、802.1Q タグが付けられたフレームのみが許可され、ネイティブ VLAN のタグなしトラフィックを含むすべてのタグなしトラフィックはドロップされます。

**vlan dot1q tag native** コマンドがイネーブルになっていても、トランク ポートのネイティブ VLAN では、制御トラフィックはタグなしとして引き続き許可されます。



(注) **dot1q tag vlan native** コマンドがグローバルレベルで設定されている場合、トランクポートでの dot1x 再認証は失敗します。

次に、デバイスのすべてのトランクポートでネイティブ VLAN の dot1q (IEEE 802.1Q) タグリングを有効にする例を示します。



```
Device(config)# vlan dot1q tag native
Device(config)#
```

## 関連コマンド

Command	Description
<b>show vlan dot1q tag native</b>	ネイティブ VLAN のタグging のステータスを表示します。

## vlan filter

1 つ以上の 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。

リスト 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 XE Everest 16.6.1

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。

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。

```
デバイス(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。

```
デバイス(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

<code>group-name</code>	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。
<code>vlan-list vlan-list</code>	VLAN グループに追加される 1 つ以上の VLAN を指定します。 <code>vlan-list</code> 引数には単一の VLAN ID、VLAN ID のリスト、または VLAN ID の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 XE Everest 16.6.1	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。

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。

```
デバイス(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。

```
デバイス(config)# no vlan group group1 vlan-list 7
```

