セキュリティ

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、およびアカウンティング（AAA）アカウンティング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 {**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

auth-proxy	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。
system	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ティングを実行します。
network	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ティングを実行します。
exec	EXEC シェルセッションのアカウンティングを実行します。このキーワードは、**autocommand** コマンドによって生成される情報などのユーザプロファイル情報を返すことができます。
connection	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。
commands *level*	指定した特権レベルですべてのコマンドのアカウン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。
default	この引数のあとにリストされるアカウンティング方式を、アカウンティング サービスのデフォルトリストとして使用します。
list-name	次に記載されているアカウン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：
start-stop	プロセスの開始時に "start" accounting 通知を送信し、プロセスの終了時に "stop" accounting 通知を送信します。"start" アカウンティングレコードはバックグラ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す。
stop-only	要求されたユーザ プロセスの終了時に、"stop" アカウンティング通知を送信します。
none	この回線またはインターフェイスでアカウンティングサービスをディセーブルにします。

broadcast	（任意）複数の AAA サーバへのアカウン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。
group groupname	「AAA アカウンティングの方式」に記述されているキーワードの 1 つ以上を使用します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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* アカウンティング方式

キーワード	説明
group radius	**aaa group server radius** 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。
group tacacs+	**aaa group server tacacs+** 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。
group *group-name*	group-name サーバグループで定義したように、アカウンティングのための RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

「AAA アカウンティングの方式」の表では、**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 XE ソフトウェアは次の 2 つのアカウン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。各アカウンティングレ

コードにはアカウンティングの 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。各アカウンティングレコードにはアカウンティングの 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。

アカウンティングの方式リストは、アカウンティングの実行方法を定義します。名前付きアカウン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、アカウンティングは実行されません。

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

最小のアカウンティングの場合、**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 レコードアカウンティング通知を送信します。詳細なアカウンティングの場合、**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 アカウンティング通知を送信し、プロセスの終了時に stop アカウンティング通知を送信するようにできます。アカウンティングは 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ティングサービスをディセーブルにします。

AAA アカウンティ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、接続に関係する RADIUS アカウンティング属性または 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ティングレコードとしてレポートし、アカウンティングレコードはその後セキュリティサーバのアカウンティングログに保存されます。

（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ティング方式リストを定義しています。この例のアカウンティングサービスは TACACS+ セキュリティサーバによって提供され、stop-only 制限で特権レベル 15 コマンドに設定されています。

```
Device> enable
Device# configure terminal
Device(config)# aaa accounting commands 15 default stop-only group TACACS+
Device(config)# exit
```

次の例では、アカウンティングサービスが TACACS+ セキュリティサーバで提供され、stop-only 制限があるデフォルトの auth-proxy アカウンティ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ティングをアクティブにします。

```
Device> enable
Device# configure terminal
Device(config)# aaa new model
Device(config)# aaa authentication login default group TACACS+
Device(config)# aaa authorization auth-proxy default group TACACS+
Device(config)# aaa accounting auth-proxy default start-stop group TACACS+
Device(config)# exit
```

aaa accounting dot1x

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

aaa accounting dot1x {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**]}
no aaa accounting dot1x {*name* | **default** }

構文の説明

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

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド 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 Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# exit
```

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）アカウンティング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

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

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド 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 Fuji 16.9.2	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。

```
Device# 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.

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

aaa authentication dot1x

IEEE 802.1X 認証に準拠するポートで使用する認証、許可、およびアカウンティング（AAA）方式を指定するには、グローバル コンフィギュレーション モードで **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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# exit
```

aaa new-model

認証、認可、およびアカウンティング（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 Fuji 16.9.2	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、**aaa new-model** コマンドを削除するときは、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。

例

次に、AAA を初期化する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# exit
```

次に、VTY が設定済みで **aaa new-model** コマンドが削除された例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# line vty 0 15
Device(config-line)# login local
Device(config-line)# exit
Device(config)# no aaa new-model
Device(config)# exit
Device# show running-config | b line vty

line vty 0 4
```

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

関連コマンド

Command	Description
aaa accounting	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。
aaa authentication arap	TACACS+ を使用する ARAP の AAA 認証方式を有効にします。
aaa authentication enable default	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。
aaa authentication login	ログイン時の AAA 認証を設定します。
aaa authentication ppp	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。
aaa authorization	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

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

コマンド デフォルト

シングルホストモードがイネーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication host-mode multi-auth
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication host-mode multi-domain
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication host-mode multi-host
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication host-mode single-host
Device(config-if)# end
```

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 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 Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# authentication logging verbose
Device(config)# exit
```

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
authentication logging verbose	認証システ
dot1x logging verbose	802.1X シス
mab logging verbose	MAC 認証バ ルタリング

authentication mac-move permit

デバイス上での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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、認証済みホストをデバイス上の認証対応ポート（MAC 認証バイパス（MAB）、802.1X、または Web-auth）間で移動することができます。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、デバイス上で MAC 移動をイネーブルにする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# authentication mac-move permit
Device(config)# exit
```

関連コマンド

コマンド	説明
access-session mac-move deny	デバイスで MAC 移動をディセーブルに
authentication event	特定の認証イベントのアクションを設定
authentication fallback	IEEE 802.1X 認証をサポートしないクラ証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャモードを設定し
authentication open	ポートでオープンアクセスをイネーブル

コマンド	説明
authentication order	ポートで使用する認証方式の順序を設定し
authentication periodic	ポートの再認証をイネーブルまたはディセ
authentication port-control	ポートの認証ステートの手動制御をイネー
authentication priority	ポートプライオリティリストに認証方式を
authentication timer	802.1X 対応ポートのタイムアウトパラメー
authentication violation	新しいデバイスがポートに接続するか、ポ るときに、新しいデバイスがポートに接続し
show authentication	デバイスの認証マネージャイベントに関す

authentication priority

プライオリティリストに認証方式を追加するには、インターフェイス コンフィギュレーション モードで **authentication priority** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

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

構文の説明

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

コマンド デフォルト

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

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、デバイス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 番めの認証方式として設定する方法を示します。

```
Device(config-if)# authentication priority dot1x webauth
```

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

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/1/2
Device(config-if)# authentication priority mab webauth
Device(config-if)# end
```

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event fail	認証マネージャが認証エラーを認識されないユーザクレデ 定します。
authentication event no-response action	認証マネージャが認証エラーを応答のないホストの結果と
authentication event server alive action reinitialize	以前に到達不能であった認証、許可、アカウンティングサー ジャセッションを再初期化します。
authentication event server dead action authorize	認証、許可、アカウンティングサーバが到達不能になった します。
authentication fallback	Web 認証のフォール バック方式をイネーブルにします。
authentication host-mode	ホストの制御ポートへのアクセスを許可します。
authentication open	ポートでオープンアクセスをイネーブルにします。
authentication order	認証マネージャがポート上のクライアントの認証を試みる
authentication periodic	ポートの自動再認証をイネーブルにします。
authentication port-control	制御ポートの許可ステートを設定します。
authentication timer inactivity	機能しない認証マネージャセッションを強制終了するまで
authentication timer reauthenticate	認証マネージャが許可ポートの再認証を試みる間隔を指定
authentication timer restart	認証マネージャが無許可ポートの認証を試みる間隔を指定
authentication violation	ポート上でセキュリティ違反が生じた場合に取るアクショ
mab	ポートの MAC 認証バイパスをイネーブルにします。
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を
show authentication sessions	現在の認証マネージャセッションに関する情報を表示しま

コマンド	説明
show authentication sessions interface	特定のインターフェイスの認証マネージャに関する情報

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

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

コマンド デフォルト

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

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation shutdown
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
```

```
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation restrict
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation protect
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation replace
Device(config-if)# end
```

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

cisp enable

デバイス上で Client Information Signalling Protocol（CISP）をイネーブルにして、サプリカントデバイス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デバイスのサプ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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

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

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

- VLAN が異なる 2 台のデバイスに設定されていないこと。同じドメインに VTP サーバが 2 台存在することがこの状態の原因になることがあります。
- 両方のデバイスで、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。

```
Device> enable
Device# configure terminal
Device(config)# cisp enable
Device(config)# exit
```

関連コマンド

コマンド	説明
dot1x credentialsプロファイル	プロファイルをサプリカントデバイスに設
dot1x supplicant force-multicast	802.1X サプリカントがマルチキャストパケ に強制します。
dot1x supplicant controlled transient	802.1X サプリカントによる制御アクセスを

コマンド	説明
show cisp	指定されたインターフェイスの CISP 情

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

interface-id	インターフェイスを指定します。
vlan list	（任意）再びイネーブルにする VLAN のリストを 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（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

例

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

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

関連コマンド

コマンド	説明
errdisable detect cause	特定の原因、またはすべての す。
errdisable recovery	回復メカニズム変数を設定し
show errdisable detect	errdisable 検出ステータスを表
show errdisable recovery	errdisable 回復タイマーの情報
show interfaces status err-disabled	errdisable ステートになってい 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
address *mac-addr*	（任意）指定されたダイナミック MAC アド
interface *interface-id*	（任意）指定された物理ポートまたはポート
vlan *vlan-id*	（任意）指定された VLAN のすべてのダイナ です。
move update	MAC アドレステーブルの move-update カウ
notification	履歴テーブルの通知をクリアし、カウンタを

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 Fuji 16.9.2	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** 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。

```
Device> enable
Device# clear mac address-table dynamic address 0008.0070.0007
```

関連コマンド

コマンド	説明
mac address-table notification	MAC アドレス通知機能をイネーブルにします。

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

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 Fuji 16.9.2	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
mka policy	MKA ポリシーを設定します。
delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。
send-secure-announcements	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。
ssci-based-on-sci	SCI に基づいて SSCI を計算します。
use-updated-eth-header	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。

crypto pki trustpool import

既存の認証局（CA）証明書バンドルを更新または交換するために CA 証明書バンドルを公開キーインフラストラクチャ（PKI）トラストプールにインポート（ダウンロード）するには、グローバル コンフィギュレーション モードで **crypto pki trustpool import** コマンドを使用します。設定されたパラメータをすべて削除するには、このコマンドの **no** 形式を使用します。

crypto pki trustpool import {**ca-bundle** | **clean** [{**terminal** | **url** *url*}] | **terminal** | **url** *url*}
no crypto pki trustpool import {**ca-bundle** | **clean** [{**terminal** | **url** *url*}] | **terminal** | **url** *url*}

構文の説明

ca-bundle	トラストプールポリシーで設定されている CA 証明書バンドルをインポートします。
clean	新しい証明書をダウンロードする前に、ダウンロード済みの PKI トラストプール証明書を削除します。既存の CA 証明書バンドルの端末設定を削除する場合はオプションの **terminal** キーワードを使用し、URL ファイルシステム設定を削除する場合は **url** キーワードと *url* 引数を使用します。
terminal	CA 証明書バンドルをプライバシー強化メール（PEM）の形式で端末からカットアンドペーストでインポートします。
url *url*	指定した URL から CA 証明書バンドルをインポートします。

コマンド デフォルト

PKI トラストプール機能が有効になっています。PKI トラストプール内の組み込みの CA 証明書バンドルがデバイスで使用されます。このバンドルは自動的に更新されます。

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 Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

PKI トラストプール証明書は自動的に更新されます。PKI トラストプール証明書が最新でない場合は、**crypto pki trustpool import** コマンドを使用して別の場所から更新します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Cryptography』ホワイトペーパーを参照してください。

url 引数で CA の URL ファイルシステムを指定または変更します。次の表に、使用可能な URL ファイルシステムを示します。

表 *2 : URL* ファイルシステム

ファイルシステム	説明
archive:	アーカイブファイルシステムからインポートします。
cns:	クラスタ名前空間（CNS）ファイルシステムからインポートします。
disk0:	disc0 ファイルシステムからインポートします。
disk1:	disc1 ファイルシステムからインポートします。
ftp:	FTP ファイルシステムからインポートします。
http:	HTTP ファイルシステムからインポートします。URL は次の形式にする必要があります。 • http://*CAname*:80：*CAname* はドメインネームシステム（DNS）です。 • http://*ipv4-address*:80：たとえば、http://10.10.10.1:80 のようになります。 • http://*[ipv6-address]*:80：たとえば、http://[2001:DB8:1:1::1]:80 のようになります。URL 内の IPv6 アドレスは 16 進数表記とし、括弧で囲む必要があります。
https:	HTTPS ファイルシステムからインポートします。URL は HTTP: ファイルシステムの形式と同じ形式にする必要があります。
null:	null ファイルシステムからインポートします。
nvram:	NVRAM ファイルシステムからインポートします。
pram:	パラメータ ランダムアクセス メモリ（PRAM）ファイルシステムからインポートします。
rcp:	リモートコピープロトコル（RCP）ファイルシステムからインポートします。
scp:	Secure Copy Protocol（SCP）ファイルシステムからインポートします。
snmp:	Simple Network Management Protocol（SNMP）ファイルシステムからインポートします。
system:	システムファイルからインポートします。
tar:	UNIX TAR ファイルシステムからインポートします。
tftp:	TFTP ファイルシステムからインポートします。 （注） URL は tftp://*CAname/filespecification* の形式にする必要があります。

ファイルシステム	説明
tmpsys:	Cisco IOS tmpsys ファイルシステムからインポートします。
unix:	UNIX ファイルシステムからインポートします。
xmodem:	xmodem 簡易ファイル転送プロトコルシステムからインポートします。
ymodem:	ymodem 簡易ファイル転送プロトコルシステムからインポートします。

例

次に、ダウンロード済みのすべての PKI トラストプール CA 証明書を削除してから、新しい CA 証明書バンドルをダウンロードして PKI トラストプール内の CA 証明書を更新する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto pki trustpool import clean
```

次に、ダウンロード済みの PKI トラストプール CA 証明書は削除せずに、新しい CA 証明書バンドルをダウンロードして PKI トラストプール内のすべての CA 証明書を更新する例を示します。

```
Device(config)# crypto pki trustpool import url
http://www.cisco.com/security/pki/trs/ios.p7b
```

関連コマンド

コマンド	説明
crypto pki trustpool policy	PKI トラストプール ポリシー パラメータを設定します。
show crypto pki trustpool	デバイスの PKI トラストプール証明書を表示し、オプションで PKI トラストプールポリシーを表示します。

debug aaa dead-criteria transaction

認証、許可、およびアカウンティング（AAA）の dead-criteria ランザクション値を表示するには、**debugaaadead-criteriatransaction** コマンドを特権 EXEC モードで使用します。dead-criteria のデバッ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。

debug aaa dead-criteria transaction
no debug aaa dead-criteria transaction

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

コマンドが設定されていない場合、デバッグはオンになりません。

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 Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

dead-criteriaトランザクションの値は、AAAトランザクションごとに異なる場合があります。表示される可能性のある値の一部は、推定される未処理のトランザクション、再送信の試行、および dead 検出間隔です。これらの値については、次の表で説明します。

例

次に、特定のサーバグループの dead-criteria トランザクションの情報の例を示します。

```
Device> enable
Device# debug aaa dead-criteria transaction

AAA Transaction debugs debugging is on
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Retransmit Tries: 10, Current Tries: 3,
Current Max Tries: 10
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Dead Detect Interval: 10s, Elapsed Time:
 317s, Current Max Interval: 10s
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Estimated Outstanding Transaction: 6, Current Max
 Transaction: 6
```

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 *3 : debug aaa dead-criteria transaction* フィールドの説明

フィールド	説明
AAA/SG/TRANSAC	AAA サーバグループ トランザクション。
Computed Retransmit Tries	サーバが dead としてマークされるまでの、現在計算されている再送信回数。
Current Tries	最後の有効な応答以降の連続失敗回数。

フィールド	説明
Current Max Tries	最後に成功したトランザクション以降の最大試行回数。
Computed Dead Detect Interval	サーバが dead としてマークされる前に経過する可能性がある非アクティブ期間（最後の正常なトランザクションからの秒数）。非アクティブ期間は、live と見なされるサーバにランザクションが送信されたときに開始されます。dead 検出間隔は、デバイスがサーバを dead としてマークする前に、サーバからの応答をデバイスが待機する期間です。
経過時間（Elapsed Time）	最後の有効な応答以降に経過した時間。
Current Max Interval	最後に成功したトランザクション以降の非アクティブ期間の最大値。
Estimated Outstanding Transaction	サーバに関連付けられているトランザクションの推定数。
Current Max Transaction	最後に成功したトランザクション以降の最大トランザクション。

関連コマンド

コマンド	説明
radius-server dead-criteria	RADIUS サーバをデッド状態と指定するための条件のいずれかまたは両方を、指定した定数で適用します。
show aaa dead-criteria	AAA サーバの dead-criteria 検出情報を表示します。

debug umbrella

Cisco Umbrella 統合機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug umbrella** コマンドを使用します。デバッ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。

debug umbrella {**config** | **device-registration** | **dnscrypt** | **redundancy**}
no debug umbrella {**config** | **device-registration** | **dnscrypt** | **redundancy**}

構文の説明

config	設定のデバッグをイネーブルにします。
device-registration	デバイス登録のデバッグをイネーブルにします。
dnscrypt	DNSCrypt のデバッグをイネーブルにします。
redundancy	冗長性のデバッグをイネーブルにします。

コマンド デフォルト

デバッグはディセーブルです。

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 Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、Cisco Umbrella の設定のデバッグをイネーブルにする例を示します。

```
Device> enable
Device# debug umbrella config

Umbrella config debugging is on

Device# configure terminal
Device(config)# interface gigabitethernet 1/0/12
Device(config-if)# umbrella in test

*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Umbrella token configured, so set mode as TOKEN
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:check user configured resolver count
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Umbrella interface with no direct cloud access
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Umbrella mandatory parameter 'token' or
'api-key/secret/orgid' configured
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Processing is umbrella enabled check
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Is umbrella enabled check failed:sw idb info not
found
*Nov 27 08:34:41.088: UMBRELLA-CONFIG:Send the interface info to device registration
proces
*Nov 27 08:34:41.089: UMBRELLA-CONFIG:Add interface GigabitEthernet1/0/12 request sent
to DP
*Nov 27 08:34:41.089: UMBRELLA-CONFIG:Configured 'umbrella in test' on interface
GigabitEthernet1/0/12
```

```
*Nov 27 08:34:41.089: UMBRELLA-CONFIG:Cannot add domain patterns to DSA: Nothing to add
```

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 Fuji 16.9.2	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
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。
send-secure-announcements	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。
ssci-based-on-sci	SCI に基づいて SSCI を計算します。
use-updated-eth-header	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ないようにするには、MAC アクセスリスト拡張コンフィギュレーション モードで **deny** コマンドを使用します。名前付き MAC アクセス リストから拒否条件を削除するには、このコマンドの **no** 形式を使用します。

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

構文の説明

any	すべての送信元または宛先 MAC アドレス
host *src-MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット アドレスが定義されたアドレスに一致す フィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット レスが定義されたアドレスに一致する場 は拒否されます。
type mask	（任意）パケットの EtherType 番号と、E して、パケットのプロトコルを識別しま type には、0 ～ 65535 の 16 進数を指定で mask は、一致をテストする前に EtherTyp です。
aarp	（任意）データリンク アドレスをネットワ AppleTalk Address Resolution Protocol を指
amber	（任意）EtherType DEC-Amber を指定しま
appletalk	（任意）EtherType AppleTalk/EtherTalk を
dec-spanning	（任意）EtherType Digital Equipment Corpo ます。
decnet-iv	（任意）EtherType DECnet Phase IV プロト
diagnostic	（任意）EtherType DEC-Diagnostic を指定

dsm	（任意）EtherType DEC-DSM を指定し
etype-6000	（任意）EtherType 0x6000 を指定しま
etype-8042	（任意）EtherType 0x8042 を指定しま
lat	（任意）EtherType DEC-LAT を指定し
lavc-sca	（任意）EtherType DEC-LAVC-SCA を
lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ ケットのプロトコルを指定します。 *mask* は、一致をテストする前に LSAP です。
mop-console	（任意）EtherType DEC-MOP Remote C
mop-dump	（任意）EtherType DEC-MOP Dump を
msdos	（任意）EtherType DEC-MSDOS を指定
mumps	（任意）EtherType DEC-MUMPS を指定
netbios	（任意）EtherType DEC-Network Basic す。
vines-echo	（任意）Banyan Systems による EtherTy Echo を指定します。
vines-ip	（任意）EtherType VINES IP を指定し
xns-idp	（任意）10 進数、16 進数、または 8 進 Network Systems（XNS）プロトコル ス
cos *cos*	（任意）プライオリティを設定するた を指定します。CoS に基づくフィルタ す。**cos** オプションが設定されている 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 アクセスリスト拡張コンフィギュレーション（config-ext-macl）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

MAC アクセスリスト拡張コンフィギュレーション モードを開始するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

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

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

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

表 *4: IPX* フィルタ基準

IPX カプセル化タイプ		**フィルタ基準**
Cisco IOS XE 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。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
Device(config-ext-macl)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
Device(config-ext-macl)# end
```

次に、EtherType 0x4321 のすべてのパケットを拒否する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# deny any any 0x4321 0
Device(config-ext-macl)# end
```

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

関連コマンド

コマンド	説明
mac access-list extended	非 IP トラフィック用に MAC アドレス
permit	MAC アクセスリスト コンフィギュレー 条件が一致した場合に非 IP トラフィッ
show access-lists	デバイスに設定されたアクセス制御リス

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。この指定を削除するには、このコマンドの **no** 形式を使用します。

device-role {**node** | **switch**}
no 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デバイスに設定します。

コマンド デフォルト

デバイスのロールはノードです。

コマンド モード

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
Device(config-ipv6-snooping)# end
```

device-role（IPv6 ND インスペクション）

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）インスペクション ポリシー コンフィギュレーション モードで **device-role** コマンドを使用します。

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

構文の説明

host	接続されたデバイスのロールをホストに設定します。
switch	接続されたデバイスのロールをスイッチに設定します。

コマンド デフォルト

デバイスのロールはホストです。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション（config-nd-inspection）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 インスペクション ポリシー コンフィギュレーション モードにして、デバイスをホストとして設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)#  ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
Device(config-nd-inspection)# end
```

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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す。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。

```
Device> enable
Device# configure terminal
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
Device(config-device-tracking)# end
```

dnscrypt（パラメータマップ）

シスコデバイスと Cisco Umbrella 統合機能の間の通信を認証するためにドメインネームシステム（DNS）パケット暗号化をイネーブルにするには、パラメータマップタイプ検査コンフィギュレーション モードで **dnscrypt** コマンドを使用します。DNS パケット暗号化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。

dnscrypt
no dnscrypt

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

Umbrella モードの DNS パケット暗号化は設定されていません。

コマンド モード

パラメータマップタイプ検査コンフィギュレーション（config-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

DNSCrypt を使用する場合は、DNS 要求パケットサイズが 512 バイトよりも大きくなります。これらのパケットが中間デバイスで許可されていることを確認します。そうしないと、応答が目的の受信者に到達しない可能性があります。

例

次に、DNS パケット暗号化をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type umbrella global
Device(config-profile)# dnscrypt
```

関連コマンド

コマンド	説明
parameter-map type umbrella global	Umbrella モードでパラメータマップタイプを設定します。

dot1x critical（グローバル コンフィギュレーション）

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

dot1x critical eapol

構文の説明

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

コマンド デフォルト

eapol はディセーブルです

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

次に、デバイスがクリティカルポートを正常に認証すると、デバイスが EAPOL 成功メッセージを送信するように指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# dot1x critical eapol
Device(config)# exit
```

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、デバイススタックまたはスタンドアロンデバイス上で **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 Fuji 16.9.2	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。

次に、verbose 802.1X システムメッセージをフィルタリングする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# dot1x logging verbose
Device(config)# exit
```

関連コマンド

コマンド	説明
authentication logging verbose	認証システムメッセージから詳
dot1x logging verbose	802.1X システムメッセージから
mab logging verbose	MAC 認証バイパス（MAB）シ

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

コマンド デフォルト

PAE タイプは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

IEEE 802.1X 認証をポート上でディセーブルにする場合は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

dot1x port-control インターフェイス コンフィギュレーション コマンドを入力するなどしてポート上で IEEE 802.1X 認証を設定した場合、デバイス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プリカントとして動作するように設定されている例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# dot1x pae supplicant
Device(config-if)# end
```

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、BPCU ガードがイネーブルにされたオーセンティケータスイッチにサプリカントのデバイスを接続する場合、オーセンティケータのポートはサプリカントスイッチが認証する前にスパニングツリープロトコル（STP）のブリッジプロトコルデータユニット（BPDU）を受信した場合、errdisable 状態になる可能性があります。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** 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** 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、サプリカントデバイスで **dot1x supplicant controlled transient** コマンドを使用することを推奨します。

次に、認証の間にデバイスの 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。

```
Device> enable
Device# configure terminal
Device(config)# dot1x supplicant controlled transient
Device(config)# exit
```

dot1x supplicant force-multicast

サプ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

サプリカントデバイスは、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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

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

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

```
Device> enable
Device# configure terminal
Device(config)# dot1x supplicant force-multicast
Device(config)# end
```

関連コマンド

コマンド	説明
cisp enable	デバイス上で CISP をイネー タとして機能するようにしま
dot1x credentials	ポートに 802.1X サプリカン
dot1x pae supplicant	インターフェイスがサプリカ

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、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 Fuji 16.9.2	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。

```
Device> enable
Device# dot1x test eapol-capable interface gigabitethernet1/0/13

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

関連コマンド

コマンド	説明
dot1x test timeout *timeout*	IEEE 802.1X 準備クエリーにされるタイムアウトを設定

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、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

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

コマンド デフォルト

デフォルト設定は 10 秒です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# 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 running-config** コマンドを入力します。

関連コマンド

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

dot1x timeout

再試行タイムアウトの値を設定するには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。再試行タイムアウト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

auth-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。
held-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。
quiet-period *seconds*	認証情報の交換に失敗したあと、クライアントの再認証を試みるまでにオーセンティケータ（サーバ）が待機状態（HELD 状態）を続ける秒数を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。
ratelimit-period *seconds*	動作の不正なクライアント PC（たとえば、デバイス処理電力の無駄につながる、EAP-START パケットを送信する PC）から送信される EAP-START パケットを抑制します。 • オーセンティケータはレート制限時間中、認証に成功したクライアントからの EAPOL-Start パケットを無視します。 • 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。
server-timeout *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 • 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 サーバが指定時間内に 802.1X パケットへの応答を送信しない場合、パケットは再度送信されます。

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

コマンド デフォルト

定期的な再認証と定期的なレート制限が行われます。

コマンド モード

グローバル コンフィギュレーション（config）

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 Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

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

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

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

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。

```
Device> enable
Device(config)# configure terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x timeout auth-period 2000
Device(config-if)# dot1x timeout held-period 2400
Device(config-if)# dot1x timeout quiet-period 600
Device(config-if)# dot1x timeout start-period 90
Device(config-if)# dot1x timeout supp-timeout 300
Device(config-if)# dot1x timeout tx-period 60
Device(config-if)# dot1x timeout server-timeout 60
Device(config-if)# end
```

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** | **ipv6** }] { **radius source-interface** *interface-name* | **vrf forwarding** *forwarding-table-name* } | **match-server-identity** { **email-address** *email-address* | **hostname** *hostname* | **ip-address** *ip-address* } | **port** *port-number* | **retries** *number-of-connection-retries* | **trustpoint** { **client** *trustpoint name* | **server** *trustpoint name* }

no dtls

構文の説明

connectiontimeout *connection-timeout-value*	（任意）DTLS 接続タイムアウト値を設定します。
idletimeout *idle-timeout-value*	（任意）DTLS アイドルタイムアウト値を設定します。
[**ip	ipv6**] {**radius source-interface** *interface-name*	**vrf forwarding** *forwarding-table-name*}	（任意）IP または IPv6 送信元パラメータを設定します。
match-server-identity { **email-address** *email-address*	**hostname** *host-name*	**ip-address** *ip-address*}	RadSec 認定検証パラメータを設定します。
port *port-number*	（任意）DTLS ポート番号を設定します。
retries *number-of-connection-retries*	（任意）DTLS接続再試行の回数を設定します。
trustpoint {**client** *trustpoint name*	**server** *trustpoint name*}	（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 Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.10.1	**match-server-identity**キーワードが導入されました。
Cisco IOS XE Amsterdam 17.1.1	**ipv6**キーワードが導入されました。

使用上のガイドライン

認証、許可、およびアカウンティング（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
show aaa servers	DTLS サーバに関連する情報を表示します。
clear aaa counters servers radius {*server id* | **all**}	RADIUS DTLS 固有の統計情報をクリアします。
debug radius dtls	RADIUS DTLS 固有のデバッグを有効にします。

有効化パスワード

さまざまな権限レベルへのアクセスを制御するローカルパスワードを設定するには、グローバル コンフィギュレーション モードで **enable password** コマンドを使用します。ローカルパスワードの制御アクセスを削除するには、このコマンドの **no** 形式を使用します。

enable password [**level** *level*] {[**0**] *unencrypted-password* | [*encryption-type*] *encrypted-password*}
no enable password [**level** *level*]

構文の説明

level *level*	（任意）パスワードが適用されるレベルを指定します。0 ～ 15 の数字 権限レベルを指定できます。レベル 1 が通常のユーザ EXEC モード コマンドまたはコマンドの **no** 形式で指定されていない場合、権限レ になります。
0	（任意）暗号化されていないクリアテキストパスワードを指定しま ア ハッシュ アルゴリズム（SHA）256 シークレットに変換されてデ
unencrypted-password	イネーブルモードを開始するためのパスワードを指定します。
encryption-type	（任意）パスワードの暗号化に使用するシスコ独自のアルゴリズム。 る場合、入力する次の引数は暗号化されたパスワード（すでにシス 化されたパスワード）である必要があります。非表示のパスワード 7 を指定できます。
encrypted-password	別のデバイス設定からコピーした暗号化パスワード。

コマンド デフォルト

パスワード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（config）

コマンド履歴

リリース	変
Cisco IOS XE Fuji 16.9.2	こ し

使用上のガイドライン

enable password コマンドと **enable secret** コマンドのいずれも設定されていない場合、コンソールの回線パスワードが設定されていれば、コンソールの回線パスワードがすべての VTY（Telnet およびセキュアシェル（SSH））セッションのイネーブルパスワードとして機能します。

特定の権限レベルのパスワードを定義する場合は、**level** オプションを指定して **enable password** コマンドを使用します。レベルとパスワードを設定したら、このレベルにアクセスする必要のあるユーザとパスワードを共有します。各レベルでアクセスできるコマンドを指定するには、**privilege level** コンフィギュレーション コマンドを使用します。

通常、暗号化タイプは、シスコデバイスによってすでに暗号化されているパスワードをコピーしてこのコマンドに貼り付ける場合にのみ入力します。

注意 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再び特権EXECモードを開始することはできません。以前に暗号化されたパスワードを忘れた場合、回復することはできません。

service password-encryption コマンドが設定されている場合、**more nvram:startup-config** コマンドを実行すると、**enable password** コマンドで作成するパスワードが暗号化された形式で表示されます。

service password-encryption コマンドを使用して、パスワードの暗号化を有効または無効にすることができます。

イネーブルパスワードの定義は次のとおりです。

- 数字、大文字、小文字を組み合わせた 1 ～ 25 文字の英数字を含める必要があります。
- 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。
- パスワードを作成するときに、Crtl+V キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、*abc?123* というパスワードを作成するには、次の手順を実行します。

  1. **abc** を入力します。
  2. **Crtl-v** を押します。
  3. **?123** を入力します。

（注） システムから **enable password** コマンドを入力するように求められた場合、疑問符の前に Ctrl+V を入力する必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。

例

次に、特権レベル 2 のパスワード pswd2 を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 pswd2
```

次に、暗号化タイプ 7 を使用して、デバイスのコンフィギュレーション ファイルからコピーした権限レベル 2 の暗号化パスワード 1i5Rkls3LoyxzS8t9 を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

関連コマンド

Command	Description
enable secret	**enable password** コマンドよりも強化したセキュ す。
service password-encryption	パスワードを暗号化します。
more nvram:startup-config	NVRAM に保管されている、またはCONFIG_FI されているスタートアップ コンフィギュレーシ す。
privilege level	ユーザの権限レベルを設定します。

enable secret

enable password コマンドよりも強化したセキュリティレイヤを指定するには、グローバル コンフィギュレーション モードで **enable secret** コマンドを使用します。イネーブルシークレット機能をオフにするには、このコマンドの **no** 形式を使用します。

enable secret [**level** *level*] {[**0**] *unencrypted-password* | *encryption-type encrypted-password*}
no enable secret [**level** *level*] [*encryption-type encrypted-password*]

構文の説明

level *level*	（任意）パスワードが適用されるレベルを指定します。1 ～ 15 の数字を権限レベルを指定できます。レベル 1 が通常のユーザ EXEC モード権限ドまたはコマンドの **no** 形式で指定されていない場合、権限レベルはデフす。
0	（任意）暗号化されていないクリアテキストパスワードを指定します。ハッシュ アルゴリズム（SHA）256 シークレットに変換されてデバイス
unencrypted-password	ユーザがイネーブルモードを開始するためのパスワードを指定します。**enable password** コマンドで作成したパスワードとは異なるものにする必
encryption-type	パスワードのハッシュに使用するシスコ独自のアルゴリズム。 • **5**：メッセージダイジェストアルゴリズム 5（MD5）で暗号化されたします。 • **8**：パスワードベースキー派生関数 2（PBKDF2）の SHA-256 でハッシトを指定します。 • **9**：スクリプトでハッシュされたシークレットを指定します。
encrypted-password	別のデバイス設定からコピーしたハッシュパスワード。

コマンド デフォルト

パスワード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（config）

コマンド履歴

リリース	変更内
Cisco IOS XE Fuji 16.9.2	このコした。

使用上のガイドライン

enable password コマンドと **enable secret** コマンドのいずれも設定されていない場合、コンソールの回線パスワードが設定されていれば、コンソールの回線パスワードがすべての VTY（Telnet およびセキュアシェル（SSH））セッションのイネーブルパスワードとして機能します。

enable secret コマンドは、**enable password** パスワードよりも強化したセキュリティレイヤを指定するために使用します。**enable secret** コマンドでは、不可逆的な暗号化機能を使用してパスワードを保存することでセキュリティを向上させます。この追加のセキュリティ暗号化レイヤは、パスワードがネットワークで送信される環境や TFTP サーバに保存される環境において役立ちます。

通常、暗号化タイプは、デバイスのコンフィギュレーションファイルからコピーした暗号化パスワードをこのコマンドに貼り付ける場合にのみ入力します。

注意 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。以前に暗号化されたパスワードを忘れた場合、回復することはできません。

enable password コマンドと **enable secret** コマンドに同じパスワードを使用した場合、推奨されない方法であることを警告するエラーメッセージが表示されますが、パスワードは受け入れられます。ただし、同じパスワードを使用すると、**enable secret** コマンドによって提供される追加のセキュリティが損なわれます。

（注） **enable secret** コマンドを使用してパスワードを設定した後、 **enable password** コマンドを使用して設定したパスワードは、**enable secret** が無効になっている場合にのみ機能します。また、いずれの方法で暗号化したパスワードも、忘れた場合は回復できません。

service password-encryption コマンドが設定されている場合、**more nvram:startup-config** コマンドを実行すると、作成するパスワードが暗号化された形式で表示されます。

service password-encryption コマンドを使用して、パスワードの暗号化を有効または無効にすることができます。

イネーブルパスワードの定義は次のとおりです。

- 数字、大文字、小文字を組み合わせた 1 ～ 25 文字の英数字を含める必要があります。
- 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。
- パスワードを作成するときに、Crtl+V キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、*abc?123* というパスワードを作成するには、次の手順を実行します。

  1. **abc** を入力します。
  2. **Crtl-v** を押します。
  3. **?123** を入力します。

（注） システムから **enable password** コマンドを入力するように求められた場合、疑問符の前に Ctrl+V を入力する必要はなく、パスワードのプロンプトにそのまま **abc?123** と入力できます。

例

次に、**enable secret** コマンドを使用してパスワードを指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable secret password
```

enable secret コマンドを使用してパスワードを指定した後、ユーザはこのパスワードを入力してアクセスする必要があります。**enable password** コマンドを使用して設定されたパスワードは機能しなくなります。

```
Password: password
```

次に、暗号化タイプ 4 を使用して、デバイスのコンフィギュレーション ファイルからコピーした権限レベル 2 の暗号化パスワード 1FaD0$Xyti5Rkls3LoyxzS8 を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 4 $1$FaD0$Xyti5Rkls3LoyxzS8
```

次に、ユーザが **enable secret 4** *encrypted-password* コマンドを入力したときに表示される警告メッセージの例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

WARNING: Command has been added to the configuration but Type 4 passwords have been
deprecated.
Migrate to a supported password type

Device(config)# end
Device# show running-config | inc secret

enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

関連コマンド

コマンド	説明
enable password	さまざまな権限レベルへのアクセスを制御するロ設定します。

コマンド	説明
more nvram:startup-config	NVRAM に保管されている、またはCONFIG_F 定されているスタートアップ コンフィギュレ します。
service password-encryption	パスワードを暗号化します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

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

設定を確認するには、**show running-config** 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。

```
Device> enable
Device# configure terminal
Device(config)# epm access-control open
Device(config)# exit
```

関連コマンド

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

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 Fuji 16.9.2	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
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDUの送信で遅延保護を使用するようにMKAを設定します。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。
send-secure-announcements	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。
ssci-based-on-sci	SCI に基づいて SSCI を計算します。
use-updated-eth-header	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

IP アクセスリストまたはオブジェクトグループ アクセス コントロール リスト（ACL）を名前または番号によって定義する場合、または、IPヘルパーアドレス宛先をもつパケットのフィルタリングを有効にする場合は、グローバル コンフィギュレーション モードで **ip access-list** コマンドを使用します。IP アクセスリストまたはオブジェクトグループ ACL を削除する場合、または、IPヘルパーアドレス宛先をもつパケットのフィルタリングを無効にする場合は、このコマンドの **no** 形式を使用します。

ip access-list {{**extended** | **resequence** | **standard**}{*access-list-numberaccess-list-name*} | **helper egress check** | **log-update threshold** *threshold-number* | **logging** {**hash-generation** | **interval** *time*} | **persistent** | **role-based** *access-list-name*}
ip access-list {{**extended** | **resequence** | **standard**}{*access-list-numberaccess-list-name*} | **helper egress check** | **log-update threshold** | **logging** {**hash-generation** | **interval**} | **persistent** | **role-based** *access-list-name*}

構文の説明

standard	標準 IP アクセスリストを指定します。
resequence	並べ直した IP アクセスリストを指定します。
extended	拡張 IP アクセスリストを指定します。オブジェクトグループ ACL の場合は必須です。
access-list-name	IP アクセスリストまたはオブジェクトグループ ACL の名前。この名前にはスペースまたは引用符を含めることはできず、番号付けされたアクセスリストと紛らわしくならないよう、英文字で始める必要があります。
access-list-number	アクセス リストの番号。 • 標準 IP アクセスリストの範囲は 1 ー 99 または 1300 ー 1999 です。 • 拡張 IP アクセスリストの範囲は 100 ー 199 または 2000 ー 2699 です。
helper egress check	IP ヘルパー機能を介して宛先サーバアドレスにリレーされるトラフィックについて、インターフェイスに適用される発信アクセスリストの許可または拒否の照合機能を有効にします。
log-update	アクセスリストログの更新を制御します。
threshold *threshold-number*	アクセスリストログのしきい値を設定します。指定できる範囲は 0 ～ 2147483647 です。
logging	アクセスリストのロギングを制御します。
hash-generation	syslog ハッシュコードの生成を有効にします。

interval *time*	アクセスリストのロギング間隔をミリ秒単位で設定します。指定できる範囲は 0 ～ 2147483647 です。
persistent	アクセス コントロール エントリ（ACE）のシーケンス番号は、リロード後も保持されます。 （注） これはデフォルトで有効であり、無効にすることはできません。
role-based	ロールベースの IP アクセスリストを指定します。

コマンド デフォルト

IP アクセスリストまたはオブジェクトグループ ACL が定義されていないため、発信 ACL は IP ヘルパーによってリレーされたトラフィックを照合およびフィルタリングしません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

名前付きまたは番号付き IP アクセスリストまたはオブジェクトグループ ACL を設定するには、このコマンドを使用します。コマンドによって、デバイスはアクセスリスト コンフィギュレーション モードを開始します。ここで、**deny** コマンドおよび **permit** コマンドを使用して、拒否アクセス条件または許可アクセス条件を定義しなければなりません。

ip access-list コマンドで **standard** または **extended** のキーワードを指定することで、アクセスリスト コンフィギュレーション モードを開始したときに表示されるプロンプトが決定されます。オブジェクトグループ ACL を定義する場合は、**extended** キーワードを使用する必要があります。

オブジェクトグループと IP アクセスリスト、またはオブジェクトグループ ACL を個別に作成できます。つまり、まだ存在しないオブジェクトグループ名を使用できます。

ip access-group コマンドを使用して、アクセスリストをインターフェイスに適用します。

ip access-list helper egress check コマンドは、IP ヘルパーアドレス宛先をもつパケットの許可または拒否機能の発信 ACL マッチングを有効にします。このコマンドで発信拡張 ACL を使用すると、送信元または宛先の User Datagram Protocol（UDP）ポートに基づいて、IP ヘルパーリレートラフィックを許可または拒否できます。**ip access-list helper egress check** コマンドはデフォルトでは無効です。発信 ACL は、IP ヘルパーによってリレーされたトラフィックを照合およびフィルタリングしません。

例

次に、Internetfilter という名前の標準アクセスリストを定義する方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard Internetfilter
Device(config-std-nacl)# permit 192.168.255.0 0.0.0.255
```

```
Device(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Device(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

次に、プロトコル ポートが my_service_object_group で指定されたポートと一致する場合に、my_network_object_group 内のユーザからのパケットを許可するオブジェクトグループ ACL を作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended my_ogacl_policy
Device(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
 my_service_object_group any
Device(config-ext-nacl)# deny tcp any any
```

次に、ヘルパーアドレスの宛先をもつパケットで発信ACLフィルタリングを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list helper egress check
```

関連コマンド

Command	Description
deny	パケットを拒否する名前付き IP アクセスリストまたはオブジェクトグループ ACL の条件を設定します。
ip access-group	ACLまたはオブジェクトグループACLをインターフェイスまたはサービスポリシーマップに適用します。
object-group network	オブジェクトグループ ACL で使用するネットワーク オブジェクト グループを定義します。
object-group service	オブジェクトグループ ACL で使用するサービス オブジェクト グループを定義します。
permit	パケットを許可する名前付き IP アクセスリストまたはオブジェクトグループ ACL の条件を設定します。
show ip access-list	IP アクセスリストまたはオブジェクトグループ ACL の内容を表示します。
show object-group	設定されているオブジェクトグループに関する情報を表示します。

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 Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list role-based rbacl1
Device(config-rb-acl)# permit ip log
Device(config-rb-acl)# end
```

関連コマンド

コマンド	説明
permit ip log	設定されたエントリに一致するロギングを許可します。
show ip access-list	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 モードまた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 **ip admission** 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 *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（config-if）

フォールバックプロファイル コンフィギュレーション（config-fallback-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
Device(config-fallback-profile)# end
```

ip admission name

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

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

構文の説明

name	ネットワークアドミッション制御ルールの名前。
consent	認証プロキシ同意 Web ページを *admission-name* 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。
proxy http	Web 認証のカスタムページを設定します。
absolute-timer 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）。
inactivity-time 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）。
list	（任意）指定されたルールをアクセス コントロール リスト（ACL）に関連付けます。
acl	標準、拡張リストを指定のアドミッション制御ルールに適用します。値の範囲は 1～199、または拡張範囲で 1300 から 2699 です。
acl-name	名前付きのアクセスリストを指定のアドミッション制御ルールに適用します。
service-policy type tag	（任意）コントロール プレーン サービス ポリシーを設定できます。
service-policy-name	**policy-map type control tag***policyname* コマンド、キーワード、および引数を使用して設定されたコントロールプレーンタグのサービスポリシー。このポリシーマップは、タグを受信したときのホストでの処理を適用するために使用されます。

コマンド デフォルト

Web 認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

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

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

関連コマンド

コマンド	説明
dot1x fallback	IEEE 802.1X 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
fallback profile	Web 認証のフォールバック プロファイルを作成します。

コマンド	説明
ip admission	ポートで Web 認証をイネーブルにします。
show authentication sessions interface *interface* **detail**	Web 認証セッションのステータスに関する情報を表示します。
show ip admission	NAC のキャッシュされたエントリまたはNAC設定についての情報を表示します。

ip 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。

ip dhcp snooping database { **crashinfo:** *url* | **flash:** *url* | **ftp:** *url* | **http:** *url* | **https:** *url* | **rcp:** *url* | **scp:** *url* | **tftp:** *url* | **timeout** *seconds* | **usbflash0:** *url* | **write-delay** *seconds* }
no ip dhcp snooping database [**timeout** | **write-delay**]
abor

構文の説明

crashinfo:*url*	crashinfo 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。
flash:*url*	flash を使用して、エントリを格納するためのデータベースの URL を指定します。
ftp:*url*	FTP を使用して、エントリを格納するためのデータベースの URL を指定します。
http:*url*	HTTP を使用して、エントリを格納するためのデータベースの URL を指定します。
https:*url*	セキュア HTTP（HTTPS）を使用して、エントリを格納するためのデータベースの URL を指定します。
rcp:*url*	リモートコピー（RCP）を使用して、エントリを格納するためのデータベースの URL を指定します。
scp:*url*	セキュアコピー（SCP）を使用して、エントリを格納するためのデータベースの URL を指定します。
tftp:*url*	TFTP を使用して、エントリを格納するためのデータベースの URL を指定します。

timeout *seconds*	キャンセル 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。
usbflash0:*url*	USB 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。
write-delay *seconds*	ローカル DHCP スヌーピング データベースにデータが追加されてから、DHCP スヌーピングエントリを外部サーバに書き込みするまでの時間を指定します。有効値は 15 ～ 86,400 秒です。

コマンド デフォルト

DHCP スヌーピングデータベースは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)#  ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
Device(config)# exit
```

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。

```
evice> enable
Device# configure terminal
Device(config)#  ip dhcp snooping database write-delay 15
Device(config)# exit
```

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、デバイスのグローバル 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	デバイス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

デバイスの 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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 サブオプションはデバイスの MAC アドレスです。このコマンドを使用すると、デバイスのホスト名または 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。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping information option format remote-id hostname
Device(config)# exit
```

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# no ip dhcp snooping verify no-relay-agent-address
Device(config)# exit
```

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。

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

access-list-number	グローバル コンフィギュレーション コマンド **access-list** 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。
ipv4	セキュア HTTP サーバ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。
access-list-name	**ip access-list** コマンドで設定された標準 IPv4 アクセスリストの名前。
ipv6	セキュア HTTP サーバ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。

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 Fuji 16.9.2	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> enable
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
Device(config-std-nacl)# exit
```

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> enable
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
Device(config)# exit
```

関連コマンド

コマンド	説明
ip access-list	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。
ip http server	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

interface-name	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。
vrf *vrf-name*	（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 Fuji 16.9.2	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

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

コマンド デフォルト

IP 送信元バインディングは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

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

no 形式は、対応する IP ソース バインディング エントリを削除します。削除が正常に実行されるためには、すべての必須パラメータが正確に一致しなければなりません。各スタティック IP バインディング エントリは MAC アドレスと VLAN 番号がキーであることに注意してください。コマンドに既存の MAC アドレスと VLAN 番号が含まれる場合、別のバインディング エントリが作成される代わりに既存のバインディングエントリが新しいパラメータで更新されます。

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。

```
Device> enable
Device# configure terminal
Device(config) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
```

```
gigabitethernet1/0/1
Device(config)# exit
```

ip ssh source-interface

インターフェイスのIPアドレスをセキュアシェル（SSH）クライアントデバイスの送信元アドレスとして指定するには、グローバル コンフィギュレーション モードで**ip ssh source-interface** コマンドを使用します。送信元アドレスとして指定した IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

ip ssh source-interface *interface*
no ip ssh source-interface *interface*

構文の説明

interface	アドレスをSSHクライアントの送信元アドレスとして使用するインターフェイス。

コマンド デフォルト

宛先に最も近いインターフェイスのアドレスが送信元アドレスとして使用されます（最も近いインターフェイスは SSH パケットが送信される出力インターフェイスです）。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを指定することにより、SSH クライアントの送信元アドレスとして送信元インターフェイスの IP アドレスを使用するように強制できます。

例

次の例では、GigabitEthernet インターフェイス 1/0/1 に割り当てられた IP アドレスが SSH クライアントの送信元アドレスとして使用されます。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh source-interface GigabitEthernet 1/0/1
Device(config)# exit
```

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

mac-check	（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。
tracking	（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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source mac-check
```

```
Device(config-if)# end
```

設定を確認するには、**show ip verify source** 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

ipv6 *access-list-name*	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。 *access-list-name*：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。
match-local-traffic	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。
log-update threshold *threshold-in-msgs*	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。 *threshold-in-msgs*：生成されるパケット数。
role-based *list-name*	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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 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> enable
Device# configure terminal
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)# end
```

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 GigabitEthernet インターフェイス 0/1/2 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 番めのエントリは、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> enable
Device# configure terminal
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 gigabitethernet 0/1/2
```

```
Device(config-if)# ipv6 traffic-filter list2 out
Device(config-if)# end
```

ipv6 snooping policy

IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 snooping policy** コマンドを使用します。IPv6 スヌーピング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 snooping policy *snooping-policy*
no ipv6 snooping policy *snooping-policy*

構文の説明

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

コマンド デフォルト

IPv6 スヌーピング ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
```

```
Device(config-ipv6-snooping)# end
```

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 *name***macsec**
no key chain *name*[**macsec**]

構文の説明

name	キーを取得するために使用するキー チェーンの名前。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# key chain kc1 macsec
Device(config-keychain-macsec)# key 1000
Device(config-keychain-macsec)# cryptographic-algorithm aes-128-cmac
Device(config-keychain-macsec-key)# key-string fb63e0269e2768c49bab8ee9a5c2258f
Device(config-keychain-macsec-key)# end
Device#
```

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。

```
Device> enable
Device# configure terminal
Device(config)# key chain kc1 macsec
Device(config-keychain-macsec)# key 2000
Device(config-keychain-macsec)# cryptographic-algorithm aes-256-cmac
Device(config-keychain-macsec-key)# key-string c865632acb269022447c417504a1b
f5db1c296449b52627ba01f2ba2574c2878
Device(config-keychain-macsec-key)# end
Device#
```

key config-key password-encrypt

タイプ 6 の暗号キーをプライベート NVRAM に保存するには、グローバル コンフィギュレーション モードで **key config-key password-encrypt** コマンドを使用します。暗号化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 config-key password-encrypt [*text*]
no key config-key password-encrypt [*text*]

構文の説明

text （任意）**Password** または **master** キー。

（注） 事前共有キーがどこにも出力されないようにするために、*text* 引数は使用せず、代わりにインタラクティブモードを使用（**key config-key password-encrypt** コマンドを入力した後に **Enter** キーを使用）することを推奨します。

コマンド デフォルト

タイプ 6 パスワード暗号キーはプライベート NVRAM に保存されません。

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
Cisco IOS XE Fuji 16.9.2	こ し

使用上のガイドライン

CLI を使用して、プレーンテキストのパスワードをタイプ 6 形式で NVRAM に安全に保存できます。タイプ 6 のパスワードは暗号化されています。暗号化されたパスワード自体を、確認したり取得したりすることは可能ですが、それを復号化して実際のパスワードを特定することは困難です。**key config-key password-encrypt** コマンドを **password encryption aes** コマンドとともに使用すると、パスワードを設定してイネーブルにできます（キーの暗号化には対称キー暗号である高度暗号化規格（AES）が使用されます）。**key config-key password-encrypt** コマンドを使用して設定されたパスワード（キー）は、デバイス内のその他すべてのキーを暗号化するマスター暗号キーとして使用されます。

password encryption aes コマンドを設定する際、同時に **key config-key password-encrypt** コマンドを設定しないと、**show running-config** コマンドや **copy running-config startup-config** コマンドなどが設定されている起動時や不揮発性生成（NVGEN）プロセス中に次のようなメッセージが出力されます。

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

パスワードの変更

key config-key password-encrypt コマンドを使用してパスワード（マスターキー）が変更された場合、または再暗号化された場合には、リストレジストリから、タイプ 6 暗号が使用されているアプリケーションモジュールへ、変更前のキーと変更後のキーが渡されます。

パスワードの削除

key config-key password-encrypt コマンドを使用して設定されたマスターキーがシステムから削除されると、タイプ6のパスワードすべてが使用不可になるという内容の警告が出力されます（同時に、確認用のプロンプトも表示されます）。セキュリティ対策として、暗号化されたパスワードは、Cisco IOS ソフトウェアによって復号化されることはなくなります。ただし、すでに説明したように、パスワードを再暗号化することはできます。

⚠

注意 **key config-key password-encrypt** コマンドを使用して設定されたパスワードは、一度失われると回復できません。そのため、パスワードは安全な場所に保存しておくことを推奨します。

パスワード暗号化の設定解除

no password encryption aes コマンドを使用してパスワード暗号化の設定を解除しても、既存のタイプ 6 パスワードはすべて変更されずに残されます。**key config-key password-encrypt** コマンドを使用して設定したパスワード（マスターキー）があれば、アプリケーションで必要に応じてタイプ 6 パスワードを復号化できます。

パスワードの保存

（**key config-key password-encrypt** コマンドを使用して設定された）パスワードは誰にも「判読」できないため、デバイスからパスワードを取得する方法はありません。既存の管理ステーションでは、その内部にキーが格納されるよう強化されることで初めて、パスワードの内容を「知る」ことができます。その場合、パスワードは管理ステーション内部に安全に保存する必要があります。TFTP を使用して保存された設定は、スタンドアロンではないため、デバイスにはロードできません。設定をデバイスにロードする前後には、（**key config-key password-encrypt** コマンドを使用して）パスワードを手動で追加する必要があります。このパスワードは、保存された設定に手動で追加できます。ただし、それによって設定内のすべてのパスワードを誰もが復号化できるようになるため、手動によるパスワードの追加は行わないことを推奨します。

新規パスワードまたは不明パスワードの設定

入力またはカットアンドペーストした暗号文は、それがマスターキーに適合しない場合やマスターキーが存在しない場合でも、受理または保存されます。ただしこの場合にはアラートメッセージが表示されます。

```
“ciphertext>[for username bar>] is incompatible with the configured master key.”
```

マスターキーを新規に設定すると、プレーンテキストのキーはすべて暗号化され、タイプ6のキーになります。すでにタイプ 6 であるキーは暗号化されず、現在の状態が維持されます。

既存のマスターキーが失われた場合、またはその内容が不明の場合は、**no key config-key password-encrypt** コマンドを使用してそのマスターキーを削除できます。マスターキーを削除しても、既存の暗号化パスワードは、暗号化された状態のままデバイス設定内に保持されます。これらのパスワードは復号化できません。

例

次に、タイプ 6 の暗号キーを NVRAM に保存する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# key config-key password-encrypt
```

関連コマンド

コマンド	説明
password encryption aes	タイプ 6 の暗号化事前 します。

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 Fuji 16.9.2	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
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDUの送信で遅延保護を使用するようにMKAを設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。
send-secure-announcements	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。
ssci-based-on-sci	SCI に基づいて SSCI を計算します。

Command	Description
use-updated-eth-header	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

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

ND インスペクション ポリシー コンフィギュレーション（config-nd-inspection）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、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。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
Device(config-nd-inspection)# end
```

次に、IPv6 スヌーピングポリシー名を policy1 と定義し、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。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
Device(config-ipv6-snooping)# end
```

local-domain（パラメータマップ）

Cisco Umbrella 統合機能のローカルドメインを設定するには、パラメータマップタイプ検査コンフィギュレーション モードで **local-domain** コマンドを使用します。ローカルドメインを削除するには、このコマンドの **no** 形式を使用します。

local-domain *regex_param_map_name*
no local-domain *regex_param_map_name*

構文の説明

regex_param_map_name	正規表現パラメータマップの名前。

コマンド デフォルト

パラメータマップのローカルドメインは作成されていません。

コマンド モード

パラメータマップタイプ検査コンフィギュレーション（config-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

最大 64 のローカルドメインを設定できます。許可されるドメイン名の長さは 100 文字です。

例

次に、ローカルドメインを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type umbrella global
Device(config-profile)# local-domain dns_bypass
```

関連コマンド

コマンド	説明
parameter-map type umbrella global	Umbrella モードでパラメータマップタイプを設定します。

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、グローバル コンフィギュレーション モードで **mab logging verbose** コマンドを使用します。MAB システムメッセージのロギ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。

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 Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# mab logging verbose
Device(config)# exit
```

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

関連コマンド

コマンド	説明
authentication logging verbose	認証システムメッセージから詳細情報をフィルタリングしま
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
mab logging verbose	MAC 認証バイパス（MAB）システムメッセージから詳細情タリングします。

mab request format attribute 32

デバイス上でVLAN ID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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

次に、デバイスで VLAN ID ベースの MAC 認証をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mab request format attribute 32 vlan access-vlan
Device(config)# exit
```

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1X 認証をサポートしないクライアント用の ク方式として Web 認証を使用するようポートを設定
authentication host-mode	ポートで認証マネージャモードを設定します。
authentication open	ポートでオープンアクセスをイネーブルまたはディ す。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルに
authentication port-control	ポートの認証ステートの手動制御をイネーブルにし

コマンド	説明
authentication priority	ポートプライオリティリストに認証方式を追加します。
authentication timer	802.1X 対応ポートのタイムアウトパラメータと再認証 を設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに バイスが接続しているときに、新しいデバイスがポート 場合に発生する違反モードを設定します。
mab	ポートの MAC-based 認証をイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するよう 定します。
show authentication	デバイスの認証マネージャイベントに関する情報を表示

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
no macsec-cipher-suite gcm-aes-128

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。

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 Fuji 16.9.2	このコマンドが導入されました。

例

次に、128 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-128
```

関連コマンド

Command	Description
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
sak-rekey	SAK キー再生成間隔を設定します。
send-secure-announcements	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。
ssci-based-on-sci	SCI に基づいて SSCI を計算します。

Command	Description
use-updated-eth-header	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 MACsec Key Agreement（MKA）プロトコル設定を有効にするには、インターフェイス コンフィギュレーション モードで **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

no macsec network-link

構文の説明

macsec network-link	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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/20
Device(config-if)# macsec network-link
Device(config-if)# end
Device#
```

match（アクセス マップ コンフィギュレーション）

VLANマップを1つまたは複数のアクセスリストとパケットを照合するように設定するには、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** {*namenumber*} [{*namenumber*}] [{*namenumber*}]. . . | **ipv6 address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]. . . | **mac address** {*name*} [{*name*}] [{*name*}]. . .}
no match {**ip address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]. . . | **ipv6 address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]. . . | **mac address** {*name*} [{*name*}] [{*name*}]. . .}

構文の説明

ip address	パケットを IP アドレス アクセス リストと照合するようにアクセス マップを設定します。
ipv6 address	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。
mac address	パケットを MAC アドレス アクセス リストと照合するようにアクセス マップを設定します。
name	パケットを照合するアクセス リストの名前です。
number	パケットを照合するアクセスリストの番号です。このオプションは、MACアクセス リストに対しては無効です。

コマンド デフォルト

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

コマンド モード

アクセスマップ コンフィギュレーション（config-access-map）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

例

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

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

設定を確認するには、**show vlan access-map** 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イスのMACsec Key Agreement （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*
no 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 インターフェイスの 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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

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

```
Device> enable
Device# configure terminal
Device(config)# interface Gigabitethernet 1/0/20
Device(config-if)# mka pre-shared-key key-chain kc1
Device(config-if)# end
Device#
```

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 suppres syslogs sak-rekey
no mka suppres 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
```

parameter-map type regex

正規表現を使用して特定のトラフィックパターンを照合するパラメータマップタイプを設定するには、グローバル コンフィギュレーション モードで **parameter-map type regex** コマンドを使用します。正規表現を使用したパラメータマップタイプを削除するには、このコマンドの **no** 形式を使用します。

parameter-map type regex *parameter-map-name*
no parameter-map type regex

構文の説明

parameter-map-name	パラメータ マップの名前。この名前には最大 228 文字までの英数字を指定できます。 （注） 空白を使用することは推奨されません。文字列が引用符で区切られていない限り、システムは最初の空白をパラメータマップ名の末尾と解釈します。

コマンド デフォルト

正規表現パラメータマップ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 Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

正規表現では、テキスト文字列を文字列そのものとして照合することも、メタ文字を使用してテキスト文字列の複数のバリアントと照合することもできます。正規表現を使用して、特定のアプリケーショントラフィックの内容を照合できます。たとえば、HTTP インスペクション クラス マップの **match request regex** コマンドを使用すると、HTTP パケット内の Uniform Resource Identifier（URI）文字列を照合できます。

Ctrl+V を押すと、CLI において、疑問符（?）やタブなどの特殊文字がすべて無視されます。たとえば、設定で **d?g** と入力するには、**d[Ctrl-V]g** とキー入力します。

次の表に、特別な意味を持つメタ文字を示します。

表 *5: regex* メタ文字

文字	Description	注意
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語に一致します。

文字	Description	注意
(*xxx* **)**	サブ表現	文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示します。たとえば、**lo?se** は、lse または lose に一致します。 （注） 疑問符の前に **Ctrl+V** を入力する必要があります。そうしないと、ヘルプ機能が呼び出されます。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示します。たとえば、**lo*se** は、lse、lose、loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示します。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{ ○ **}**	繰り返し限定作用素	厳密に *x* 回繰り返します。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
{ ○ **,}**	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、**ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc* **]**	文字クラス	角カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。
[^ *abc* **]**	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は a、b、c 以外の任意の文字に一致し、**[^A-Z]** は大文字以外の任意の 1 文字に一致します。
[*a* **-** *c* **]**	文字範囲クラス	指定した範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字と一致します。文字と範囲を組み合わせて使用することもできます。たとえば、**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 （注） ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。

文字	Description	注意
“ ”	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**"test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	リテラル文字の前にある場合、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	フォームフィード 0x0c と一致します。
\x *nn*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
\ *nnn*	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 **040** はスペースを表します。

例

次に、URI が次の正規表現のいずれかと一致する正規表現パラメータマップを設定して HTTP アプリケーション ファイアウォール パラメータマップ タイプに適用する例を示します。

- “.*cmd.exe”
- “.*money”
- “.*shopping”

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type regex uri-regex-cm
Device(config-profile)# pattern ".*cmd.exe"
Device(config-profile)# pattern ".*money"
Device(config-profile)# pattern ".*shopping"
Device(config-profile)# exit
Device(config)# class-map type inspect http uri-check-cm
Device(config-cmap)# match request uri regex uri-regex-cm
Device(config-cmap)# exit
Device(config)# policy-map type inspect http uri-check-pm
Device(config-pmap)# class type inspect http uri-check-cm
Device(config-pmap-c)# reset
```

次に、文字列 hello の複数のバリアントと一致する大文字と小文字を区別しないパターンの正規表現パラメータマップを設定する例を示します。

```
Device# configure terminal
Device(config)# parameter-map type regex body_regex
Device(config-profile)# pattern ".*[Hh][Ee][Ll][Ll][Oo]"
Device(config-profile)# end
```

関連コマンド

コマンド	説明
class-map type inspect	レイヤ 3 とレイヤ 4 またはレイヤ 7（アプリケーション固有）の検査タイプクラスマップを作成します。
class type inspect	アクションが実行されるトラフィック（クラス）を指定します。
match request regex	要求メッセージの URI または引数（パラメータ）が定義された正規表現と一致しているかどうかに基づいてHTTP トラフィックを許可または拒否する HTTP ファイアウォールポリシーを設定します。
parameter-map type	パラメータマップを作成または変更します。
policy-map type inspect	レイヤ 3 とレイヤ 4 またはレイヤ 7（アプリケーション固有）の検査タイプポリシーマップを作成します。

parameter-map type umbrella global

Umbrellaモードのパラメータマップタイプを設定するには、グローバル コンフィギュレーション モードで **parameter-map type umbrella global** コマンドを使用します。Umbrella モードのパラメータマップタイプを削除するには、このコマンドの **no** 形式を使用します。

parameter-map type umbrella global
no parameter-map type umbrella

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

Umbrella モードのパラメータマップ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 Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、パラメータマップタイプを Umbrella モードに設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type umbrella global
Device(config-profile)#
```

関連コマンド

コマンド	説明
parameter-map type	パラメータマップを作成または変更します。

password encryption aes

タイプ6の暗号化事前共有キー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 **password encryption aes** コマンドを使用します。パスワードの暗号化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。

password encryption aes
no password encryption aes

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

事前共有キーは暗号化されていません。

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
Cisco IOS XE Fuji 16.9.2	こ し

使用上のガイドライン

CLI を使用して、プレーンテキストのパスワードをタイプ 6 形式で NVRAM に安全に保存できます。タイプ6のパスワードは暗号化されています。暗号化されたパスワード自体を、確認したり取得したりすることは可能ですが、それを復号化して実際のパスワードを特定することは困難です。**key config-key password-encrypt** コマンドを **password encryption aes** コマンドとともに使用すると、パスワードを設定してイネーブルにできます（キーの暗号化には対称キー暗号である高度暗号化規格（AES）が使用されます）。**key config-key password-encrypt** コマンドを使用して設定されたパスワード（キー）は、ルータ内のその他すべてのキーを暗号化するマスター暗号キーとして使用されます。

password encryption aes コマンドを設定する際、同時に **key config-key password-encrypt** コマンドを設定しないと、**show running-config** コマンドや **copy running-config startup-config** コマンドなどが実行される起動時や不揮発性生成（NVGEN）プロセス中に次のようなメッセージが出力されます。

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

パスワードの変更

key config-key password-encrypt コマンドを使用してパスワード（マスターキー）が変更された場合、または再暗号化された場合には、リストレジストリから、タイプ6暗号が使用されているアプリケーションモジュールへ、変更前のキーと変更後のキーが渡されます。

パスワードの削除

key config-key password-encrypt コマンドを使用して設定されたマスターキーがシステムから削除されると、タイプ6のパスワードすべてが使用不可になるという内容の警告が出力されます（同時に、確認用のプロンプトも表示されます）。セキュリティ対策として、暗号化された

パスワードは、Cisco IOS ソフトウェアによって復号化されることはなくなります。ただし、すでに説明したように、パスワードを再暗号化することはできます。

⚠

注意 **key config-key password-encrypt** コマンドを使用して設定されたパスワードは、一度失われると回復できません。そのため、パスワードは安全な場所に保存しておくことを推奨します。

パスワード暗号化の設定解除

no password encryption aes コマンドを使用してパスワード暗号化の設定を解除しても、既存のタイプ 6 パスワードはすべて変更されずに残されます。**key config-key password-encrypt** コマンドを使用して設定したパスワード（マスターキー）があれば、アプリケーションで必要に応じてタイプ 6 パスワードを復号化できます。

パスワードの保存

（**key config-key password-encrypt** コマンドを使用して設定された）パスワードは誰にも「判読」できないため、ルータからパスワードを取得する方法はありません。既存の管理ステーションでは、その内部にキーが格納されるよう強化されることで初めて、パスワードの内容を「知る」ことができます。そのため、パスワードは管理システム内部に安全に保存する必要があります。TFTPを使用して保存された設定は、スタンドアロンではないため、ルータにはロードできません。設定をルータにロードする前後には、（**key config-key password-encrypt** コマンドを使用して）パスワードを手動で追加する必要があります。このパスワードは、保存された設定に手動で追加できますが、それによって設定内のすべてのパスワードを誰もが復号化できるようになるため、手動によるパスワードの追加は行わないことを推奨します。

新規パスワードまたは不明パスワードの設定

入力またはカットアンドペーストした暗号文は、それがマスターキーに適合しない場合やマスターキーが存在しない場合でも、受理または保存されます。ただしこの場合には次のアラートメッセージが表示されます。

```
“ciphertext>[for username bar>] is incompatible with the configured master key.”
```

マスターキーを新規に設定すると、プレーンテキストのキーはすべて暗号化され、タイプ6のキーに変換されます。すでにタイプ 6 であるキーは暗号化されず、現在の状態が維持されます。

既存のマスターキーが失われた場合、またはその内容が不明の場合は、**no key config-key password-encrypt** コマンドを使用してそのマスターキーを削除できます。既存の暗号化パスワードは、暗号化された状態のままルータ設定内に保持されます。これらのパスワードは復号化されません。

例

次に、タイプ 6 の暗号化事前共有キーをイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device (config)# password encryption aes
```

関連コマンド

コマンド	説明
key config-key password-encrypt	タイプ 6 の暗号キーをブ 存します。

pattern（パラメータマップ）

ローカル URL フィルタリングで許可またはブロックする必要があるドメイン、URL キーワード、または URL メタ文字のリストを指定する照合パターンを設定するには、パラメータマップ タイプ検査コンフィギュレーション モードで **pattern** コマンドを使用します。照合パターンを削除するには、このコマンドの **no** 形式を使用します。

pattern *expression*
no pattern *expression*

構文の説明

expression	ドメイン名、URL キーワード、URL メタ文字のエントリ、または URL キーワードとメタ文字の組み合わせを参照する照合パターン引数。

コマンド デフォルト

パラメータマップのパターンは作成されていません。

コマンド モード

パラメータマップタイプ検査コンフィギュレーション（config-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

照合パターン表現は、**parameter-map type regex** コマンドで作成されたパラメータマップに対して設定されます。

パターン表現では、文字/、{、} は使用できません。疑問符（?）文字は、CLI ヘルプ機能用に予約されているため使用できません。アスタリスク（*）文字は、パターンの先頭には使用できません。

URL パターンマッチングでは、ピリオド（.）文字はドットとして解釈され、単一の文字を表すワイルドカードエントリとしては解釈されません。これは、正規表現パターンマッチングの場合と同じです。URL フィルタリングでは、ホスト名またはドメイン名に任意の文字が含まれる場合にそれらを許可またはブロックできます。

URL キーワードは、ドメイン名の後のパスに含まれるスラッシュ（/）で区切られたひとかたまりの語句です。たとえば、URL http://www.example.com/hack/123.html では、**hack** のみがキーワードとして扱われます。URL 内のキーワード全体がパターンと一致している必要があります。たとえば、**hack** というパターンを設定した場合、URL www.example.com/hacksite/123.html はパターンと一致しません。この URL を一致させるには、パターンに **hacksite** を含める必要があります。

URL メタ文字を使用すると、UNIX の glob 表現のように、パターンマッチングで URL の単一の文字または文字の範囲を照合できます。URL メタ文字を次の表に示します。

表 *6 : URL* パターンマッチングの *URL* メタ文字

文字	Description
*	アスタリスク：0 文字以上の任意のシーケンスと一致します。
[*abc*]	文字クラス：各カッコ内の任意の文字と一致します。文字のマッチングでは大文字と小文字が区別されます。たとえば、**[abc]** は、a、b、または c に一致します。
[*a-c*]	文字範囲クラス：指定した範囲内の任意の文字と一致します。文字のマッチングでは大文字と小文字が区別されます。たとえば、**[a-z]** は、任意の小文字のアルファベット文字に一致します。文字と範囲を組み合わせて使用することもできます。たとえば、**[abcq-z]** および **[a-cq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z に一致します。 （注） ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみ照合されます（**[abc-]** や **[-abc]**）。
[0-9]	数字範囲クラス：各カッコ内の任意の数字と一致します。たとえば、**[0-9]** は、0、1、2、3、4、5、6、7、8、9 に一致します。

URL メタ文字をドメイン名や URL キーワードと組み合わせてパターンパッチングに使用できます。たとえば、www.example[0-9][0-9].com というパターンを使用すると、www.example01.com、www.example33.com、www.example99.com などをブロックできます。キーワードとメタ文字を組み合わせて、URL をブロックする照合パターンを作成できます。たとえば、hack* というパターンを使用すると、www.example.com/hacksite/123.html をブロックできます。

parameter-map type regex コマンドを設定してから **pattern** コマンドを設定すると、**pattern** コマンドで指定したパターンが General Packet Radio Service（GPRS）トンネリングプロトコル（GTP）クラスのフィルタとして使用されます。

例

次に、指定した URL を照合するパターンを設定する例を示します。

```
Device(config)# parameter-map type regex dns_bypass
Device(config-profile)# pattern www.example.com
```

次に、文字列 hello の複数のバリアントと一致する大文字と小文字を区別しないパターンを指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type regex body-regex
Device(config-profile)# pattern ".*[Hh][Ee][Ll][Ll][Oo]"
```

次の例は、パターンの先頭にアスタリスク（*）文字が指定されている場合にコンソールに表示されるエラーメッセージを示しています。

```
Device(config)# parameter-map type regex gtp-map
Device(config-profile)# pattern *.gprs.com
%Invalid first char + or * in regex pattern
```

関連コマンド

コマンド	説明
parameter-map type regex	特定の正規表現パターンを照合する正規表現パラメータマップを設定し、パラメータマップ タイプ検査コンフィギュレーションモードを開始します。

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、MAC アクセスリスト コンフィギュレーション モードで **permit** コマンドを使用します。拡張 MAC アクセス リストから許可条件を削除するには、このコマンドの **no** 形式を使用します。

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

構文の説明

any	すべての送信元または宛先 MAC アドレスを
host *src-MAC-addr* |*src-MAC-addr mask*	ホストMACアドレスと任意のサブネットマ が定義されたアドレスに一致する場合、その ます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先MACアドレスと任意のサブネットマス 義されたアドレスに一致する場合、そのアド
type mask	（任意）パケットの EtherType 番号と、Ether ケットのプロトコルを識別します。 • *type* には、0 ～ 65535 の 16 進数を指定て • *mask* は、一致をテストする前に EtherTyp
aarp	（任意）データリンク アドレスをネットワー Address Resolution Protocol を指定します。
amber	（任意）EtherType DEC-Amber を指定します。
appletalk	（任意）EtherType AppleTalk/EtherTalk を指定
dec-spanning	（任意）EtherType Digital Equipment Corporati
decnet-iv	（任意）EtherType DECnet Phase IV プロトコ
diagnostic	（任意）EtherType DEC-Diagnostic を指定しま
dsm	（任意）EtherType DEC-DSM を指定します。

etype-6000	（任意）EtherType 0x6000 を指定します。
etype-8042	（任意）EtherType 0x8042 を指定します。
lat	（任意）EtherType DEC-LAT を指定します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を指定します
lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と ロトコルを指定します。 *mask* は、一致をテストする前に LSAP 番号に適
mop-console	（任意）EtherType DEC-MOP Remote Console を
mop-dump	（任意）EtherType DEC-MOP Dump を指定します
msdos	（任意）EtherType DEC-MSDOS を指定します。
mumps	（任意）EtherType DEC-MUMPS を指定します。
netbios	（任意）EtherType DEC-Network Basic Input/Outp
vines-echo	（任意）Banyan Systems による EtherType Virtual 指定します。
vines-ip	（任意）EtherType VINES IP を指定します。
xns-idp	（任意）EtherType Xerox Network Systems（XNS
cos *cos*	（任意）プライオリティを設定するため、0 ～ 7 定します。CoS に基づくフィルタリングは、ハー ンが設定されているかどうかを確認する警告メ

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 Fuji 16.9.2	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 XE 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 *7: 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。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
Device(config-ext-macl)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
Device(config-ext-macl)# end
```

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

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# permit any any 0x4321 0
Device(config-ext-macl)# end
```

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

関連コマンド

コマンド	説明
deny	MAC アクセスリ 否します。条件 が転送されるの
mac access-list extended	非 IP トラフィッ セス リストを作
show access-lists	デバイスに設定 ます。

protocol（IPv6 スヌーピング）

s

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、IPv6 スヌーピング コンフィギュレーション モードで **protocol** コマンドを使用します。DHCP または NDP によるアドレス収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

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

構文の説明

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

コマンド デフォルト

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

コマンド モード

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

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

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

次に、IPv6 スヌーピングポリシー名を policy1 と定義し、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。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
```

```
Device(config-ipv6-snooping)# protocol dhcp
Device(config-ipv6-snooping)# end
```

radius server

RADIUS アカウンティングと RADIUS 認証を含む RADIUS サーバの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 **radius server** 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

address {ipv4 | ipv6} *ip{address | hostname}*	RADIUS サーバの IP アドレスを指定します。
auth-port *udp-port*	（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。
acct-port *udp-port*	（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。
key *string*	（任意）デバイスと RADIUS デーモン間のすべての RADIUS 通信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 key 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。key にスペースが含まれる場合は、引用符が key の一部でない限り、key を引用符で囲まないでください。
automate tester *name*	（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。
retransmit *value*	（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、radius-server retransmit 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。
timeout *seconds*	（任意）device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 **radius-server timeout** コマンドを上書きします。

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

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 Fuji 16.9.2	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 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。
- RADIUS サーバ コンフィギュレーション モードで **key** *string* 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、アカウンティング 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。

```
Device> enable
Device# configure terminal
Device(config)# radius server ISE
Device(config-radius-server)# address ipv4 10.1.1 auth-port 1645 acct-port 1646
Device(config-radius-server)# key cisco123
Device(config-radius-server)# end
```

radius-server dead-criteria

RADIUS サーバを dead としてマークするために使用する基準のいずれかまたは両方を示されている定数に強制的に設定するには、**radius-server dead-criteria** コマンドをグローバル コンフィギュレーション モードで使用します。設定されていた基準を無効にするには、このコマンドの **no** 形式を使用します。

radius-server dead-criteria [**time** *seconds*] [**tries** *number-of-tries*]
no radius-server dead-criteria [{**time** *seconds* | **tries** *number-of-tries*}]

構文の説明

time *seconds*	（任意）デバイスが RADIUS サーバから有効なパケットを最後に受信してから、サーバが dead としてマークされるまでに経過する必要のある最小時間（秒単位）。デバイスの起動後にパケットを受信せずにタイムアウトになった場合は、この時間の条件は満たされたものとして処理されます。この時間は 1 ～ 120 秒に設定できます。 • *seconds* 引数を設定しない場合、この秒数はサーバのトランザクション レートに応じて 10 ～ 60 秒になります。 （注） 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。
tries *number-of-tries*	（任意）RADIUS サーバが dead としてマークされるまでにデバイスで発生する必要がある連続タイムアウト回数。サーバが認証とアカウンティングの両方を実行する場合、両方の種類のパケットがこの回数に含まれます。正しく作成されていないパケットは、タイムアウトになっているものとしてカウントされます。最初の送信と再送信を含むすべての送信がカウントされます。タイムアウト回数は 1 ～ 100 に設定できます。 • *number-of-tries* 引数を設定しない場合、連続タイムタウト回数はサーバのトランザクション レートと設定されている再送信回数に基づいて 10 ～ 100 となります。 （注） 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。

コマンド デフォルト

RADIUS サーバがデッド状態としてマークされるまでに発生する連続タイムアウトの回数と秒数は、サーバのトランザクション レートと設定されている再送信回数に応じて異なります。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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） 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。

このコマンドの **no** 形式では、次のようになります。

- *number-of-tries* 引数も *number-of-tries* 引数も **no radius-server dead-criteria** コマンドに指定されていない場合は、時間と試行回数の両方がそれらのデフォルトにリセットされます。
- 最初に設定されていた値を使用して *seconds* 引数が指定された場合、時間はデフォルトの値範囲（10 ～ 60）にリセットされます。
- 最初に設定されていた値を使用して *number-of-tries* 引数が指定された場合、時間はデフォルトの値範囲（10 ～ 100）にリセットされます。

例

次に、5 秒が経過して 4 回の試行後にデバイスが dead と見なされるようにデバイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 5 tries 4
```

次に、**radius-server dead-criteria** コマンドに設定されていた時間と試行回数の基準を無効にする例を示します。

```
Device(config)# no radius-server dead-criteria
```

次に、 **radius-server dead-criteria** コマンドに設定されていた時間の基準を無効にする例を示します。

```
Device(config)# no radius-server dead-criteria time 5
```

次に、**radius-server dead-criteria** コマンドに設定されていた試行回数の基準を無効にする例を示します。

```
Device(config)# no radius-server dead-criteria tries 4
```

関連コマンド

Command	Description
debug aaa dead-criteria transactions	デッド条件の AAA トランザクションの値を表示します。
show aaa dead-criteria	AAA サーバのデッド条件に関する情報を表示します。
show aaa server-private	すべてのプライベート RADIUS サーバのステータスを表示します。
show aaa servers	AAA サーバとの間で送受信されたパケットの数に関する情報を表示します。

radius-server deadtime

一部のサーバが使用不能な場合の RADIUS 応答時間を改善し、使用不能なサーバを即時にスキップするには、**radius-server deadtime** 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。deadtime を 0 に設定するには、このコマンドの **no** 形式を使用します。

radius-server deadtime *minutes*
no radius-server deadtime

構文の説明

minutes	トランザクション要求が RADIUS サーバをスキップする期間（分単位、最大 1440 分（24 時間））。

コマンド デフォルト

デッド タイムは 0 に設定されます。

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 Fuji 16.9.2	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、Cisco IOS ソフトウェアが認証要求に応答しない RADIUS サーバを *dead* としてマークできるようにします。これにより、設定されている次のサーバを試行する前に要求の待機がタイムアウトになることが防止されます。*dead* としてマークされた RADIUS サーバは、指定された期間（分単位）、その他の要求でスキップされます。ただし、*dead* としてマークされていないサーバが他にない場合を除きます。

（注） *dead* としてマークされた RADIUS サーバが誘導要求を受信する場合、その誘導要求は RADIUS サーバで除外されません。ダイレクト要求は RADIUS サーバに直接送信されるため、RADIUS サーバはダイレクト要求の処理を続行します。

次の両方の条件を満たした場合に RADIUS サーバが dead としてマークされます。

1. サーバへ再送信するかどうかを決定するために使用される最小限のタイムアウト期間内に、未処理のトランザクションに対する有効な応答を RADIUS サーバから受信しなかった。
2. 最小限必要な再送信回数に 1（初回送信分）を加算した回数だけ、パケットがすべてのトランザクションで連続して RADIUS サーバに送信されたが、必要なタイムアウト期間内にサーバから有効な応答を受信しなかった。

例

次に、認証要求への応答に失敗した RADIUS サーバのデッドタイムを 5 分に指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius-server deadtime 5
```

関連コマンド

Command	Description
deadtime (server-group configuration)	RADIUS サーバ グループのコンテキスト内でデッドタイムを設定します。
radius-server host	RADIUS サーバ ホストを指定します。
radius-server retransmit	Cisco IOS ソフトウェアが RADIUS サーバ ホストのリストを検索する回数の最大値を指定します。
radius-server timeout	サーバホストが応答するまでデバイスが待機する間隔を設定します。

radius-server directed-request

ユーザがシスコのネットワークアクセスサーバ（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するには、**radius-server directed-request** 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。誘導要求機能を無効にするには、このコマンドの **no** を使用します。

radius-server directed-request [**restricted**]
no radius-server directed-request [**restricted**]

構文の説明

restricted	（任意）指定したサーバが使用できない場合、ユーザがセカンダリサーバに送信されないようにします。

コマンド デフォルト

ユーザはシスコの NAS にログインできないため、認証用の RADIUS サーバを選択します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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-server directed-request コマンドは、「@」記号より前のユーザ名の部分のみを「@」記号の後に指定したホストに送信します。つまり、このコマンドを有効にすると、設定済みのサーバのいずれにも要求を送信でき、ユーザ名のみが指定したサーバに送信されます。

（注） **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した場合は、**radius-server directed-request** コマンドを設定することはできません。

次に、RADIUS サーバにメッセージを送信する一連のイベントを示します。

- **radius-server directed-request** コマンドを設定した場合は、次のようになります。
  - 要求が誘導先のサーバに送信されます。同じ IP アドレスを持つサーバが複数ある場合、要求は同じ IP アドレスを持つ最初のサーバにのみ送信されます。
  - 応答を受信しない場合、要求は最初の方式リストに示されているすべてのサーバに送信されます。
  - 最初の方式で応答を受信しなかった場合、要求は方式リストの最後に到達するまで、2 番目の方式リストに示されているすべてのサーバに送信されます。

（注） 誘導先のサーバを選択するには、指定された要求に指定された IP アドレスを持つサーバの方式リスト内の最初のサーバグループを検索します。使用できない場合、グローバルプールの同じ IP アドレスを持つ最初のサーバグループが考慮されます。

- **radius-server directed-request restricted** コマンドを方式リスト内のすべてのサーバグループに対して設定した場合、誘導先のサーバから応答を受信するまで、または方式リストの最後に到達するまで、次のアクションが実行されます。
  - 誘導先のサーバの IP アドレスを持つ最初のサーバを使用して要求が送信されます。
  - 同じ IP アドレスを持つサーバがサーバグループ内に見つからない場合は、誘導先のサーバの IP アドレスを持つグローバルプール内の最初のサーバが使用されます。

radius-server directed-request コマンドを **no radius-server directed-request** コマンドを使用して無効にした場合、文字列全体（「@」記号の前と後ろの両方）がデフォルトの RADIUS サーバに送信されます。ルータは、リスト内の最初のサーバから順にサーバのリストを照会します。文字列全体を送信し、サーバからの最初の応答を受け入れます。

ユーザをユーザ名の一部として識別された RADIUS サーバに制限するには、**radius-server directed-request restricted** コマンドを使用します。

ユーザ要求にサーバ IP アドレスがある場合、誘導先のサーバはその要求をグループに転送する前に特定のサーバに転送します。たとえば、user@10.0.0.1 などのユーザ要求が誘導先のサーバに送信され、このユーザ要求に指定されている IP アドレスがサーバの IP アドレスの場合、誘導先のサーバはユーザ要求を特定のサーバに転送します。

誘導先のサーバがサーバグループとホストサーバの両方に設定されている場合に設定したサーバ名を持つユーザ要求が誘導先のサーバに送信されると、誘導先のサーバはユーザ要求をサーバグループに転送する前にホストサーバに転送します。たとえば、user@10.0.0.1 というユーザ要求が誘導先のサーバに送信され、10.0.0.1 がホストサーバのアドレスである場合、誘導先のサーバはユーザ要求をサーバグループに転送する前に、ホストサーバに転送します。

（注） **no radius-server directed-request restricted** コマンドを入力すると、restricted フラグのみが削除され、directed-request フラグは保持されます。誘導要求機能を無効にするには、**no radius-server directed-request** コマンドも入力する必要があります。

例

次に、誘導要求機能を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# radius server rad-1
Device(config-radius-server)# address ipv4 10.1.1.2
Device(config-radius-server)# key dummy123
Device(config-radius-server)# exit
Device(config)# radius-server directed-request
```

関連コマンド

Command	Description
aaa group server	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。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
server-private （**RADIUS**）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。

radius-server domain-stripping

ユーザ名をリモートRADIUSサーバに転送する前にユーザ名からサフィックスをストリッピングするか、またはサフィックスとプレフィックスの両方をストリッピングするようにネットワークアクセスサーバ（NAS）を設定するには、**radius-server domain-stripping** コマンドをグローバル コンフィギュレーション モードで 使用します。ストリッピング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。

（注） デフォルトのvrf名が設定されるまでにデフォルトのVRF名が確実にNULL値になるように、**ip vrf default** コマンドをグローバルコンフィギュレーションモードで設定してから **radius-server domain-stripping** コマンドを設定する必要があります。

radius-server domain-stripping [{ [**right-to-left**] [**prefix-delimiter** *character* [*character2* . . . *character7*]] [**delimiter** *character* [*character2* . . . *character7*]] | **strip-suffix** *suffix* }] [**vrf** *vrf-name*]
no radius-server domain-stripping [{ [**right-to-left**] [**prefix-delimiter** *character* [*character2* . . . *character7*]] [**delimiter** *character* [*character2* . . . *character7*]] | **strip-suffix** *suffix* }] [**vrf** *vrf-name*]

構文の説明

right-to-left	（任意）完全なユーザ名を右から左に解析するときに検出された最初のデリミタでNASがストリッピング設定を適用するように指定します。デフォルトでは、NASは、完全なユーザ名を左から右に解析するときに検出された最初のデリミタでストリッピング設定を適用します。
prefix-delimiter *character* [*character2...character7*]	（任意）プレフィックスのストリッピングを有効にし、プレフィックスデリミタとして認識される1つまたは複数の文字を指定します。*character* 引数の有効な値は @、/、$、%、\、# と - です。スペースを挟むことなく複数の文字を入力できます。プレフィックスデリミタとして7文字までを定義できます。これが有効な文字の最大数です。*character* 引数の最後の文字または唯一の文字として \ を入力する場合は、\\ と入力する必要があります。デフォルトでは、プレフィックスデリミタは定義されていません。
delimiter *character* [*character2...character7*]	（任意）サフィックスデリミタとして認識される1つまたは複数の文字を指定します。*character* 引数の有効な値は @、/、$、%、\、# と - です。スペースを挟むことなく複数の文字を入力できます。サフィックスデリミタとして最大7文字を定義できます。これが有効な文字の最大数です。*character* 引数の最後の文字または唯一の文字として \ を入力する場合は、\\ と入力する必要があります。デフォルトのサフィックスデリミタは @ 文字です。
strip-suffix *suffix*	（任意）ユーザ名から削除するサフィックスを指定します。

vrf *vrf-name*	（任意）ドメインストリッピング設定をバーチャルプライベートネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスに制限します。*vrf-name* 引数は、VRF の名前を指定します。

コマンド デフォルト

ストリッピングは無効です。完全なユーザ名が RADIUS サーバに送信されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 サーバにユーザ名を転送する前に、ユーザ名からドメインをストリッピングするように NAS を設定するには、**radius-server domain-stripping** コマンドを使用します。完全なユーザ名が user1@cisco.com の場合、**radius-server domain-stripping** コマンドを有効にすると、ユーザ名の「user1」が RADIUS サーバに転送されます。

right-to-left キーワードを使用して、左から右ではなく、右から左へユーザ名のデリミタを解析するように指定します。これにより、デリミタの 2 つのインスタンスを含む文字列で、いずれのデリミタでもユーザ名をストリッピングできます。たとえば、ユーザ名が user@cisco.com@cisco.net の場合、サフィックスは次の 2 つの方向でストリッピングできます。デフォルトの方向（左から右）では、ユーザ名の「user」が RADIUS サーバに転送されます。**right-to-left** キーワードを設定すると、ユーザ名の「user@cisco.com」が RADIUS サーバに転送されます。

プレフィックスのストリッピングを有効にし、プレフィックスデリミタとして認識される 1 つまたは複数の文字を指定するには、**prefix-delimiter** キーワードを使用します。最初に設定した解析される文字がプレフィックスデリミタとして使用され、そのデリミタの前の文字はすべてストリッピングされます。

サフィックスデリミタとして認識される 1 つまたは複数の文字を指定するには、**delimiter** キーワードを使用します。最初に設定した解析される文字がサフィックスのデリミタとして使用され、そのデリミタの後の文字はすべてストリッピングされます。

ユーザ名からストリッピングする特定のサフィックスを指定するには、**strip-suffix** *suffix* を使用します。たとえば、**radius-server domain-stripping strip-suffix cisco.net** コマンドを設定すると、username user@cisco.net がストリッピングされますが、username user@cisco.com はストリッピングされません。**radius-server domain-stripping** コマンドの複数のインスタンスを発行することによって、ストリッピング用に複数のサフィックスを設定できます。デフォルトのサフィックスデリミタは @ 文字です。

（注） **radius-server domain-stripping s trip-suffix** *suffix* コマンドを発行すると、すべてのドメインからサフィックスをストリッピングする能力が無効になります。フルユーザ名からサフィックスが削除されるのは、サフィックス デリミタとサフィックスの両方が一致した場合のみです。**delimiter** キーワードを使用して別のサフィックスデリミタまたは一連のサフィックスデリミタを指定しない場合は、デフォルトのサフィックスデリミタである @ が使用されます。

指定した VRF のみにドメインストリッピング設定を適用するには、**vrf** *vrf-name* オプションを使用します。

次に、さまざまなタイプのドメインストリッピング設定間の連携動作を示します。

- **radius-server domain-stripping**[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] コマンドに設定できるインスタンスは 1 つのみです。
- **vrf** *vrf-name* に一意の値を使用した **radius-server domain-stripping**[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*] コマンドは、複数のインスタンスを設定できます。
- **radius-server domain-stripping strip-suffix** *suffix*[**vrf** *per-vrf*] コマンドのインスタンスを複数設定することで、グローバルまたはVRF ごとのルールセットの一部として複数のサフィックスをストリッピングすることができます。
- 別のデリミタまたは一連のデリミタを指定した場合を除き、任意のバージョンの **radius-server domain-stripping** コマンドを発行すると、そのルールセットにデフォルトのデリミタ文字の @ を使用するサフィックスストリッピングが自動的に有効になります。
- サフィックスごとのストリッピングルールを設定すると、そのルールセットの汎用サフィックスストリッピングが無効になります。設定された 1 つまたは複数のサフィックスと一致するサフィックスのみがユーザ名からストリッピングされます。

例

次の例では、ルータのユーザ名を右から左へ解析するように設定し、@、\、および $ を有効なサフィックス デリミタ文字として設定します。完全なユーザ名が cisco/user@cisco.com$cisco.net の場合、ユーザ名を右から左へ解析するときに $ 文字が NAS によって検出される最初の有効なデリミタであるため、ユーザ名の「cisco/user@cisco.com」が RADIUS サーバに転送されます。

```
radius-server domain-stripping right-to-left delimiter @\$
```

次の例は、ルータが、abc と名付けられた VRF インスタンスに関連するユーザのみに対して、ユーザ名からドメイン名を削除する設定を示します。デフォルトのサフィックス デリミタである @ は一般的なサフィックスの削除に使用されます。

```
radius-server domain-stripping vrf abc
```

次の例は、/ をプレフィックス デリミタとして使用して、プレフィックスの削除を有効にします。デフォルトのサフィックス デリミタ文字の @ が一般的なサフィックス

の削除に使用されます。完全なユーザ名が cisco/user@cisco.com の場合、ユーザ名の「user」が RADIUS サーバに転送されます。

```
radius-server domain-stripping prefix-delimiter /
```

次の例は、プレフィックスの削除を有効にし、/ の文字をプレフィックス デリミタとして設定し、# をサフィックスのデリミタとして設定します。完全なユーザ名が cisco/user@cisco.com#cisco.net の場合、ユーザ名の「user@cisco.com」が RADIUS サーバに転送されます。

```
radius-server domain-stripping prefix-delimiter / delimiter #
```

次の例は、プレフィックスの削除を有効にし、/ の文字をプレフィックス デリミタとして設定し、$、@、および # をサフィックスのデリミタとして設定し、cisco.com のサフィックスのサフィックスごとの削除を設定します。完全なユーザ名が cisco/user@cisco.com の場合、ユーザ名の「user」が RADIUS サーバに転送されます。フルユーザ名が cisco/user@cisco.com#cisco.net であればユーザ名の「user@cisco.com」が転送されます。

```
radius-server domain-stripping prefix-delimiter / delimiter $@#
radius-server domain-stripping strip-suffix cisco.com
```

次の例では、ルータのユーザ名を右から左へ解析するように設定し、cisco.com のサフィックスでユーザ名のサフィックス削除を有効にします。完全なユーザ名が cisco/user@cisco.net@cisco.com の場合、ユーザ名の「cisco/user@cisco.net」が RADIUS サーバに転送されます。フルユーザ名が cisco/user@cisco.com@cisco.net であれば、このフルユーザ名が転送されます。

```
radius-server domain-stripping right-to-left
radius-server domain-stripping strip-suffix cisco.com
```

次の例は、@ をデリミタとして使用して cisco.com のサフィックスを削除する一連のグローバルな削除ルールと、myvrf という名前の VRF と関連するユーザ名に対する異なった一連の削除ルールを設定します。

```
radius-server domain-stripping strip-suffix cisco.com
!
radius-server domain-stripping prefix-delimiter # vrf myvrf
radius-server domain-stripping strip-suffix cisco.net vrf myvrf
```

関連コマンド

コマンド	説明
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
ip vrf	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。
tacacs-server domain-stripping	ユーザ名を TACACS+ サーバに転送する前にユーザ名からプレフィックスまたはサフィックスをストリッピングするようにルータを設定します。

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

interval *time-interval*	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。
on-live-peer-loss	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 16.9.2	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
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDU の送信で遅延保護を使用するように MKA を設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
send-secure-announcements	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
ssci-based-on-sci	SCI に基づいて SSCI を計算します。
use-updated-eth-header	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。

security level（IPv6 スヌーピング）

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

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

構文の説明

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

コマンド デフォルト

デフォルトのセキュリティ レベルは guard です。

コマンド モード

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、セキュリティ レベルを inspect として設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
Device(config-ipv6-snooping)# end
```

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 16.9.2	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
mka policy	MKA ポリシーを設定します。
confidentiality-offset	機密性オフセットを設定して MACsec を動作させます。
delay-protection	MKPDUの送信で遅延保護を使用するようにMKAを設定します。
include-icv-indicator	MKPDU に ICV インジケータを含めます。
key-server	MKA キーサーバオプションを設定します。
macsec-cipher-suite	SAK を取得するための暗号スイートを設定します。
sak-rekey	SAK キー再生成間隔を設定します。

Command	Description
ssci-based-on-sci	SCI に基づいて SSCI を計算します。
use-updated-eth-header	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、およびアカウンティング（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

ip-address	プライベート RADIUS サーバホストの IP アドレス。
auth-port *port-number*	（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。
acct-port *port-number*	（任意）アカウンティング要求に対する UDP 宛先ポート。デフォルト値は 1646 です。
non-standard	（任意）RADIUS サーバでベンダー独自の RADIUS 属性を使用。
timeout *seconds*	（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 **radius-server timeout** 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。
retransmit *retries*	（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 **radius-server retransmit** コマンドのグローバル設定を上書きします。
key *string*	（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 **radius-server key** 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。 *string* には、**0**（暗号化されていないキーが続くことを指定）、**6**（Advanced Encryption Scheme（AES）暗号化キーが続くことを指定）**7**（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 Fuji 16.9.2	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
aaa group server	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。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
password encryption aes	タイプ 6 の暗号化事前共有キーをイネーブルにします。

コマンド	説明
radius-server host	RADIUS サーバ ホストを指定します。
radius-server directed-request	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、およびアカウンティング（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

ip4- address	プライベート TACACS+ サーバホストの IPv4 アドレスです。
ip6- address	プライベート TACACS+ サーバホストの IPv6 アドレスです。
fqdn	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）。
nat	（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。
single-connection	（任意）ルータと TACACS+ サーバ間の単一の TCP 接続を維持します。
timeout*seconds*	（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、**tacacs-server timeout** 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。
port*port-number*	（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 Fuji 16.9.2	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
aaa group server	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。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
ip tacacs source-interface	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。
ip vrf forwarding (server-group)	AAA TACACS+ サーバグループの VRF の参照を設定します。

show aaa clients

認証、許可、およびアカウンティング（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 (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# show aaa clients

Dropped request packets: 0
```

show aaa command handler

認証、許可、およびアカウンティング（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 (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device# 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 dead-criteria

認証、許可、およびアカウンティング（AAA）の dead-criteria 検出情報を表示するには、**show aaa dead-criteria** コマンドを特権 EXEC モードで使用します。

show aaa dead-criteria {**security-protocol** *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*][*server-group-name*]

構文の説明

security-protocol	指定した AAA サーバのセキュリティプロトコル。現在、サポートされているプロトコルは RADIUS のみです。
ip-address	指定した AAA サーバの IP アドレス。
auth-port	（任意）指定した RADIUS サーバの認証ポート。
port-number	（任意）認証ポートの番号。デフォルトは 1645 です（RADIUS サーバの場合）。
acct-port	（任意）指定した RADIUS サーバのアカウンティングポート。
port-number	（任意）アカウンティングポートの番号。デフォルトは 1646 です（RADIUS サーバの場合）。
server-group-name	（任意）指定したサーバが関連付けられているサーバグループ。デフォルトは *radius* です（RADIUS サーバの場合）。

コマンド デフォルト

現在、**auth-port** キーワードの *port-number* 引数と **acct-port** キーワードの *port-number* 引数は、デフォルトでそれぞれ 1645 と1646 になります。*server-group-name* 引数のデフォルトは radius です。

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 Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

同じ IP アドレスを持つ複数の RADIUS サーバをデバイスに設定できます。**auth-port** キーワードと **acct-port** キーワードはサーバを区別するために使用されます。指定したサーバグループに関連付けられているサーバの dead 検出間隔は、**server-group-name** キーワードを使用して取得できます（RADIUS サーバの dead 状態検出間隔と再送信の値は、サーバが属するサーバグループに基づいて設定されます。複数のサーバグループに同じサーバを含めることができます）。

例

次に、IP アドレス 172.19.192.80 の RADIUS サーバに対して dead-criteria 検出情報を要求した場合の例を示します。

```
Device# show aaa dead-criteria radius 172.19.192.80 radius

RADIUS Server Dead Critieria:
=============================
Server Details:
    Address : 172.19.192.80
    Auth Port : 1645
    Acct Port : 1646
Server Group : radius
Dead Criteria Details:
    Configured Retransmits : 62
    Configured Timeout : 27
    Estimated Outstanding Transactions: 5
    Dead Detect Time : 25s
    Computed Retransmit Tries: 22
    Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 5
Max Computed Dead Detect Time: 25s
Max Computed Retransmits : 22
```

Max Computed Dead Detect Time が表示されます（秒単位）。表示される他のフィールドは説明がなくてもわかります。

関連コマンド

コマンド	説明
debug aaa dead-criteria transactions	デッド条件の AAA トランザクションの値を表示します。
radius-server dead-criteria	RADIUS サーバをデッド状態と指定するための条件のいずれかまたは両方を、指定した定数で適用します。
show aaa server-private	すべてのプライベート RADIUS サーバのステータスを表示します。
show aaa servers	AAA サーバとの間で送受信されたパケットの数に関する情報を表示します。

show aaa local

認証、許可、およびアカウンティング（AAA）ローカル方式オプションを表示するには、**show aaa local** コマンドを使用します。

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

構文の説明

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

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device# 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、アカウンティング（AAA）サーバのMIBによって認識されるすべてのAAAサーバを表示するには、**show aaa servers** コマンドを使用します。

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

構文の説明

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

コマンド モード

ユーザ EXEC (>)

特権 EXEC（>）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

show aaa sessions

認証、許可、アカウンティング（AAA）セッションの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 (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device# 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

switch-number	*switch-number* 変数の有効な値は 1 ～ 9 です。
R0	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。
active	アクティブ インスタンスを指定します。
standby	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 Fuji 16.9.2	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 *8 : 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	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。 • A：ポリシーの適用中（詳細は複数行のステータスを参照） • D：取り外し待ち • F：最終の取り外しの進行中 • I：IIF ID の割り当て待ち • P：セッションをプッシュ済み • 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） • 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） • X：不明なブロック
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

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

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 *9*：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 *10*：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、デバ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。

```
Device# 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。

```
Device# show authentication sessions interface gigabitethernet2/0/47

            Interface:  GigabitEthernet2/0/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Guest Vlan
         Vlan Policy:  20
```

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

show cisp

指定されたインターフェイスの Client Information Signaling Protocol（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

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

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

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

```
Device# show cisp interface fastethernet 0/1/1

CISP not enabled on specified interface
```

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

```
Device# show cisp registrations

Interface(s) with CISP registered user(s):
-------------------------------------------
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
```

```
Gi3/0/3
Gi3/0/5
Gi3/0/23
```

関連コマンド

コマンド	説明
cisp enable	CISP をイネーブルにします。
dot1x credentials *profile*	プロファイルをサプリカントデバイスに

show dot1x

デバイス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 EXEC モードまたは特権 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 (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device# 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。

```
Device# 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。

```
Device# 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 Fuji 16.9.2	このコマンドが導入されました。

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

```
Device# show eap pac peers

No PACs stored
```

関連コマンド

コマンド	説明
clear eap sessions	デバイスまたは指定されたポートの EAP のセッショ す。

show ip access-lists

現在のすべての IP アクセスリストの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip access-lists** コマンドを使用します。

show ip access-lists [{ *access-list-number access-list-number-expanded-range access-list-name* | **dynamic** [*dynamic-access-list-name*] | **interface** *name number* [{ **in** | **out** }] }]

構文の説明

access-list-number	（任意）表示する IP アクセス リストの数です。
access-list-number-expanded-range	（任意）表示する IP アクセスリストの拡張範囲です。
access-list-name	（任意）表示する IP アクセス リストの名前です。
dynamic *dynamic-access-list-name*	（任意）指定されたダイナミック IP アクセスリストを表示します。
interface *name number*	（任意）指定されたインターフェイスのアクセスリストを表示します。
in	（任意）インターフェイスの入力統計情報を表示します。
out	（任意）インターフェイスの出力統計情報を表示します。

（注） OGACL の統計情報はサポートされていません

コマンド デフォルト

標準の IP アクセスリストおよび拡張 IP アクセスリストがすべて表示されます。

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 Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

show ip access-lists コマンドの出力は、IP 固有のもの以外は **show access-lists** コマンドの出力と同じです。また、特定のアクセスリストを指定できます。

show ip access-lists interface コマンドの出力には、dACL フィルタ ID や ACL フィルタ ID は表示されません。これは、物理インターフェイスではなく、各認証セッションのマルチドメイン認証によって作成された仮想ポートに ACL が接続されるためです。dACL フィルタ ID や ACL フィルタ IDを表示するには、**show ip access-lists** *access-list-name* コマンドを使用します。

access-list-name は、**show access-session interface** *interface-name* **detail** コマンドの出力から取得する必要があります。*access-list-name* では大文字と小文字が区別されます。

例

次に、すべてのアクセスリストを要求した場合の **show ip access-lists** コマンドの出力例を示します。

```
Device# show ip access-lists

Extended IP access list 101
   deny udp any any eq nntp
   permit tcp any any
   permit udp any any eq tftp
   permit icmp any any
   permit udp any any eq domain
```

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 *11 : show ip access-lists* フィールドの説明

フィールド	説明
Extended IP access list	拡張 IP アクセス リスト名/番号。
deny	拒否するパケット。
udp	ユーザ データグラム プロトコル。
any	送信元ホストまたは宛先ホスト。
eq	特定のポート番号のパケット。
nntp	ネットワーク ニュース トランスポート プロトコル。
permit	転送するパケット。
tcp	伝送制御プロトコル。
tftp	Trivial File Transfer Protocol。
icmp	Internet Control Message Protocol（インターネット制御メッセージ プロトコル）。
ドメイン	ドメインネームサービス。

次に、特定のアクセスリストの名前を要求した場合の **show ip access-lists** コマンドの出力例を示します。

```
Device# show ip access-lists Internetfilter

Extended IP access list Internetfilter
   permit tcp any 192.0.2.0 255.255.255.255 eq telnet
   deny tcp any any
   deny udp any 192.0.2.0 255.255.255.255 lt 1024
```

```
   deny ip any any log
```

次に、**show ip access-lists** コマンドで **dynamic** キーワードを使用した場合の出力例を示します。

```
Device# show ip access-lists dynamic CM_SF#1

Extended IP access list CM_SF#1
    10 permit udp any any eq 5060 (650 matches)
    20 permit tcp any any eq 5060
    30 permit udp any any dscp ef (806184 matches)
```

関連コマンド

Command	Description
deny	パケットを拒否する名前付き IP アクセス リストまたは OGACL の条件を設定します。
ip access-group	ACL または OGACL をインターフェイスまたはサービス ポリシーマップに適用します。
ip access-list	IP アクセス リストまたは OGACL を名前または番号で定義します。
object-group network	OGACL で使用するネットワーク オブジェクト グループを定義します。
object-group service	OGACL で使用するサービス オブジェクト グループを定義します。
permit	パケットを許可する名前付き IP アクセスリストまたは OGACL の条件を設定します。
show object-group	設定されているオブジェクトグループに関する情報を表示します。
show run interfaces cable	ケーブルモデムの統計情報を表示します。

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 EXEC モードまたは特権 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 (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

デバイススタックでは、すべての統計情報がスタックのアクティブスイッチで生成されます。新しいアクティブデバイスが選出された場合、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。

```
Device> 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。

```
Device> 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 *12 : DHCP* スヌーピング統計情報

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

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

show platform software dns-umbrella statistics

デバイスのドメインネームシステム（DNS）の Umbrella の統計を表示するには、特権 EXEC モードで **show platform software dns-umbrella statistics** コマンドを使用します。

show platform software dns-umbrella statistics

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 Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、**show platform software dns-umbrella statistics** コマンドの出力例を示します。

```
Device> enable
Device# show platform software dns-umbrella statistics

========================================
Umbrella Statistics
========================================
Total Packets : 7848
DNSCrypt queries : 3940
DNSCrypt responses : 0
DNS queries : 0
DNS bypassed queries(Regex) : 0
DNS responses(Umbrella) : 0
DNS responses(Other) : 3906
Aged queries : 34
Dropped pkts : 0
```

show platform software umbrella switch F0

Embedded Service Processor（ESP）スロット 0 の Umbrella の設定を表示するには、特権 EXEC モードで **show platform software umbrella switch** {*switch_number* | **active** | **standby**} **F0** コマンドを使用します。

show platform software umbrella switch {*switch_number* | **active** | **standby**} **F0** {**config** | **interface-info** | **local-domain**}

構文の説明

switch {*switch_number* | **active** | **standby**}	スイッチを指定します。 • *switch_number*：スイッチの ID。有効な範囲は 1 ～ 8 です。 • **active**：アクティブスイッチを指定します。 • **standby**：スタンバイスイッチを指定します。
config	ESP スロット 0 のグローバル設定を表示します。
interface-info	ESP スロット 0 のインターフェイス関連の設定を表示します。
local-domain	ESP スロット 0 のローカルドメイン関連の設定を表示します。

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 Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、**show platform software umbrella switch active F0 config** コマンドの出力例を示します。

```
Device> show platform software umbrella switch active F0 config

+++ Umbrella Config +++


Umbrella feature:
------------------
Init: Enabled
Dnscrypt: disabled

Timeout:
------------------
udp timeout: 5

OrgId :
------------------
orgid : 2427270
```

```
Resolver config:

RESOLVER IP's
---------------------
 208.67.220.220
 208.67.222.222
 2620:119:35::35
 2620:119:53::53

Dnscrypt Info:

public_key:
magic_key:
serial number:

ProfileID    DeviceID           Mode          Resolver   Local-Domain     Tag
-------------------------------------------------------------------------------
```

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、ユーザ EXEC モードまたは特権 EXEC モードで **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 Fuji 16.9.2	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。

```
Device# 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 *13 : 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、sharecount は 1 です。2 つの方式リストが同じサーバ グループを使用する場合、sharecount は 2 です。
sg_unconfigured	サーバ グループが設定解除されました。

フィールド	説明
Type	タイプは、standard または nonstandard のいずれかです。タイプはグループ内のサーバが非標準の属性を受け入れるかどうかを示します。グループ内のすべてのサーバに非標準のオプションが設定されている場合、タイプは「nonstandard」と表示されます。
Memlocks	メモリ内にあるサーバ グループ構造の内部参照の数。この数は、このサーバ グループへの参照を保持している内部データ構造パケットまたはトランザクションがいくつあるかを表します。Memlocksはメモリ管理のために内部的に使用されます。

show tech-support acl

テクニカルサポートに使用するアクセスコントロールリスト（ACL）関連の情報を表示するには、特権 EXEC モードで **show tech-support acl** コマンドを使用します。

show tech-support acl

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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	

使用上のガイドライン

show tech-support acl コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support acl | redirect flash:***show_tech_acl.txt*）。

このコマンドの出力には次のコマンドが表示されます。

（注） スタック可能なプラットフォームでは、これらのコマンドはスタック内のすべてのスイッチで実行されます。Catalyst 9400 シリーズ スイッチなどのモジュール型のプラットフォームでは、これらのコマンドはアクティブスイッチでのみ実行されます。

（注） 次のコマンドのリストは、出力で使用可能なコマンドの例です。これらはプラットフォームによって異なる場合があります。

- **show clock**
- **show version**
- **show running-config**
- **show module**
- **show interface**
- **show access-lists**
- **show logging**
- **show platform software fed switch** *switch-number* **acl counters hardware**

- **show platform software fed switch** *switch-number* **ifm mapping**
- **show platform hardware fed switch** *switch-number* **fwd-asic drops exceptions**
- **show platform software fed switch** *switch-number* **acl info**
- **show platform software fed switch** *switch-number* **acl**
- **show platform software fed switch** *switch-number* **acl usage**
- **show platform software fed switch** *switch-number* **acl policy intftype all cam**
- **show platform software fed switch** *switch-number* **acl cam brief**
- **show platform software fed switch** *switch-number* **acl policy intftype all vcu**
- **show platform hardware fed switch** *switch-number* **acl resource usage**
- **show platform hardware fed switch** *switch-number* **fwd-asic resource tcam table acl**
- **show platform hardware fed switch** *switch-number* **fwd-asic resource tcam utilization**
- **show platform software fed switch** *switch-number* **acl counters hardware**
- **show platform software classification switch** *switch-number* **all F0 class-group-manager class-group**
- **show platform software process database forwarding-manager switch** *switch-number* **R0 summary**
- **show platform software process database forwarding-manager switch** *switch-number* **F0 summary**
- **show platform software object-manager switch** *switch-number* **F0 pending-ack-update**
- **show platform software object-manager switch** *switch-number* **F0 pending-issue-update**
- **show platform software object-manager switch** *switch-number* **F0 error-object**
- **show platform software peer forwarding-manager switch** *switch-number* **F0**
- **show platform software access-list switch** *switch-number* **f0 statistics**
- **show platform software access-list switch** *switch-number* **r0 statistics**
- **show platform software trace message fed switch** *switch-number*
- **show platform software trace message forwarding-manager switch** *switch-number* **F0**
- **show platform software trace message forwarding-manager switch R0** *switch-number* **R0**

例

次に、**show tech-support acl** コマンドの出力例を示します。

```
Device# show tech-support acl

.
.
.
------------------ show platform software fed switch 1 acl cam brief ------------------

Printing entries for region ACL_CONTROL (143) type 6 asic 0
=============================================================
TAQ-4 Index-0 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
```

```
Output IPv4 VACL

 VCU Result: Not In-Use

 L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

 Source Address/Mask
 0.0.0.0/0.0.0.0
 Destination Address/Mask
 0.0.0.0/0.0.0.0

 Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

 L4 Source Port/Mask   L4 Destination Port/Mask
 0x0044 (68)/0xffff     0x0043 (67)/0xffff

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Forward L3, Forward L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-1 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 VACL

 VCU Result: Not In-Use

 L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

 Source Address/Mask
 0.0.0.0/0.0.0.0
 Destination Address/Mask
 0.0.0.0/0.0.0.0

 Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

 L4 Source Port/Mask   L4 Destination Port/Mask
 0x0043 (67)/0xffff     0x0044 (68)/0xffff

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Forward L3, Forward L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-2 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 VACL

 VCU Result: Not In-Use

 L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

 Source Address/Mask
 0.0.0.0/0.0.0.0
 Destination Address/Mask
 0.0.0.0/0.0.0.0

 Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

 L4 Source Port/Mask   L4 Destination Port/Mask
 0x0043 (67)/0xffff     0x0043 (67)/0xffff

 TCP Flags: 0x00 ( NOT SET )
```

```
 ACTIONS:  Forward L3, Forward L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-3 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Input IPv4 PACL

 VCU Result: Not In-Use

 L3 Length: 0000, L3 Protocol: 00 (HOPOPT), L3 Tos: 00

 Source Address/Mask
 0.0.0.0/0.0.0.0
 Destination Address/Mask
 0.0.0.0/0.0.0.0

 Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

 L4 Source Port/Mask   L4 Destination Port/Mask
 0x0000 (0)/0x0000     0x0000 (0)/0x0000

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Drop L3, Drop L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-4 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 PACL

 VCU Result: Not In-Use

 L3 Length: 0000, L3 Protocol: 00 (HOPOPT), L3 Tos: 00

 Source Address/Mask
 0.0.0.0/0.0.0.0
 Destination Address/Mask
 0.0.0.0/0.0.0.0

 Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

 L4 Source Port/Mask   L4 Destination Port/Mask
 0x0000 (0)/0x0000     0x0000 (0)/0x0000

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Drop L3, Drop L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-5 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output MAC PACL

 VLAN ID/MASK : 0x000 (000)/0x000

 Source MAC/Mask : 0000.0000.0000/0000.0000.0000

 Destination MAC/Mask : 0000.0000.0000/0000.0000.0000

 isSnap: Disabled, isLLC: Disabled

 ACTIONS:  Drop L3, Drop L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)
```

.
.
.

出力フィールドの意味は自明です。

show tech-support identity

テクニカルサポートに使用するアイデンティティ/802.1X 関連の情報を表示するには、特権 EXEC モードで **show tech-support identity** コマンドを使用します。

show tech-support identity mac *mac-address* **interface** *interface-name*

構文の説明

mac *mac-address*	クライアント MAC アドレスに関する情報を表示します。
interface *interface-name*	クライアントインターフェイス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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	

使用上のガイドライン

show tech-support platform コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support identity mac** *mac-address* **interface** *interface-name* **| redirect flash:***filename*）。

このコマンドの出力には次のコマンドが表示されます。

- **show clock**
- **show module**
- **show version**
- **show switch**
- **show redundancy**
- **show dot1x statistics**
- **show ip access-lists**
- **show interface**
- **show ip interface brief**
- **show vlan brief**
- **show running-config**
- **show logging**
- **show interface controller**

- **show platform authentication sbinfo interface**
- **show platform host-access-table**
- **show platform pm port-data**
- **show spanning-tree interface**
- **show access-session mac detail**
- **show platform authentication session mac**
- **show device-tracking database mac details**
- **show mac address-table address**
- **show access-session event-logging mac**
- **show authentication sessions mac details R0**
- **show ip admission cache R0**
- **show platform software wired-client R0**
- **show platform software wired-client F0**
- **show platform software process database forwarding-manager R0 summary**
- **show platform software process database forwarding-manager F0 summary**
- **show platform software object-manager F0 pending-ack-update**
- **show platform software object-manager F0 pending-issue-update**
- **show platform software object-manager F0 error-object**
- **show platform software peer forwarding-manager R0**
- **show platform software peer forwarding-manager F0**
- **show platform software VP R0 summary**
- **show platform software VP F0 summary**
- **show platform software fed punt cpuq**
- **show platform software fed punt cause summary**
- **show platform software fed inject cause summary**
- **show platform hardware fed fwd-asic drops exceptions**
- **show platform hardware fed fwd-asic resource tcam table acl**
- **show platform software fed acl counter hardware**
- **show platform software fed matm macTable**
- **show platform software fed ifm mappings**
- **show platform software trace message fed reverse**
- **show platform software trace message forwarding-manager R0 reverse**

- **show platform software trace message forwarding-manager F0 reverse**
- **show platform software trace message smd R0 reverse**
- **show authentication sessions mac details**
- **show platform software wired-client**
- **show platform software process database forwarding-manager summary**
- **show platform software object-manager pending-ack-update**
- **show platform software object-manager pending-issue-update**
- **show platform software object-manager error-object**
- **show platform software peer forwarding-manager**
- **show platform software VP summary**
- **show platform software trace message forwarding-manager reverse**
- **show ip admission cache**
- **show platform software trace message smd reverse**
- **show platform software fed punt cpuq**
- **show platform software fed punt cause summary**
- **show platform software fed inject cause summary**
- **show platform hardware fed fwd-asic drops exceptions**
- **show platform hardware fed fwd-asic resource tcam table acl**
- **show platform software fed acl counter hardware**
- **show platform software fed matm macTable**
- **show platform software fed ifm mappings**
- **show platform software trace message fed reverse**

例

次に、**show tech-support identity** コマンドの出力例を示します。

```
Device# show tech-support identity mac 0000.0001.0003 interface gigabitethernet1/0/1

.
.
.
------------------ show platform software peer forwarding-manager R0  ------------------

IOSD Connection Information:

  MQIPC (reader) Connection State: Connected, Read-selected
    Connections: 1, Failures: 22
    3897 packet received (0 dropped), 466929 bytes
    Read attempts: 2352, Yields: 0
  BIPC Connection state: Connected, Ready
    Accepted: 1, Rejected: 0, Closed: 0, Backpressures: 0
    36 packets sent, 2808 bytes
```

```
SMD Connection Information:

  MQIPC (reader) Connection State: Connected, Read-selected
    Connections: 1, Failures: 30
    0 packet received (0 dropped), 0 bytes
    Read attempts: 1, Yields: 0
  MQIPC (writer) Connection State: Connected, Ready
    Connections: 1, Failures: 0, Backpressures: 0
    0 packet sent, 0 bytes

FP Peers Information:

  Slot: 0
    Peer state: connected
    OM ID: 0, Download attempts: 638
      Complete: 638, Yields: 0, Spurious: 0
      IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
    Back-Pressure asserted for IPC: 0, IPC-Log: 1
    Number of FP FMAN peer connection expected: 7
    Number of FP FMAN online msg received: 1
    IPC state: unknown

    Config IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf3d48e8, BIPC FD: 36, Peer Context: 0xdf3e7158
      Tx Packets: 688, Messages: 2392, ACKs: 36
      Rx Packets: 37, Bytes: 2068

      IPC Log:
        Peer name: fman-log-bay0-peer0
        Flags: Recovery-Complete
        Send Seq: 36, Recv Seq: 36, Msgs Sent: 0, Msgs Recovered: 0

    Upstream FMRP IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf3e7308, BIPC FD: 37, Peer Context: 0xdf3e7158
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0

    Upstream FMRP-IOSd IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf3f9c38, BIPC FD: 38, Peer Context: 0xdf3e7158
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 37, Bytes: 2864
      Rx ACK Requests: 1, Tx ACK Responses: 1

    Upstream FMRP-SMD IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf40c568, BIPC FD: 39, Peer Context: 0xdf3e7158
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0

    Upstream FMRP-WNCD_0 IPC Context:
      State: Connected
      BIPC Handle: 0xdf4317c8, BIPC FD: 41, Peer Context: 0xdf3e7158
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0

    Upstream FMRP-WNCMGRD IPC Context:
      State: Connected
      BIPC Handle: 0xdf41ee98, BIPC FD: 40, Peer Context: 0xdf3e7158
```

```
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-MOBILITYD IPC Context:
    State: Connected
    BIPC Handle: 0xdf4440f8, BIPC FD: 42, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

Slot: 1
Peer state: connected
  OM ID: 1, Download attempts: 1
    Complete: 1, Yields: 0, Spurious: 0
    IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
  Back-Pressure asserted for IPC: 0, IPC-Log: 0
  Number of FP FMAN peer connection expected: 7
  Number of FP FMAN online msg received: 1
  IPC state: unknown

  Config IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf45e4d8, BIPC FD: 48, Peer Context: 0xdf470e18
    Tx Packets: 20, Messages: 704, ACKs: 1
    Rx Packets: 2, Bytes: 108

    IPC Log:
      Peer name: fman-log-bay0-peer1
      Flags: Recovery-Complete
      Send Seq: 1, Recv Seq: 1, Msgs Sent: 0, Msgs Recovered: 0

  Upstream FMRP IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf470fc8, BIPC FD: 49, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0

  Upstream FMRP-IOSd IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf4838f8, BIPC FD: 50, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-SMD IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf496228, BIPC FD: 51, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-WNCD_0 IPC Context:
    State: Connected
    BIPC Handle: 0xdf4bb488, BIPC FD: 53, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-WNCMGRD IPC Context:
    State: Connected
    BIPC Handle: 0xdf4a8b58, BIPC FD: 52, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
```

```
      Rx ACK Requests: 0, Tx ACK Responses: 0

    Upstream FMRP-MOBILITYD IPC Context:
      State: Connected
      BIPC Handle: 0xdf4cddb8, BIPC FD: 54, Peer Context: 0xdf470e18
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0



------------------ show platform software peer forwarding-manager R0  ------------------

IOSD Connection Information:

  MQIPC (reader) Connection State: Connected, Read-selected
    Connections: 1, Failures: 22
    3897 packet received (0 dropped), 466929 bytes
    Read attempts: 2352, Yields: 0
  BIPC Connection state: Connected, Ready
    Accepted: 1, Rejected: 0, Closed: 0, Backpressures: 0
    36 packets sent, 2808 bytes

SMD Connection Information:

  MQIPC (reader) Connection State: Connected, Read-selected
    Connections: 1, Failures: 30
    0 packet received (0 dropped), 0 bytes
    Read attempts: 1, Yields: 0
  MQIPC (writer) Connection State: Connected, Ready
    Connections: 1, Failures: 0, Backpressures: 0
    0 packet sent, 0 bytes

FP Peers Information:

  Slot: 0
    Peer state: connected
    OM ID: 0, Download attempts: 638
      Complete: 638, Yields: 0, Spurious: 0
      IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
    Back-Pressure asserted for IPC: 0, IPC-Log: 1
    Number of FP FMAN peer connection expected: 7
    Number of FP FMAN online msg received: 1
    IPC state: unknown

    Config IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf3d48e8, BIPC FD: 36, Peer Context: 0xdf3e7158
      Tx Packets: 688, Messages: 2392, ACKs: 36
      Rx Packets: 37, Bytes: 2068

      IPC Log:
        Peer name: fman-log-bay0-peer0
        Flags: Recovery-Complete
        Send Seq: 36, Recv Seq: 36, Msgs Sent: 0, Msgs Recovered: 0

    Upstream FMRP IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf3e7308, BIPC FD: 37, Peer Context: 0xdf3e7158
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0

    Upstream FMRP-IOSd IPC Context:
```

```
    State: Connected, Read-selected
    BIPC Handle: 0xdf3f9c38, BIPC FD: 38, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 37, Bytes: 2864
    Rx ACK Requests: 1, Tx ACK Responses: 1

  Upstream FMRP-SMD IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf40c568, BIPC FD: 39, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-WNCD_0 IPC Context:
    State: Connected
    BIPC Handle: 0xdf4317c8, BIPC FD: 41, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-WNCMGRD IPC Context:
    State: Connected
    BIPC Handle: 0xdf41ee98, BIPC FD: 40, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-MOBILITYD IPC Context:
    State: Connected
    BIPC Handle: 0xdf4440f8, BIPC FD: 42, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

Slot: 1
Peer state: connected
  OM ID: 1, Download attempts: 1
    Complete: 1, Yields: 0, Spurious: 0
    IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
  Back-Pressure asserted for IPC: 0, IPC-Log: 0
  Number of FP FMAN peer connection expected: 7
  Number of FP FMAN online msg received: 1
  IPC state: unknown

  Config IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf45e4d8, BIPC FD: 48, Peer Context: 0xdf470e18
    Tx Packets: 20, Messages: 704, ACKs: 1
    Rx Packets: 2, Bytes: 108

    IPC Log:
      Peer name: fman-log-bay0-peer1
      Flags: Recovery-Complete
      Send Seq: 1, Recv Seq: 1, Msgs Sent: 0, Msgs Recovered: 0

  Upstream FMRP IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf470fc8, BIPC FD: 49, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0

  Upstream FMRP-IOSd IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf4838f8, BIPC FD: 50, Peer Context: 0xdf470e18
```

```
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-SMD IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf496228, BIPC FD: 51, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-WNCD_0 IPC Context:
    State: Connected
    BIPC Handle: 0xdf4bb488, BIPC FD: 53, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-WNCMGRD IPC Context:
    State: Connected
    BIPC Handle: 0xdf4a8b58, BIPC FD: 52, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-MOBILITYD IPC Context:
    State: Connected
    BIPC Handle: 0xdf4cddb8, BIPC FD: 54, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0



------------------ show platform software VP R0 summary ------------------

Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       7           Forwarding
  1       9           Forwarding
  1       17          Forwarding
  1       27          Forwarding
  1       28          Forwarding
  1       29          Forwarding
  1       30          Forwarding
  1       31          Forwarding
  1       40          Forwarding
  1       41          Forwarding


Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       49          Forwarding
  1       51          Forwarding
  1       63          Forwarding
  1       72          Forwarding
  1       73          Forwarding
  1       74          Forwarding
```

```
------------------ show platform software VP R0 summary ------------------


Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       7           Forwarding
  1       9           Forwarding
  1       17          Forwarding
  1       27          Forwarding
  1       28          Forwarding
  1       29          Forwarding
  1       30          Forwarding
  1       31          Forwarding
  1       40          Forwarding
  1       41          Forwarding


Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       49          Forwarding
  1       51          Forwarding
  1       63          Forwarding
  1       72          Forwarding
  1       73          Forwarding
  1       74          Forwarding
.
.
.
```

show umbrella

Cisco Umbrella 統合機能に関連する設定を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show umbrella** コマンドを使用します。

show umbrella {**config** | **deviceid** [**detailed**] | **dnscrypt**}

構文の説明

config	デバイスのグローバル設定を表示します。
deviceid	デバイス登録の詳細を表示します。
dnscrypt	DNSCrypt 関連の設定を表示します。

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 Amsterdam 17.1.1	このコマンドが導入されました。

例

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

```
Device> show umbrella config

Umbrella Configuration
=======================
   Token: 0C6ED7E376DD4D2E04492CE7EDFF1A7C00250986
   API-KEY: NONE
   OrganizationID: 2427270
   Local Domain Regex parameter-map name: NONE
   DNSCrypt: Enabled
   Public-key:
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
   UDP Timeout: 5 seconds
   Resolver address:
       1. 208.67.220.220
       2. 208.67.222.222
       3. 2620:119:53::53
       4. 2620:119:35::35
Umbrella Interface Config:
       Number of interfaces with "umbrella out" config: 1
         1. GigabitEthernet1/0/48
              Mode     :  OUT
              VRF      : global(Id: 0)
       Number of interfaces with "umbrella in" config: 1
         1. GigabitEthernet1/0/1
              Mode       : IN
              DCA        : Disabled
              Tag        : test
              Device-id  : 010a2c41b8ab019c
              VRF        : global(Id: 0)
```

```
   Configured Umbrella Parameter-maps:
        1. global
```

次に、**show umbrella deviceid detailed** コマンドの出力例を示します。

```
Device> show umbrella deviceid detailed

Device registration details
 1.GigabitEthernet1/0/2
      Tag               : guest
      Device-id         : 010a6aef0b443f0f
      Description       : Device Id received successfully
      WAN interface     : GigabitEthernet1/0/1
      WAN VRF used      : global(Id: 0)
```

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

```
Device> show umbrella dnscrypt

DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
Certificate Update Status:
Last Successful Attempt : 10:55:40 UTC Apr 14 2016
Last Failed Attempt : 10:55:10 UTC Apr 14 2016
Certificate Details:
Certificate Magic : DNSC
Major Version : 0x0001
Minor Version : 0x0000
Query Magic : 0x717744506545635A
Serial Number : 1435874751
Start Time : 1435874751 (22:05:51 UTC Jul 2 2015)
End Time : 1467410751 (22:05:51 UTC Jul 1 2016)
Server Public Key :
ABA1:F000:D394:8045:672D:73E0:EAE6:F181:19D0:2A62:3791:EFAD:B04E:40B7:B6F9:C40B
Client Secret Key Hash :
BBC3:409F:5CB5:C3F3:06BD:A385:78DA:4CED:62BC:3985:1C41:BCCE:1342:DF13:B71E:F4CF
Client Public key :
ECE2:8295:2157:6797:6BE2:C563:A5A9:C5FC:C20D:ADAF:EB3C:A1A2:C09A:40AD:CAEA:FF76
NM key Hash :
F9C2:2C2C:330A:1972:D484:4DD8:8E5C:71FF:6775:53A7:0344:5484:B78D:01B1:B938:E884
```

show vlan access-map

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

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

構文の説明

map-name	（任意）特定の VLAN アクセスマップ名。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

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

```
Device# show vlan access-map

Vlan access-map "vmap4"  10
  Match clauses:
    ip  address: al2
  Action:
    forward
Vlan access-map "vmap4"  20
  Match clauses:
    ip  address: al2
  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

access-map *name*	（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。
vlan *vlan-id*	（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 モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

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

```
Device# 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

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

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

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

例

次の例では、特定の VLAN グループのメンバを表示する方法を示します。

```
Device# show vlan group group-name group2
vlan group group1 :40-45
```

次に、グループ内の各 VLAN のユーザ数を表示する例を示します。

```
Device# show vlan group group-name group2 user_count

  VLAN     : Count
--------------------
  40        : 5
  41        : 8
  42        : 12
  43        : 2
  44        : 9
  45        : 0
```

ssci-based-on-sci

Secure Channel Identifier（SCI）値に基づいてShort Secure Channel Identifier（SSCI）値を計算するには、MKA ポリシー コンフィギュレーション モードで **ssci-based-on-sci** コマンドを使用します。SCI に基づく SSCI 計算を無効にするには、このコマンドの **no** 形式を使用します。

ssci-based-on-sci
no ssci-based-on-sci

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

SCI 値に基づく SSCI 値の計算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 Gibraltar 16.12.3	このコマンドが導入されました。

使用上のガイドライン

SCI 値が高いほど、SSCI 値は低くなります。

例

次に、SCI に基づく SSCI 計算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)# ssci-based-on-sci
```

関連コマンド

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

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

static	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。
time *time*	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。time 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。
type	エージング タイプを設定します。
absolute	absolute 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。
inactivity	inactivity 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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport port-security aging time 2
Device(config-if)# switchport port-security aging type inactivity
Device(config-if)# switchport port-security aging static
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport port-security aging static
Device(config-if)# end
```

switchport port-security mac-address

セキュアMACアドレスまたはスティッキ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。
vlan 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。
sticky	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。
mac-address	（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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。
- スティッキーセキュア 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、デバイスの再起動時、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すみます。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** 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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
Device(config-if)# end
```

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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Device(config-if)# switchport port-security mac-address sticky 0000.0000.000f
Device(config-if)# end
```

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、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。
- 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** 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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# end
```

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

protect	セキュリティ違反保護モードを設定します。
restrict	セキュリティ違反制限モードを設定します。
shutdown	セキュリティ違反シャットダウン モードを設定します。
shutdown vlan	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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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パケット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パケット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。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/2
Device(config)# switchport port-security violation shutdown vlan
Device(config)# exit
```

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

name	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 Fuji 16.9.2	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> enable
Device# configure terminal
Device(config)# tacacs server server1
Device(config-server-tacacs)# end
```

関連コマンド

Command	Description
address ipv6 (TACACS+)	TACACS+ サーバの IPv6 アドレスを設定します。
key (TACACS+)	TACACS+ サーバでサーバ単位の暗号キーを設定します。
port (TACACS+)	TACACS+ 接続に使用する TCP ポートを指定します。
send-nat-address (TACACS+)	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。
single-connection (TACACS+)	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に送信できるようにします。

Command	Description
timeout(TACACS+)	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。

token（パラメータマップ）

デバイス登録で承認に使用するアプリケーション プログラミング インターフェイス（API）キーを設定するには、パラメータマップタイプ検査コンフィギュレーションモードで**token**コマンドを使用します。固有識別子を削除するには、このコマンドの **no** 形式を使用します。

token *value*
no token

構文の説明

value	API トークン。これは Cisco Umbrella 登録サーバから取得できます。

コマンド デフォルト

パラメータマップのトークンは作成されていません。

コマンド モード

パラメータマップタイプ検査コンフィギュレーション（config-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

token コマンドは、**umbrella in** および **umbrella out** コマンドに対する必須の設定です。

既存のトークンを新しいトークンに変更するには、**umbrella in** コマンドを削除し、適用する新しいトークンのポリシーに対応するようにインターフェイスで再設定します。

例

次に、Cisco Umbrella のトークンを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type umbrella global
Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF
```

関連コマンド

コマンド	説明
parameter-map type umbrella global	Umbrella モードでパラメータマップタイプを設定します。
umbrella	インターフェイスで Cisco Umbrella Connector 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

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

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（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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す。

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、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。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# tracking disable stale-lifetime infinite
Device(config-ipv6-snooping)# end
```

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 コンフィギュレーション（config-nd-inspection）

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、ポートを信頼するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6  nd inspection  policy1
Device(config-nd-inspection)# trusted-port
Device(config-nd-inspection)# end
```

次に、IPv6 スヌーピングポリシー名を policy1 と定義し、ポートを信頼するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
Device(config-ipv6-snooping)# end
```

umbrella

インターフェイスでCisco Umbrella Connector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 **umbrella** コマンドを使用します。この設定を削除するには、このコマンドの **no** 形式を使用します。

umbrella {**in** *tag-name* | **out**}
no umbrella {**in** | **out**}

構文の説明

in	クライアントに接続されているインターフェイスでCisco Umbrella Connectorを設定します。
tag-name	インターフェイスタグ名。 長さは49文字までです。
out	Umbrella サーバに到達するために使用されるインターフェイスで Cisco Umbrella Connector を設定します。

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

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 Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

umbrella in コマンドを設定する前に、**umbrella out** コマンドを設定する必要があります。登録は、ポート443がオープン状態にあり、既存のファイアウォールへのトラフィックのパススルーが許可される場合にのみ成功します。

umbrella in コマンドと **umbrella out** コマンドを同じインターフェイスで設定することはできません。

例

次に、インターフェイスでCisco Umbrella Connectorを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# umbrella out
Device(config-if)# exit
Device(config)# interface GigabitEthernet 1/0/2
Device(config-if)# umbrella in mydevice_tag
```

関連コマンド

コマンド	説明
show umbrella config	デバイスの Cisco Umbrella 統合設定を表示します。

use-updated-eth-header

整合性チェック値（ICV）の計算のために MACsec Key Agreement Protocol Data Unit（MKPDU）の更新されたイーサネットヘッダーを含むデバイスとデバイス上の任意のポートの間の相互運用性を有効にするには、MKA ポリシー コンフィギュレーション モードで **ssci-based-on-sci** コマンドを使用します。ICV 計算のために MKPDU の更新されたイーサネットヘッダ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。

use-updated-eth-header
no use-updated-eth-header

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 計算のためのイーサネットヘッダー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 Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

更新されたイーサネットヘッダーは非標準です。このオプションを有効にすると、デバイス間の MACsec Key Agreement（MKA）セッションを設定できます。

例

次に、ICV 計算のために MKPDU の更新されたイーサネットヘッダー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)# use-updated-eth-header
```

関連コマンド

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

Command	Description
send-secure-announcements	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。
ssci-based-on-sci	SCI に基づいて SSCI を計算します。

username

ユーザ名ベースの認証システムを確立するには、グローバル コンフィギュレーション モードで **username** コマンドを使用します。確立されたユーザ名ベースの認証を削除するには、このコマンドの **no** 形式を使用します。

username *name* [**aaa attribute list** *aaa-list-name*]
username *name*[**access-class** *access-list-number*]
username *name*[**algorithm-type** {**md5** | **scrypt** | **sha256** }]
username *name*[**autocommand** *command*]
username *name*[**callback-dialstring** *telephone-number*]
username *name*[**callback-line** [**tty**]*line-number* [*ending-line-number*]]
username *name*[**callback-rotary** *rotary-group-number*]
username *name*[**common-criteria-policy** *policy-name*]
username *name*[**dnis**]
username *name*[**mac**]
username *name*[**nocallback-verify**]
username *name*[**noescape**]
username *name*[**nohangup**]
username *name*[{**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}]
username *name*[**one-time** {**password** {**0** | **6** | **7** |*password* } | **secret** {**0** | **5** | **8** | **9** |*password*}}]
username *name*[**password** *secret*]
username *name*[**privilege** *level*]
username *name*[**secret** {**0** | **5** |*password*}]
username *name*[**serial-number**]
username *name*[**user-maxlinks** *number*]
username *name*[**view** *view-name*]
no username *name*

構文の説明

name	ホスト名、サーバ名、ユーザ ID、またはコマンド名。*name* 引数には 1 つの単語だけ使用できます。空白や引用符は使用できません。
aaa attribute list *aaa-list-name*	（任意）指定した認証、許可、およびアカウンティング（AAA）方式リストを使用します。
access-class *access-list-number*	（任意）ライン コンフィギュレーション モードで使用可能な **access-class** コマンドで指定されたアクセスリストをオーバーライドする発信アクセスリストを指定します。これはユーザのセッションで使用されます。

algorithm-type	（任意）ユーザのプレーンテキストのシークレットをハッシュするために使用するアルゴリズムを指定します。 • **md5**：MD5アルゴリズムを使用してパスワードをエンコードします。 • **scrypt**：SCRYPT ハッシュアルゴリズムを使用してパスワードをエンコードします。 • **sha256**：PBKDF2 ハッシュアルゴリズムを使用してパスワードをエンコードします。
autocommand *command*	（任意）指定した **autocommand** コマンドがユーザのログイン後に自動的に発行されるようにします。指定した **autocommand** コマンドが完了するとセッションが終了します。このコマンドは任意の長さにすることができ、途中にスペースを含めることもできるため、**autocommand** キーワードを使用するコマンドは行の最後のオプションにする必要があります。
callback-dialstring *telephone-number*	（任意）データ回線終端装置（DCE）デバイスに渡す電話番号を指定できます（非同期コールバックの場合のみ）。
callback-line *line-number*	（任意）特定のユーザ名をコールバックに対して有効にする端末回線（または連続したグループの最初の回線）の相対番号を指定します（非同期コールバックの場合のみ）。番号はゼロから始まります。
ending-line-number	（任意）特定のユーザ名をコールバックに対して有効にする連続したグループの最後の回線の相対番号。キーワード（**tty** など）を省略した場合 、line-number および ending-line-number は相対回線番号ではなく絶対回線番号となります。
tty	（任意）標準の非同期回線を指定します（非同期コールバックの場合のみ）。
callback-rotary *rotary-group-number*	（任意）特定のユーザ名をコールバックに対して有効にするロータリーグループ番号を指定できます（非同期コールバックの場合のみ）。ロータリーグループで次に使用可能な回線が選択されます。範囲は1～100です。
common-criteria-policy	（任意）コモンクライテリアポリシーの名前を指定します。
dnis	（任意）着信番号識別サービス（DNIS）から取得された場合にパスワードを不要にします。
mac	（任意）MAC アドレスをローカルで実行される MAC フィルタリングのユーザ名として使用できるようにします。
nocallback-verify	（任意）指定した回線の EXEC コールバックに認証が不要であることを指定します。

noescape	（任意）ユーザが接続されているホストでエスケープ文字を使用できないようにします。
nohangup	（任意）自動コマンド（**autocommand** キーワードを使用して設定）の実行後に Cisco IOS ソフトウェアでユーザを切断しないようにします。ユーザには、代わりに別のユーザ EXEC プロンプトが表示されます。
nopassword	（任意）ユーザがログインする際のパスワードを不要にします。通常、このキーワードは **autocommand** キーワードを使用する場合に組み合わせて使用すると役立ちます。
password	（任意）*name* 引数にアクセスするためのパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。
password	ユーザが入力するパスワード。
encryption-type	**password** の直後のテキストが暗号化されるかどうか、および暗号化される場合は使用される暗号化タイプを定義する 1 桁の数字。定義されている暗号化タイプは、0（**password** の直後のテキストは暗号化されない）および 6 と 7（テキストはシスコが定義した暗号化アルゴリズムを使用して暗号化される）です。
encrypted-password	ユーザが入力する暗号化パスワード。
one-time	（任意）ユーザ名とパスワードが 1 回だけ有効であることを指定します。この設定は、デフォルトのクレデンシャルがユーザ設定に残らないようにするために使用されます。 • **0**：暗号化されていないパスワードまたはシークレット（設定に依存）が続くことを指定します。 • **6**：暗号化パスワードが続くことを指定します。 • **7**：非表示のパスワードが続くことを指定します。 • **5**：MD5 でハッシュされたシークレットが続くことを指定します。 • **8**：PBKDF2 でハッシュされたシークレットが続くことを指定します。 • **9**：SCRYPT でハッシュされたシークレットが続くことを指定します。
secret	（任意）ユーザのシークレットを指定します。

secret	チャレンジハンドシェイク認証プロトコル（CHAP）認証に使用します。ローカルデバイスまたはリモートデバイスのシークレットを指定します。シークレットはローカルデバイスに暗号化されて格納されます。最大11文字のASCII文字からなる任意の文字列で構成できます。指定できるユーザ名とパスワードの組み合わせの数に制限はないため、任意の数のリモートデバイスを認証できます。
privilege *privilege-level*	（任意）ユーザの特権レベルを設定します。範囲：1 ～ 15。
serial-number	（任意）シリアル番号を指定します。
user-maxlinks *number*	（任意）ユーザに許可されるインバウンドリンクの最大数を指定します。
view *view-name*	（任意）**parser view** コマンドで指定されたCLIビュー名をローカルAAAデータベースに関連付けます（CLIビューの場合のみ）。

コマンド デフォルト

ユーザ名に基づく認証システムは確立されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変
Cisco IOS XE Fuji 16.9.2	こ し

使用上のガイドライン

username コマンドは、ログインだけを目的としてユーザ名、パスワード、またはその両方の認証を行います。

複数の **username** コマンドを使用して、単一ユーザのオプションを指定できます。

ローカルデバイスと通信を行う、認証が必要になるリモートシステムごとに、ユーザ名のエントリを追加します。リモートデバイスには、ローカルデバイスのユーザ名のエントリが必要です。このエントリは、そのリモートデバイスに対応するローカルデバイスのエントリと同じパスワードにする必要があります。

このコマンドは、特殊な取り扱いが必要なユーザ名を定義する場合に便利です。たとえば、このコマンドを使用すると、パスワードが不要で、ユーザを汎用の情報サービスに接続する *info* ユーザ名を定義できます。

username コマンドは、CHAPの設定の一部として必要です。ローカルデバイスが認証を必要とするリモートシステムごとにユーザ名のエントリを追加します。

ローカルデバイスをリモートのCHAPチャレンジに応答できるようにするには、一方の **username** *name* エントリを他方のデバイスにすでに割り当てられている **hostname** エントリと同じにする必要があります。権限レベル1のユーザが上位の権限レベルを開始する状況を回避するには、ユーザ単位の権限レベルを1以外に設定します（たとえば0または2 ～ 15）。ユーザ単位の権限レベルは仮想端末の権限レベルよりも優先されます。

CLI ビューと合法的傍受ビュー

CLI ビューと合法的傍受ビューは、どちらも特定のコマンドと設定情報へのアクセスを制限します。合法的傍受ビューを使用すれば、ユーザは、コールとユーザに関する情報を保存する SNMP コマンドの特別なセットである TAP-MIB 内に保持された合法的傍受コマンドへのアクセスを保護できます。

lawful-intercept キーワードを使用して指定されたユーザは、他の権限レベルまたはビュー名が明示的に指定されていない場合、デフォルトで合法的傍受ビューになります。

secret 引数に値が指定されていない場合、 **debug serial-interface** コマンドが有効になっていると、リンクの確立時にエラーが表示され、CHAP チャレンジは実装されません。CHAP デバッグ情報は、**debug ppp negotiation**、**debug serial-interface**、および **debug serial-packet** コマンドを使用して確認できます。

例

次に、ログインプロンプトで入力できる UNIX の **who** コマンドに似た、デバイスの現在のユーザを一覧表示するサービスを実装する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# username who nopassword nohangup autocommand show users
```

次に、パスワードを使用する必要がない情報サービスを実装する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# username info nopassword noescape autocommand telnet nic.ddn.mil
```

次に、すべての TACACS+ サーバが切断された場合でも機能する ID を実装する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# username superuser password superpassword
```

次に、server_1 のシリアルインターフェイス 0 で CHAP を有効にする例を示します。server_r という名前のリモートサーバのパスワードも定義しています。

```
hostname server_1
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

次に、暗号化されたパスワードを表示する **show running-config** コマンドの出力例を示します。

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

次に、権限レベル 1 のユーザによる 1 よりも高い権限レベルへのアクセスを拒否する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# username user privilege 0 password 0 cisco
Device(config)# username user2 privilege 2 password 0 cisco
```

次に、user2 のユーザ名ベースの認証を削除する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no username user2
```

関連コマンド

Command	Description
debug ppp negotiation	PPP の始動時に、PPP オプションをネゴシエートするパケットを表示します。
debug serial-interface	シリアル接続の障害に関する情報を表示します。
debug serial-packet	**debug serial interface** コマンドを使用して取得できるルインターフェイスのデバッグ情報を表示します。

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、デバイス上でグローバル 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*]

構文の説明

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

コマンド デフォルト

VLAN に適用する VLAN マップ エントリまたは VLAN マップはありません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

例

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

```
Device> enable
Device# configure terminal
Device(config)# vlan access-map vac1
Device(config-access-map)# match ip address acl1
Device(config-access-map)# action forward
Device(config-access-map)# end
```

次の例では、VLAN マップ vac1 を削除する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# no vlan access-map vac1
Device(config)# exit
```

vlan dot1Q tag native

トランクポートのネイティブVLANでdot1q（IEEE 802.1Q）のタギ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ギングが取り除かれます。

ネイティブ VLAN でのタギングを維持し、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）タギ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
show vlan dot1q tag native	ネイティブVLANのタギングのステータスを表示します。

vlan filter

VLAN マップを 1 つまたは複数の VLAN に適用するには、グローバル コンフィギュレーション モードで **vlan 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**}

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

例

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

```
Device> enable
Device# configure terminal
Device(config)# vlan filter map1 vlan-list 20, 30
Device(config)# exit
```

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。

```
Device> enable
Device# configure terminal
Device(config)# no vlan filter map1 vlan-list 20
Device(config)# exit
```

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

vlan group

VLANグループを作成または変更するには、グローバルコンフィギュレーションモードで**vlan group**コマンドを使用します。VLANグループからVLANリストを削除するには、このコマンドの**no**形式を使用します。

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

構文の説明

group-name	VLANグループの名前。名前は最大32文字で、文字から始める必要があります。
vlan-list *vlan-list*	VLANグループに追加される1つ以上のVLANを指定します。*vlan-list*引数には単一のVLAN ID、VLAN ID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 Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

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

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

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

例

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

```
Device> enable
Device# configure terminal
Device(config)# vlan group group1 vlan-list 7-9,11
Device(config)# exit
```

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。

```
Device> enable
Device# configure terminal
Device(config)# no vlan group group1 vlan-list 7
Device(config)# exit
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。