CHAPTER 2

Catalyst 4500 シリーズ スイッチの Cisco IOS コマンド

この章では、Catalyst 4500 シリーズ スイッチの Cisco IOS コマンドをアルファベット順に説明します。このマニュアルに記載されていない Cisco IOS コマンドの詳細については、次の URL で Cisco IOS Release 12.2 に関するコンフィギュレーション ガイドおよびコマンド リファレンスを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_product_indices_list.html

#macro keywords

macro キーワードに関するヘルプ ストリングを指定するには、**#macro keywords** コマンドを使用します。

#macro keywords [**keyword1**] [**keyword2**] [**keyword3**]

構文の説明

keyword 1	（任意）インターフェイスにマクロを適用する場合に必要なキーワードを指定します。
keyword 2	（任意）インターフェイスにマクロを適用する場合に必要なキーワードを指定します。
keyword 3	（任意）インターフェイスにマクロを適用する場合に必要なキーワードを指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

マクロの必須キーワードを指定しない場合、マクロは無効と見なされ、適用しようとすると失敗します。**#macro keywords** コマンドを入力すると、構文を有効にするために指定する必要があるものを示すメッセージが表示されます。

例

次の例では、test という名前のマクロに関連付けられているキーワードのヘルプ ストリングを指定する方法を示します。

```
Switch(config)# macro name test
macro name test
Enter macro commands one per line. End with the character '@'.
#macro keywords $VLAN $MAX
swichport
@

Switch(config)# int gi1/1
Switch(config-if)# macro apply test ?
  WORD  Keyword to replace with a value e.g $VLAN, $MAX   << It is shown as help
  <cr>
```

関連コマンド

コマンド	説明
macro apply cisco-desktop	スイッチ ポートを標準デスクトップに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-phone	スイッチ ポートを標準デスクトップおよび Cisco IP Phone に接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-router	スイッチ ポートをルータに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-switch	スイッチ ポートを別のスイッチに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。

aaa accounting dot1x default start-stop group radius

802.1X 認証セッションのアカウンティングをイネーブルにするには、**aaa accounting dot1x default start-stop group radius** コマンドを使用します。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 default start-stop group radius

no aaa accounting dot1x default start-stop group radius

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。

デフォルト

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 モード

コマンド履歴

リリース	変更箇所
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

802.1X アカウンティングには、RADIUS サーバが必要です。

このコマンドは、認証、許可、アカウンティング（AAA）クライアントのアカウンティング機能をイネーブルにして、802.1X サプリカント（ワークステーション クライアント）から認証（RADIUS）サーバに 802.1X 更新およびウォッチドッグ パケットを転送できるようにします。（ウォッチドッグ パケットは EAPOL-LOGON、EAPOL-LOGOFF、EAPOL-INTERIM メッセージのことです）。これらのパケットが有効と見なされ、転送される前に、認証サーバによるサプリカントの正常な認証および許可が必要です。クライアントが再認証されると、暫定アップデート アカウンティング通知がアカウンティング サーバに送信されます。

例

次の例では、802.1X アカウンティングを設定する方法を示します。

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

（注）　RADIUS 認証サーバは、AAA クライアントから更新パケットやウォッチドッグ パケットを受け入れて記録するよう、適切に設定する必要があります。

関連コマンド

コマンド	説明
aaa accounting system default start-stop group radius	スイッチの再起動後にセッション終了メッセージを受信します。

aaa accounting system default start-stop group radius

スイッチの再起動後にセッション終了メッセージを受信するには、**aaa accounting system default start-stop group radius** コマンドを使用します。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 system default start-stop group radius

no aaa accounting system default start-stop group radius

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。

デフォルト

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 モード

コマンド履歴

リリース	変更箇所
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

802.1X アカウンティングには、RADIUS サーバが必要です。

このコマンドは、AAA クライアントのアカウンティング機能をイネーブルにして、802.1X サプリカント（ワークステーション クライアント）から認証（RADIUS）サーバに 802.1X 更新およびウォッチドッグ パケットを転送できるようにします。（ウォッチドッグ パケットは EAPOL-LOGON、EAPOL-LOGOFF、EAPOL-INTERIM メッセージのことです）。これらのパケットが有効と見なされ、転送される前に、認証サーバによるサプリカントの正常な認証および許可が必要です。クライアントが再認証されると、暫定アップデート アカウンティング通知がアカウンティング サーバに送信されます。

例

次の例では、スイッチの再起動後にログオフを生成する方法を示します。

```
Switch(config)# aaa accounting system default start-stop group radius
```

（注）　RADIUS 認証サーバは、AAA クライアントから更新パケットやウォッチドッグ パケットを受け入れて記録するよう、適切に設定する必要があります。

関連コマンド

コマンド	説明
aaa accounting dot1x default start-stop group radius	802.1X 認証セッションのアカウンティングをイネーブルにします。

access-group mode

優先モード（たとえば、VACL は PACL よりも優先されます）および非優先モード（たとえば、マージ モードまたはストリクト モード）を指定するには、**access-group mode** コマンドを使用します。優先ポート モードに戻すには、このコマンドの **no** 形式を使用します。

access-group mode {**prefer** {**port** | **vlan**} | **merge**}

no access-group mode {**prefer** {**port** | **vlan**} | **merge**}

構文の説明

prefer port	PACL が設定されている場合、PACL モードが優先するように指定します。PACL 機能がポートで設定されていない場合、インターフェイスに適用可能なその他の機能がこのインターフェイスに統合され、適用されます。
prefer vlan	VLAN-based ACL モードが優先するように指定します。ポートの VLAN に VLAN-based ACL 機能が設定されていない場合は、ポートの PACL 機能が適用されます。
merge	適用可能な ACL 機能をマージしてからハードウェアにプログラムします。

デフォルト

PACL 優先モード

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

レイヤ 2 インターフェイスでは、prefer port、prefer VLAN、および merge の各モードがサポートされています。レイヤ 2 インターフェイスには、どちらの方向（受信側に 1 つおよび発信側に 1 つ）にも適用される 1 つの IP ACL を設定できます。

例

次の例では、スイッチで PACL モードを有効にする方法を示します。

```
(config-if)# access-group mode prefer port
```

次の例では、適用可能な ACL 機能を統合する方法を示します。

```
(config-if)# access-group mode merge
```

関連コマンド

コマンド	説明
show access-group mode interface	レイヤ 2 インターフェイスの ACL コンフィギュレーションを表示します。
show ip interface（Cisco IOS のマニュアルを参照）	IP インターフェイス コンフィギュレーションを表示します。
show mac access-group interface	レイヤ 2 インターフェイスの ACL コンフィギュレーションを表示します。

access-list hardware capture mode

制御パケットのキャプチャ モードを選択するには、**access-list hardware capture mode** コマンドを使用します。

access-list hardware capture mode {**global** | **vlan**}

構文の説明

global	すべての VLAN で制御パケットのキャプチャをグローバルに指定します。
vlan	特定の VLAN で制御パケットのキャプチャを指定します。

デフォルト

制御パケットはグローバルにキャプチャされます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(40)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

キャプチャ モードを設定する前に、設定を確認し変更して、グローバルに DHCP スヌーピングまたは IGMP スヌーピングなどの機能をディセーブルにし、代わりに特定の VLAN でこれらの機能をイネーブルにすることを推奨します。

パス管理モードに変更すると、VLAN ごとに CAM エントリがハードウェアにプログラミングされるまで、制御トラフィックは最初にハードウェアでブリッジングされるか、またはドロップされる可能性があることに注意してください。

VLAN でイネーブルになっている機能のために、メンバ ポートまたは VLAN のアクセス コントロール設定によって、CPU への制御パケットの転送が拒否されたりドロップされたりしないようにする必要があります。制御パケットが許可されていない場合、特定の機能は機能しません。

例

次の例では、制御パケットのキャプチャをイネーブルにするように設定されている VLAN で制御パケットをキャプチャするようにスイッチを設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# access-list hardware capture mode vlan
Switch(config)# end
Switch#
```

次の例では、（スタティック ACL を使用して）すべての VLAN 上でグローバルに制御パケットをキャプチャするようにスイッチを設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# access-list hardware capture mode global
Switch(config)# end
Switch#
```

次の例では、すべての VLAN で制御パケットをグローバルにキャプチャするようにスイッチを設定するもう 1 つの方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no access-list hardware capture mode vlan
Switch(config)# end
Switch#
```

access-list hardware entries

スイッチのハードウェアに ACL をプログラムする方法を指定するには、**access-list hardware entries** コマンドを使用します。

access-list hardware entries {**packed** | **scattered**}

構文の説明

packed	ACL の ACE をプログラムするために、ACL TCAM からエントリを選択するとき、条件に一致する（マスク使用）最初のエントリをソフトウェアが使用するように指定します。
scattered	ACL の ACE をプログラムするために、ACL TCAM からエントリを選択するとき、マスクなしで最初のエントリをソフトウェアが使用するように指定します。

デフォルト

ACL は packed としてプログラムされます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(20)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ACL をプログラムすると、エントリおよびマスクの 2 種類のハードウェア リソースが使用されます。これらのリソースの 1 つが消費されると、新たな ACL をハードウェアにプログラミングすることはできません。マスクは消費されるが、エントリが使用できる場合は、マスクを使用可能にするためにプログラミング アルゴリズムを **packed** から **scattered** に変更します。この操作により、新たな ACL をハードウェアにプログラムできるようになります。

目的は、TCAM リソースをより効率的に使用すること、つまり、ACL エントリごとのマスク数を最小化することです。**scattered** アルゴリズムまたは **packed** アルゴリズムを使用している場合の TCAM 使用率を比較するには、**show platform hardware acl statistics utilization brief** コマンドを使用します。アルゴリズムを **packed** から **scattered** に変更するには、**access-list hardware entries** コマンドを使用します。

例

次の例では、ACL を packed としてハードウェアにプログラムする方法を示します。プログラミング後、ACL エントリの 49% だけをプログラムするためにマスクの 89% が必要になります。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# access-list hardware entries packed
Switch(config)# end
Switch#
01:15:34: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch# show platform hardware acl statistics utilization brief
Entries/Total(%)  Masks/Total(%)
                                    -----------------  ---------------
```

```
            Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   460 /  512 ( 89)
            Input  Acl(PortOrVlan)      6 / 4096 (  0)     4 /  512 (  0)
            Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)

            L4Ops: used 2 out of 64
Switch#
```

This example shows how to reserve space (scatter) between ACL entries in the hardware. The number of masks required to program 49 percent of the entries has decreased to 49 percent.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# access-list hardware entries scattered
Switch(config)# end
Switch#
01:39:37: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch# show platform hardware acl statistics utilization brief
Entries/Total(%)  Masks/Total(%)
                                    -----------------  ---------------
            Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   252 /  512 ( 49)
            Input  Acl(PortOrVlan)      6 / 4096 (  0)     5 /  512 (  0)
            Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)

            L4Ops: used 2 out of 64
Switch#
```

access-list hardware region

ハードウェアの TCAM 領域のバランスを変更するには、**access-list hardware region** コマンドを使用します。

access-list hardware region {**feature** | **qos**} {**input** | **output**} **balance** {*bal-num*}

構文の説明

feature	ACL の領域バランスを調整します。
qos	QoS の領域バランスを調整します。
input	入力 ACL および入力 QoS の領域バランスを調整します。
output	出力 ACL および出力 QoS の領域バランスを調整します。
balance *bal-num*	TCAM 内の PandV 領域および PorV 領域の相対サイズを指定します。有効値の範囲は 1 ～ 99 です。

デフォルト

各 TCAM のデフォルトの領域バランスは 50 です。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

PandV は、フロー ラベルのポート部分および VLAN タグ部分の両方をマスクするエントリを含む TCAM 領域です。

PorV は、フロー ラベルのポート部分または VLAN タグ部分のどちらか一方だけをマスクするエントリを含む TCAM 領域です。

バランスを 1 にすると、割り当てられる PandV 領域のエントリ数が最小になり、PorV 領域のエントリ数が最大になります。バランスを 99 にすると、割り当てられる PandV 領域のエントリ数が最大になり、PorV 領域のエントリ数が最小になります。バランスを 50 にすると、指定した TCAM 内の PandV 領域および PorV 領域に割り当てられるエントリ数が同じになります。

4 つの TCAM のバランスは別々に変更できます。

例

次の例では、MAC アドレスがポートに追加されたときに MAC 通知トラップをイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# access-list hardware region feature input balance 75
Switch(config)#
```

action

VACL で一致するものがあった場合に実行されるアクションを指定するには、**action** コマンドを使用します。action 句を削除するには、このコマンドの **no** 形式を使用します。

action {**drop** | **forward**}

no action {**drop** | **forward**}

構文の説明

drop	パケットをドロップするようにアクションを設定します。
forward	パケットを宛先に転送するようにアクションを設定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

VLAN アクセスマップ モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

VLAN アクセス マップでは、特定のパケット タイプ（IP または MAC）に ACL が 1 つ以上設定されている場合、そのパケット タイプのデフォルト アクションは **drop**（拒否）です。

特定のパケット タイプに ACL が設定されていない場合、そのパケット タイプのデフォルト アクションは **forward**（許可）です。

特定のパケット タイプに ACL が設定されていて、その ACL が空または未定義の場合、設定されたアクションがこのパケット タイプに適用されます。

例

次の例では、ドロップ アクションを定義する方法を示します。

```
Switch(config-access-map)# action drop
Switch(config-access-map)#
```

次の例では、転送アクションを定義する方法を示します。

```
Switch(config-access-map)# action forward
Switch(config-access-map)#
```

構文の説明

コマンド	説明
match	VLAN アクセス マップ シーケンスの 1 つまたは複数の ACL を選択して、match 句を指定します。
show vlan access-map	VLAN アクセス マップの内容を表示します。
vlan access-map	VLAN アクセス マップを作成するための VLAN アクセス マップ コマンド モードを開始します。

active

宛先プロファイルをイネーブルにするには、**active** コマンドを使用します。

active

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

cfg-call-home-profile

コマンド履歴

リリース	変更箇所
12.2(52)SG	Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

デフォルトでは、プロファイルは作成時にイネーブルになります。

例

次の例では、宛先プロファイルをイネーブルにする方法を示します。

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# active
```

関連コマンド

コマンド	説明
destination address	Call Home メッセージが送信される宛先電子メール アドレスまたは URL を設定します。
destination message-size-limit bytes	宛先プロファイルの最大宛先メッセージ サイズを設定します。
destination preferred-msg-format	優先するメッセージ形式を設定します。
destination transport-method	メッセージの転送形式をイネーブルにします。
profile	プロファイル call-home コンフィギュレーション サブモードを開始します
subscribe-to-alert-group all	使用可能なすべてのアラート グループに登録します。
subscribe-to-alert-group configuration	この宛先プロファイルを Configuration アラート グループに登録します。
subscribe-to-alert-group diagnostic	この宛先プロファイルを Diagnostic アラート グループに登録します。
subscribe-to-alert-group environment	この宛先プロファイルを Environment アラート グループに登録します。

コマンド	説明
subscribe-to-alert-group inventory	この宛先プロファイルを Inventory アラート グループに登録します。
subscribe-to-alert-group syslog	この宛先プロファイルを Syslog アラート グループに登録します。

ancp client port identifier

ANCP クライアントのマッピングを作成して、ANCP がマルチキャスト ストリームを開始または停止する必要があるインターフェイスを識別するには、**ancp client port identifier** コマンドを使用します。

ancp client port identifier *identifying name* **vlan** *vlan number* **interface** *interface*

構文の説明

identifier name	VLAN のインターフェイス メンバを指定するために ANCP サーバによって使用される ID。
vlan number	VLAN 識別番号。
interface	この VLAN のインターフェイス メンバ。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ANCP サーバは、DHCP オプション 82 回線 ID またはこのコマンドで作成された ID を使用してポートを識別します。2 つの方法のいずれかだけを使用します。交互に使用しないでください。DHCP オプション 82 を使用すると、ANCP サーバによって使用されるポート ID（16 進数）は 0x01060004[vlan][intf] になります。たとえば、VLAN 19 およびファスト イーサネット インターフェイス 2/3 は 0x0106000400130203 になります。ただし、ポート ID を使用する場合は、CLI で出力される文字列と同じ文字列を使用します。

（注）　このコマンドを使用できるのは、ANCP クライアント モードで **ancp mode client** コンフィギュレーション コマンドを使ってボックスを設定した場合だけです。

例

次の例では、文字列 NArmstrong で VLAN 10 にあるファスト イーサネット インターフェイス 7/3 を識別する方法を示します。

```
Switch# ancp client port identifier NArmstrong vlan 10 interface FastEthernet 7/3
```

関連コマンド

コマンド	説明
ancp mode client	ルータを ANCP クライアントになるよう設定します。

ancp client server

リモート ANCP サーバの IP アドレスを設定するには、**ancp client server** コマンドを使用します。

ancp client server *ipaddr of server* **interface** *interface*

構文の説明

ipaddr of server	クライアントが TCP で接続する必要がある ANCP サーバの IP アドレス。
interface	接続に使用するインターフェイス。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

複数のインターフェイスをサーバへの接続に使用でき、適切なルーティングが設定されている場合、インターフェイスには ANCP サーバに対して接続されたダイレクト インターフェイス（1 つだけの場合）またはループバック インターフェイスを指定できます。（IP アドレスがこのインターフェイスで設定されている必要があり、シャットダウン ステートにしないでください）。ANCP クライアントをアクティブにするには、**ancp mode client** コマンドとともに **ancp client server** コマンドが必要です。このコマンドを入力すると、ANCP クライアントはリモート サーバへの接続を試行します。

例

次の例では、ANCP クライアントが接続する必要がある ANCP サーバの IP アドレスを ANCP クライアントに示す方法を示します。

```
Switch# ancp client server 10.1.2.31 interface FastEthernet 2/1
```

関連コマンド

コマンド	説明
ancp mode client	ルータを ANCP クライアントになるよう設定します。

ancp mode client

ルータを ANCP クライアントになるように設定するには、**ancp mode client** コマンドを使用します。

ancp mode client

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

完全に ANCP をアクティブにするには、管理者は、ANCP クライアントが接続する必要がある ANCP サーバの IP アドレスも設定する必要があります。

例

次の例では、ANCP クライアントになるようにルータを設定する方法を示します。

```
Switch# ancp mode client
```

関連コマンド

コマンド	説明
ancp client server	ANCP によってアクティブにされたマルチキャスト ストリームを表示します。

apply

新しい VLAN データベースの実装、設定番号の増分、NVRAM への設定番号の保存、管理ドメイン全体への設定番号の伝播を行うには、**apply** コマンドを使用します。

apply

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

VLAN コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

apply コマンドは、VLAN データベース モードを開始したあとに行った設定変更を適用し、この設定変更を実行コンフィギュレーションに使用します。このコマンドを実行しても、VLAN データベース モードのまま変更はありません。

スイッチが VTP クライアント モードの場合は、このコマンドを使用できません。

VLAN データベースが変更されたことを確認するには、特権 EXEC モードから **show vlan** コマンドを入力します。

例

次の例では、新しく設定中の VLAN データベースを実装し、これを現在のデータベースとして認識させる方法を示します。

```
Switch(config-vlan)# apply
Switch(config-vlan)#
```

関連コマンド

コマンド	説明
exit（Cisco IOS のマニュアルを参照）	スイッチからログアウトして、アクティブなターミナル セッションを閉じます。
reset	新しく設定しようとしている VLAN データベースの設定内容を放棄し、VLAN コンフィギュレーション モードを継続したまま、現在実行中の VLAN データベースと同じ設定内容になるよう新規設定中のデータベースをリセットします。
show vlan	VLAN 情報を表示します。
shutdown vlan（Cisco IOS のマニュアルを参照）	VLAN のスイッチングをシャットダウンします。
vtp（グローバル コンフィギュレーション モード）	VTP コンフィギュレーション ストレージ ファイルの名前を変更します。

arp access-list

ARP アクセス リストを定義したり、定義済みリストの末尾に句を追加するには、**arp access-list** コマンドを使用します。

arp access-list *name*

構文の説明

name	アクセス コントロール リストの名前を指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、static-hosts という名前の ARP アクセス リストを定義する方法を示します。

```
Switch(config)# arp access-list static-hosts
Switch(config)#
```

関連コマンド

コマンド	説明
deny	DHCP バインディングとの照合に基づいて ARP パケットを拒否します。
ip arp inspection filter vlan	DAI がイネーブルの場合にスタティック IP が設定されたホストからの ARP を許可したり、ARP アクセス リストを定義して VLAN に適用したりします。
permit	DHCP バインディングとの一致に基づいて ARP パケットを許可します。

attach module

特定のモジュールにリモートから接続するには、**attach module** コンフィギュレーション コマンドを使用します。

attach module *mod*

構文の説明

mod	コマンドのターゲット モジュール。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドが適用されるのは、Catalyst 4500 シリーズ スイッチのアクセス ゲートウェイ モジュールのみです。

mod に指定できる値は、使用するシャーシによって異なります。たとえば、Catalyst 4506 シャーシを使用する場合、モジュールに指定できる値は 2 ～ 6 です。4507R シャーシを使用する場合、有効値の範囲は 3 ～ 7 です。

attach module *mod* コマンドを実行すると、プロンプトが Gateway# に変化します。

このコマンドは、**session module** *mod* コマンドおよび **remote login module** *mod* コマンドで実行されるアクションと同じです。

例

次の例では、アクセス ゲートウェイ モジュールにリモートからログインする方法を示します。

```
Switch# attach module 5
Attaching console to module 5
Type 'exit' at the remote prompt to end the session

Gateway>
```

関連コマンド

コマンド	説明
remote login module	特定のモジュールにリモートから接続します。
session module	仮想コンソールを使用して、スタンバイ スーパーバイザ エンジンにログインします。

authentication control-direction

ポート制御を単方向または双方向に変更するには、インターフェイス コンフィギュレーション モードで **authentication control-direction** 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 control-direction {**both** | **in**}

no authentication control-direction

構文の説明

both	ポートで双方向制御をイネーブルにします。
in	ポートで単方向制御をイネーブルにします。

コマンド デフォルト

both

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

authentication control-direction コマンドは、Cisco IOS Release 12.2(50)SG およびそれ以降のリリースで推奨されなくなった、次の dot1x コマンドに替わるコマンドです。

dot1x control-direction {**both** | **in**}

IEEE 802.1X 標準では、認証されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、クライアント/サーバベースのアクセス コントロールと認証プロトコルが定義されています。

IEEE 802.1X は、ポートごとに 2 つの異なる仮想アクセス ポイントを作成してネットワーク アクセスを制御します。一方のアクセス ポイントが未制御ポート、もう一方は制御ポートです。単一のポートを通過するすべてのトラフィックは、両方のアクセス ポイントを利用できます。IEEE 802.1X では、スイッチ ポートに接続している各ユーザ デバイスを認証し、VLAN にポートを割り当ててから、スイッチまたは LAN で提供されるサービスを利用できるようにします。802.1X アクセス コントロールでは、デバイスが認証されるまで、そのデバイスが接続しているポートを介して Extensible Authentication Protocol（EAP）over LAN（EAPOL）トラフィックだけを許可します。認証が成功すると、通常のトラフィックがポートを通過できるようになります。

- 単方向状態：**dot1x control-direction** 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単方向に設定した場合、そのポートのスパニングツリーはフォワーディング ステートに変化します。

  単方向制御ポートがイネーブルになると、接続したホストはスリーピング モードまたは電源切断状態になります。ホストはそのネットワークの他の装置とトラフィックを交換しません。ホストがネットワークにトラフィックを送信できない単方向ポートに接続されている場合、ホストはネットワークの他の装置からのトラフィックだけを受信します。

- 双方向状態：**dot1x control-direction** 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双方向に設定した場合、そのポートは双方向でアクセス コントロールされます。この状態のスイッチ ポートが送信できるのは EAPOL のみです。

both キーワードを使用するか、またはこのコマンドの **no** 形式を使用すると、ポートはデフォルト設定の双方向モードに変更されます。

ポートを双方向に設定すると、Wake-on-LAN（WoL）による 802.1X 認証がイネーブルになります。

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

例

次の例では、単方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# authentication control-direction in
Switch(config-if)#
```

次の例では、双方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# authentication control-direction both
Switch(config-if)#
```

次の例では、デフォルト設定に戻す方法を示します。

```
Switch(config-if)# no authentication control-direction
Switch(config-if)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication critical recovery delay

802.1X クリティカル認証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 **authentication critical recovery delay** 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 critical recovery delay *milliseconds*

no authentication critical recovery delay

構文の説明

milliseconds	使用不能になっていた RADIUS サーバが使用可能になったときに、クリティカルなポートの再初期化を待機するリカバリ遅延期間（ミリ秒）を指定します。有効値の範囲は 1 ～ 10000 ミリ秒です。

コマンド デフォルト

10000 ミリ秒

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

authentication critical recovery delay コマンドは、Cisco IOS Release 12.2(50)SG およびそれ以降のリリースで推奨されなくなった、次の dot1x コマンドに替わるコマンドです。

dot1x critical recovery delay *milliseconds*

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

例

次の例では、使用不能になっていた RADIUS サーバが使用可能になったときに、クリティカルなポートの再初期化をスイッチが待機するリカバリ遅延期間を設定する方法を示します。

```
Switch(config)# authentication critical recovery delay 1500
Switch(config)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication event

認証イベントにアクションを設定するには、**authentication event** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

authentication event fail [**retry** *count*] **action** [**authorize vlan** *vlan* | **next-method**}

authentication event server {**alive action reinitialize** | **dead action authorize [vlan** *vlan*] | **voice** | **dead action reinitialize [vlan** *vlan*]}}

authentication event no-response action authorize vlan *vlan*]}

no authentication event {**fail}** | {**server** {**alive** | **dead**}} | {**no-response**}

構文の説明

fail	間違ったユーザ資格情報によって認証が失敗した場合の動作を指定します。
retry *count*	（任意）失敗した認証を再試行する回数を指定します。有効値の範囲は 0 ～ 5 です。デフォルトは 2 です。
fail action authorize vlan *vlan*	間違ったユーザ資格情報によって認証が失敗した場合に、特定の VLAN に対してポートを許可します。
fail action next-method	認証イベントに必要なアクションが次の認証方式に移行することを指定します。
server alive action reinitialize	認証イベントで許可されたすべてのクライアントを再初期化するように、認証、許可、アカウンティング（AAA）サーバのアライブ アクションを設定します。
server dead action authorize [vlan ***vlan*** **| voice**	認証イベントのデータまたは音声クライアントを許可するように、AAA サーバのデッド アクションを設定します。
server dead action reinitialize vlan *vlan*	認証イベントのすべての許可済みのデータ クライアントを再初期化するように、AAA サーバのデッド アクションを設定します。
no-response action authorize	クライアントが 802.1X をサポートしていない場合に、特定の VLAN に対してポートを許可します。

コマンド デフォルト

デフォルト設定は、次のとおりです。

- デフォルトの *count* は 2 です。
- 現在の認証方式は、AAA サーバが到達可能になるまで無制限に再試行されます（常に失敗します）。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

authentication event fail コマンドは、Cisco IOS Release 12.2(50)SG およびそれ以降のリリースで推奨されなくなった、次の 802.1X コマンドに替わるコマンドです。

- [**no**] **dot1x auth-fail max-attempts** *count*
- [**no**] **dot1x auth-fail vlan** *vlan*

authentication event fail コマンドがサポートされている唯一の目的は、802.1X で認証エラーを伝えることです。デフォルトでは、この障害タイプでは認証方式が再試行されます。設定された VLAN のポートを許可するか、または次の認証方式にフェールオーバーするように設定できます。任意で、このアクションを実行する前に認証のリトライ回数を指定できます。

authentication event server コマンドは、Cisco IOS Release 12.2(50)SG およびそれ以降のリリースで推奨されなくなった、次の 802.1X コマンドに替わるコマンドです。

- [**no**] **dot1x critical**
- [**no**] **dot1x critical vlan** *vlan*
- [**no**] **dot1x critical recover action initialize**

authentication event server コマンドは、AAA サーバが到達不能になり、指定した VLAN でポートを許可する場合の動作を指定します。

authentication server alive action コマンドは、AAA サーバが再び到達可能になったときに実行されるアクションを指定します。

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

authentication event no-response コマンドは、Cisco IOS Release 12.2(50)SG およびそれ以降のリリースで推奨されなくなった、次の 802.1X コマンドに替わるコマンドです。

- [**no**] **dot1x guest-vlan** *vlan*

authentication event no-response コマンドは、クライアントが 802.1X をサポートしていない場合に実行するアクションを指定します。

例

次の例では、間違ったユーザ資格情報によって認証が失敗した場合に、次の認証方式に処理を進めるように指定する方法を示します。

```
Switch(config-if)# authentication event fail action next-method
Switch(config-if)#
```

次の例では、認証イベントで許可されたすべてのクライアントを再初期化するように AAA サーバのアライブ アクションを指定する方法を示します。

```
Switch(config-if)# authentication event server alive action reinitialize
Switch(config-if)#
```

次の例では、認証イベントでポートを許可するように AAA サーバのデッド アクションを指定する方法を示します。

```
Switch(config-if)# authentication event server dead action authorize
Switch(config-if)#
```

次の例では、クライアントが 802.1X をサポートしていない場合に、認証イベントでポートを許可する条件を指定する方法を示します。

```
Switch(config-if)# authentication event authentication event no-response action authorize
vlan 10
Switch(config-if)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication fallback

WebAuth フォールバックをイネーブルにして、WebAuth にフェールオーバーする場合に使用するフォールバック プロファイルを指定するには、**authentication fallback** インターフェイス 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 fallback *profile*

構文の説明

profile	WebAuth にフェールオーバーする場合に使用する名前（最大 200 文字）。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、802.1X がタイムアウトし、MAB が失敗すると、WebAuth がイネーブルになります。

authentication fallback コマンドは、Cisco IOS Release 12.2(50)SG およびそれ以降のリリースで推奨されなくなった、次の dot1x コマンドに替わるコマンドです。

[no] dot1x fallback profile

WebAuth フォール バック機能では、802.1X サプリカントが存在せず、WebAuth 方式にフォール バックする管理対象デバイスでないクライアントの使用が可能になります。

show authentication 特権 EXEC コマンドを使用して設定を確認できます。

例

次の例では、WebAuth フォール バックをイネーブルにして、WebAuth にフェールオーバーする場合に使用するフォール バック プロファイルを指定する方法を示します。

```
Switch(config-if)# authentication fallback fallbacktest1
Switch(config-if)#
```

次の例では、WebAuth フォールバックをディセーブルにする方法を示します。

```
Switch(config-if)# no authentication fallback fallbacktest1
Switch(config-if)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication host-mode

ホスト モード コンフィギュレーションでアクセス ポリシーを適用するときに使用するセッションの分類を定義するには、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 {**single-host** | **multi-auth** | **multi-domain** | **multi-host**} [**open**]

[no] authentication host-mode {**single-host** | **multi-auth** | **multi-domain** | **multi-host**} [**open**]

構文の説明

single-host	セッションをインターフェイス セッションとして指定し、ポートで 1 つのクライアントだけを許可します。これは、802.1X をイネーブルにした場合のデフォルトのホスト モードです。
multi-auth	セッションを MAC-based セッションとして指定します。データ ドメインのポートでは任意の数のクライアントを許可し、音声ドメインでは 1 つのクライアントだけを許可します。ただし、各クライアントは個別に認証する必要があります。
multi-domain	MAC アドレスとドメインの組み合わせに基づいてセッションを指定します。ドメイン単位では 1 つの MAC アドレスだけが許可されるという制限が付きます。
multi-host	セッションをインターフェイス セッションとして指定します。ただし、ポートでは複数のクライアントを許可します。
open	（任意）ポートにオープン ポリシーのホスト モードを設定します。

コマンド デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

single-host モードでは、セッションがインターフェイス セッションとして分類されます（インターフェイスごとに 1 つの MAC アドレスなど）。ポートではクライアントが 1 つだけ許可され、クライアントにダウンロードされたポリシーはポート全体に適用されます。複数のクライアントが検出された場合は、セキュリティ違反がトリガーされます。

multi-host モードでは、セッションがインターフェイス セッションとして分類されますが、single-host モードと異なり、複数のクライアントをポートに適用できます。ポートで最初に検出されたクライアントだけが認証され、残りのクライアントは最初のクライアントと同じアクセス権を継承します。最初のクライアントにダウンロードされたポリシーは、ポート全体に適用されます。

multi-domain モードでは、MAC アドレスとドメインの組み合わせに基づいてセッションを分類します。ドメイン単位で許可される MAC アドレスは 1 つだけという制限があります。スイッチング環境のドメインは VLAN を示し、データ ドメインと音声ドメインの 2 つのドメインがサポートされます。特

定のドメインで許可されるクライアントは 1 つだけです。したがって、サポートされるクライアント（MAC）はポート 1 つに対して 2 つだけです。各クライアントは個別に認証する必要があります。クライアントにダウンロードされたポリシーは、そのクライアントの MAC/IP だけに適用されるので、同じポート上のもう一方のクライアントには影響しません。クライアントは、別の方法を使用して認証できます（PC の 802.1X、IP 電話の MAB など、またはその逆）。認証の順序に制限はありません。

上記の説明に関して 1 つだけ注意する点は、Web ベースの認証を使用できるのはデータ デバイスだけだということです。これは、データ デバイスを操作するのがほとんどの場合にユーザであることと、HTTP 機能を持つためです。また、Web ベースの認証が MDA モードに設定されている場合、デバイスの種類を問わず実行できるのは、Downloadable ACL（dACL; ダウンロード可能 ACL）形式だけです。Web ベースの認証は VLAN 割り当てをサポートしていないため、制限が適用されます。さらに、データ デバイスに dACL を使用し、音声デバイスには使用していない場合、ユーザのデータが WebAuth にフォール バックすると、音声トラフィックはフォールバック ポリシーに基づいて適用される ACL の影響を受けます。したがって、MDA 対応ポートのフォールバックとして WebAuth を設定した場合、サポートされる実行方式は dACL だけです。

multi-auth モードでは、セッションが MAC-based として分類されます。ポート データ ドメインで許可されるクライアント数に制限はありません。音声ドメインで許可されるクライアントは 1 つだけです。各クライアントは個別に認証する必要があります。クライアントにダウンロードされたポリシーは、そのクライアントの MAC または IP だけに適用されるので、同じポートに接続する他のクライアントには影響しません。

オプションである認証前オープン アクセス モードを使用すると、認証の実行前にネットワークにアクセスできます。このモードが必要なのは主に PXE ブートの場合ですが、この他にも使用例が考えられます。PXE ブートの場合は、PXE がタイムアウトして、サプリカントを含む可能性のあるブート イメージをダウンロードする前に、デバイスがネットワークにアクセスする必要があります。

この機能に関連するコンフィギュレーションはホスト モード コンフィギュレーションに適用され、その場合、ホスト モード自体はコントロール プレーンで有効ですが、オープン アクセス コンフィギュレーションはデータ プレーンで有効となります。オープン アクセス コンフィギュレーションは、セッション分類とはまったく関係がありません。セッション分類を制御するのはホスト モード コンフィギュレーションです。single-host モードにオープン アクセスが定義されている場合、ポートでは 1 つの MAC アドレスだけが許可されます。ポートは最初からトラフィックを転送し、ポートに設定されている内容によってのみ制限を受けます。このような設定は 802.1X とは関係がありません。したがって、アクセス制限の **no** 形式がポートに設定されている場合、クライアント デバイスは設定されている VLAN にフル アクセスできます。

show authentication 特権 EXEC コマンドを使用して設定を確認できます。

例

次の例では、ホスト モード コンフィギュレーションを使用して、アクセス ポリシーの適用に使用するセッションの分類を定義する方法を示します。

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

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication open

このポートでオープン アクセスをイネーブルにするには、インターフェイス コンフィギュレーション モードで **authentication open** コマンドを使用します。このポートでオープン アクセスを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 open

no authentication 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

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

オープン アクセスでは、認証が実行される前にクライアントまたはデバイスがネットワーク アクセスを取得できます。

show authentication 特権 EXEC コマンドを使用して設定を確認できます。

このコマンドは、ポートに対してのみ **authentication host-mode** *session-type* **open** グローバル コンフィギュレーション コマンドよりも優先されます。

このコマンドは、グローバルではなく、ポート単位で動作します。

例

次の例では、ポートに対してオープン アクセスをイネーブルにする方法を示します。

```
Switch(config-if)# authentication open
Switch(config-if)#
```

次の例では、ポートに対してオープン アクセスをイネーブルにする方法を示します。

```
Switch(config-if)# no authentication open
Switch(config-if)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication order

認証方式がインターフェイスのクライアントに試行される順序を指定するには、インターフェイス コンフィギュレーション モードで **authentication order** 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 order *method1* [*method2*] [*method3*]

no authentication order

構文の説明

method1	試行する認証方式。有効な値は次のとおりです。 • **dot1x**：dot1x 認証方式を追加します。 • **mab**：MAB 認証方式を追加します。 • **webauth**：WebAuth 認証方式を追加します。
method2 *method3*	（任意）試行する認証方式。有効な値は次のとおりです。 • **dot1x**：dot1x 認証方式を追加します。 • **mab**：MAB 認証方式を追加します。 • **webauth**：WebAuth 認証方式を追加します。

コマンド デフォルト

デフォルトの順序は dot1x、MAB、WebAuth です。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

authentication order コマンドを入力すると、明示的に示されている方式だけが実行されます。実行リストには各方式を 1 回だけ入力でき、**webauth** キーワードは最後に指定する必要があります。

認証方式は、設定された（またはデフォルト）順序で認証が成功するまで適用されます。認証が失敗した場合は、（認証イベント処理の設定に従って）次の認証方式にフェールオーバーします。

show authentication 特権 EXEC コマンドを使用して設定を確認できます。

例

次の例では、インターフェイスでクライアントの認証方式を試行する順序を指定する方法を示します。

```
Switch(config-if)# authentication order mab dot1x webauth
Switch(config-if)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication periodic

このポートの再認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **authentication periodic** コマンドを使用します。このポートの再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。

authentication periodic

no authentication periodic

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

authentication periodic コマンドは、Cisco IOS Release 12.2(50)SG およびそれ以降のリリースで推奨されなくなった、次の dot1x コマンドに替わるコマンドです。

[no] dot1x reauthentication

再認証の間隔は、**authentication timer** コマンドを使用して設定できます。

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

例

次の例では、このポートの再認証をイネーブルにする方法を示します。

```
Switch(config-if)# authentication reauthentication
Switch(config-if)#
```

次の例では、このポートの再認証をディセーブルにする方法を示します。

```
Switch(config-if)# no authentication reauthentication
Switch(config-if)#
```

関連コマンド

コマンド	説明
authentication timer	認証タイマーを設定します。
show authentication	認証マネージャ情報を表示します。

authentication port-control

ポート制御値を設定するには、インターフェイス コンフィギュレーション モードで **authentication port-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

authentication port-control [**auto** | **force-authorized** | **force-unauthorized**]

no authentication port-control

構文の説明

auto	（任意）802.1X ポートベース認証をイネーブルにし、ポートに無許可ステートを開始させます。
force-authorized	（任意）インターフェイスの 802.1X をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントの 802.1x ベース認証なしで通常のトラフィックを送受信します。**force-authorized** キーワードはデフォルトです。
force-unauthorized	（任意）クライアントからの認証試行をすべて無視し、ポートを強制的に無許可ステートに変更して、このインターフェイス経由のすべてのアクセスを拒否します。

コマンド デフォルト

force-authorized

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

authentication port-control コマンドは、Cisco IOS Release 12.2(50)SG およびそれ以降のリリースで推奨されなくなった、次の dot1x コマンドに替わるコマンドです。

[**no**] **dot1x port-control** [**auto** | **force-authorized** | **force-unauthorized**]

イーサネット スイッチ ネットワーク モジュールには、次の注意事項が適用されます。

- 802.1X プロトコルは、レイヤ 2 スタティック アクセス ポートでサポートされます。
- ポートが、次のタイプの 1 つとして設定されていない場合にかぎり、**auto** キーワードを使用できます。
  - トランク ポート：トランク ポートで 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、802.1X はイネーブルになりません。802.1X をイネーブルにしたポートをトランク モードに変更しようとしても、ポートのモードは変更されません。
  - EtherChannel ポート：ポート上で 802.1X をイネーブルにする前に、EtherChannel から 802.1X を削除する必要があります。EtherChannel または EtherChannel 内のアクティブなポート上で 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。まだアクティブになっていない EtherChannel のポートで 802.1X をイネーブルにしても、そのポートが EtherChannel に加入することはありません。

- スイッチド ポート アナライザ（SPAN）宛先ポート：SPAN 宛先ポートで 802.1X をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、802.1X はディセーブルに設定されます。SPAN 送信元ポートでは 802.1X をイネーブルにすることができます。

デバイスで 802.1X をグローバルにディセーブルにするには、各ポートで 802.1X をディセーブルにする必要があります。このタスクのグローバル コンフィギュレーション コマンドはありません。

show authentication 特権 EXEC コマンドを使用して設定を確認できます。

auto キーワードを使用すると、ポートで Extensible Authentication Protocol over LAN（EAPOL）フレームだけを送受信できます。ポートのリンク ステートがダウンからアップに移行するか、または EAPOL-Start フレームを受信すると、認証プロセスが開始されます。システムはクライアントの識別情報を要求して、クライアントと認証サーバ間で認証メッセージのリレーを開始します。クライアントの MAC アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。

例

次の例では、クライアント PC の認証ステータスが認証プロセスによって決定されることを示します。

```
Switch(config-if)# authentication port-control auto
Switch(config-if)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication priority

インターフェイスで認証方式のプライオリティを指定するには、インターフェイス コンフィギュレーション モードで **authentication priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

authentication priority *method1* [*method2*] [*method3*]

no authentication priority

構文の説明

method1	試行する認証方式。有効な値は次のとおりです。 • **dot1x**：dot1x 認証方式を追加します。 • **mab**：MAB 認証方式を追加します。 • **webauth**：WebAuth 認証方式を追加します。
method2 *method3*	（任意）試行する認証方式。有効な値は次のとおりです。 • **dot1x**：dot1x 認証方式を追加します。 • **mab**：MAB 認証方式を追加します。 • **webauth**：WebAuth 認証方式を追加します。

コマンド デフォルト

デフォルトの順序は dot1x、MAB、WebAuth です。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

認証方式にプライオリティを設定すると、（現在実行されていない）プライオリティの高い方式が、プライオリティの低い方式を使用して進行している認証に割り込むことができます。また、クライアントが認証済みの場合は、プライオリティの高い方式による割り込みによって、プライオリティの低い方式を使用してすでに認証されているクライアントを再認証できます。

ある方式のデフォルト プライオリティは、実行順序リストの位置と同じプライオリティになります。プライオリティを設定しない場合の相対プライオリティは、（プライオリティの高い順に）dot1x、MAB、WebAuth です。**authentication order** コマンドを入力した場合、デフォルトのプライオリティは、設定された順序と同じです。

show authentication 特権 EXEC コマンドを使用して設定を確認できます。

例

次の例では、インターフェイスでクライアントの認証方式を試行するプライオリティを指定する方法を示します。

```
Switch(config-if)# authentication priority mab dot1x webauth
Switch(config-if)#
```

関連コマンド

コマンド	説明
authentication order	インターフェイスでクライアントの認証方式を試行する順序を指定します。
show authentication	認証マネージャ情報を表示します。

authentication timer

認証タイマーを設定するには、インターフェイス コンフィギュレーション モードで **authentication timer** 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 timer {{**inactivity** *value*} | {**reauthenticate** {**server** | *value*}} | {**restart** *value*}}

no authentication timer {{**inactivity** *value*} | {**reauthenticate** *value*} | {**restart** *value*}}

構文の説明

inactivity *value*	ホストが非アクティブになってから許可されるまでの許容時間（秒）を指定します。有効値の範囲は 1 ～ 65535 です。デフォルトはオフです。 **（注）** inactivity 値は再認証タイマー値よりも小さい必要がありますが、再認証タイマー値より大きい値に設定してもエラーと見なされません。
reauthenticate server	クライアントの再認証期間値を認証、許可、アカウンティング（AAA）サーバからセッション タイムアウト（RADIUS 属性 27）として取得することを指定します。
reauthenticate *value*	自動再認証が開始されるまでの時間を秒単位で指定します。有効値の範囲は 1 ～ 65535 です。デフォルトは 3600 です。
restart *value*	無許可ポートの認証を試行するまでの時間を秒単位で指定します。有効値の範囲は 1 ～ 65535 です。デフォルトはオフです。

コマンド デフォルト

デフォルト設定は、次のとおりです。

- **inactivity** *value*：オフ
- **reauthenticate** *value*：3600
- **restart** *value*：オフ

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが追加されました。

使用上のガイドライン

再認証は、インターフェイスで再認証がイネーブルである場合にのみ実行されます。

authentication timer reauthenticate *value* コマンドは、Cisco IOS Release 12.2(50)SG およびそれ以降のリリースで推奨されなくなった、次の dot1x コマンドに替わるコマンドです。

[**no**] **dot1x timeout** {**reauth-period** *seconds* | **quiet-period** seconds | **tx-period** *seconds* | **supp-timeout** *seconds* | **server-timeout** *seconds*}

（注）　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。

非アクティブ期間中は、イーサネット スイッチ ネットワーク モジュールは認証要求を受け入れまたは開始しなくなります。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。

reauthenticate キーワードは、**authentication reauthentication** 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定期的な再認証をイネーブルにしてある場合にのみ、イーサネット スイッチ ネットワーク モジュールの動作に影響します。

例

次の例では、クライアントの再認証期間値を認証、許可、アカウンティング（AAA）サーバからセッション タイムアウト（RADIUS 属性 27）として取得することを指定する方法を示します。

```
Switch(config-if)# authentication timer reauthenticate server
Switch(config-if)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication violation

違反モード（restrict、shutdown、および replace）を設定するには、**authentication violation** インターフェイス コンフィギュレーション コマンドを使用します。

シングルホスト モードでは、セキュリティ違反はデータ VLAN で複数のデバイスが検出された場合に発生します。マルチドメイン認証モードでは、セキュリティ違反は複数のデバイスがデータまたは音声 VLAN で検出された場合に発生します。

セキュリティ違反は複数ホストまたはマルチ認証モードでは発生しません。

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

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

構文の説明

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（仮想）ポートがディセーブルになります。
replace	ポートを errordisable にしたり、制限することなく、既存のポートを新しいホストと置き換えます。

デフォルト

ポートをシャット ダウンします。**restrict** キーワードが設定されている場合、ポートはシャットダウンしません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(54)SG	**replace** キーワードのサポートが追加されました。

使用上のガイドライン

新しいホストが 1 つまたは複数ドメインのモードで確認されると、**replace** モードは古いセッションを破棄し、新しいホストを認証します。

例

次の例では、違反モードをスイッチでシャットダウンするように設定する方法を示します。

```
Switch# configure terminal
Switch(config)# authentication violation shutdown
```

シャットダウン モードでセキュリティ違反が発生すると、ポートは errordisable になります。次の syslog メッセージが表示されます。

```
%AUTHMGR-5-SECURITY_VIOLATION: Security violation on the interface <interface name>, new
MAC address <mac-address> is seen.
%PM-4-ERR_DISABLE: security-violation error detected on <interface name>, putting
<interface name> in err-disable state
```

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	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フォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

auto qos classify

信頼できないインターフェイスの QoS 設定を生成するには、**auto qos classify** interface コマンドを使用します。

auto qos classify

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
15.1(1)SG、 15.1(1)SG IOS-XE 3.3.0	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、信頼できないインターフェイスの QoS 設定を生成します。信頼できないデスクトップまたはデバイスからのトラフィックを分類するためのサービス ポリシーを配置して、それを適宜示します。生成されたサービス ポリシーは、ポリシングしません。

生成されたグローバル レベル コマンド

グローバルなテンプレートは A、B、C で定義されます。

A.ACL および **auto qos classify** コマンドで使用されるアプリケーション クラスのテンプレート。

```
ip access-list extended AutoQos-4.0-ACL-Multimedia-Conf
      permit udp any any range 16384 32767
    ip access-list extended AutoQos-4.0-ACL-Signaling
      permit tcp any any range 2000 2002
      permit tcp any any range 5060 5061
            permit udp any any range 5060 5061
    ip access-list extended AutoQos-4.0-ACL-Transactional-Data
      permit tcp any any eq 443
      permit tcp any any eq 1521
      permit udp any any eq 1521
      permit tcp any any eq 1526
      permit udp any any eq 1526
      permit tcp any any eq 1575
      permit udp any any eq 1575
      permit tcp any any eq 1630
      permit udp any any eq 1630
    ip access-list extended AutoQos-4.0-ACL-Bulk-Data
      permit tcp any any eq ftp
      permit tcp any any eq ftp-data
      permit tcp any any eq 22
permit tcp any any eq smtp
      permit tcp any any eq 465
      permit tcp any any eq 143
      permit tcp any any eq 993
```

```
    permit tcp any any eq pop3
    permit tcp any any eq 995
    permit tcp any any eq 1914
  ip access-list extended AutoQos-4.0-ACL-Scavenger
    permit tcp any any eq 1214
    permit udp any any eq 1214
    permit tcp any any range 2300 2400
    permit udp any any range 2300 2400
    permit tcp any any eq 3689
    permit udp any any eq 3689
    permit tcp any any range 6881 6999
    permit tcp any any eq 11999
    permit tcp any any range 28800 29100
  ip access-list extended AutoQos-4.0-ACL-Default
    permit ip any any

class-map match-any AutoQos-4.0-VoIP-Data
        match dscp ef
        match cos 5
      class-map match-all AutoQos-4.0-VoIP-Data-Cos
        match cos 5
      class-map match-any AutoQos-4.0-VoIP-Signal
        match dscp cs3
        match cos 3
      class-map match-all AutoQos-4.0-VoIP-Signal-Cos
        match cos 3
class-map match-all AutoQos-4.0-Multimedia-Conf-Classify
        match access-group name AutoQos-4.0-ACL-Multimedia-Conf
class-map match-all AutoQos-4.0-Signaling-Classify
  match access-group name AutoQos-4.0-ACL-Signaling
class-map match-all AutoQos-4.0-Transaction-Classify
  match access-group name AutoQos-4.0-ACL-Transactional-Data
class-map match-all AutoQos-4.0-Bulk-Data-Classify
  match access-group name AutoQos-4.0-ACL-Bulk-Data
class-map match-all AutoQos-4.0-Scavenger-Classify
  match access-group name AutoQos-4.0-ACL-Scavenger
      class-map match-all AutoQos-4.0-Default-Classify
  match access-group name AutoQos-4.0-ACL-Default
```

インターフェイスに IP 電話を接続し、そのインターフェイス上で **auto qos voip cisco-phone** コマンドを呼び出す場合に対処するために AutoQos-4.0-VoIP-Data-Cos と AutoQos-4.0-VoIP-Signal-Cos が必要です。この場合は、インターフェイスの入力サービス ポリシーは CoS マーキングで VoIP およびシグナリング パケットにだけ一致する必要があります。これは、Cisco IP Phone のスイッチング ASIC が VoIP およびシグナリング トラフィックの CoS ビットの再マーキングのみに限定されるためです。スイッチに接続された IP 電話に PC が接続されたユーザは、PC の NIC を使用してその PC から dscp ef へのトラフィックの DSCP マーキングを再マーキングできるため、DSCP マーキングが一致するとセキュリティの脆弱性の原因になります。これにより、出力方向のプライオリティ キューに非リアルタイム トラフィックが誤って配置されます。

B.**auto qos classify** コマンドの入力サービス ポリシーのテンプレート。

```
policy-map AutoQos-4.0-Classify-Input-Policy
  class AutoQos-4.0-Multimedia-Conf-Classify
     set dscp af41
     set cos 4
     set qos-group 34
   class AutoQos-4.0-Signaling-Classify
     set dscp cs3
     set cos 3
     set qos-group 16
   class AutoQos-4.0-Transaction-Classify
     set dscp af21
     set cos 2
```

```
        set qos-group 18
  class AutoQos-4.0-Bulk-Data-Classify
    set dscp af11
    set cos 1
    set qos-group 10
  class AutoQos-4.0-Scavenger-Classify
    set dscp cs1
    set cos 1
    set qos-group 8
  class AutoQos-4.0-Default-Classify
    set dscp default
    set cos 0
```

C.8 個のキューを割り当てるために出力クラスを使用する SRND4 出力ポリシーおよび出力キュー クラスのテンプレート。このテンプレートはすべての SRND4 コマンドに必要です。

```
class-map match-all AutoQos-4.0-Priority-Queue
  match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
  match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
       match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1
```

ポリシー マップ コンフィギュレーション モードで実行される **police** コマンドは、定義されているレート制限を超えたトラフィック フローの qos-group の再マーキングを許可しないため、qos-group 7 または dscp af11 と一致するように AutoQos-4.0-Scavenger-Queue を設定する必要があります。**auto qos classify** police コマンドを入力すると、定義されているレート制限に違反したトラフィック フローは cs1 に再マーキングされますが、qos-group を超過アクションとして再マーキングできないため、元の qos-group 分類を保持します。ただし、AutoQos-4.0-Scavenger-Queue は出力ポリシー マップ内の他のすべてのキューより先に定義されるため、元の qos-group ラベルを保持しているにもかかわらず、再マーキングされたパケットはこのキューに分類されます。

```
     policy-map AutoQos-4.0-Output-Policye
    bandwidth remaining percent 1
  class AutoQos-4.0-Priority-Queue
    priority
    police cir percent 30 bc 33 ms
             conform-action transmit exceed-action drop
  class AutoQos-4.0-Control-Mgmt-Queue
    bandwidth remaining percent 10
  class AutoQos-4.0-Multimedia-Conf-Queue
    bandwidth remaining percent 10
  class AutoQos-4.0-Multimedia-Stream-Queue
    bandwidth remaining percent 10
  class AutoQos-4.0-Trans-Data-Queue
    bandwidth remaining percent 10
    dbl
  class AutoQos-4.0-Bulk-Data-Queue
    bandwidth remaining percent 4
    dbl
  class class-default
    bandwidth remaining percent 25
          dbl
```

生成されたインターフェイス レベル コマンド

Fa/Gig ポート :

```
Switch(config-if)# service-policy input AutoQos-4.0-Classify-Input-Policy
                   service-policy output AutoQos-4.0-Output-Policy
```

例

次の例では、信頼できないインターフェイス gigabitethernet1/1 の QoS 設定を生成する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos classify
```

関連コマンド

コマンド	説明
auto qos trust	信頼できるインターフェイスの QoS 設定を生成します。
auto qos voip cisco-softphone	Cisco IP SoftPhone アプリケーションを実行している PC に接続されたインターフェイスの QoS 設定を生成し、このようなインターフェイスからのポリシング トラフィックをマーキングします。

auto qos classify police

信頼できないインターフェイスからのトラフィックをポリシングするには、**auto qos classify police** インターフェイス コマンドを使用します。

auto qos classify police

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
15.1(1)SG、 15.1(1)SG IOS-XE 3.3.0	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、信頼できないインターフェイスの QoS 設定を生成します。これらの信頼できないデスクトップまたはデバイスから着信するトラフィックを分類するためのサービス ポリシーを配置して、それを適宜示します。生成されたサービス ポリシーは、パケットをポリシングし、マークダウンまたはドロップします。

生成されたグローバル レベル コマンド

Auto QoS srn4 コマンドは、インターフェイスに適用されると、グローバル コンフィギュレーション レベルで次のテンプレート（A、B、および C）を 1 つ以上生成します。通常、コマンドは、アプリケーション クラスにトラフィックを分類するために ACL または DSCP 値もしくは CoS 値に一致する一連のクラス マップを生成します。生成されたクラスと一致し、クラスで qos-group を設定し、場合によっては設定された帯域幅にクラスをポリシングする入力ポリシーが生成されます。（qos-group は、異なるアプリケーション クラスが 1 つの単位として扱われるようにする数値のタグにすぎません。スイッチのコンテキスト外では重要ではありません）。さらに、入力ポリシーで設定された qos-group と一致する 8 個の出力キュー クラス マップが生成されます。実際の出力ポリシーは、この 8 個の出力キューのクラス マップそれぞれにキューを割り当てます。

コマンドは、必要に応じて次のテンプレートを生成します。たとえば、新しいコマンドを最初に使用するときに、8 個のキューの出力サービス ポリシーを定義するグローバル設定が生成されます（下記のテンプレート C）。その後、他のインターフェイスに適用された **auto qos** コマンドは出力キューイング用のテンプレートを生成しません。これは、すべての **auto qos** コマンドが移行後も同じ 8 個のキューのモデルに依存し、コマンドを最初に使用した時点からすでに生成されているためです。

グローバルなテンプレートは A、B、C で定義されます。

A.ACL および **auto qos classify police** コマンドで使用されるアプリケーション クラスのテンプレート

```
ip access-list extended AutoQos-4.0-ACL-Multimedia-Conf
  permit udp any any range 16384 32767
ip access-list extended AutoQos-4.0-ACL-Signaling
  permit tcp any any range 2000 2002
  permit tcp any any range 5060 5061
```

```
            permit udp any any range 5060 5061
     ip access-list extended AutoQos-4.0-ACL-Transactional-Data
       permit tcp any any eq 443
       permit tcp any any eq 1521
       permit tcp any any eq 1521
       permit udp any any eq 1521
       permit tcp any any eq 1526
       permit udp any any eq 1526
       permit tcp any any eq 1575
       permit udp any any eq 1575
       permit tcp any any eq 1630
       permit udp any any eq 1630
     ip access-list extended AutoQos-4.0-ACL-Bulk-Data
       permit tcp any any eq ftp
       permit tcp any any eq ftp-data
       permit tcp any any eq 22
permit tcp any any eq smtp
       permit tcp any any eq 465
       permit tcp any any eq 143
       permit tcp any any eq 993
       permit tcp any any eq pop3
       permit tcp any any eq 995
       permit tcp any any eq 1914
     ip access-list extended AutoQos-4.0-ACL-Scavenger
       permit tcp any any eq 1214
       permit udp any any eq 1214
       permit tcp any any range 2300 2400
       permit udp any any range 2300 2400
       permit tcp any any eq 3689
       permit udp any any eq 3689
       permit tcp any any range 6881 6999
       permit tcp any any eq 11999
       permit tcp any any range 28800 29100
     ip access-list extended AutoQos-4.0-ACL-Default
       permit ip any any

   class-map match-any AutoQos-4.0-VoIP-Data
           match dscp ef
           match cos 5
         class-map match-all AutoQos-4.0-VoIP-Data-Cos
           match cos 5
         class-map match-any AutoQos-4.0-VoIP-Signal
           match dscp cs3
           match cos 3
         class-map match-all AutoQos-4.0-VoIP-Signal-Cos
           match cos 3
   class-map match-all AutoQos-4.0-Multimedia-Conf-Classify
           match access-group name AutoQos-4.0-ACL-Multimedia-Conf
   class-map match-all AutoQos-4.0-Signaling-Classify
     match access-group name AutoQos-4.0-ACL-Signaling
   class-map match-all AutoQos-4.0-Transaction-Classify
     match access-group name AutoQos-4.0-ACL-Transactional-Data
   class-map match-all AutoQos-4.0-Bulk-Data-Classify
     match access-group name AutoQos-4.0-ACL-Bulk-Data
   class-map match-all AutoQos-4.0-Scavenger-Classify
     match access-group name AutoQos-4.0-ACL-Scavenger
         class-map match-all AutoQos-4.0-Default-Classify
     match access-group name AutoQos-4.0-ACL-Default
```

AutoQos-4.0-VoIP-Data-Cos および AutoQos-4.0-VoIP-Signal-Cos は、インターフェイスに IP 電話を接続し、そのインターフェイス上で **auto qos voip cisco-phone** コマンドを呼び出す場合に対処するために必要です。この場合は、インターフェイスの入力サービス ポリシーは、CoS マーキングで VoIP およびシグナリング パケットにだけ一致する必要があります。これは、Cisco IP Phone のスイッチング

ASIC が VoIP およびシグナリング トラフィックの CoS ビットの再マーキングのみに限定されるためです。スイッチに接続された IP 電話に PC が接続されたユーザは、PC の NIC を使用してその PC から dscp ef へのトラフィックの DSCP マーキングを再マーキングできるため、DSCP マーキングが一致するとセキュリティの脆弱性の原因になります。これにより、出力方向のプライオリティ キューに非リアルタイム トラフィックが配置されます。

B.**auto qos classify police** コマンドの入力サービス ポリシーのテンプレート

```
policy-map AutoQos-4.0-Classify-Police-Input-Policy
  class AutoQos-4.0-Multimedia-Conf-Classify
    set dscp af41
    set cos 4
    set qos-group 34
    police cir 5000000 bc 8000
    exceed-action drop
  class AutoQos-4.0-Signaling-Classify
    set dscp cs3
    set cos 3
    set qos-group 16
    police cir 32000 bc 8000
    exceed-action drop
  class AutoQos-4.0-Transaction-Classify
    set dscp af21
    set cos 2
    set qos-group 18
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1
  class AutoQos-4.0-Bulk-Data-Classify
    set dscp af11
    set cos 1
    set qos-group 10
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
         exceed-action set-cos-transmit 1
  class AutoQos-4.0-Scavenger-Classify
    set dscp cs1
    set cos 1
    set qos-group 8
    police cir 10000000 bc 8000
    exceed-action drop
  class AutoQos-4.0-Default-Classify
    set dscp default
    set cos 0
    police cir 10000000 bc 8000
    exceed-action set-dscp-transmit cs1
    exceed-action set-cos-transmit 1
```

C.8 個のキューを割り当てるために出力クラスを使用する SRND4 出力ポリシーおよび出力キュー クラスのテンプレート。このテンプレートは 4 つの SRND4 コマンドに必要です。

```
class-map match-all AutoQos-4.0-Priority-Queue
  match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
  match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
        match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
```

```
      match qos-group 8
      match dscp cs1
```

AutoQos-4.0-Scavenger-Queue は、qos-group 7 または dscp af11 と一致するように設定する必要があります。ポリシー マップ コンフィギュレーション モードで実行される police コマンドは、定義されているレート制限を超えたトラフィック フローの qos-group の再マーキングを許可しないためです。**auto qos classify police** コマンドを入力した後、定義されているレート制限に違反したトラフィック フローは cs1 に再マーキングされますが、qos-group を超過アクションとして再マーキングできないため、元の qos-group 分類を保持します。ただし、AutoQos-4.0-Scavenger-Queue は出力ポリシー マップ内の他のすべてのキューより先に定義されるため、元の qos-group ラベルを保持しているにもかかわらず、再マーキングされたパケットはこのキューに分類されます。

```
       policy-map AutoQos-4.0-Output-Policye
      bandwidth remaining percent 1
   class AutoQos-4.0-Priority-Queue
      priority
      police cir percent 30 bc 33 ms
               conform-action transmit exceed-action drop
   class AutoQos-4.0-Control-Mgmt-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Multimedia-Conf-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Multimedia-Stream-Queue
      bandwidth remaining percent 10
   class AutoQos-4.0-Trans-Data-Queue
      bandwidth remaining percent 10
      dbl
   class AutoQos-4.0-Bulk-Data-Queue
      bandwidth remaining percent 4
      dbl
   class class-default
      bandwidth remaining percent 25
            dbl
```

生成されたインターフェイス レベル コマンド

Fa/Gig ポート :

```
Switch(config-if)#
                service-policy input AutoQos-4.0-Classify-Police-Input-Policy
                service-policy output AutoQos-4.0-Output-Policy
```

例

次の例では、信頼できないインターフェイス gigabitethernet1/1 からのトラフィックをポリシングする方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos classify police
Switch(config-if)# do sh run interface gigabitethernet1
Interface gigabitethernet1
   auto qos classify police
    service-policy input AutoQos-4.0-Classify-Police-Input-Policy
    service-policy output AutoQos-4.0-Output-Policy
end
```

関連コマンド

コマンド	説明
auto qos voip cisco-softphone	Cisco IP SoftPhone アプリケーションを実行している PC に接続されたインターフェイスの QoS 設定を生成し、このようなインターフェイスからのポリシング トラフィックをマーキングします。
auto qos classify	信頼できないインターフェイスの QoS 設定を生成します。
auto qos srnd4	ソリューション リファレンス ネットワーク デザイン 4.0 に基づいて QoS 設定を生成します。

auto qos srnd4

ソリューション リファレンス ネットワーク デザイン 4.0 に基づいて QoS 設定を生成するには、**auto qos srnd4** グローバル コマンドを使用します。

auto qos srnd4

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
15.1(1)SG、 15.1(1)SG IOS-XE 3.3.0	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、新しい auto-QoS コマンドがインターフェイスに設定されている場合に生成されます。

AutoQos SRND4 コマンドは、インターフェイスに適用されると、グローバル コンフィギュレーション レベルで次のテンプレート（A および B）を 1 つ以上生成します。

通常、コマンドは、アプリケーション クラスにトラフィックを分類するために ACL または DSCP 値および CoS 値に一致する一連のクラス マップを生成します。生成されたクラスと一致し、クラスで qos-group を設定し、場合によっては設定された帯域幅にクラスをポリシングする入力ポリシーも生成されます。（qos-group は、異なるアプリケーション クラスが 1 つの単位として扱われるようにする数値のタグです。qos-group が設定されたスイッチのコンテキスト外では重要ではありません）。さらに、入力ポリシーで設定された qos-group と一致する 8 個の出力キュー クラス マップが生成されます。実際の出力ポリシーは、8 個の出力キュー クラス マップそれぞれにキューを割り当てます。

AutoQos srnd4 コマンドは必要に応じてテンプレートだけを生成します。たとえば、新しい srnd4 コマンドを最初に使用すると、8 個のキューの出力サービス ポリシーを定義するグローバル設定が生成されます（下記のテンプレート B）。その後、他のインターフェイスに適用された **auto qos** コマンドは出力キューイング用のテンプレートを生成しません。これは、すべての auto-QoS コマンドが移行後も同じ 8 個のキューのモデルに依存し、コマンドを最初に使用した時点からすでに生成されているためです。

auto qos voip trust がイネーブルのインターフェイス

—生成されたグローバル レベル コマンド

グローバルなテンプレートは A および B で定義されます（下記を参照）。

A. アプリケーション クラスのこのテンプレートは、auto-QoS video cts、**auto qos video ip-camera**、および **auto qos trust** コマンドで使用されます。このテンプレートのクラスには、**auto qos video cts**、**auto qos video ip-camera**、および **auto qos trust** コマンドの入力サービス ポリシーも含まれます。この 3 つのコマンドは AutoQos-4.0-Input-Policy を使用する唯一のものであるため、前述の 3 つのコマンドが使用するアプリケーション クラスを定義する同じテンプレートにそのポリシーを含めることを推奨します。

```
 class-map match-any AutoQos-4.0-VoIP
   match dscp ef
   match cos 5
 class-map match-all AutoQos-4.0-Broadcast-Vid
   match dscp cs5
 class-map match-all AutoQos-4.0-Realtime-Interact
   match dscp cs4
 class-map match-all AutoQos-4.0-Network-Ctrl
   match dscp cs7
 class-map match-all AutoQos-4.0-Internetwork-Ctrl
   match dscp cs6
 class-map match-any AutoQos-4.0-Signaling
   match dscp cs3
   match cos 3
 class-map match-all AutoQos-4.0-Network-Mgmt
   match dscp cs2
 class-map match-any AutoQos-4.0-Multimedia-Conf
   match dscp af41
   match dscp af42
   match dscp af43
class-map match-any AutoQos-4.0-Multimedia-Stream
   match dscp af31
   match dscp af32
   match dscp af33
 class-map match-any AutoQos-4.0-Transaction-Data
   match dscp af21
   match dscp af22
   match dscp af23
 class-map match-any AutoQos-4.0-Bulk-Data
   match dscp af11
   match dscp af12
   match dscp af13
 class-map match-all AutoQos-4.0-Scavenger
   match dscp cs1
```

AutoQos-4.0-Signaling および AutoQos-4.0-VoIP クラスは、IP 電話がインターフェイスに接続されている場合に対処するために、Cos に一致する必要があります。（Cisco IP Phone は、DSCP ではなく、CoS ビットだけを再マーキングできます）。

```
policy-map AutoQos-4.0-Input-Policy
      class AutoQos-4.0-VoIP
        set qos-group 32
      class AutoQos-4.0-Broadcast-Vid
        set qos-group 32
      class AutoQos-4.0-Realtime-Interact
        set qos-group 32
      class AutoQos-4.0-Network-Ctrl
        set qos-group 16
      class AutoQos-4.0-Internetwork-Ctrl
        set qos-group 16
      class AutoQos-4.0-Signaling
        set qos-group 16
      class AutoQos-4.0-Network-Mgmt
        set qos-group 16
      class AutoQos-4.0-Multimedia-Conf
        set qos-group 34
      class AutoQos-4.0-Multimedia-Stream
        set qos-group 26
      class AutoQos-4.0-Transaction-Data
        set qos-group 18
      class AutoQos-4.0-Bulk-Data
        set qos-group 10
      class AutoQos-4.0-Scavenger
        set qos-group 8
```

B. 出力キュー クラスのこのテンプレートは（SRND4 出力ポリシーとともに）8 個のキューを割り当てます。このテンプレートはすべての SRND4 コマンドに必要です。

```
class-map match-all AutoQos-4.0-Priority-Queue
  match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
  match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
        match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1
```

ポリシー マップ コンフィギュレーション モードで実行される **police** コマンドは、定義されているレート制限を超えたトラフィック フローの qos-group の再マーキングを許可しないため、qos-group 7 または dscp af11 と一致するように AutoQos-4.0-Scavenger-Queue を設定する必要があります。**auto qos classify police** コマンドを入力すると、定義されているレート制限に違反したトラフィック フローは cs1 に再マーキングされますが、qos-group を超過アクションとして再マーキングできないため、元の qos-group 分類を保持します。ただし、AutoQos-4.0-Scavenger-Queue は出力ポリシー マップ内の他のすべてのキューより先に定義されるため、元の qos-group ラベルを保持しているにもかかわらず、再マーキングされたパケットはこのキューに分類されます。

```
    policy-map AutoQos-4.0-Output-Policy
 class AutoQos-4.0-Scavenger-Queue
   bandwidth remaining percent 1
 class AutoQos-4.0-Priority-Queue
   priority
   police cir percent 30 bc 33 ms
            conform-action transmit exceed-action drop
 class AutoQos-4.0-Control-Mgmt-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Conf-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Stream-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Trans-Data-Queue
   bandwidth remaining percent 10
   dbl
 class AutoQos-4.0-Bulk-Data-Queue
   bandwidth remaining percent 4
   dbl
 class class-default
   bandwidth remaining percent 25
         dbl
```

—生成されたインターフェイス レベル コマンド

Fa/Gig ポート :

レイヤ 2 インターフェイスの場合

```
Switch(config-if)# no service-policy input AutoQos-VoIP-Input-Cos-Policy
                   no service-policy output AutoQos-VoIP-Output-Policy
                   service-policy input AutoQos-4.0-Input-Policy
                   service-policy output AutoQos-4.0-Output-Policy
```

レイヤ 3 インターフェイスの場合

```
Switch(config-if)# no service-policy input AutoQos-VoIP-Input-Dscp-Policy
                   no service-policy output AutoQos-VoIP-Output-Policy
                   service-policy input AutoQos-4.0-Input-Policy
                   service-policy output AutoQos-4.0-Output-Policy
```

auto qos voip cisco-phone がイネーブルのインターフェイス

—生成されたグローバル レベル コマンド

A および B（上記）で定義されたグローバルなテンプレート。

—生成されたインターフェイス レベル コマンド

Fa/Gig ポート :

```
Switch(config-if)# no qos trust device cisco-phone
                   no service-policy input AutoQos-VoIP-Input-Cos-Policy
                   no service-policy output AutoQos-VoIP-Output-Policy
                   qos trust device cisco-phone
                   service-policy input AutoQos-4.0-Cisco-Phone-Input-Policy
                   service-policy output AutoQos-4.0-Output-Policy
```

例

ソリューション リファレンス ネットワーク デザイン 4.0 に基づいて QoS 設定を生成するには、次のようにします。

```
Switch# auto qos srnd4
```

関連コマンド

コマンド	説明
auto qos trust	信頼できるインターフェイスの QoS 設定を生成します。
auto qos voip cisco-softphone	Cisco IP SoftPhone アプリケーションを実行している PC に接続されたインターフェイスの QoS 設定を生成し、このようなインターフェイスからのポリシング トラフィックをマーキングします。

auto qos trust

信頼できるインターフェイスの QoS 設定を生成するには、**auto qos trust** interface コマンドを使用します。

auto qos trust

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
15.1(1)SG、 15.1(1)SG IOS-XE 3.3.0	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

生成されたグローバル レベル コマンド

インターフェイスに auto-QoS srnd4 コマンドを適用すると、コマンドによりグローバル コンフィギュレーション レベルで次のテンプレート（A および B）の 1 つまたは複数が生成されます。通常、コマンドは、アプリケーション クラスにトラフィックを分類するために ACL または DSCP 値もしくは CoS 値に一致する一連のクラス マップを生成します。生成されたクラスと一致し、クラスで qos-group を設定し、場合によっては設定された帯域幅にクラスをポリシングする入力ポリシーが生成されます。（qos-group は、異なるアプリケーション クラスが 1 つの単位として扱われるようにする数値のタグにすぎません。スイッチのコンテキスト外では重要ではありません）。さらに、入力ポリシーで設定された qos-group と一致する 8 個の出力キュー クラス マップが生成されます。実際の出力ポリシーは、この 8 個のクラス マップそれぞれにキューを割り当てます。

コマンドは必要な場合にだけテンプレートを生成します。たとえば、新しいコマンドを初めて使用すると、8 個のキューの出力サービス ポリシーを定義するグローバル設定が生成されます。その後、他のインターフェイスに適用された auto-QoS コマンドは出力キューイングのテンプレートを生成しません。これは、すべての auto-QoS コマンドが移行後も同じ 8 個のキューのモデルに依存し、コマンドの最初の使用時からすでに生成されているためです。

A および B で定義されたグローバルなテンプレート。

A.**auto qos trust** コマンドで使用されるアプリケーション クラスのテンプレート。

このテンプレートには、**auto qos video cts**、**auto qos video ip-camera**、および **auto qos trust** コマンドの入力サービス ポリシーも含まれます。この 3 つのコマンドは AutoQos-4.0-Input-Policy を使用する唯一のものであるため、コマンドで使用されるアプリケーション クラスを定義するテンプレートにそのポリシーを含める必要があります。

```
class-map match-any AutoQos-4.0-VoIP
  match dscp ef
  match cos 5
class-map match-all AutoQos-4.0-Broadcast-Vid
  match dscp cs5
```

```
class-map match-all AutoQos-4.0-Realtime-Interact
  match dscp cs4
class-map match-all AutoQos-4.0-Network-Ctrl
  match dscp cs7
class-map match-all AutoQos-4.0-Internetwork-Ctrl
  match dscp cs6
class-map match-any AutoQos-4.0-Signaling
  match dscp cs3
  match cos 3
class-map match-all AutoQos-4.0-Network-Mgmt
  match dscp cs2
class-map match-any AutoQos-4.0-Multimedia-Conf
  match dscp af41
  match dscp af42
  match dscp af43
class-map match-any AutoQos-4.0-Multimedia-Stream
  match dscp af31
  match dscp af32
  match dscp af33
class-map match-any AutoQos-4.0-Transaction-Data
  match dscp af21
  match dscp af22
  match dscp af23
class-map match-any AutoQos-4.0-Bulk-Data
  match dscp af11
  match dscp af12
  match dscp af13
class-map match-all AutoQos-4.0-Scavenger
  match dscp cs1
```

AutoQos-4.0-Signaling および AutoQos-4.0-VoIP クラスは、IP 電話がインターフェイスに接続されている場合に対処するために、Cos に一致する必要もあります。（Cisco IP Phone は、DSCP ではなく、CoS ビットだけを再マーキングできます）。

```
policy-map AutoQos-4.0-Input-Policy
    class AutoQos-4.0-VoIP
      set qos-group 32
    class AutoQos-4.0-Broadcast-Vid
      set qos-group 32
    class AutoQos-4.0-Realtime-Interact
      set qos-group 32
    class AutoQos-4.0-Network-Ctrl
      set qos-group 16
    class AutoQos-4.0-Internetwork-Ctrl
      set qos-group 16
    class AutoQos-4.0-Signaling
      set qos-group 16
    class AutoQos-4.0-Network-Mgmt
      set qos-group 16
    class AutoQos-4.0-Multimedia-Conf
      set qos-group 34
    class AutoQos-4.0-Multimedia-Stream
      set qos-group 26
    class AutoQos-4.0-Transaction-Data
      set qos-group 18
    class AutoQos-4.0-Bulk-Data
      set qos-group 10
    class AutoQos-4.0-Scavenger
      set qos-group 8
```

B.8 個のキューを割り当てるために出力クラスを使用する srnd4 出力ポリシーおよび出力キュー クラスのテンプレート。このテンプレートはすべての srnd4 コマンドに必要です。

```
class-map match-all AutoQos-4.0-Priority-Queue
```

```
  match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
  match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
        match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1
```

ポリシー マップ コンフィギュレーション モードで実行される **police** コマンドは、定義されているレート制限を超えたトラフィック フローの qos-group の再マーキングを許可しないため、AutoQos-4.0-Scavenger-Queue は qos-group 7 または dscp af11 と一致するように設定する必要があります。**auto qos classify police** コマンドを実行すると、定義されているレート制限に違反したトラフィック フローは cs1 に再マーキングされますが、元の qos-group 分類を保持します。これは qos-group を超過アクションとして再マーキングすることができないためです。ただし、AutoQos-4.0-Scavenger-Queue は出力ポリシー マップ内の他のすべてのキューより先に定義されるため、元の qos-group ラベルを保持しているにもかかわらず、再マーキングされたパケットはこのキューに分類されます。

```
    policy-map AutoQos-4.0-Output-Policy
 class AutoQos-4.0-Scavenger-Queue
   bandwidth remaining percent 1
 class AutoQos-4.0-Priority-Queue
   priority
   police cir percent 30 bc 33 ms
            conform-action transmit exceed-action drop
 class AutoQos-4.0-Control-Mgmt-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Conf-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Stream-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Trans-Data-Queue
   bandwidth remaining percent 10
   dbl
 class AutoQos-4.0-Bulk-Data-Queue
   bandwidth remaining percent 4
   dbl
 class class-default
   bandwidth remaining percent 25
```

生成されたインターフェイス レベル コマンド

Fa/Gig ポート :

```
Switch(config-if)# service-policy input AutoQos-4.0-Input-Policy
                   service-policy output AutoQos-4.0-Output-Policy
```

例

次の例では、信頼できないインターフェイス gigabitethernet1/1 からのトラフィックをポリシングする方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos trust
Switch(config-if)# do sh running interface interface-id
interface FastEthernet2/1
```

```
 auto qos trust
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
end
```

関連コマンド

コマンド	説明
auto qos voip cisco-softphone	Cisco IP SoftPhone アプリケーションを実行している PC に接続されたインターフェイスの QoS 設定を生成し、このようなインターフェイスからのポリシング トラフィックをマーキングします。
auto qos classify	信頼できないインターフェイスの QoS 設定を生成します。
auto qos srnd4	ソリューション リファレンス ネットワーク デザイン 4.0 に基づいて QoS 設定を生成します。

auto qos video

Cisco TelePresence または Cisco カメラのインターフェイスの QoS 設定を生成するには（CDP を介した条件付き信頼）、**auto qos video** 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。

auto qos video {**cts** | **ip-camera**}

構文の説明

cts	Cisco Telepresence デバイスの QoS マーキングを信頼します。
ip-camera	Cisco のビデオ サーベイランス カメラの QoS マーキングを信頼します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
15.1(1)SG、 15.1(1)SG IOS-XE 3.3.0	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

auto qos video コマンドは Cisco TelePresence が検出された場合だけ、インターフェイスを信頼します。それ以外の場合は、ポートは信頼できない状態です。

生成されたグローバル レベル コマンド

auto-Qos srnd4 コマンドは、インターフェイスに適用されると、グローバル コンフィギュレーション レベルで次のテンプレートの 1 つまたは複数を生成します。通常、コマンドは、アプリケーション クラスにトラフィックを分類するために ACL または DSCP（または CoS）値に一致する一連のクラス マップを生成します。生成されたクラスと一致し、クラスで qos-group を設定し、場合によっては設定された帯域幅にクラスをポリシングする入力ポリシーも生成されます。（qos-group は、異なるアプリケーション クラスが 1 つの単位として扱われるようにする数値のタグにすぎません。スイッチのコンテキスト外では重要ではありません）。さらに、入力ポリシーで設定された qos-group と一致する 8 個の出力キュー クラス マップが生成されます。実際の出力ポリシーは、8 個の出力キュー クラス マップそれぞれにキューを割り当てます。

srnd4 コマンドは必要な場合にだけ、テンプレートを生成します。たとえば、新しいコマンドを初めて使用すると、8 個のキューの出力サービス ポリシーを定義するグローバル設定が生成されます。その後、他のインターフェイスに適用された auto-QoS コマンドは出力キューイングのテンプレートを生成しません。これは、すべての auto-QoS コマンドが移行後も同じ 8 個のキューのモデルに依存し、コマンドの最初の使用時からすでに生成されているためです。

A および B で定義されたグローバルなテンプレート。

A.**auto qos video** コマンドで使用されるアプリケーション クラスのテンプレート。

このテンプレートには、**auto qos video cts**、**auto qos video ip-camera**、および **auto qos trust** コマンドの入力サービス ポリシーも含まれます。この 3 つのコマンドは AutoQos-4.0-Input-Policy を使用する唯一のものであるため、コマンドで使用されるアプリケーション クラスを定義する同じテンプレートにそのポリシーを含めることを推奨します。

```
class-map match-any AutoQos-4.0-VoIP
```

```
    match dscp ef
    match cos 5
  class-map match-all AutoQos-4.0-Broadcast-Vid
    match dscp cs5
  class-map match-all AutoQos-4.0-Realtime-Interact
    match dscp cs4
  class-map match-all AutoQos-4.0-Network-Ctrl
    match dscp cs7
  class-map match-all AutoQos-4.0-Internetwork-Ctrl
    match dscp cs6
  class-map match-any AutoQos-4.0-Signaling
    match dscp cs3
    match cos 3
  class-map match-all AutoQos-4.0-Network-Mgmt
    match dscp cs2
  class-map match-any AutoQos-4.0-Multimedia-Conf
    match dscp af41
    match dscp af42
    match dscp af43
 class-map match-any AutoQos-4.0-Multimedia-Stream
    match dscp af31
    match dscp af32
    match dscp af33
  class-map match-any AutoQos-4.0-Transaction-Data
    match dscp af21
    match dscp af22
    match dscp af23
  class-map match-any AutoQos-4.0-Bulk-Data
    match dscp af11
    match dscp af12
    match dscp af13
  class-map match-all AutoQos-4.0-Scavenger
    match dscp cs1
```

AutoQos-4.0-Signaling および AutoQos-4.0-VoIP クラスは、IP 電話がインターフェイスに接続されている場合に対処するために、Cos に一致する必要もあります。（Cisco IP Phone は、DSCP ではなく、CoS ビットだけを再マーキングできます）。

```
policy-map AutoQos-4.0-Input-Policy
      class AutoQos-4.0-VoIP
        set qos-group 32
      class AutoQos-4.0-Broadcast-Vid
        set qos-group 32
      class AutoQos-4.0-Realtime-Interact
        set qos-group 32
      class AutoQos-4.0-Network-Ctrl
        set qos-group 16
      class AutoQos-4.0-Internetwork-Ctrl
        set qos-group 16
      class AutoQos-4.0-Signaling
        set qos-group 16
      class AutoQos-4.0-Network-Mgmt
        set qos-group 16
      class AutoQos-4.0-Multimedia-Conf
        set qos-group 34
      class AutoQos-4.0-Multimedia-Stream
        set qos-group 26
      class AutoQos-4.0-Transaction-Data
        set qos-group 18
      class AutoQos-4.0-Bulk-Data
        set qos-group 10
      class AutoQos-4.0-Scavenger
        set qos-group 8
```

B.8 個のキューを割り当てるために出力クラスを使用する srnd4 出力ポリシーおよび出力キュー クラスのテンプレート。このテンプレートはすべての srnd コマンドに必要です。

```
class-map match-all AutoQos-4.0-Priority-Queue
  match qos-group 32
class-map match-all AutoQos-4.0-Control-Mgmt-Queue
  match qos-group 16
class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
class-map match-all AutoQos-4.0-Bulk-Data-Queue
       match qos-group 10
class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1
```

ポリシー マップ コンフィギュレーション モードで実行される **police** コマンドは、定義されているレート制限を超えたトラフィック フローの qos-group の再マーキングを許可しないため、AutoQos-4.0-Scavenger-Queue は qos-group 7 または dscp af11 と一致するように設定する必要があります。**auto qos classify police** コマンドが実行された場合、定義されているレート制限に違反したトラフィック フローは cs1 に再マーキングされますが、qos-group を超過アクションとして再マーキングできないため、元の qos-group 分類を保持します。ただし、AutoQos-4.0-Scavenger-Queue は出力ポリシー マップ内の他のすべてのキューより先に定義されるため、元の qos-group ラベルを保持しているにもかかわらず、再マーキングされたパケットはこのキューに分類されます。

```
    policy-map AutoQos-4.0-Output-Policy
 class AutoQos-4.0-Scavenger-Queue
   bandwidth remaining percent 1
 class AutoQos-4.0-Priority-Queue
   priority
   police cir percent 30 bc 33 ms
            conform-action transmit exceed-action drop
 class AutoQos-4.0-Control-Mgmt-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Conf-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Stream-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Trans-Data-Queue
   bandwidth remaining percent 10
   dbl
 class AutoQos-4.0-Bulk-Data-Queue
   bandwidth remaining percent 4
   dbl
 class class-default
   bandwidth remaining percent 25
```

生成されたインターフェイス レベル コマンド

Fa/Gig ポート :

```
Switch(config-if)# service-policy input AutoQos-4.0-Input-Policy
                   service-policy output AutoQos-4.0-Output-Policy
```

例

次の例では、Cisco TelePresence インターフェイス gigabitethernet1/1 に QoS 設定を生成する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
```

```
Switch(config-if)# auto qos video cts
Switch(config-if)# do sh running interface gigabitethernet1/1
interface interface-id
 auto qos video cts
 qos trust device cts
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
end
```

次の例では、Cisco カメラのインターフェイス gigabitethernet1/1 の QoS 設定を生成する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos video ip-camera
Switch(config-if)# do sh running interface interface-id
interface interface-id
 auto qos video ip-camera
 qos trust device ip-camera
 service-policy input AutoQos-4.0-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
end
```

関連コマンド

コマンド	説明
auto qos trust	信頼できるインターフェイスの QoS 設定を生成します。
auto qos srnd4	ソリューション リファレンス ネットワーク デザイン 4.0 に基づいて QoS 設定を生成します。

auto qos voip

自動的に QoS ドメイン内の Voice over IP（VoIP）の Quality of Service を設定（auto-QoS）するには、**auto qos voip** 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。auto-QoS 設定を標準 QoS デフォルトに変更するには、このコマンドの **no** 形式を使用します。

auto qos voip {**cisco-phone** | **trust**}

no auto qos voip {**cisco-phone** | **trust**}

構文の説明

cisco-phone	Cisco IP Phone インターフェイスの QoS 設定を生成します（CDP を介した条件付き信頼）。着信パケットの CoS ラベルが信頼されるのは、IP Phone が検出される場合に限ります。
trust	インターフェイスを信頼できるスイッチまたはルータに接続し、自動的に VoIP の QoS を設定します。着信パケットの CoS および DSCP ラベルは信頼されます。

デフォルト

すべてのインターフェイスで auto-QoS 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 モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドを使用して、スイッチを含む QoS ドメイン内、ネットワーク内部、および QoS の着信トラフィックを分類できるエッジ デバイスの VoIP トラフィックに適した QoS を設定します。

Cisco IP Phone に接続された（ネットワーク エッジの）ポート上で **cisco-phone** キーワードを適用します。スイッチは、Cisco Discovery Protocol（CDP）を介して IP Phone を検出し、その IP Phone から受信したパケット内の CoS ラベルを信頼します。

ネットワーク内部に接続されているポート上で **trust** キーワードを適用します。トラフィックが他のエッジ デバイスによってすでに分類されていると想定します。そのため、これらのパケットの CoS/DSCP ラベルは信頼されます。

指定したインターフェイスで auto-QoS 機能をイネーブルにすると、自動的に次のアクションが行われます。

- QoS がグローバルにイネーブルになります（**qos** グローバル コンフィギュレーション コマンド）。
- DBL がグローバルにイネーブルになります（**qos dbl** グローバル コンフィギュレーション コマンド）。
- **auto qos voip cisco-phone** 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と、信頼境界機能がイネーブルになります。この機能は、Cisco Discovery Protocol（CDP）を使用して、Cisco IP Phone が存在するかしないかを検出します。Cisco IP Phone が検出されると、特定のインターフェイス上の入力分類は、パケットで受信した CoS ラベルを信頼するように設定されます。これは、一部の古い IP Phone で DSCP がマーキングされないためです。Cisco IP Phone が存在しない場合は、パケットの CoS ラベルを信頼しないように入力分類が設定されます。

- **auto qos voip trust** 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と、指定したインターフェイスがレイヤ 2 として設定されている場合は、このインターフェイス上の入力分類がパケットで受信した CoS ラベルを信頼するように設定されます(このインターフェイスがレイヤ 3 として設定されている場合は、DSCP を信頼するように設定されます)。

自動 QoS は、スタティック アクセス、ダイナミックアクセス、音声 VLAN アクセス、およびトランク ポートでイネーブルにできます。

auto-QoS がイネーブルのときに自動的に生成される QoS 設定を表示するには、(Auto-QoS をイネーブルにする前に) **debug auto qos** 特権 EXEC コマンドを使用してデバッグをイネーブルにします。

インターフェイス上で auto-QoS をディセーブルにするには、**no auto qos voip** インターフェイス コンフィギュレーション コマンドを使用します。このコマンドを入力すると、スイッチは標準 QoS をイネーブルにして、そのインターフェイスの auto-QoS 設定を標準 QoS デフォルト設定に変更します。このアクションは、auto-QoS によって実行されるグローバル設定を変更しません。グローバル設定は同じままです。

例

次の例では、ギガビット イーサネット インターフェイス 1/1 に接続されているスイッチまたはルータが信頼できるデバイスである場合に、auto-QoS をイネーブルにし、着信パケットで受信した CoS および DSCP ラベルを信頼する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
```

次の例では、ファスト イーサネット インターフェイス 2/1 に接続されているデバイスが Cisco IP Phone として検出されたときに、auto-QoS をイネーブルにし、着信パケットで受信した CoS ラベルを信頼する方法を示します。

```
Switch(config)# interface fastethernet2/1
Switch(config-if)# auto qos voip cisco-phone
```

次の例では、Supervisor Engine 6-E のインターフェイス上で、auto-QoS がイネーブルの場合に自動生成される QoS 設定を表示する方法を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitethernet3/10
Switch(config-if)#auto qos voip trust
Switch(config-if)#
1d03h:  service-policy input AutoQos-VoIP-Input-Cos-Policy
1d03h:  service-policy output AutoQos-VoIP-Output-Policy
Switch(config-if)#intface gigabitethernet3/11
Switch(config-if)#auto qos voip
cisco-phone
Switch(config-if)#
1d03h:  qos trust device cisco-phone
1d03h:  service-policy input AutoQos-VoIP-Input-Cos-Policy
1d03h:  service-policy output AutoQos-VoIP-Output-Policy
Switch(config-if)#end
Switch#
```

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

関連コマンド

コマンド	説明
debug auto qos（Cisco IOS のマニュアルを参照）	自動 QoS をデバッグします。
qos trust	インターフェイスの信頼状態を設定します。

コマンド	説明
show auto qos	適用される Automatic Quality of Service（auto-QoS）設定を表示します。
show qos	QoS 情報を表示します。
show qos interface	キューイング情報を表示します。
show qos maps	QoS マップ情報を表示します。

auto qos voip cisco-softphone

Cisco IP SoftPhone アプリケーションを実行する PC に接続しているインターフェイスの QoS 設定を生成し、そのようなインターフェイスからのポリシング トラフィックをマーキングするには、**auto qos voip** 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。

auto qos voip cisco-softphone

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
15.1(1)SG、 15.1(1)SG IOS-XE 3.3.0	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

auto qos voip コマンドで設定されたポートは信頼できないものとされます。

生成されたグローバル レベル コマンド

auto-QoS srnd4 コマンドがインターフェイスに適用されると、グローバル コンフィギュレーション レベルで次のテンプレート（A、B、および C）が 1 つまたは複数生成されます。通常、コマンドは、アプリケーション クラスにトラフィックを分類するために ACL または DSCP（または CoS）値に一致する一連のクラス マップを生成します。生成されたクラスと一致し、クラスで qos-group を設定し、場合によっては設定された帯域幅にクラスをポリシングする入力ポリシーも生成されます。（qos-group は、異なるアプリケーション クラスが 1 つの単位として扱われるようにする数値のタグです。スイッチのコンテキスト外では重要ではありません）。さらに、入力ポリシーで設定された qos-group と一致する 8 個の出力キュー クラス マップが生成されます。実際の出力ポリシーは、この 8 個のクラス マップそれぞれにキューを割り当てます。

コマンドは必要な場合にだけテンプレートを生成します。たとえば、新しいコマンドを初めて使用すると、8 個のキューの出力サービス ポリシーを定義するグローバル設定が生成されます。その後、他のインターフェイスに適用された auto-QoS は出力キューイングのテンプレートを生成しません。これは、すべての auto-Qos コマンドが移行後も同じ 8 個のキューのモデルに依存し、コマンドの最初の使用時からすでに生成されているためです。

グローバルなテンプレートは A、B、および C によって定義されます。

A.ACL および **auto qos voip cisco-softphone** コマンドで使用されるアプリケーション クラスのテンプレート。

```
ip access-list extended AutoQos-4.0-ACL-Multimedia-Conf
      permit udp any any range 16384 32767
    ip access-list extended AutoQos-4.0-ACL-Signaling
      permit tcp any any range 2000 2002
      permit tcp any any range 5060 5061
            permit udp any any range 5060 5061
```

```
 ip access-list extended AutoQos-4.0-ACL-Transactional-Data
   permit tcp any any eq 443
   permit tcp any any eq 1521
   permit udp any any eq 1521
   permit tcp any any eq 1526
   permit udp any any eq 1526
   permit tcp any any eq 1575
   permit udp any any eq 1575
   permit tcp any any eq 1630
   permit udp any any eq 1630
 ip access-list extended AutoQos-4.0-ACL-Bulk-Data
   permit tcp any any eq ftp
   permit tcp any any eq ftp-data
   permit tcp any any eq 22
   permit tcp any any eq smtp
   permit tcp any any eq 465
   permit tcp any any eq 143
   permit tcp any any eq 993
   permit tcp any any eq pop3
   permit tcp any any eq 995
   permit tcp any any eq 1914
 ip access-list extended AutoQos-4.0-ACL-Scavenger
   permit tcp any any eq 1214
   permit udp any any eq 1214
   permit tcp any any range 2300 2400
   permit udp any any range 2300 2400
   permit tcp any any eq 3689
   permit udp any any eq 3689
   permit tcp any any range 6881 6999
   permit tcp any any eq 11999
   permit tcp any any range 28800 29100
 ip access-list extended AutoQos-4.0-ACL-Default
   permit ip any any

class-map match-any AutoQos-4.0-VoIP-Data
        match dscp ef
        match cos 5
      class-map match-all AutoQos-4.0-VoIP-Data-Cos
        match cos 5
      class-map match-any AutoQos-4.0-VoIP-Signal
        match dscp cs3
        match cos 3
      class-map match-all AutoQos-4.0-VoIP-Signal-Cos
        match cos 3
class-map match-all AutoQos-4.0-Multimedia-Conf-Classify
        match access-group name AutoQos-4.0-ACL-Multimedia-Conf
class-map match-all AutoQos-4.0-Signaling-Classify
  match access-group name AutoQos-4.0-ACL-Signaling
class-map match-all AutoQos-4.0-Transaction-Classify
  match access-group name AutoQos-4.0-ACL-Transactional-Data
class-map match-all AutoQos-4.0-Bulk-Data-Classify
  match access-group name AutoQos-4.0-ACL-Bulk-Data
class-map match-all AutoQos-4.0-Scavenger-Classify
  match access-group name AutoQos-4.0-ACL-Scavenger
      class-map match-all AutoQos-4.0-Default-Classify
  match access-group name AutoQos-4.0-ACL-Default
```

AutoQos-4.0-VoIP-Data-Cos および AutoQos-4.0-VoIP-Signal-Cos は、ユーザがインターフェイスに IP 電話を接続し、そのインターフェイス上で **auto qos voip cisco-phone** コマンドを入力する場合に対処します。この場合は、インターフェイスの入力サービス ポリシーは、CoS マーキングだけに基づいて VoIP およびシグナリング パケットに一致する必要があります。これは、Cisco IP Phone のスイッチング ASIC が VoIP およびシグナリング トラフィックの CoS ビットの再マーキングのみに限定される

ためです。スイッチに接続された IP 電話に PC が接続されたユーザは、PC の NIC を使用してその PC から DSCP ef へのトラフィックの DSCP マーキングを再マーキングできるため、DSCP マーキングが一致するとセキュリティの脆弱性の原因になります。これにより、出力方向のプライオリティ キューに非リアルタイム トラフィックが誤って配置されます。

B.**auto qos voip cisco-softphone** コマンドの入力サービス ポリシーのテンプレート。

```
    policy-map AutoQos-4.0-Cisco-Softphone-Input-Policy
 class AutoQos-4.0-VoIP-Data
   set dscp ef
   set cos 5
   set qos-group 32
   police cir 128000 bc 8000
   exceed-action set-dscp-transmit cs1
   exceed-action set-cos-transmit 1
       class AutoQos-4.0-VoIP-Signal
   set dscp cs3
   set cos 3
   set qos-group 16
   police cir 32000 bc 8000
   exceed-action set-dscp-transmit cs1
         exceed-action set-cos-transmit 1
class AutoQos-4.0-Multimedia-Conf-Classify
   set dscp af41
   set cos 4
   set qos-group 34
   police cir 5000000 bc 8000
   exceed-action drop
 class AutoQos-4.0-Signaling-Classify
   set dscp cs3
   set cos 3
   set qos-group 16
   police cir 32000 bc 8000
   exceed-action drop
 class AutoQos-4.0-Transaction-Classify
   set dscp af21
   set cos 2
   set qos-group 18
   police cir 10000000 bc 8000
   exceed-action set-dscp-transmit cs1
   exceed-action set-cos-transmit 1
 class AutoQos-4.0-Bulk-Data-Classify
   set dscp af11
   set cos 1
   set qos-group 10
   police cir 10000000 bc 8000
   exceed-action set-dscp-transmit cs1
         exceed-action set-cos-transmit 1
 class AutoQos-4.0-Scavenger-Classify
   set dscp cs1
   set cos 1
   set qos-group 8
   police cir 10000000 bc 8000
   exceed-action drop
 class AutoQos-4.0-Default-Classify
   set dscp default
   set cos 0
```

C.8 個のキューを割り当てるために出力クラスを使用する srnd4 出力ポリシーおよび出力キュー クラスのテンプレート。このテンプレートはすべての srnd4 コマンドに必要です。

```
class-map match-all AutoQos-4.0-Priority-Queue
      match qos-group 32
    class-map match-all AutoQos-4.0-Control-Mgmt-Queue
```

```
  match qos-group 16
 class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
  match qos-group 34
 class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
  match qos-group 26
 class-map match-all AutoQos-4.0-Trans-Data-Queue
  match qos-group 18
 class-map match-all AutoQos-4.0-Bulk-Data-Queue
        match qos-group 10
 class-map match-any AutoQos-4.0-Scavenger-Queue
  match qos-group 8
  match dscp cs1
```

ポリシー マップ コンフィギュレーション モードで実行される **police** コマンドは、定義されているレート制限を超えたトラフィック フローの qos-group の再マーキングを許可しないため、AutoQos-4.0-Scavenger-Queue は qos-group 7 または dscp af11 と一致するように設定する必要があります。**auto qos classify police** コマンドが実行された場合、定義されているレート制限に違反したトラフィック フローは cs1 に再マーキングされますが、qos-group を超過アクションとして再マーキングできないため、元の qos-group 分類を保持します。ただし、AutoQos-4.0-Scavenger-Queue は出力ポリシー マップ内の他のすべてのキューより先に定義されるため、元の qos-group ラベルを保持しているにもかかわらず、再マーキングされたパケットはこのキューに分類されます。

```
    policy-map AutoQos-4.0-Output-Policy
 class AutoQos-4.0-Scavenger-Queue
   bandwidth remaining percent 1
 class AutoQos-4.0-Priority-Queue
   priority
   police cir percent 30 bc 33 ms
            conform-action transmit exceed-action drop
 class AutoQos-4.0-Control-Mgmt-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Conf-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Multimedia-Stream-Queue
   bandwidth remaining percent 10
 class AutoQos-4.0-Trans-Data-Queue
   bandwidth remaining percent 10
   dbl
 class AutoQos-4.0-Bulk-Data-Queue
   bandwidth remaining percent 4
   dbl
 class class-default
   bandwidth remaining percent 25
         dbl
```

生成されたインターフェイス レベル コマンド

Fa/Gig ポート :

```
Switch(config-if)#
               service-policy input AutoQos-4.0-Cisco-Softphone-Input-Policy
               service-policy input AutoQos-4.0-Output-Policy
```

例

次の例では、Cisco IP SoftPhone アプリケーションを実行している PC に接続されているギガビット イーサネット インターフェイス 1/1 の QoS 設定を生成する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-softphone
Switch(config-if)# do sh running interface gigabitethernet1/1
interface gigabitethernet1/1
 auto qos voip cisco-phone
```

```
 qos trust device cisco-phone
 service-policy input AutoQos-4.0-Cisco-Phone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
end
```

関連コマンド

コマンド	説明
auto qos voip cisco-softphone	Cisco IP SoftPhone アプリケーションを実行している PC に接続されたインターフェイスの QoS 設定を生成し、このようなインターフェイスからのポリシング トラフィックをマーキングします。
auto qos classify	信頼できないインターフェイスの QoS 設定を生成します。
auto qos classify police	信頼できないインターフェイスからのトラフィックをポリシングします。

auto-sync

NVRAM にあるコンフィギュレーション ファイルの自動同期化をイネーブルにするには、**auto-sync** コマンドを使用します。自動同期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。

auto-sync {**startup-config** | **config-register** | **bootvar** | **standard**}

no auto-sync {**startup-config** | **config-register** | **bootvar** | **standard**}

構文の説明

startup-config	スタートアップ コンフィギュレーションの自動同期化を指定します。
config-register	コンフィギュレーション レジスタ設定の自動同期化を指定します。
bootvar	BOOTVAR コンフィギュレーションの自動同期化を指定します。
standard	スタートアップ コンフィギュレーション、BOOTVAR、およびコンフィギュレーション レジスタの自動同期化を指定します。

デフォルト

すべてのコンフィギュレーション ファイルの自動同期化は standard

コマンド モード

冗長メイン CPU モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました（Catalyst 4507R のみ）。

使用上のガイドライン

no auto-sync standard コマンドを入力すると、自動同期化は行われません。

例

次の例では、メイン CPU で（デフォルト設定から）コンフィギュレーション レジスタの自動同期化をイネーブルにする方法を示します。

```
Switch# config terminal
Switch (config)# redundancy
Switch (config-r)# main-cpu
Switch (config-r-mc)# no auto-sync standard
Switch (config-r-mc)# auto-sync configure-register
Switch (config-r-mc)#
```

関連コマンド

コマンド	説明
redundancy	冗長コンフィギュレーション モードを開始します。

average-packet-size（netflow-lite モニタ サブモード）

netflow-lite モニタ サブモードの観測ポイントでの平均パケット サイズを指定するには、**average-packet-size** コマンドを使用します。サンプラを削除するには、このコマンドの **no** 形式を使用します。

average-packet-size *average-packet-size*

no average-packet-size *average-packet-size*

構文の説明

average-packer-size	観測ポイントで予測される平均パケット サイズをバイトで指定します。

デフォルト

0 バイト

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

物理ポート インターフェイス モード、ポート チャネル インターフェイス モード、または config VLAN モードでこのコマンドを入力できます。

パケット サンプリング メカニズムでは、ランダムな 1/N サンプリングを試みます。内部的には、2 つのレベルのサンプリングが実行されます。最初のサンプリングのレベルの精度は、特定のインターフェイスに到着したパケットのサイズによって異なります。アルゴリズムの精度を調整するには **average-packet-size** パラメータを使用します。

システムによって自動的に入力トラフィックの監視に基づいてインターフェイスでの平均パケット サイズが決定され、最初のレベルのサンプリングでの値が使用されます。

アルゴリズムには、64 ～ 9216 バイトのパケット サイズ範囲が必要です。0 の値は、平均パケット サイズの自動決定が必要であることを意味します。

例

次の例では、ポートのギガビット インターフェイス 1/3 のモニタを設定する方法を示します。

```
Switch# config terminal
Switch(config)# int GigabitEthernet1/3
Switch(config-if)# netflow-lite monitor 1
Switch(config-netflow-lite-monitor)# sampler sampler1
Switch(config-netflow-lite-monitor)# exporter exporter1
Switch(config-netflow-lite-monitor)# average-packet-size 128
Switch(config-netflow-lite-monitor)# exit
Switch(config-if)# exit
Switch(config)# exit
Switch(config)#
```

```
Switch# show netflow-lite monitor 1 interface gi1/3
Interface GigabitEthernet1/3:
  Netflow-lite  Monitor-1:
    Active:               TRUE
    Sampler:              sampler1
    Exporter:             exporter1
    Average Packet Size:  0
  Statistics:
    Packets exported:     0
    Packets observed:     0
    Packets dropped:      0
    Average Packet Size observed: 64
    Average Packet Size used: 64
```

show netflow-lite exporter 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
sampler（netflow-lite モニタ サブモード）	netflow-lite モニタ サブモードのインターフェイスでサンプリングをアクティブにします。
exporter（netflow-lite モニタ サブモード）	netflow-lite モニタ サブモードのエクスポータを割り当てます。

bandwidth

物理ポートに適用されているポリシー マップに属するクラスに割り当てる最小帯域幅を指定または変更するには、**bandwidth** ポリシーマップ クラス 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。

bandwidth {*bandwidth-kbps* | **percent** *percent* | **remaining percent** *percent*}

no bandwidth

構文の説明

bandwidth-kbps	クラスに割り当てる帯域幅の量（kbps 単位）。指定できる範囲は 32 ～ 16000000 です
percent *percent*	親クラスに割り当てる、使用可能な帯域幅の割合。指定できる範囲は 1 ～ 100 です。
remaining percent *percent*	親クラスに割り当てる、帯域幅の残りの割合。指定できる範囲は 1 ～ 100 です。このコマンドは、プライオリティ キューイング クラスが設定されている場合に限りサポートされ、プライオリティ キューイング クラスはレート制限されません。

デフォルト

帯域幅は指定されていません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(40)SG	このコマンドが、Supervisor Engine 6E を使用する Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

bandwidth コマンドは、物理ポートに適用されているポリシー マップでのみ使用します。

bandwidth コマンドでは、スイッチでトラフィックの輻輳が発生した場合の、クラスのトラフィックの最小帯域幅を指定します。スイッチで輻輳が発生していない場合、そのクラスにはこのコマンドで指定した帯域幅より大きい帯域幅が適用されます。

帯域幅を明示的に指定しないでキューイング クラスを設定した場合、キューの最小帯域幅がまったく保証されないため、そのキューはポートに割り当てられていない帯域幅の一部を使用します。

新しいキューの未割り当て帯域幅がない場合、または明示的な帯域幅設定を持たないすべてのキューの最小設定可能レートを満たすのに未割り当て帯域幅が十分でない場合、ポリシーの関連付けは拒否されます。

bandwidth コマンドには次の制限が適用されます。

- **percent** キーワードを使用する場合は、1 つのポリシー マップ内のクラス帯域幅の割合の合計が 100% を超えることはできません。割合の計算は、ポートで使用可能な帯域幅が基準となります。

- 帯域幅は、レイヤ 2 オーバーヘッドを収容できる大きさに設定する必要があります。
- 1 つのポリシー マップ内では、すべてのクラス帯域幅を kbps またはパーセント単位で指定できますが、これらを混在させることはできません。

例

次の例では、*silver-class* という名前のクラスの最小帯域幅を 2000 kbps に設定する方法を示します。このクラスは、スイッチのコンフィギュレーションにすでに存在します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map polmap6
Switch(config-pmap)# class silver-class
Switch(config-pmap-c)# bandwidth 2000
Switch(config-pmap-c)# end
```

次の例では、CBWFQ が設定されている場合に、*class1* に 30% の帯域幅を、*class2* に 25% の帯域幅を保証する方法を示します。2 種類のクラスがあるポリシー マップが作成され、物理ポートに接続されます。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input policy1
Switch(config-if)# end
```

次の例では、Low-Latency Queueing（LLQ; 低遅延キューイング）および帯域幅が設定されている場合に、帯域幅を保証する方法を示します。この例では、voice1 というクラスで LLQ がイネーブルにされています。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# bandwidth remaining percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# class voice1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# end
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
```

設定を確認するには、**show policy-map** 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
class	トラフィック ポリシーを作成または変更するクラスの名前を指定します。
dbl	トラフィックのクラスが使用する送信キュー上で、アクティブキュー管理をイネーブルにします。
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
priority	完全プライオリティ キュー（低遅延キューイング（LLQ）をイネーブルにして、物理ポートに適用されているポリシー マップに属するトラフィックのクラスにプライオリティを指定します。
service-policy（ポリシー マップ クラス）	ポリシー マップ内に QoS（Quality of Service）ポリシーとしてサービス ポリシーを作成します。
shape（クラス ベース キューイング）	物理ポートに適用されているポリシー マップに含まれるトラフィック クラスのトラフィック シェーピングをイネーブルにします。
show policy-map	ポリシー マップ情報を表示します。

call-home（グローバル コンフィギュレーション）

Call Home 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 **call-home** コマンドを使用します。

call-home

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

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが Supervisor Engine 6E および Catalyst 4900M に追加されました。

使用上のガイドライン

call-home コマンドを入力すると、プロンプトが Switch (cfg-call-home)# に変化し、次の Call Home コンフィギュレーション コマンドを使用できるようになります。

- **alert-group**：アラート グループをイネーブルまたはディセーブルにします。**alert-group** コマンドを参照してください。
- **contact-email-addr** *email-address*：システムの担当者の電子メール アドレスを割り当てます。電子メール アドレス形式で最大 128 文字の英数字を入力できます（スペースなし）。
- **contract-id** *alphanumeric*：Cisco AutoNotification のカスタマー契約 ID を指定します。最大 64 文字の英数字を入力できます。スペースを入力する場合は、エントリを引用符（""）で囲む必要があります。
- **copy profile** *source-profile target-profile*：既存のプロファイル（*source-profile*）と同じ設定で新しい宛先プロファイル（*target-profile*）を作成します。
- **customer-id** *name*：Cisco AutoNotify 用のカスタマー ID を指定します。最大 256 文字の英数字を入力できます。スペースを入力する場合は、エントリを引用符（""）で囲む必要があります。
- **default**：コマンドをデフォルト値に設定します。
- **exit**：Call Home コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
- **mail-server** {*ipv4-address* | *name*} **priority** *priority*：カスタマーの電子メール サーバのアドレスおよび相対プライオリティを割り当てます。IP アドレスまたは完全修飾ドメイン名（FQDN）を入力し、1（最高）～100（最低）のプライオリティを割り当てることができます。

  mail-server コマンドを繰り返し、別の **priority** 番号を入力することで、バックアップ電子メール サーバを定義できます。
- **no**：コマンドを無効にするか、そのデフォルトに設定します。

- **phone-number +***phone-number* : 担当者の電話番号を指定します。*phone-number* 値は、プラス プレフィックス（+）で始まる必要があります。使用できるのはダッシュ（-）と数値だけです。最大 16 文字を入力できます。スペースを入力する場合は、エントリを引用符（""）で囲む必要があります。
- **profile** *name* : call-home プロファイル コンフィギュレーション モードを開始します。**profile** コマンドを参照してください。
- **rate-limit** *threshold* : Call Home メッセージのレート制限しきい値を設定します。有効値の範囲は 1 分あたり 1 ～ 60 メッセージです。
- **sender** {**from** | **reply-to**} *email-address* : call-home メッセージ送信元の電子メール アドレスを指定します。電子メール アドレス形式で最大 128 文字の英数字を入力できます（スペースなし）。
- **site-id** *alphanumeric* : Cisco AutoNotify 用のサイト ID を指定します。最大 256 文字の英数字を入力できます。スペースを入力する場合は、エントリを引用符（""）で囲む必要があります。
- **street-address** *street-address* : RMA 部品の送付先住所を指定します。最大 256 文字の英数字を入力できます。スペースを入力する場合は、エントリを引用符（""）で囲む必要があります。
- **vrf** : VPN Routing/Forwarding（VRF; VPN ルーティング / 転送）インスタンス名を指定します。名前の長さは 32 文字以内です。

例

次の例では、連絡先情報を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# call-home
Switch(cfg-call-home)# contact-email-addr username@example.com
Switch(cfg-call-home)# phone-number +1-800-555-4567
Switch(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345”
Switch(cfg-call-home)# customer-id Customer1234
Switch(cfg-call-home)# site-id Site1ManhattanNY
Switch(cfg-call-home)# contract-id Company1234
Switch(cfg-call-home)# exit
Switch(config)#
```

次の例では、call-home メッセージのレート制限しきい値を設定する方法を示します。

```
Switch(config)# call-home
Switch(cfg-call-home)# rate-limit 50
```

次の例では、call-home メッセージのレート制限しきい値をデフォルト設定に設定する方法を示します。

```
Switch(config)# call-home
Switch(cfg-call-home)# default rate-limit
```

次の例では、既存のプロファイルと同じコンフィギュレーション設定の新しい宛先プロファイルを作成する方法を示します。

```
Switch(config)# call-home
Switch(cfg-call-home)# copy profile profile1 profile1a
```

次の例では、一般的な電子メール パラメータおよびプライマリとセカンダリの電子メール サーバを設定する方法を示します。

```
Switch# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# call-home
Switch(cfg-call-home)# mail-server smtp.example.com priority 1
Switch(cfg-call-home)# mail-server 192.168.0.1 priority 2
Switch(cfg-call-home)# sender from username@example.com
Switch(cfg-call-home)# sender reply-to username@example.com
Switch(cfg-call-home)# exit
Switch(config)#
```

次の例では、call-home 電子メール メッセージを転送する vrf 名として MgmtVrf を指定する方法を示します。

```
Switch(cfg-call-home)# vrf MgmtVrf
```

関連コマンド

コマンド	説明
alert-group（Cisco IOS のマニュアルを参照）	アラート グループをイネーブルにします。
profile（Cisco IOS のマニュアルを参照）	call-home プロファイル コンフィギュレーション モードを開始します。
show call-home	Call Home コンフィギュレーション情報を表示します。

call-home request

システムの情報をシスコに送信して、Cisco アウトプット インタープリタ ツールからレポートおよび分析情報を得るには、特権 EXEC モードで **call-home request** コマンドを使用します。シスコからの分析レポートは、設定した連絡先の電子メール アドレスに送信されます。

call-home request {**output-analysis "***show-command***"** | **config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*]

構文の説明

output-analysis "*show-command***"**	分析用として指定した CLI show コマンドの出力を送信します。show コマンドは二重引用符（" "）で囲む必要があります。
config-sanity **bugs-list** **command-reference** **product-advisory**	要求するレポートのタイプを指定します。このキーワードに基づいて、**show running-config all**、**show version**、**show module**（スタンドアロン）、**show module switch all**（VS システム）コマンドなど、あらかじめ定義されたコマンド セットの出力がシスコに送信されて分析されます。
profile *name*	（任意）要求が送信される既存のプロファイルを指定します。プロファイルが指定されていない場合、要求は Cisco TAC プロファイルに送信されます。
ccoid *user-id*	（任意）登録済み Smart Call Home ユーザの ID を指定します。*user-id* を指定すると、結果の分析レポートは登録ユーザの電子メール アドレスに送信されます。*user-id* を指定しない場合、レポートはデバイスの連絡先電子メール アドレスに送信されます。

コマンド デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが Supervisor Engine 6E および Catalyst 4900M に追加されました。

使用上のガイドライン

Call Home 要求の受信者プロファイルをイネーブルにする必要はありません。要求メッセージを Cisco TAC に転送し、Smart Call Home サービスから返信を受信できるように、Transport Gateway が設定された電子メール アドレスをプロファイルに指定します。

要求するレポートのタイプを指定するキーワードに基づき、要求に対して次の情報が返されます。

- **config-sanity**：現在の実行コンフィギュレーションに関連するベスト プラクティスの情報。
- **bugs-list**：実行中のバージョンおよび現在適用されている機能の既知のバグ。
- **command-reference**：実行コンフィギュレーションに含まれるすべてのコマンドへの参照リンク。
- **product-advisory**：ネットワークのデバイスに影響する可能性のある Product Security Incident Response Team（PSIRT）通知、End of Life（EOL）または End of Sales（EOS）通知、あるいは Field Notice（FN）。

例

次に、ユーザが指定した show コマンドの分析を要求する例を示します。

```
Switch# call-home request output-analysis "show diagnostic result module all" profile TG
```

関連コマンド

call-home（グローバル コンフィギュレーション）	Call Home コンフィギュレーション モードを開始します。
call-home send	実行する CLI コマンドを、電子メールで送信するコマンド出力とともに送信します。
call-home send alert-group	特定のアラート グループ メッセージを送信します。
service call-home（Cisco IOS のマニュアルを参照）	Call Home をイネーブルまたはディセーブルにします。
show call-home	call-home コンフィギュレーション情報を表示します。

call-home send

CLI コマンドを実行し、コマンド出力を電子メールで送信するには、特権 EXEC モードで **call-home send** コマンドを使用します。

call-home send "*cli-command***" {email** *email-addr* **[service-number** *SR***] | service-number** *SR***}**

構文の説明

"*cli-command***"**	実行する CLI コマンドを指定します。コマンド出力は電子メールで送信されます。
email *email-addr*	CLI コマンド出力の送信先の電子メール アドレスを指定します。電子メール アドレスを指定していない場合、コマンド出力は Cisco TAC（attach@cisco.com）に送信されます。
service-number *SR*	コマンド出力が関係するアクティブな TAC ケース番号を指定します。この番号は、電子メール アドレス（または TAC 電子メール アドレス）が指定されていない場合にのみ必要で、電子メールの件名行に表示されます。

コマンド デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが Supervisor Engine 6E および Catalyst 4900M に追加されました。

使用上のガイドライン

このコマンドを使用すると、指定した CLI コマンドがシステム上で実行されます。指定する CLI コマンドは、引用符（""）で囲む必要があります。また、任意の run コマンドまたは show コマンド（すべてのモジュール用のコマンドを含む）を指定できます。

その後、コマンド出力は、電子メールで指定の電子メール アドレスに送信されます。電子メール アドレスを指定していない場合、コマンド出力は Cisco TAC（attach@cisco.com）に送信されます。電子メールは、件名行にサービス番号を付けて（指定した場合）ロング テキスト形式で送信されます。

例

次の例では、CLI コマンドを送信して、コマンド出力を電子メールで受け取る方法を示します。

```
Switch# call-home send "show diagnostic result module all" email support@example.com
```

関連コマンド

call-home（グローバル コンフィギュレーション）	Call Home コンフィギュレーション モードを開始します。
call-home send alert-group	特定のアラート グループ メッセージを送信します。

service call-home（Cisco IOS のマニュアルを参照）	Call Home をイネーブルまたはディセーブルにします。
show call-home	call-home コンフィギュレーション情報を表示します。

call-home send alert-group

特定のアラート グループ メッセージを送信するには、特権 EXEC モードで **call-home send alert-group** コマンドを使用します。

call-home send alert-group {**configuration** | **diagnostic module** *number* | **inventory**} [**profile** *profile-name*]

構文の説明

configuration	コンフィギュレーション アラート グループ メッセージを宛先プロファイルに送信します。
diagnostic module *number*	診断アラート グループ メッセージを特定のモジュール番号の宛先プロファイルに送信します。
inventory	インベントリ call-home メッセージを送信します。
profile *profile-name*	（任意）宛先プロファイルの名前を指定します。

コマンド デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが Supervisor Engine 6E および Catalyst 4900M に追加されました。

使用上のガイドライン

モジュール番号を入力する場合、モジュールの数を入力できます。

profile *profile-name* を指定しない場合は、登録されたすべての宛先プロファイルにメッセージが送信されます。

手動で送信できるのは、コンフィギュレーション、診断、およびインベントリ アラート グループだけです。宛先プロファイルは、アラート グループに登録される必要はありません。

例

次に、設定アラート グループ メッセージを宛先プロファイルに送信する例を示します。

```
Switch# call-home send alert-group configuration
```

次の例では、診断アラート グループ メッセージを特定のモジュール番号の宛先プロファイルに送信する方法を示します。

```
Switch# call-home send alert-group diagnostic module 3
```

次の例では、診断アラート グループ メッセージを特定のモジュール番号のすべての宛先プロファイルに送信する方法を示します。

```
Switch# call-home send alert-group diagnostic module 3 profile Ciscotac1
```

次の例では、インベントリ call-home メッセージを送信する方法を示します。

```
Switch# call-home send alert-group inventory
```

関連コマンド

call-home（グローバル コンフィギュレーション）	Call Home コンフィギュレーション モードを開始します。
call-home test	定義した call-home テスト メッセージを送信します。
service call-home（Cisco IOS のマニュアルを参照）	Call Home をイネーブルまたはディセーブルにします。
show call-home	call-home コンフィギュレーション情報を表示します。

call-home test

Call Home テスト メッセージを手動で送信するには、特権 EXEC モードで **call-home test** コマンドを使用します。

call-home test [**"***test-message***"**] **profile** *profile-name*

構文の説明

"*test-message***"**	（任意）テスト メッセージ テキスト。
profile *profile-name*	宛先プロファイルの名前を指定します。

コマンド デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが Supervisor Engine 6E および Catalyst 4900M に追加されました。

使用上のガイドライン

このコマンドを使用すると、テスト メッセージが指定の宛先プロファイルに送信されます。テスト メッセージ テキストを入力する場合、テキストにスペースが含まれている場合は、このテキストを引用符（""）で囲む必要があります。メッセージを入力しない場合、デフォルト メッセージが送信されます。

例

次に、Call Home テスト メッセージを手動で送信する例を示します。

```
Switch# call-home test "test of the day" profile Ciscotac1
```

関連コマンド

call-home（グローバル コンフィギュレーション）	Call Home コンフィギュレーション モードを開始します。
call-home send alert-group	特定のアラート グループ メッセージを送信します。
service call-home（Cisco IOS のマニュアルを参照）	Call Home をイネーブルまたはディセーブルにします。
show call-home	call-home コンフィギュレーション情報を表示します。

channel-group

EtherChannel グループに EtherChannel インターフェイスを割り当てて設定するには、**channel-group** コマンドを使用します。インターフェイスからチャネル グループ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

channel-group *number* **mode** {**active** | **on** | **auto** [**non-silent**]} | {**passive** | **desirable** [**non-silent**]}

no channel-group

構文の説明

number	チャネル グループ番号を指定します。有効値の範囲は 1 ～ 64 です。
mode	インターフェイスの EtherChannel モードを指定します。
active	LACP を無条件にイネーブルにします。
on	PAgP を使用せず、ポートを強制的にチャネル化します。
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。
non-silent	（任意）トラフィックが他の装置から送信されることが予想される場合に auto または desirable モードとともに使用されます。
passive	LACP デバイスが検出された場合にかぎり、LACP をイネーブルにします。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。

デフォルト

チャネル グループは割り当てることができません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(13)EW	LACP のサポートが追加されました。

使用上のガイドライン

物理インターフェイスをチャネル グループに割り当てる前にポートチャネル インターフェイスを作成する必要はありません。ポートチャネル インターフェイスが作成されていない場合、このインターフェイスはチャネル グループの最初の物理インターフェイスが作成されたときに自動的に作成されます。

チャネル グループの PAgP がイネーブルになっているインターフェイスに特定のチャネル番号が使用されている場合、LACP がイネーブルであるインターフェイスを含むチャネルの設定には、同じチャネル番号を使用できません。その逆の場合も同様です。

interface port-channel コマンドを入力してポート チャネルを作成することもできます。この場合には、レイヤ 3 ポート チャネルが作成されます。レイヤ 3 ポート チャネルをレイヤ 2 ポート チャネルに変更するには、物理インターフェイスをチャネル グループに割り当てる前に **switchport** コマンドを使用します。ポート チャネルにメンバ ポートがある場合は、ポート チャネルをレイヤ 3 からレイヤ 2 に、またはレイヤ 2 からレイヤ 3 に変更できません。

チャネル グループに含まれる物理インターフェイスに割り当てられた IP アドレスをディセーブルにする必要はありませんが、これはディセーブルにしておくことを推奨します。

ポート チャネル インターフェイスに行われた設定変更または属性変更は、ポート チャネルと同じチャネル グループ内のすべてのインターフェイスに伝播されます（たとえば、設定変更は、そのポート チャネルの一部ではないが、そのチャネル グループの一部である物理インターフェイスにも伝えられます）。

on モードで 2 つのポート グループを接続することにより、使用可能な EtherChannel を作成できます。

注意　物理 EtherChannel インターフェイス上で、レイヤ 3 のアドレスをイネーブルにしないでください。物理 EtherChannel インターフェイス上でブリッジ グループを割り当てることは、ループが発生する原因になるため、行わないでください。

例

次の例では、ポート チャネル 45 によって指定された EtherChannel グループにギガビット イーサネット インターフェイス 1/1 を追加する方法を示します。

```
Switch(config-if)# channel-group 45 mode on
Creating a port-channel interface Port-channel45
Switch(config-if)#
```

関連コマンド

コマンド	説明
interface port-channel	ポートチャネル インターフェイスへのアクセスまたはポート チャネル インターフェイスの作成を行います。
show interfaces port-channel（Cisco IOS のマニュアルを参照）	Fast EtherChannel の情報を表示します。

channel-protocol

インターフェイスで LACP または PAgP をイネーブルにするには、**channel-protocol** コマンドを使用します。プロトコル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。

channel-protocol {**lacp** | **pagp**}

no channel-protocol {**lacp** | **pagp**}

構文の説明

lacp	チャネリングを管理するために LACP をイネーブルにします。
pagp	チャネリングを管理するために PAgP をイネーブルにします。

デフォルト

pagp

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

channel-group コマンドを使用して、プロトコルを選択することもできます。

インターフェイスがチャネルに属する場合は、このコマンドの **no** 形式を使用しても拒否されます。

同じ EtherChannel に属するすべてのポートでは、同じプロトコルを使用する必要があります。1 つのモジュールで 2 つのプロトコルは実行できません。

PAgP と LACP には互換性がありません。両方ともチャネルの終端は同じプロトコルを使用する必要があります。

スイッチを手動で設定すると、一方の側で PAgP、反対側で LACP を **on** モードにすることができます。

プロトコルはいつでも変更できます。ただし、変更した場合は、既存のすべての EtherChannel が、変更後のプロトコルのデフォルト チャネル モードにリセットされます。**channel-protocol** コマンドを使用すると、選択したプロトコルに適用できないモードが選択されないように制限できます。

EtherChannel 内のポートは、すべて同じ速度およびデュプレックス モードで動作するように設定してください（LACP モードの場合は全二重のみ）。

詳細な注意事項については、『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*』の「Configuring EtherChannel」を参照してください。

例

次の例では、インターフェイスでチャネリングを管理するために LACP を選択する方法を示します。

```
Switch(config-if)# channel-protocol lacp
Switch(config-if)#
```

関連コマンド

コマンド	説明
channel-group	EtherChannel グループに EtherChannel インターフェイスを割り当てて設定します。
show etherchannel	チャネルの EtherChannel 情報を表示します。

cisp enable

スイッチの Client Information Signalling Protocol（CISP）をイネーブルにするには、**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

cisp enable	CISP をイネーブルにします。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(54)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

オーセンティケータ スイッチとサプリカント スイッチの両方の CISP プロトコルを（グローバルな **cisp enable** コマンドを使用して）イネーブルにする必要があります。CISP プロトコルは、サプリカント スイッチからオーセンティケータ スイッチにクライアント情報を伝送し、それによってオーセンティケータ スイッチを介してサプリカント スイッチのクライアントにアクセスが提供されるため、重要です。

例

次の例では、CISP をイネーブルにする方法を示します。

```
switch(config)# cisp enable
```

関連コマンド

コマンド	説明
dot1x credentials（グローバル コンフィギュレーション）	プロファイルをサプリカント スイッチに設定します。
show cisp	指定されたインターフェイスの CISP 情報を表示します。

class

トラフィック ポリシーを作成または変更するクラスの名前を指定するには、**class** ポリシーマップ コンフィギュレーション コマンドを使用します。ポリシー マップから既存のクラスを削除するには、このコマンドの **no** 形式を使用します。

class *class-name*

no class *class-name*

構文の説明

class-name	トラフィック ポリシーを設定または変更する、あらかじめ定義されたトラフィック クラスの名前。クラスは、以前は **class-map** *class-map-name* グローバル コンフィギュレーション コマンドによって作成されました。

デフォルト

class-default 以外のクラスは定義されていません。

コマンド モード

ポリシーマップ コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

class コマンドを使用する前に、**class-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、クラスに対応するパケットのクラス マップを作成する必要があります。また、**policy-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、ポリシー マップを識別し、ポリシー マップ コンフィギュレーション モードを開始する必要があります。ポリシー マップを指定すると、そのポリシー マップ内で新規クラスのトラフィック ポリシーを設定したり、既存クラスのトラフィック ポリシーを変更したりできます。**class** コマンドを使用してポリシー マップに指定するクラス名は、**class-map** グローバル コンフィギュレーション コマンドで設定したように、クラスの特性（ポリシー）をクラス マップおよびその一致基準に関連付けます。ポリシー マップは、**service-policy（インターフェイス コンフィギュレーション）**コンフィギュレーション コマンドを使用してポートに適用します。

class コマンドを入力すると、スイッチがポリシーマップ クラス コンフィギュレーション モードになり、次のコンフィギュレーション コマンドを使用できるようになります。

- **bandwidth**：ポリシー マップに属するクラスに割り当てられる最小帯域幅を指定または修正します。詳細については、**bandwidth** コマンドを参照してください。
- **dbl**：このクラスに一致するトラフィックに対してダイナミック バッファ制限をイネーブルにします。**dbl** パラメータの詳細については、**show qos dbl** コマンドを参照してください。
- **exit**：ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードに戻ります。
- **no**：コマンドをデフォルト設定に戻します。
- **police**：単一レート ポリサー、集約ポリサー、またはトラフィックのクラスに Committed Information Rate（CIR; 認定情報レート）および Peak Information Rate（PIR; 最大情報レート）を使用する 2 レート トラフィック ポリサーを設定します。ポリサーは、帯域幅の限度およびその

限度を超過した場合に実行するアクションを指定します。詳細については、police コマンドを参照してください。2 レート ポリサーの詳細については、**police（2 つのレート）**および **police（割合）**コマンドを参照してください。

- **priority**：トラフィック クラスの完全プライオリティ キューをイネーブルにします。詳細については、**priority** コマンドを参照してください。
- **service-policy（ポリシー マップ クラス）**：ポリシー マップ内に QoS（Quality of Service）ポリシー（階層サービス ポリシー）としてサービス ポリシーを作成します。詳細については、**service-policy（ポリシー マップ クラス）**コマンドを参照してください。このコマンドは、インターフェイスに適用されている階層ポリシー マップでのみ有効です。
- **set**：パケットにサービス クラス（CoS）、DiffServ コード ポイント（DSCP）、または IP-precedence を設定して IP トラフィックを分類します。詳細については、**set** コマンドを参照してください。
- **shape（クラス ベース キューイング）**：ポリシー マップにトークン バケットの Committed Information Rate（CIR; 認定情報レート）を設定します。詳細については、**shape（クラス ベース キューイング）**コマンドを参照してください。
- trust ：トラフィック クラスの信頼状態を定義します。詳細については、**trust** コマンドを参照してください。このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

スイッチは、ポリシー マップでデフォルト クラスを含む最大 256 のクラスをサポートします。一致基準を満たさないパケットは、デフォルトのトラフィック クラスのメンバとして分類されます。デフォルト トラフィック クラスを設定するには、**class** ポリシーマップ クラス コンフィギュレーション コマンドで、クラス名に **class-default** を指定します。デフォルト トラフィック クラスは他のトラフィック クラスと同様に操作できますが（ポリシングまたはシェーピングのためにポリシーを設定するなど）、このクラスの削除はできません。

ポリシー マップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

例

次の例では、policy1 という名前のポリシー マップを作成する方法を示します。入力ポートに適用した場合、ポリシーは、class1 で定義されたすべての着信トラフィックを照合し、IP DSCP を 10 に設定し、1 Mbps の平均レートおよび 20 KB のバーストでトラフィックをポリシングします。プロファイルを超えるトラフィックは、ポリシングされた DSCP マップから取得した DSCP 値がマーク ダウンされてから送信されます。

```
Switch# configure terminal
Switch(config)# class-map class1
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet1/0/4
Switch(config-if)# service-policy input policy1
Switch#
```

設定を確認するには、**show policy-map** 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
bandwidth	物理ポートに適用されているポリシー マップに属するクラスに割り当てる最小帯域幅を指定または変更します。
class-map	名前を指定したクラスとパケットの照合に使用するクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
dbl	トラフィックのクラスが使用する送信キュー上で、アクティブ キュー管理をイネーブルにします。
police	トラフィック ポリシング機能を設定します。
police（割合）	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
police rate	単一レート ポリサーまたは 2 レート ポリサーを設定します。
policy-map	複数ポートに適用可能なポリシー マップを作成し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
priority	完全プライオリティ キュー（低遅延キューイング（LLQ）をイネーブルにして、物理ポートに適用されているポリシー マップに属するトラフィックのクラスにプライオリティを指定します。
service-policy（インターフェイス コンフィギュレーション）	ポリシー マップをインターフェイスに関連付けます。
service-policy（ポリシー マップ クラス）	ポリシー マップ内に QoS（Quality of Service）ポリシーとしてサービス ポリシーを作成します。
set	パケットにサービス クラス（CoS）、DiffServ コード ポイント（DSCP）、または IP-precedence を設定して IP トラフィックをマークします。
shape（クラス ベース キューイング）	物理ポートに適用されているポリシー マップに含まれるトラフィック クラスのトラフィック シェーピングをイネーブルにします。
show policy-map	ポリシー マップ情報を表示します。
trust	**class** ポリシーマップ コンフィギュレーション コマンドを使用して分類されたトラフィックの信頼状態を定義します。

class-map

指定したクラス名にパケットを照合するクラス マップを作成して、クラス マップ コンフィギュレーション モードを開始するには、**class-map** グローバル コンフィギュレーション コマンドを使用します。既存のクラス マップを削除して、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

class-map [**match-all** | **match-any**] *class-map-name*

no class-map [**match-all** | **match-any**] *class-map-name*

構文の説明

match-all	（任意）このクラス マップ内のすべての一致の論理積をとります。クラス マップ内のすべての基準が一致する必要があります。
match-any	（任意）このクラス マップ内の一致ステートメントの論理和をとります。クラス マップ内の 1 つまたは複数の基準が一致する必要があります。
class-map-name	クラス マップ名です。

デフォルト

クラス マップは定義されていません。

match-all または **match-any** のどちらのキーワードも指定しない場合、デフォルトは **match-all** です。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

クラス マップ一致基準を作成または変更するクラスの名前を指定し、クラス マップ コンフィギュレーション モードを開始する場合は、このコマンドを使用します。パケットは、クラス マップに設定されている一致基準と照合され、パケットがそのクラスに属しているかどうか判断されます。指定した基準にパケットが一致する場合、そのパケットはクラスのメンバと見なされ、トラフィック ポリシーに設定された QoS（Quality of Service）の仕様に従って転送されます。

class-map コマンドを入力すると、スイッチがクラスマップ コンフィギュレーション モードになり、次のコンフィギュレーション コマンドが使用可能になります。

- **description**：クラス マップを説明します（最大 200 文字）。**show class-map** 特権 EXEC コマンドを実行すると、クラス マップの説明と名前が表示されます。
- **exit**：QoS クラスマップ コンフィギュレーション モードを終了します。
- **match**：分類基準を設定します。詳細については、**match（クラスマップ コンフィギュレーション）**コマンドを参照してください。
- **no**：クラス マップから一致ステートメントを削除します。

例

次の例では、クラス マップ class1 に 1 つの一致基準（アクセス リスト 103）を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# access-list 103 permit any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
Switch#
```

次の例では、class1 クラス マップを削除する方法を示します。

```
Switch# configure terminal
Switch(config)# no class-map class1
Switch#
```

show class-map 特権 EXEC コマンドを入力すると、設定を確認できます。

関連コマンド

コマンド	説明
class	トラフィック ポリシーを作成または変更するクラスの名前を指定します。
match（クラスマップ コンフィギュレーション）	クラス マップの一致基準を定義します。
policy-map	複数ポートに適用可能なポリシー マップを作成し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
show class-map	クラス マップ情報を表示します。

clear counters

インターフェイス カウンタをクリアするには、**clear counters** コマンドを使用します。

clear counters [{**FastEthernet** *interface_number*} | {**GigabitEthernet** *interface_number*} | {**null** *interface_number*} | {**port-channel** *number*} | {**vlan** *vlan_id*}]

構文の説明

FastEthernet *interface_number*	（任意）ファスト イーサネット インターフェイスを指定します。有効値の範囲は 1 ～ 9 です。
GigabitEthernet *interface_number*	（任意）ギガビット イーサネット インターフェイスを指定します。有効値の範囲は 1 ～ 9 です。
null *interface_number*	（任意）ヌル インターフェイスを指定します。有効な値は 0 です。
port-channel *number*	（任意）チャネル インターフェイスを指定します。有効値の範囲は 1 ～ 64 です。
vlan *vlan_id*	（任意）VLAN を指定します。有効値の範囲は 1 ～ 4096 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張 VLAN アドレスのサポートが追加されました。

使用上のガイドライン

インターフェイスが指定されていない場合、このコマンドはすべてのインターフェイスの現在のインターフェイス カウンタをすべてクリアします。

（注）　このコマンドは、SNMP を使用して取得されたカウンタはクリアしませんが、**show interface counters** コマンドを入力したときに表示されるカウンタだけをクリアします。

例

次の例では、すべてのインターフェイス カウンタをクリアする方法を示します。

```
Switch# clear counters
Clear "show interface" counters on all interfaces [confirm] y
Switch#
```

次の例では、特定のインターフェイスのカウンタをクリアする方法を示します。

```
Switch# clear counters vlan 200
Clear "show interface" counters on this interface [confirm]y
Switch#
```

関連コマンド

コマンド	説明
show interface counters（Cisco IOS のマニュアルを参照）	インターフェイス カウンタ情報を表示します。

clear energywise neighbors

EnergyWise ネイバー テーブルを削除するには、**clear energywise neighbors** 特権 EXEC コマンドを使用します。

clear energywise neighbors

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。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、ネイバー テーブルを削除する方法を示します。

```
Switch# clear energywise neighbors
Cleared all non static energywise neighbors
```

対象となるテーブルが削除されたかどうかを確認するには、**show energywise neighbors** 特権 EXEC コマンドを入力します。

（注）　**clear energywise neighbors** コマンドは、検出されたネイバーをすべてクリアします。

関連コマンド

コマンド	説明
show energywise	エンティティおよび PoE ポートの EnergyWise の設定およびステータスを表示します。

clear errdisable

インターフェイス上で errdisable になっている VLAN を再度イネーブルにするには、**clear errdisable** コマンドを使用します。

clear errdisable interface {*name*} **vlan** [*range*]

構文の説明

interface *name*	回復する VLAN インターフェイスを指定します。
vlan	回復するインターフェイス上のすべての VLAN を指定します。
range	（任意）回復対象の VLAN 範囲を指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(52)SG	VLAN 単位の errdisable 検出のサポートが追加されました。

使用上のガイドライン

VLAN の範囲を指定しないと、指定したインターフェイス上のすべての VLAN が再びイネーブルになります。**clear errdisable** コマンドは、インターフェイス上でディセーブルになっている VLAN を回復します。

仮想ポートから errdisable ステートをクリアしても、物理ポートのリンク ステートは変更されず、物理ポートの他の VLAN ポートには影響しません。STP にイベントを送信し、スパニング ツリーにはその VLAN ポートを適切なブロッキングまたはフォワーディング ステートにする通常のプロセスが行われます。

例

次の例では、インターフェイス上でディセーブルになっている VLAN の範囲を再度イネーブルにする方法を示します。

```
Switch# clear errdisable interface ethernet2 vlan 10-15
Switch#
```

関連コマンド

コマンド	説明
errdisable detect	errdisable 検出をイネーブルにします。
show errdisable detect	errdisable 検出ステータスを表示します。
show interfaces status	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。
switchport port-security	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します。

clear hw-module slot password

インテリジェント回線モジュールのパスワードをクリアするには、**clear hw-module slot password** コマンドを使用します。

clear hw-module slot *slot_num* **password**

構文の説明

slot_num	回線モジュール上のスロット。

デフォルト

パスワードはクリアされていません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

パスワードをリセットしないかぎり、パスワードの変更が必要なのは 1 回だけです。

例

次の例では、回線モジュールのスロット 5 のパスワードをクリアする方法を示します。

```
Switch# clear hw-module slot 5 password
Switch#
```

関連コマンド

コマンド	説明
hw-module power	スロットまたは回線モジュールの電源をオフにします。

clear interface gigabitethernet

ギガビット イーサネット IEEE 802.3z インターフェイスからハードウェア ロジックをクリアするには、**clear interface gigabitethernet** コマンドを使用します。

（注）　このコマンドを実行しても **show interface gigabitethernet mod/port** コマンドで表示される **interface resets** は増分されません。

clear interface gigabitethernet *mod/port*

構文の説明

mod/port	モジュール番号とポート番号。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、ギガビット イーサネット IEEE 802.3z インターフェイスのハードウェア ロジックをクリアする方法を示します。

```
Switch# clear interface gigabitethernet 1/1
Switch#
```

関連コマンド

コマンド	説明
show interfaces status	インターフェイスのステータスを表示します。

clear interface vlan

VLAN からハードウェア ロジックをクリアするには、**clear interface vlan** コマンドを使用します。

clear interface vlan *number*

構文の説明

number	VLAN インターフェイスの番号。有効値の範囲は 1 ～ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張 VLAN アドレスのサポートが追加されました。

例

次の例では、特定の VLAN からハードウェア ロジックをクリアする方法を示します。

```
Switch# clear interface vlan 5
Switch#
```

関連コマンド

コマンド	説明
show interfaces status	インターフェイスのステータスを表示します。

clear ip access-template

アクセス リストの統計情報をクリアするには、**clear ip access-template** コマンドを使用します。

clear ip access-template *access-list*

構文の説明

access-list	アクセス リストの番号。有効な値は IP 拡張アクセス リストについては 100 ～ 199、拡張範囲 IP 拡張アクセス リストについては 2000 ～ 2699 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、アクセス リストの統計情報をクリアする方法を示します。

```
Switch# clear ip access-template 201
Switch#
```

clear ip arp inspection log

ログ バッファのステータスをクリアするには、**clear ip arp inspection log** コマンドを使用します。

clear ip arp inspection log

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、ログ バッファの内容をクリアする方法を示します。

```
Switch# clear ip arp inspection log
Switch#
```

関連コマンド

コマンド	説明
arp access-list	ARP アクセス リストを定義したり、定義済みリストの最後に句を追加したりします。
show ip arp inspection log	ログ バッファのステータスを表示します。

clear ip arp inspection statistics

ダイナミック ARP インスペクションの統計情報をクリアするには、**clear ip arp inspection statistics** コマンドを使用します。

clear ip arp inspection statistics [**vlan** *vlan-range*]

構文の説明

vlan *vlan-range*	（任意）VLAN 範囲を指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、VLAN 1 から DAI 統計情報をクリアする方法および消去を確認する方法を示します。

```
Switch# clear ip arp inspection statistics vlan 1
Switch# show ip arp inspection statistics vlan 1

 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1              0              0              0             0

 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                  0                        0
Switch#
```

関連コマンド

コマンド	説明
arp access-list	ARP アクセス リストを定義したり、定義済みリストの最後に句を追加したりします。
clear ip arp inspection log	ログ バッファのステータスをクリアします。
show ip arp inspection log	ログ バッファのステータスを表示します。

clear ip dhcp snooping binding

DHCP スヌーピング バインディングをクリアするには、**clear ip dhcp snooping binding** コマンドを使用します。

clear ip dhcp snooping binding [*] [*ip-address*] [**vlan** *vlan_num*] [**interface** *interface_num*]

構文の説明

*	（任意）すべての DHCP スヌーピング バインディング エントリをクリアします。
ip-address	（任意）DHCP スヌーピング バインディング エントリの IP アドレス。
vlan *vlan_num*	（任意）VLAN を指定します。
interface *interface_num*	（任意）インターフェイスを指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(44)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

これらのコマンドは、主に DHCP スヌーピング バインディング エントリをクリアするために使用されます。

グローバル スヌーピングおよび VLAN スヌーピングがどちらもイネーブルの場合にのみ、VLAN 上で DHCP スヌーピングがイネーブルになります。

例

次の例では、すべての DHCP スヌープ バインディング エントリをクリアする方法を示します。

```
Switch# clear ip dhcp snooping binding *
Switch#
```

次の例では、特定の DHCP スヌープ バインディング エントリをクリアする方法を示します。

```
Switch# clear ip dhcp snooping binding 1.2.3.4
Switch#
```

次の例では、ギガビット イーサネット インターフェイス 1/1 上のすべての DHCP スヌープ バインディング エントリをクリアする方法を示します。

```
Switch# clear ip dhcp snooping binding interface gigabitEthernet 1/1
Switch#
```

次の例では、VLAN 40 のすべての DHCP スヌープ バインディング エントリをクリアする方法を示します。

```
Switch# clear ip dhcp snooping binding vlan 40
```

```
Switch#
```

関連コマンド

コマンド	説明
ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping binding	DHCP バインディング コンフィギュレーションを設定および生成し、再起動後もバインディングを復元します。
ip dhcp snooping information option	DHCP オプション 82 データ挿入をイネーブルにします。
ip dhcp snooping trust	信頼できる VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング エントリを表示します。

clear ip dhcp snooping database

DHCP バインディング データベースをクリアするには、**clear ip dhcp snooping database** コマンドを使用します。

clear ip dhcp snooping database

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、DHCP スヌーピング バインディング データベースをクリアする方法を示します。

```
Switch# clear ip dhcp snooping database
Switch#
```

関連コマンド

コマンド	説明
ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping binding	DHCP バインディング コンフィギュレーションを設定および生成し、再起動後もバインディングを復元します。
ip dhcp snooping information option	DHCP オプション 82 データ挿入をイネーブルにします。
ip dhcp snooping trust	信頼できる VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング エントリを表示します。

clear ip dhcp snooping database statistics

DHCP バインディング データベースの統計情報をクリアするには、**clear ip dhcp snooping database statistics** コマンドを使用します。

clear ip dhcp snooping database 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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、DHCP スヌーピング バインディング データベースをクリアする方法を示します。

```
Switch# clear ip dhcp snooping database statistics
Switch#
```

関連コマンド

コマンド	説明
ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping binding	DHCP バインディング コンフィギュレーションを設定および生成し、再起動後もバインディングを復元します。
ip dhcp snooping information option	DHCP オプション 82 データ挿入をイネーブルにします。
ip dhcp snooping trust	信頼できる VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング エントリを表示します。

clear ip igmp group

IGMP グループ キャッシュ エントリを削除するには、**clear ip igmp group** コマンドを使用します。

clear ip igmp group [{**fastethernet** *mod/port*} | {**GigabitEthernet** *mod/port*} | {*host_name* | *group_address*} {**Loopback** *interface_number*} | {**null** *interface_number*} | {**port-channel** *number*} | {**vlan** *vlan_id*}]

構文の説明

fastethernet	（任意）ファスト イーサネット インターフェイスを指定します。
mod/port	（任意）モジュールおよびポートの番号。
GigabitEthernet	（任意）ギガビット イーサネット インターフェイスを指定します。
host_name	（任意）DNS ホスト テーブルまたは **ip host** コマンドで定義されているホスト名。
group_address	（任意）4 分割ドット表記で指定されたマルチキャスト グループのアドレス。
Loopback *interface_number*	（任意）ループバック インターフェイスを指定します。有効値は 0 ～ 2,147,483,647 です。
null *interface_number*	（任意）ヌル インターフェイスを指定します。有効な値は 0 です。
port-channel *number*	（任意）チャネル インターフェイスを指定します。有効値の範囲は 1 ～ 64 です。
vlan *vlan_id*	（任意）VLAN を指定します。有効値の範囲は 1 ～ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

IGMP キャッシュには、直接接続された LAN 上のホストがメンバであるマルチキャスト グループのリストが含まれます。

IGMP キャッシュからすべてのエントリを削除するには、引数を指定せずに **clear ip igmp group** コマンドを入力します。

例

次の例では、IGMP キャッシュから特定のグループのエントリをクリアする方法を示します。

```
Switch# clear ip igmp group 224.0.255.1
Switch#
```

次の例では、特定のインターフェイスから IGMP グループ キャッシュ エントリをクリアする方法を示します。

```
Switch# clear ip igmp group gigabitethernet 2/2
Switch#
```

関連コマンド

コマンド	説明
ip host（Cisco IOS のマニュアルを参照）	スタティック ホストの名前/アドレス マッピングをホスト キャッシュに定義します。
show ip igmp groups（Cisco IOS のマニュアルを参照）	ルータに直接接続されていて、インターネット グループ管理プロトコル（IGMP）経由で学習されたレシーバを持つマルチキャスト グループを表示します。**show ip igmp groups** コマンドは EXEC モードで使用します。
show ip igmp interface	IGMP インターフェイスのステータス情報およびコンフィギュレーション情報を表示します。

clear ip igmp snooping membership

明示的なホスト トラッキング データベースをクリアするには、**clear ip igmp snooping membership** コマンドを使用します。

clear ip igmp snooping membership [vlan *vlan_id*]

構文の説明

vlan *vlan_id*	（任意）VLAN を指定します。有効値の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(20)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

デフォルトでは、明示的なホスト トラッキング データベースは、最大 1 KB エントリを維持します。この制限に達すると、エントリはそれ以上データベースに作成できません。さらにエントリを作成するには、**clear ip igmp snooping statistics vlan** コマンドを使用してデータベースを削除する必要があります。

例

次の例では、VLAN 25 の IGMP スヌーピング統計情報を表示する方法を示します。

```
Switch# clear ip igmp snooping membership vlan 25
Switch#
```

関連コマンド

コマンド	説明
ip igmp snooping vlan explicit-tracking	VLAN 単位の明示的ホスト トラッキングをイネーブルにします。
show ip igmp snooping membership	ホスト メンバーシップ情報を表示します。

clear ip mfib counters

グローバル MFIB カウンタおよびすべてのアクティブ MFIB ルートのカウンタをクリアするには、**clear ip mfib counters** コマンドを使用します。

clear ip mfib counters

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、アクティブなすべての MFIB ルートおよびグローバル カウンタをクリアする方法を示します。

```
Switch# clear ip mfib counters
Switch#
```

関連コマンド

コマンド	説明
show ip mfib	アクティブな Multicast Forwarding Information Base（MFIB; マルチキャスト転送情報ベース）ルートをすべて表示します。

clear ip mfib fastdrop

すべての MFIB 高速ドロップ エントリをクリアするには、**clear ip mfib fastdrop** コマンドを使用します。

clear ip mfib fastdrop

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

新しい高速ドロップされたパケットが到着した場合、新しい高速ドロップ エントリが作成されます。

例

次の例では、すべての高速ドロップ エントリをクリアする方法を示します。

```
Switch# clear ip mfib fastdrop
Switch#
```

関連コマンド

コマンド	説明
ip mfib fastdrop	MFIB 高速ドロップをイネーブルにします。
show ip mfib fastdrop	現在アクティブな高速ドロップ エントリをすべて表示し、高速ドロップがイネーブルであるかどうかも示します。

clear ip wccp

特定のサービスのスイッチに保存されている Web キャッシュ通信プロトコル（WCCP）の統計情報（カウント）を削除するには、特権 EXEC モードで **clear ip wccp** コマンドを使用します。

clear ip wccp [**vrf** *vrf-name* {**web-cache** | *service-number*}] [**web-cache** | *service-number*]

構文の説明

web-cache	（任意）Web キャッシュ サービスの統計情報を削除するようにルータに指示します。
service-number	（任意）削除するキャッシュ サービスの番号。番号は、0 ～ 99 です。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更箇所
15.0(2)SG	このコマンドが、Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948E に追加されました。

使用上のガイドライン

WCCP 統計情報を表示するには、**show ip wccp** and **show ip wccp detail** コマンドを使用します。

すべての VRF のすべての WCCP サービス用の WCCP のカウンタをクリアするには、**clear ip wccp** コマンドを使用します。

例

次の例では、Web キャッシュ サービスに関連付けられたすべての統計情報をクリアする方法を示します。

```
Switch# clear ip wccp web-cache
```

関連コマンド

コマンド	説明
ip wccp	サービス グループに参加できるように、指定した WCCP サービスのサポートをイネーブルにします。
show ip wccp	WCCP に関連するグローバル統計情報を表示します。

clear lacp counters

特定のチャネル グループに属するすべてのインターフェイスの統計情報をクリアするには、**clear lacp counters** コマンドを使用します。

clear lacp [*channel-group*] **counters**

構文の説明

channel-group	（任意）チャネル グループ番号。有効値の範囲は 1 ～ 64 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

channel-group を指定しない場合は、すべてのチャネル グループがクリアされます。

PAgP モードのメンバが含まれるチャネル グループにこのコマンドを入力しても、コマンドは無視されます。

例

次の例では、特定のグループの統計情報をクリアする方法を示します。

```
Switch# clear lacp 1 counters
Switch#
```

関連コマンド

コマンド	説明
show lacp	LACP 情報を表示します。

clear mac-address-table

レイヤ 2 MAC アドレス テーブルからグローバル カウンタ エントリをクリアするには、**clear mac-address-table** コマンドを使用します。

clear mac-address-table {dynamic [{**address** *mac_addr*} | {**interface** *interface*}] [**vlan** *vlan_id*] | **notification**}

構文の説明

dynamic	ダイナミック エントリ タイプを指定します。
address *mac_addr*	（任意）MAC アドレスを指定します。
interface *interface*	（任意）インターフェイスを指定して、そのインターフェイスに関連付けられたエントリをクリアします。有効な値は **FastEthernet** および **GigabitEthernet** です。
vlan *vlan_id*	（任意）VLAN を指定します。有効値の範囲は 1 ～ 4094 です。
notification	MAC 変更通知のグローバル カウンタを指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張 VLAN アドレスのサポートが追加されました。
12.2(31)SG	MAC アドレス通知のグローバル カウンタのサポートが追加されました。

使用上のガイドライン

テーブルからすべてのダイナミック エントリを削除するには、引数を指定せずに **clear mac-address-table dynamic** コマンドを入力します。

clear mac-address-table notification コマンドは、**show mac-address-table notification** コマンドによって表示されるグローバル カウンタだけをクリアします。CISCO-MAC-NATIFICATION-MIB のグローバル カウンタおよび履歴テーブルはクリアされません。

例

次の例では、特定のインターフェイス（gi1/1）のすべてのダイナミック レイヤ 2 エントリをクリアする方法を示します。

```
Switch# clear mac-address-table dynamic interface gi1/1
Switch#
```

次の例では、MAC アドレス通知カウンタをクリアする方法を示します。

```
Switch# clear mac-address-table notification
Switch#
```

関連コマンド

コマンド	説明
clear mac-address-table dynamic	レイヤ 2 MAC アドレス テーブルから、ダイナミック アドレス エントリをクリアします。
mac-address-table aging-time	レイヤ 2 テーブル内のエントリにエージング タイムを設定します。
mac-address-table notification	スイッチで MAC アドレス通知をイネーブルにします。
main-cpu	メイン CPU サブモードを開始し、2 つのスーパーバイザ エンジン上のコンフィギュレーションを手動で同期化します。
show mac-address-table address	MAC アドレス テーブル情報を表示します。
snmp-server enable traps	SNMP 通知をイネーブルにします。

clear mac-address-table dynamic

レイヤ 2 MAC アドレス テーブルからダイナミック アドレス エントリをクリアするには、**clear mac-address-table dynamic** コマンドを使用します。

clear mac-address-table dynamic [{**address** *mac_addr*} | {**interface** *interface*}] [**vlan** *vlan_id*]

構文の説明

address *mac_addr*	（任意）MAC アドレスを指定します。
interface *interface*	（任意）インターフェイスを指定して、そのインターフェイスに関連付けられたエントリをクリアします。有効な値は **FastEthernet** および **GigabitEthernet** です。
vlan *vlan_id*	（任意）VLAN を指定します。有効値の範囲は 1 ～ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張 VLAN アドレスのサポートが追加されました。

使用上のガイドライン

テーブルからすべてのダイナミック エントリを削除するには、引数を指定せずに **clear mac-address-table dynamic** コマンドを入力します。

例

次の例では、特定のインターフェイス（gi1/1）のすべてのダイナミック レイヤ 2 エントリをクリアする方法を示します。

```
Switch# clear mac-address-table dynamic interface gi1/1
Switch#
```

関連コマンド

コマンド	説明
mac-address-table aging-time	レイヤ 2 テーブル内のエントリにエージング タイムを設定します。
main-cpu	メイン CPU サブモードを開始し、2 つのスーパーバイザ エンジン上のコンフィギュレーションを手動で同期化します。
show mac-address-table address	MAC アドレス テーブル情報を表示します。

clear netflow-lite exporter statistics

（注）　NetFlow-lite は Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチでのみサポートされます。

コレクタの統計情報をクリアするには、**clear netflow-lite exporter statistics** コマンドを使用します。

clear netflow-lite exporter *exporter-name* **statistics**

構文の説明

exporter-name	エクスポータを指定します。

デフォルト

なし

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
15.0(2)SG	コマンドが Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチに追加されました。

例

次の例では、モニタでパケットのサンプラの統計情報をクリアする方法を示します。

```
Switch# clear netflow-lite exporter e1 statistics
```

関連コマンド

コマンド	説明
clear netflow-lite monitor statistics interface	モニタでパケットのサンプラの統計情報をクリアします。

clear netflow-lite monitor statistics interface

（注）　NetFlow-lite は Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチでのみサポートされます。

モニタでパケットのサンプラの統計情報をクリアするには、**clear netflow-lite monitor statistics interface** コマンドを使用します。

clear netflow-lite monitor statistics interface *vlan-id*

構文の説明

vlan-id	インターフェイスを指定します。

デフォルト

なし

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
15.0(2)SG	コマンドが Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチに追加されました。

例

次の例では、モニタでパケットのサンプラの統計情報をクリアする方法を示します。

```
Switch# clear netflow-lite monitor 1 statistics int gi1/1
Switch# clear netflow-lite monitor 1 statistics vlan 10
```

関連コマンド

コマンド	説明
clear netflow-lite exporter statistics	コレクタの統計情報をクリアします。

clear nmsp statistics

ネットワーク モビリティ サービス プロトコル（NMSP）の統計情報をクリアするには、**clear nmsp statistics** コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。

clear nmsp 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。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、NMSP の統計情報をクリアする方法を示します。

```
Switch# clear nmsp statistics
Switch#
```

情報が削除されたかどうかを確認するには、**show nmsp statistics** コマンドを入力します。

関連コマンド

コマンド	説明
show nmsp	NMSP 情報を表示します。

clear pagp

ポート チャネル情報をクリアするには、**clear pagp** コマンドを使用します。

clear pagp {*group-number* | **counters**}

構文の説明

group-number	チャネル グループ番号。有効値の範囲は 1 ～ 64 です。
counters	トラフィック フィルタをクリアします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、特定グループのポート チャネル情報をクリアする方法を示します。

```
Switch# clear pagp 32
Switch#
```

次の例では、すべてのポート チャネル トラフィック フィルタをクリアする方法を示します。

```
Switch# clear pagp counters
Switch#
```

関連コマンド

コマンド	説明
show pagp	ポート チャネル情報を表示します。

clear port-security

MAC アドレス テーブルから、すべての設定済みセキュア アドレス、あるいはインターフェイス上の特定のダイナミック セキュア アドレスまたはスティッキ セキュア アドレスを削除するには、**clear port-security** コマンドを使用します。

clear port-security dynamic [**address** *mac-addr* [**vlan** *vlan-id*]] | [**interface** *interface-id*] [**vlan access** | **voice**]

構文の説明

dynamic	すべてのダイナミック セキュア MAC アドレスを削除します。
address *mac-addr*	（任意）指定したセキュア MAC アドレスを削除します。
vlan *vlan-id*	（任意）指定した VLAN から指定したセキュア MAC アドレスを削除します。
interface *interface-id*	（任意）指定した物理ポートまたはポート チャネルのセキュア MAC アドレスを削除します。
vlan access	（任意）アクセス VLAN からセキュア MAC アドレスを削除します。
vlan voice	（任意）音声 VLAN からセキュア MAC アドレスを削除します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

使用上のガイドライン

clear port-security all コマンドを入力した場合、MAC アドレス テーブルからすべてのダイナミック セキュア MAC アドレスが削除されます。

（注）　スティッキおよびスタティックのセキュア MAC アドレスは、**no switchport port-security mac-address** コマンドを使用すると、一度に 1 つずつクリアできます。

clear port-security dynamic interface *interface-id* コマンドを入力すると、スイッチはインターフェイス上のすべてのダイナミック セキュア MAC アドレスを MAC アドレス テーブルから削除します。

コマンド履歴

リリース	変更箇所
12.2(18)EW	このコマンドが、Catalyst 4500 シリーズ スイッチに初めて追加されました。
12.2(31)SG	スティッキ ポート セキュリティのサポートを追加します。

例

次の例では、MAC アドレス テーブルからすべてのダイナミック セキュア アドレスを削除する方法を示します。

```
Switch# clear port-security dynamic
```

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

```
Switch# clear port-security dynamic address 0008.0070.0007
```

次の例では、特定のインターフェイスで学習されたすべてのダイナミック セキュア アドレスを削除する方法を示します。

```
Switch# clear port-security dynamic interface gigabitethernet0/1
```

情報が削除されたことを確認するには、**show port-security** コマンドを入力します。

関連コマンド

コマンド	説明
show port-security	ポート セキュリティ設定情報を表示します。
switchport port-security	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します。

clear pppoe intermediate-agent statistics

PPPoE 中継エージェント統計情報（パケット カウンタ）をクリアするには、**clear pppoe intermediate-agent statistics** コマンドを使用します。

clear ppoe intermediate-agent statistics

構文の説明

このコマンドには、引数はありません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、PPPoE 中継エージェントの統計情報をクリアする方法を示します。

```
Switch# clear pppoe intermediate-agent statistics
```

関連コマンド

コマンド	説明
show pppoe intermediate-agent interface	PPPoE 中継エージェント統計情報（パケット カウンタ）を表示します。

clear qos

グローバルおよびインターフェイス単位の集約 QoS カウンタをクリアするには、**clear qos** コマンドを使用します。

clear qos [**aggregate-policer** [*name*] | **interface** {{**fastethernet** | **GigabitEthernet**} {*mod/interface*}} | **vlan** {*vlan_num*} | **port-channel** {*number*}]

構文の説明

aggregate-policer *name*	（任意）集約ポリサーを指定します。
interface	（任意）インターフェイスを指定します。
fastethernet	（任意）ファスト イーサネット 802.3 インターフェイスを指定します。
GigabitEthernet	（任意）ギガビット イーサネット 802.3z インターフェイスを指定します。
mod/interface	（任意）モジュールおよびインターフェイスの番号。
vlan *vlan_num*	（任意）VLAN を指定します。
port-channel *number*	（任意）チャネル インターフェイスを指定します。有効値の範囲は 1 ～ 64 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

（注）　**clear qos** コマンドを入力すると、カウンタの動作に影響が出て、通常は制限されるトラフィックが短期間転送される可能性があります。

clear qos コマンドは、インターフェイスの QoS ポリシー カウンタをリセットします。インターフェイスが指定されていない場合、**clear qos** コマンドはすべてのインターフェイスの QoS ポリシー カウンタをリセットします。

例

次の例では、すべてのプロトコルのグローバルおよびインターフェイス単位の集約 QoS カウンタをクリアする方法を示します。

```
Switch# clear qos
Switch#
```

次の例では、すべてのインターフェイスで特定プロトコルの集約 QoS カウンタをクリアする方法を示します。

```
Switch# clear qos aggregate-policer
Switch#
```

関連コマンド

コマンド	説明
show qos	QoS 情報を表示します。

clear vlan counters

指定した VLAN またはすべての既存 VLAN のソフトウェア キャッシュ カウンタ値をクリアして、0 から再開するには、**clear vlan counters** コマンドを使用します。

clear vlan [*vlan-id*] **counters**

構文の説明

vlan-id	（任意）VLAN 番号。有効な値については、「使用上のガイドライン」を参照してください。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

vlan-id 値を指定しない場合は、すべての既存 VLAN のソフトウェア キャッシュ カウンタ値がクリアされます。

例

次の例では、特定の VLAN のソフトウェア キャッシュ カウンタ値をクリアする方法を示します。

```
Switch# clear vlan 10 counters
Clear "show vlan" counters on this vlan [confirm] y
Switch#
```

関連コマンド

コマンド	説明
show vlan counters	VLAN のカウンタ情報を表示します。

clear vmps statistics

VMPS 統計情報をクリアするには、**clear vmps statistics** コマンドを使用します。

clear vmps 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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、VMPS 統計情報をクリアする方法を示します。

```
Switch# clear vmps statistics
Switch#
```

関連コマンド

コマンド	説明
show vmps	VMPS 情報を表示します。
vmps reconfirm（特権 EXEC）	VLAN Query Protocol（VQP）クライアントの再確認間隔を変更します。

control-plane

コントロール プレーン コンフィギュレーション モードでは、デバイスのコントロール プレーンに関連付けられた属性またはパラメータ（サービス ポリシーなど）の関連付けまたは変更を実行できます。このモードを開始するには、**control-plane** コマンドを使用します。

control-plane

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。

デフォルト

デフォルト サービス ポリシー *system-cpp-policy* が適用されています。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(31)SG	Catalyst 4500 シリーズ スイッチでサポートされるようになりました。
12.2(50)SG	Supervisor 6-E および Catalyst 4900M でサポートされるようになりました。
12.2(52)XO	Supervisor Engine 6L-E でサポートされるようになりました。
12.2(54)XO	Catalyst 4948-E でサポートされるようになりました。

使用上のガイドライン

control-plane コマンドを入力すると、ルート プロセッサに対してコントロール プレーン サービスを定義できます。たとえば、サービス ポリシーをコントロール プレーンに関連付けて、コントロール プレーン宛てのすべてのトラフィックをポリシングできます。

例

次の例では、送信元アドレス 10.1.1.1 および 10.1.1.2 の信頼できるホストを設定して、Telnet パケットをコントロール プレーンに制約なしで転送する方法を示します。残りのすべての Telnet パケットは、指定したレートでポリシングされます。

```
Switch(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic.
Switch(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Switch(config)# class-map telnet-class
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map control-plane
Switch(config-pmap)# class telnet-class
Switch(config-pmap-c)# police 32000 1000 conform transmit exceed drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

```
! Define aggregate control plane service for the active Route Processor.
Switch(config)# macro global apply system-cpp
Switch(config)# control-plane
Switch(config-cp)# service-police input system-cpp-policy
Switch(config-cp)# exit
```

関連コマンド

コマンド	説明
class	トラフィック ポリシーを作成または変更するクラスの名前を指定します。
class-map	名前を指定したクラスとパケットの照合に使用するクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
match access-group（『*Cisco IOS Release 12.2 Command Reference*』を参照）	指定したアクセス コントロール リスト（ACL）に基づいて、クラス マップの一致基準を設定します。
policy-map	複数ポートに適用可能なポリシー マップを作成し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
service-policy（インターフェイス コンフィギュレーション）	ポリシー マップをインターフェイスに関連付けます。
show policy-map control-plane	1 つまたはすべてのクラスについて、コントロール プレーンのポリシー マップのコンフィギュレーションを表示します。

cos（netflow-lite エクスポータ サブモード）

（注）　NetFlow-lite は Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチでのみサポートされます。

NetFlow-lite コレクタの CoS 値を指定するには、**cos** コマンドを使用します。この値を削除するには、このコマンドの **no** 形式を使用します。

cos *cos-value*

no cos *cos-value*

構文の説明

cos-value	NetFlow-lite コレクタの CoS 値を指定します。有効な値は 0 ～ 7 です。

デフォルト

0

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)SG	このコマンドが Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチに追加されました。

使用上のガイドライン

このオプションを使用すると、fpga によってのみエクスポートされるサンプル パケットの VLAN タグの CoS 値を設定できます。

例

次の例では、NetFlow-lite コレクタの CoS 値を指定する方法を示します。

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

```
Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite  Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address:   5.5.5.6
    Source IP Address:        5.5.5.5
    VRF label:
    DSCP:                     0x20
    TTL:                      128
    COS:                      7
  Transport Protocol Configuration:
    Transport Protocol:       UDP
    Destination Port:         8188
    Source Port:              61670
  Export Protocol Configuration:
    Export Protocol:                  netflow-v9
    Template data timeout:            60
    Options sampler-table timeout:    1800
    Options interface-table timeout:  1800
  Exporter Statistics:
    Packets Exported:         0
```

show netflow-lite exporter 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
destination（netflow-lite エクスポータ サブモード）	netflow-lite サブモードでの宛先アドレスを指定します。
source（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの送信元レイヤ 3 インターフェイスを指定します。
transport udp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの UDP トランスポート宛先ポートを指定します。
ttl（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの TTL 値を指定します。
dscp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの CoS 値を指定します。
template data timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのテンプレート データ タイムアウトを指定します。
options timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのオプションのタイムアウトを指定します。
export-protocol（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのエクスポート プロトコルを指定します。

counter

レイヤ 3 インターフェイスにカウンタを割り当てるには、**counter** interface コマンドを使用します。カウンタの割り当てを削除するには、このコマンドの **no** 形式を使用します。

counter {**ipv4** | **ipv6** | **ipv4 ipv6 separate**}

no counter

（注）　Supervisor Engine 6-E および Supervisor Engine 6L-E ではレイヤ 2 インターフェイス カウンタはサポートされません。

構文の説明

ipv4	IPv4 統計情報のみの収集をイネーブルにします。
ipv6	IPv6 統計情報のみの収集をイネーブルにします。
ipv4 ipv6 separate	IPv4 および IPv6 統計情報の収集をイネーブルにし、個別に表示します。

デフォルト

イネーブルになっていません

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(40)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(54)SG	IPv4 および IPv6 カウンタのサポートが追加されました。

使用上のガイドライン

キーワードを指定しないで **counter** コマンドを入力すると、統計情報が合計として表示されます。

送信カウンタおよび受信カウンタを所有できるスイッチ ポートの合計数は 4092 です。

カウンタが割り当てられたレイヤ 3 ポートをレイヤ 2 ポートに変更すると、ハードウェア カウンタがクリアされます。この動作は **no counter** コマンドを入力した場合の動作と同様です。

例

次の例では、インターフェイス VLAN 1 上でカウンタをイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# counter ipv4
Switch(config-if)# end
Switch#
00:17:15: %SYS-5-CONFIG_I: Configured from console by console
Switch# show run interface vlan 1
Building configuration...
```

```
Current configuration : 63 bytes
!
interface Vlan1
 ip address 10.0.0.1 255.0.0.0
 counter ipv4
end
```

（注）　カウンタの割り当てを解除するには、**no counter** コマンドを使用します。

すでにカウンタの最大数を割り当てている場合は、**counter** コマンドは失敗し、次のエラー メッセージが表示されます。

```
Switch# config terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# interface fa3/2
Switch(config-if)# no switchport
Switch(config-if)# counter ipv6
 Counter resource exhausted for interface fa3/2
Switch(config-if)# end
Switch#
00:24:18: %SYS-5-CONFIG_I: Configured from console by console
```

この場合、別のインターフェイスのカウンタを解放して新しいインターフェイスが使用できるようにする必要があります。

dbl

トラフィックのクラスで使用する送信キューで、アクティブ キュー管理をイネーブルにするには、**dbl** 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。

dbl

no dbl

構文の説明

このコマンドには、キーワードと引数はありません。

デフォルト

アクティブ キュー管理はディセーブルです。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(40)SG	Supervisor Engine 6-E でサポートされるようになりました。

使用上のガイドライン

DBL 設定のセマンティックスは、WRED アルゴリズムと類似しています。**dbl** コマンドは class-default では単独で動作しますが、それ以外ではクラスに対して **bandwidth** コマンドまたは **shape** コマンドを設定する必要があります。

例

次の例では、クラスで dbl の動作をイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
```

関連コマンド

コマンド	説明
bandwidth	名前で参照可能なシグナリング クラス構造を作成します。
class	名前を指定したクラスとパケットの照合に使用するクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。

コマンド	説明
policy-map	複数ポートに適用可能なポリシー マップを作成し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
service-policy（ポリシー マップ クラス）	ポリシー マップ内に QoS（Quality of Service）ポリシーとしてサービス ポリシーを作成します。
show policy-map	ポリシー マップ情報を表示します。

debug adjacency

隣接デバッグ情報を表示するには、**debug adjacency** コマンドを使用します。デバッグ出力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 adjacency [**ipc**]

no debug adjacency

構文の説明

ipc	（任意）隣接データベースの IPC エントリを表示します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、隣接データベース内の情報を表示する方法を示します。

```
Switch# debug adjacency
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
4d02h: ADJ: add 172.20.52.36 (GigabitEthernet1/1) via ARP will expire: 04:00:00
<... output truncated...>
Switch#
```

関連コマンド

コマンド	説明
undebug adjacency（no debug adjacency と同じ）	デバッグ出力をディセーブルにします。

debug backup

バックアップ イベントをデバッグするには、**debug backup** コマンドを使用します。デバッグ出力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 backup

no debug backup

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、バックアップ イベントをデバッグする方法を示します。

```
Switch# debug backup
Backup events debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug backup（no debug backup と同じ）	デバッグ出力をディセーブルにします。

debug condition interface

インターフェイス関連のアクティビティのデバッグ出力を制限するには、**debug condition interface** コマンドを使用します。デバッグ出力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 condition interface {**fastethernet** *mod/port* | **GigabitEthernet** *mod/port* | **null** *interface_num* | **port-channel** *interface-num* | **vlan** *vlan_id*}

no debug condition interface {**fastethernet** *mod/port* | **GigabitEthernet** *mod/port* | **null** *interface_num* | **port-channel** *interface-num* | **vlan** *vlan_id*}

構文の説明

fastethernet	ファスト イーサネット インターフェイスにデバッグを制限します。
mod/port	モジュール番号とポート番号。
GigabitEthernet	ギガビット イーサネット インターフェイスにデバッグを制限します。
null *interface-num*	ヌル インターフェイスにデバッグを制限します。有効な値は 0 です。
port-channel *interface-num*	ポート チャネル インターフェイスにデバッグを制限します。有効な値は 1 ～ 64 です。
vlan *vlan_id*	VLAN インターフェイス番号を指定します。有効な値は 1 ～ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張 VLAN アドレスのサポートが追加されました。

例

次の例では、VLAN インターフェイス 1 にデバッグ出力を制限する方法を示します。

```
Switch# debug condition interface vlan 1
Condition 2 set
Switch#
```

関連コマンド

コマンド	説明
debug interface	**debug condition interface** コマンドのエントリを省略します。
undebug condition interface（no debug condition interface と同じ）	インターフェイス関連アクティビティをディセーブルにします。

debug condition standby

スタンバイ ステート変化のデバッグ出力を制限するには、**debug condition standby** コマンドを使用します。デバッグ出力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 condition standby {**fastethernet** *mod/port* | **GigabitEthernet** *mod/port* | **port-channel** *interface-num* | **vlan** *vlan_id group-number*}

no debug condition standby {**fastethernet** *mod/port* | **GigabitEthernet** *mod/port* | **port-channel** *interface-num* | **vlan** *vlan_id group-number*}

構文の説明

fastethernet	ファスト イーサネット インターフェイスにデバッグを制限します。
mod/port	モジュール番号とポート番号。
GigabitEthernet	ギガビット イーサネット インターフェイスにデバッグを制限します。
port-channel *interface_num*	ポート チャネル インターフェイスにデバッグ出力を制限します。有効な値は 1 ～ 64 です。
vlan *vlan_id*	VLAN インターフェイスで条件付きデバッグを制限します。有効値の範囲は 1 ～ 4094 です。
group-number	VLAN グループ番号です。有効値の範囲は 0 ～ 255 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張 VLAN アドレスのサポートが追加されました。

使用上のガイドライン

唯一の条件セットを削除しようとすると、削除を中断するかどうかを確認するメッセージが表示されます。削除を中断するには **n** を入力し、削除を続行するには **y** を入力します。唯一の条件セットを削除すると、過剰な数のデバッグ メッセージが表示されることがあります。

例

次の例では、VLAN 1 のグループ 0 にデバッグ出力を制限する方法を示します。

```
Switch# debug condition standby vlan 1 0
Condition 3 set
Switch#
```

次に、最後のスタンバイ デバッグ条件をオフにしようとした場合の表示例を示します。

```
Switch# no debug condition standby vlan 1 0
This condition is the last standby condition set.
Removing all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/no]: n
% Operation aborted
Switch#
```

関連コマンド

コマンド	説明
undebug condition standby（no debug condition standby と同じ）	デバッグ出力をディセーブルにします。

debug condition vlan

指定された VLAN の VLAN デバッグ出力を制限するには、**debug condition vlan** コマンドを使用します。デバッグ出力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 condition vlan {*vlan_id*}

no debug condition vlan {*vlan_id*}

構文の説明

vlan_id	VLAN の番号です。有効値の範囲は 1 ～ 4096 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張 VLAN アドレスのサポートが追加されました。

使用上のガイドライン

唯一の VLAN の条件セットを削除しようとすると、削除を中断するかどうかを確認するメッセージが表示されます。削除を中断するには **n** を入力し、削除を続行するには **y** を入力します。唯一の条件セットを削除すると、過剰な数のメッセージが表示される場合があります。

例

次の例では、VLAN 1 にデバッグ出力を制限する方法を示します。

```
Switch# debug condition vlan 1
Condition 4 set
Switch#
```

次の例では、最後の VLAN デバッグ条件をディセーブルにしようとしたときに表示されるメッセージを示します。

```
Switch# no debug condition vlan 1
This condition is the last vlan condition set.
Removing all conditions may cause a flood of debugging
messages to result, unless specific debugging flags
are first removed.

Proceed with removal? [yes/no]: n
% Operation aborted
Switch#
```

関連コマンド

コマンド	説明
undebug condition vlan（no debug condition vlan と同じ）	デバッグ出力をディセーブルにします。

debug device-sensor

デバイス センサーのデバッグをイネーブルにするには、特権 EXEC モードで **debug device-sensor** コマンドを使用します。

debug device-sensor errors events

構文の説明

errors	デバイス センサーのエラー メッセージを表示します。
events	セッション マネージャに送信されるイベント（プロトコル パケットの到着、アイデンティティのアップデート、リリース イベントなど）に関するメッセージを表示します。

デフォルト

このコマンドにはデフォルトはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
IOS XE 3.4.0SG and IOS 15.1(2)SG)	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

debug device-sensor コマンドを **debug authentication all** コマンドとともに使用して、接続されているデバイスのデバイス センサー キャッシュ エントリが作成されないケースをトラブルシューティングします。

例

次に、**debug device-sensor events** コマンドの出力例を示します。デバッグ出力には、Cisco Discovery Protocol パケットおよび TLV が、インターフェイス GigabitEthernet 2/1 に接続されているデバイスから受信された方法が示されます。

```
Switch# debug device-sensor events

Switch#
*Nov 30 23:58:45.811: DSensor: Received cdp packet from GigabitEthernet2/1:00d0.2bdf.08a5
*Nov 30 23:58:45.811: DSensor: SM returned no or invalid session label for
GigabitEthernet2/1:00d0.2bdf.08a5
*Nov 30 23:58:45.811: DSensor: Updating SM with identity attribute list
  cdp-tlv              0   00 01 00 0B 4A 41 45 30 37 34 31 31 50 53 32
  cdp-tlv              0   00 03 00 03 32 2F 38
  cdp-tlv              0   00 04 00 04 00 00 00 0A
  cdp-tlv              0   00 05 00 68 57 53 2D 43 32 39 34 38 20 53 6F 66 74 77 61 72 65
2C 20 56 65 72 73 69 6F 6E 20 4D 63 70 53 57 3A 20 36 2E 34 28 35 2E
 30 29 20 4E 6D 70 53 57 3A 20 36 2E 34 28 35 29 0A 43 6F 70 79 72 69 67 68 74 20 28 63 29
20 31 39 39 35 2D 32 30 30 33 20 62 79 20 43 69 73 63 6F 20 53 79 73
74 65 6D 73 2C 20 49 6E 63 2E 0A
 cdp-tlv              0   00 06 00 08 57 53 2D 43 32 39 34 38
 cdp-tlv              0   00 09 00 00
 cdp-tlv              0   00 0A 00 02 00 21
 cdp-tlv              0   00 0B 00 01 01
 cdp-tlv              0   00 12 00 01 00
 cdp-tlv              0   00 13 00 01 00
```

```
 cdp-tlv              0   00 14 00 00
 cdp-tlv              0   00 15 00 0A 06 08 2B 06 01 04 01 09 05 2A
 cdp-tlv              0   00 16 00 16 00 00 00 02 01 01 CC 00 04 00 00 00 0001 01 CC 00 04
01 01 01 01
 cdp-tlv              0   00 17 00 01 00
 swidb                0   604702240 (0x240B0620)
 clid-mac-addr        0   00 D0 2B DF 08 A5
*Nov 30 23:58:46.831: DSensor: Received cdp packet from
GigabitEthernet2/1:00d0.2bdf.08a5exi
Switch#
*Nov 30 23:58:51.171: %SYS-5-CONFIG_I: Configured from console by console
```

関連コマンド

コマンド	説明
debug authentication all	認証マネージャおよびすべての機能に関するすべてのデバッグ情報を表示します。
device-sensor accounting	新しいセンサー データの検出時に、デバイス センサー プロトコル データをアカウンティング レコードに追加し、追加のアカウンティング イベントを生成します。

debug dot1x

802.1X 機能のデバッグをイネーブルにするには、**debug dot1x** コマンドを使用します。デバッグ出力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 dot1x {**all** | **errors** | **events** | **packets** | **registry** | **state-machine**}

no debug dot1x {**all** | **errors** | **events** | **packets** | **registry** | **state-machine**}

構文の説明

all	すべての条件のデバッグをイネーブルにします。
errors	dot1x エラー フラグによってガードされた印刷ステートメントのデバッグをイネーブルにします。
events	dot1x イベント フラグによってガードされた印刷ステートメントのデバッグをイネーブルにします。
packets	着信したすべての dot1x パケットのパケット情報およびインターフェイス情報が印刷されます。
registry	dot1x レジストリ フラグによってガードされた印刷ステートメントのデバッグをイネーブルにします。
state-machine	dot1x レジストリ フラグによってガードされた印刷ステートメントのデバッグをイネーブルにします。

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 モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、すべての条件の 802.1X デバッグをイネーブルにする方法を示します。

```
Switch# debug dot1x all
Switch#
```

関連コマンド

コマンド	説明
show dot1x	dot1x 情報を表示します。
undebug dot1x（no debug dot1x と同じ）	デバッグ出力をディセーブルにします。

debug etherchnl

EtherChannel をデバッグするには、**debug etherchnl** コマンドを使用します。デバッグ出力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 etherchnl [**all** | **detail** | **error** | **event** | **idb** | **linecard**]

no debug etherchnl

構文の説明

all	（任意）EtherChannel デバッグ メッセージをすべて表示します。
detail	（任意）詳細な EtherChannel デバッグ メッセージを表示します。
error	（任意）EtherChannel エラー メッセージを表示します。
event	（任意）主な EtherChannel イベント メッセージをデバッグします。
idb	（任意）PAgP IDB メッセージをデバッグします。
linecard	（任意）モジュールに SCP メッセージをデバッグします。

デフォルト

デフォルト設定は、次のとおりです。

- デバッグはディセーブルです。
- すべてのメッセージが表示されます。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

キーワードを指定しない場合は、すべてのデバッグ メッセージが表示されます。

例

次の例では、すべての EtherChannel デバッグ メッセージを表示する方法を示します。

```
Switch# debug etherchnl
PAgP Shim/FEC debugging is on
22:46:30:FEC:returning agport Po15 for port (Fa2/1)
22:46:31:FEC:returning agport Po15 for port (Fa4/14)
22:46:33:FEC:comparing GC values of Fa2/25 Fa2/15 flag = 1 1
22:46:33:FEC:port_attrib:Fa2/25 Fa2/15 same
22:46:33:FEC:EC - attrib incompatable for Fa2/25; duplex of Fa2/25 is half, Fa2/15 is full
22:46:33:FEC:pagp_switch_choose_unique:Fa2/25, port Fa2/15 in agport Po3 is incompatable
Switch#
```

次の例では、EtherChannel IDB デバッグ メッセージを表示する方法を示します。

```
Switch# debug etherchnl idb
Agport idb related debugging is on
Switch#
```

次の例では、デバッグをディセーブルにする方法を示します。

```
Switch# no debug etherchnl
Switch#
```

関連コマンド

コマンド	説明
undebug etherchnl（no debug etherchnl と同じ）	デバッグ出力をディセーブルにします。

debug interface

debug condition interface コマンドのエントリを省略するには、**debug interface** コマンドを使用します。デバッグ出力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 interface {**FastEthernet** *mod/port* | **GigabitEthernet** *mod/port* | **null** | **port-channel** *interface-num* | **vlan** *vlan_id*}

no debug interface {**FastEthernet** *mod/port* | **GigabitEthernet** *mod/port* | **null** | **port-channel** *interface-num* | **vlan** *vlan_id*}

構文の説明

FastEthernet	ファスト イーサネット インターフェイスにデバッグを制限します。
mod/port	モジュール番号とポート番号。
GigabitEthernet	ギガビット イーサネット インターフェイスにデバッグを制限します。
null	ヌル インターフェイスにデバッグを制限します。有効な値は 0 だけです。
port-channel *interface-num*	ポート チャネル インターフェイスにデバッグを制限します。有効な値は 1 ～ 64 です。
vlan *vlan_id*	VLAN インターフェイス番号を指定します。有効な値は 1 ～ 4094 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張 VLAN アドレスのサポートが追加されました。

例

次の例では、インターフェイス VLAN 1 にデバッグを制限する方法を示します。

```
Switch# debug interface vlan 1
Condition 1 set
Switch#
```

関連コマンド

コマンド	説明
debug condition interface	インターフェイス関連のアクティビティのデバッグ出力を制限します。
undebug etherchnl（no debug etherchnl と同じ）	デバッグ出力をディセーブルにします。

debug ipc

IPC アクティビティをデバッグするには、**debug ipc** コマンドを使用します。デバッグ出力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 ipc {**all** | **errors** | **events** | **headers** | **packets** | **ports** | **seats**}

no debug ipc {**all** | **errors** | **events** | **headers** | **packets** | **ports** | **seats**}

構文の説明

all	すべての IPC デバッグをイネーブルにします。
errors	IPC エラー デバッグをイネーブルにします。
events	IPC イベント デバッグをイネーブルにします。
headers	IPC ヘッダー デバッグをイネーブルにします。
packets	IPC パケット デバッグをイネーブルにします。
ports	ポートの作成および削除のデバッグをイネーブルにします。
seats	ノードの作成および削除のデバッグをイネーブルにします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、IPC イベントのデバッグをイネーブルにする方法を示します。

```
Switch# debug ipc events
Special Events debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug ipc（no debug ipc と同じ）	デバッグ出力をディセーブルにします。

debug ip dhcp snooping event

DHCP スヌーピング イベントをデバッグするには、**debug ip dhcp snooping event** コマンドを使用します。デバッグ出力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 ip dhcp snooping event

no debug ip dhcp snooping event

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。

デフォルト

スヌーピング イベントのデバッグはディセーブルです。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、DHCP スヌーピング イベントのデバッグをイネーブルにする方法を示します。

```
Switch# debug ip dhcp snooping event
Switch#
```

次の例では、DHCP スヌーピング イベントのデバッグをディセーブルにする方法を示します。

```
Switch# no debug ip dhcp snooping event
Switch#
```

関連コマンド

コマンド	説明
debug ip dhcp snooping packet	DHCP スヌーピング メッセージをデバッグします。

debug ip dhcp snooping packet

DHCP スヌーピング メッセージをデバッグするには、**debug ip dhcp snooping packet** コマンドを使用します。デバッグ出力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 ip dhcp snooping packet

no debug ip dhcp snooping packet

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。

デフォルト

スヌーピング パケットのデバッグはディセーブルです。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、DHCP スヌーピング パケットのデバッグをイネーブルにする方法を示します。

```
Switch# debug ip dhcp snooping packet
Switch#
```

次の例では、DHCP スヌーピング パケットのデバッグをディセーブルにする方法を示します。

```
Switch# no debug ip dhcp snooping packet
Switch#
```

関連コマンド

コマンド	説明
debug ip dhcp snooping event	DHCP スヌーピング イベントをデバッグします。

debug ip verify source packet

IP ソース ガード メッセージをデバッグするには、**debug ip verify source packet** コマンドを使用します。デバッグ出力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 ip verify source packet

no debug ip verify source packet

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。

デフォルト

スヌーピング セキュリティ パケットのデバッグはディセーブルです。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、IP ソース ガードのデバッグをイネーブルにする方法を示します。

```
Switch# debug ip verify source packet
Switch#
```

次の例では、IP ソース ガードのデバッグをディセーブルにする方法を示します。

```
Switch# no debug ip verify source packet
Switch#
```

関連コマンド

コマンド	説明
ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping limit rate	DHCP オプション 82 データ挿入をイネーブルにします。
ip dhcp snooping trust	信頼できる VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング エントリを表示します。

debug lacp

LACP アクティビティをデバッグするには、**debug lacp** コマンドを使用します。デバッグ出力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 lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp

構文の説明

all	（任意）すべての LACP デバッグをイネーブルにします。
event	（任意）LACP イベントのデバッグをイネーブルにします。
fsm	（任意）LACP 有限状態マシンのデバッグをイネーブルにします。
misc	（任意）各種 LACP デバッグをイネーブルにします。
packet	（任意）LACP パケットのデバッグをイネーブルにします。

デフォルト

LACP アクティビティのデバッグはディセーブルです。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドをサポートするのはスーパーバイザ エンジンだけです。また、このコマンドを入力できるのは、Catalyst 4500 シリーズ スイッチ コンソールからにかぎられます。

例

次の例では、LACP の各種デバッグをイネーブルにする方法を示します。

```
Switch# debug lacp
Port Aggregation Protocol Miscellaneous debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug pagp（no debug pagp と同じ）	デバッグ出力をディセーブルにします。

debug monitor

モニタリング アクティビティを表示するには、**debug monitor** コマンドを使用します。デバッグ出力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 monitor {**all** | **errors** | **idb-update** | **list** | **notifications** | **platform** | **requests**}

no debug monitor {**all** | **errors** | **idb-update** | **list** | **notifications** | **platform** | **requests**}

構文の説明

all	すべての SPAN デバッグ メッセージを表示します。
errors	SPAN エラーの詳細を表示します。
idb-update	SPAN IDB の更新追跡を表示します。
list	SPAN リスト追跡および VLAN リスト追跡を表示します。
notifications	SPAN 通知を表示します。
platform	SPAN プラットフォーム追跡を表示します。
requests	SPAN 要求を表示します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、モニタリング エラーをデバッグする方法を示します。

```
Switch# debug monitor errors
SPAN error detail debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug monitor（no debug monitor と同じ）	デバッグ出力をディセーブルにします。

debug nmsp

スイッチのネットワーク モビリティ サービス プロトコル（NMSP）のデバッグをイネーブルにするには、**debug nmsp** コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug nmsp {**all** | **connection** | **error** | **event** | **packet** | **rx** | **tx**}

no debug nmsp

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。

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 モード

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

undebug nmsp コマンドは、**no debug nmsp** コマンドと同じです。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。
show nmsp	NMSP 情報を表示します。

debug nvram

NVRAM アクティビティをデバッグするには、**debug nvram** コマンドを使用します。デバッグ出力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 nvram

no debug nvram

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、NVRAM をデバッグする方法を示します。

```
Switch# debug nvram
NVRAM behavior debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug nvram（no debug nvram と同じ）	デバッグ出力をディセーブルにします。

debug pagp

PAgP アクティビティをデバッグするには、**debug pagp** コマンドを使用します。デバッグ出力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 pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp

構文の説明

all	（任意）すべての PAgP デバッグをイネーブルにします。
dual-active	（任意）PAgP デュアルアクティブのデバッグをイネーブルにします。
event	（任意）PAgP イベントのデバッグをイネーブルにします。
fsm	（任意）PAgP 有限状態マシンのデバッグをイネーブルにします。
misc	（任意）各種 PAgP デバッグをイネーブルにします。
packet	（任意）PAgP パケットのデバッグをイネーブルにします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドをサポートするのはスーパーバイザ エンジンだけです。また、このコマンドを入力できるのは、Catalyst 4500 シリーズ スイッチ コンソールからに限られます。

例

次の例では、PAgP の各種デバッグをイネーブルにする方法を示します。

```
Switch# debug pagp misc
Port Aggregation Protocol Miscellaneous debugging is on
Switch#
*Sep 30 10:13:03: SP: PAgP: pagp_h(Fa5/6) expired
*Sep 30 10:13:03: SP: PAgP: 135 bytes out Fa5/6
*Sep 30 10:13:03: SP: PAgP: Fa5/6 Transmitting information packet
*Sep 30 10:13:03: SP: PAgP: timer pagp_h(Fa5/6) started with interval 30000
<... output truncated...>
Switch#
```

関連コマンド

コマンド	説明
undebug pagp（no debug pagp と同じ）	デバッグ出力をディセーブルにします。

debug platform packet protocol lacp

LACP プロトコルのパケットをデバッグするには、**debug platform packet protocol lacp** コマンドを使用します。デバッグ出力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 platform packet protocol lacp [**receive** | **transmit** | **vlan**]

no debug platform packet protocol lacp [**receive** | **transmit** | **vlan**]

構文の説明

receive	（任意）プラットフォームのパケット受信デバッグ機能をイネーブルにします。
transmit	（任意）プラットフォームのパケット送信デバッグ機能をイネーブルにします。
vlan	（任意）プラットフォームのパケット VLAN デバッグ機能をイネーブルにします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、すべての PM デバッグをイネーブルにする方法を示します。

```
Switch# debug platform packet protocol lacp
Switch#
```

関連コマンド

コマンド	説明
undebug platform packet protocol lacp（no debug platform packet protocol lacp と同じ）	デバッグ出力をディセーブルにします。

debug platform packet protocol pagp

PAgP プロトコルのパケットをデバッグするには、**debug platform packet protocol pagp** コマンドを使用します。デバッグ出力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 platform packet protocol pagp [**receive** | **transmit** | **vlan**]

no debug platform packet protocol pagp [**receive** | **transmit** | **vlan**]

構文の説明

receive	（任意）プラットフォームのパケット受信デバッグ機能をイネーブルにします。
transmit	（任意）プラットフォームのパケット送信デバッグ機能をイネーブルにします。
vlan	（任意）プラットフォームのパケット VLAN デバッグ機能をイネーブルにします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、すべての PM デバッグをイネーブルにする方法を示します。

```
Switch# debug platform packet protocol pagp
Switch#
```

関連コマンド

コマンド	説明
undebug platform packet protocol pagp（no debug platform packet protocol pagp と同じ）	デバッグ出力をディセーブルにします。

debug pm

ポート マネージャ（PM）アクティビティをデバッグするには、**debug pm** コマンドを使用します。デバッグ出力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 pm {**all** | **card** | **cookies** | **etherchnl** | **messages** | **port** | **registry** | **scp** | **sm** | **span** | **split** |
vlan | **vp**}

no debug pm {**all** | **card** | **cookies** | **etherchnl** | **messages** | **port** | **registry** | **scp** | **sm** | **span** | **split** |
vlan | **vp**}

構文の説明

all	すべての PM デバッグ メッセージを表示します。
card	モジュール関連イベントをデバッグします。
cookies	内部 PM クッキー検証をイネーブルにします。
etherchnl	EtherChannel 関連イベントをデバッグします。
messages	PM メッセージをデバッグします。
port	ポート関連イベントをデバッグします。
registry	PM レジストリ呼び出しをデバッグします。
scp	SCP モジュール メッセージングをデバッグします。
sm	ステート マシン関連イベントをデバッグします。
span	スパニングツリー関連イベントをデバッグします。
split	スプリットプロセッサをデバッグします。
vlan	VLAN 関連イベントをデバッグします。
vp	仮想ポート関連イベントをデバッグします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、すべての PM デバッグをイネーブルにする方法を示します。

```
Switch# debug pm all
Switch#
```

関連コマンド

コマンド	説明
undebug pm（no debug pm と同じ）	デバッグ出力をディセーブルにします。

debug port-security

ポート セキュリティをデバッグするには、**debug port-security** コマンドを使用します。デバッグ出力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 port-security

no debug port-security

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。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、すべての PM デバッグをイネーブルにする方法を示します。

```
Switch# debug port-security
Switch#
```

関連コマンド

コマンド	説明
switchport port-security	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します。

debug pppoe intermediate-agent

PPPoE 中継エージェント機能のデバッグをオンにするには、**debug pppoe intermediate-agent** コマンドを使用します。デバッグをオフにするには、このコマンドの **no** 形式を使用します。

debug pppoe intermediate-agent {**event** | **packet** | **all**}

no debug pppoe intermediate-agent {**event** | **packet** | **all**}

構文の説明

event	イベント デバッグをアクティブにします。
packet	パケット デバッグをアクティブにします。
all	イベントおよびパケットのデバッグの両方をアクティブにします。

デフォルト

すべてのデバッグをオフにします。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(50)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、パケット デバッグをオンにする方法を示します。

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet debugging is on

*Sep  2 06:12:56.133: PPPOE_IA: Process new PPPoE packet, Message type: PADI, input
interface: Gi3/7, vlan : 2 MAC da: ffff.ffff.ffff, MAC sa: aabb.cc00.0000
*Sep  2 06:12:56.137: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/4)
*Sep  2 06:12:56.137: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/8)
*Sep  2 06:12:56.137: PPPOE_IA: Process new PPPoE packet, Message type: PADO, input
interface: Gi3/4, vlan : 2 MAC da: aabb.cc00.0000, MAC sa: 001d.e64c.6512
*Sep  2 06:12:56.137: PPPOE_IA: Process new PPPoE packet, Message type: PADO, input
interface: Gi3/8, vlan : 2 MAC da: aabb.cc00.0000, MAC sa: aabb.cc80.0000
*Sep  2 06:12:56.137: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/7)
*Sep  2 06:12:56.137: PPPOE_IA: Process new PPPoE packet, Message type: PADR, input
interface: Gi3/7, vlan : 2 MAC da: 001d.e64c.6512, MAC sa: aabb.cc00.0000
*Sep  2 06:12:56.145: PPPOE_IA: received new PPPOE packet from inputinterface
(GigabitEthernet3/4)
*Sep  2 06:12:56.145: PPPOE_IA: Process new PPPoE packet, Message type: PADS, input
interface: Gi3/4, vlan : 2 MAC da: aabb.cc00.0000, MAC sa: 001d.e64c.6512
```

次の例では、パケット デバッグをオフにする方法を示します。

```
Switch# debug pppoe intermediate-agent packet
PPPOE IA Packet debugging is off
```

関連コマンド

コマンド	説明
pppoe intermediate-agent（インターフェイス）	インターフェイスで PPPoE 中継エージェント機能をイネーブルにします。
pppoe intermediate-agent limit rate	インターフェイスに着信する PPPoE ディスカバリ パケットのレートを制限します。
pppoe intermediate-agent trust	インターフェイスの信頼設定を設定します。

debug redundancy

スーパーバイザ エンジンの冗長性をデバッグするには、**debug redundancy** コマンドを使用します。デバッグ出力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 redundancy {**errors | fsm | kpa | msg | progression | status | timer**}

no debug redundancy

構文の説明

errors	エラー デバッグの冗長ファシリティをイネーブルにします。
fsm	FSM イベント デバッグの冗長ファシリティをイネーブルにします。
kpa	キープアライブ デバッグの冗長ファシリティをイネーブルにします。
msg	メッセージング イベント デバッグの冗長ファシリティをイネーブルにします。
progression	プログレッション イベント デバッグの冗長ファシリティをイネーブルにします。
status	ステータス イベント デバッグの冗長ファシリティをイネーブルにします。
timer	タイマー イベント デバッグの冗長ファシリティをイネーブルにします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました（Catalyst 4507R のみ）。

例

次の例では、冗長ファシリティ タイマー イベントをデバッグする方法を示します。

```
Switch# debug redundancy timer
Redundancy timer debugging is on
Switch#
```

debug spanning-tree

スパニング ツリー アクティビティをデバッグするには、**debug spanning-tree** コマンドを使用します。デバッグ出力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 spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **etherchannel** | **config** | **events** | **exceptions** | **general** | **ha** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **uplinkfast**}

no debug spanning-tree {**all** | **bpdu** | **bpdu-opt** | **etherchannel** | **config** | **events** | **exceptions** | **general** | **mst** | **pvst+** | **root** | **snmp**}

構文の説明

all	すべてのスパニング ツリー デバッグ メッセージを表示します。
backbonefast	BackboneFast イベントをデバッグします。
bpdu	スパニング ツリー BPDU をデバッグします。
bpdu-opt	最適化された BPDU 処理をデバッグします。
etherchannel	スパニング ツリー EtherChannel サポートをデバッグします。
config	スパニング ツリー設定変更をデバッグします。
events	TCAM イベントをデバッグします。
exceptions	スパニング ツリーの例外をデバッグします。
general	一般スパニング ツリー アクティビティをデバッグします。
ha	HA イベントをデバッグします。
mstp	複数のスパニング ツリー イベントをデバッグします。
pvst+	PVST+ イベントをデバッグします。
root	スパニング ツリー ルート イベントをデバッグします。
snmp	スパニング ツリー SNMP イベントをデバッグします。
switch	スイッチのデバッグ イベントをデバッグします。
synchronization	STP ステート同期イベントをデバッグします。
uplinkfast	UplinkFast イベントをデバッグします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、スパニングツリー PVST+ をデバッグする方法を示します。

```
Switch# debug spanning-tree pvst+
Spanning Tree PVST+ debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug spanning-tree（no debug spanning-tree と同じ）	デバッグ出力をディセーブルにします。

debug spanning-tree backbonefast

スパニング ツリー BackboneFast イベントのデバッグをイネーブルにするには、**debug spanning-tree backbonefast** コマンドを使用します。デバッグ出力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 spanning-tree backbonefast [**detail** | **exceptions**]

no debug spanning-tree backbonefast

構文の説明

detail	（任意）詳細な BackboneFast デバッグ メッセージを表示します。
exceptions	（任意）スパニング ツリー BackboneFast 例外のデバッグをイネーブルにします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、スーパーバイザ エンジンだけでサポートされ、スイッチ コンソールからだけ入力できます。

例

次の例では、デバッグをイネーブルにして、詳細なスパニング ツリー BackboneFast デバッグ情報を表示する方法を示します。

```
Switch# debug spanning-tree backbonefast detail
Spanning Tree backbonefast detail debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug spanning-tree backbonefast（no debug spanning-tree backbonefast と同じ）	デバッグ出力をディセーブルにします。

debug spanning-tree switch

スイッチ シムのデバッグをイネーブルにするには、**debug spanning-tree switch** コマンドを使用します。デバッグ出力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 spanning-tree switch {**all** | **errors** | **general** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

no debug spanning-tree switch {**all** | **errors** | **general** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

構文の説明

all	すべてのスパニングツリー スイッチ シム デバッグ メッセージを表示します。
errors	スイッチ シム エラーまたは例外のデバッグをイネーブルにします。
general	一般イベントのデバッグをイネーブルにします。
pm	ポート マネージャ イベントのデバッグをイネーブルにします。
rx	受信した BPDU-handling デバッグ メッセージを表示します。
decode	スパニングツリー スイッチ シムのデコード済み受信パケットのデバッグをイネーブルにします。
errors	スパニングツリー スイッチ シムの受信エラーのデバッグをイネーブルにします。
interrupt	スパニングツリー スイッチのシム ISR 受信 BPDU のデバッグをイネーブルにします。
process	スパニングツリー スイッチのプロセス受信 BPDU のデバッグをイネーブルにします。
state	スパニングツリー ポートのステート変更のデバッグをイネーブルにします。
tx	スパニングツリー スイッチ シムの送信 BPDU のデバッグをイネーブルにします。
decode	（任意）スパニングツリー スイッチ シムのデコード送信済みパケットのデバッグをイネーブルにします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、スーパーバイザ エンジンだけでサポートされ、スイッチ コンソールからだけ入力できます。

例

次の例では、スパニング ツリー スイッチ シムの送信 BPDU のデバッグをイネーブルにする方法を示します。

```
Switch# debug spanning-tree switch tx
Spanning Tree Switch Shim transmit bpdu debugging is on
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 303
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 304
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 305
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 349
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 350
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 351
*Sep 30 08:47:33: SP: STP SW: TX: bpdu of type ieee-st size 92 on FastEthernet5/9 801
<... output truncated...>
Switch#
```

関連コマンド

コマンド	説明
undebug spanning-tree switch（no debug spanning-tree switch と同じ）	デバッグ出力をディセーブルにします。

debug spanning-tree uplinkfast

スパニングツリー UplinkFast イベントのデバッグをイネーブルにするには、**debug spanning-tree uplinkfast** コマンドを使用します。デバッグ出力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 spanning-tree uplinkfast [**exceptions**]

no debug spanning-tree uplinkfast

構文の説明

exceptions	（任意）スパニング ツリー UplinkFast 例外のデバッグをイネーブルにします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、スーパーバイザ エンジンだけでサポートされ、スイッチ コンソールからだけ入力できます。

例

次の例では、スパニング ツリー UplinkFast 例外をデバッグする方法を示します。

```
Switch# debug spanning-tree uplinkfast exceptions
Spanning Tree uplinkfast exceptions debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug spanning-tree uplinkfast（no debug spanning-tree uplinkfast と同じ）	デバッグ出力をディセーブルにします。

debug sw-vlan

VLAN マネージャ アクティビティをデバッグするには、**debug sw-vlan** コマンドを使用します。デバッグ出力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 sw-vlan {**badpmcookies** | **events** | **management** | **packets** | **registries**}

no debug sw-vlan {**badpmcookies** | **events** | **management** | **packets** | **registries**}

構文の説明

badpmcookies	不良ポート マネージャ クッキーの VLAN マネージャ インシデントを表示します。
events	VLAN マネージャ イベントをデバッグします。
management	内部 VLAN の VLAN マネージャ管理をデバッグします。
packets	パケット処理およびカプセル化プロセスをデバッグします。
registries	VLAN マネージャ レジストリをデバッグします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、ソフトウェア VLAN イベントをデバッグする方法を示します。

```
Switch# debug sw-vlan events
vlan manager events debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug sw-vlan（no debug sw-vlan と同じ）	デバッグ出力をディセーブルにします。

debug sw-vlan ifs

VLAN マネージャ Cisco IOS File System（IFS）エラー テストをイネーブルにするには、**debug sw-vlan ifs** コマンドを使用します。デバッグ出力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 sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

no debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

構文の説明

open	IFS ファイル オープン操作のエラーの VLAN マネージャ IFS デバッグをイネーブルにします。
read	IFS VLAN コンフィギュレーション ファイルを開いて読み取るときに発生するエラーをデバッグします。
write	IFS VLAN コンフィギュレーション ファイルを開いて書き込むときに発生するエラーをデバッグします。
{**1** | **2** | **3** | **4**}	ファイル読み取り動作を判別します。動作レベルについては、「使用上のガイドライン」を参照してください。
write	IFS ファイル書き込み動作中に発生するエラーをデバッグします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

次に、4 種類のファイル読み取り動作を示します。

- 動作 **1**：ヘッダー検証ワードおよびファイル バージョン番号が格納されたファイル ヘッダーを読み取ります。
- 動作 **2**：ドメインおよび VLAN 情報の大部分が格納されたファイル本体を読み取ります。
- 動作 **3**：TLV 記述子構造を読み取ります。
- 動作 **4**：TLV データを読み取ります。

例

次の例では、ファイル読み取り動作時に TLV データ エラーをデバッグする方法を示します。

```
Switch# debug sw-vlan ifs read 4
vlan manager ifs read # 4 errors debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug sw-vlan ifs（no debug sw-vlan ifs と同じ）	デバッグ出力をディセーブルにします。

debug sw-vlan notification

ISL VLAN ID のアクティブ化および非アクティブ化を追跡するメッセージのデバッグをイネーブルにするには、**debug sw-vlan notification** コマンドを使用します。デバッグ出力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 sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

no debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

構文の説明

accfwdchange	集約アクセス インターフェイス STP 転送変更に関する VLAN マネージャ通知をイネーブルにします。
allowedvlancfgchange	許可 VLAN 設定変更に関する VLAN マネージャ通知をイネーブルにします。
fwdchange	STP 転送変更に関する VLAN マネージャ通知をイネーブルにします。
linkchange	インターフェイスのリンク ステート変更に関する VLAN マネージャ通知をイネーブルにします。
modechange	インターフェイス モード変更に関する VLAN マネージャ通知をイネーブルにします。
pruningcfgchange	プルーニング設定変更に関する VLAN マネージャ通知をイネーブルにします。
statechange	インターフェイス ステート変更に関する VLAN マネージャ通知をイネーブルにします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、ソフトウェア VLAN インターフェイス モード変更通知をデバッグする方法を示します。

```
Switch# debug sw-vlan notification modechange
vlan manager port mode change notification debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug sw-vlan notification（no debug sw-vlan notification と同じ）	デバッグ出力をディセーブルにします。

debug sw-vlan vtp

VTP プロトコル コードによって生成されるメッセージのデバッグをイネーブルにするには、**debug sw-vlan vtp** コマンドを使用します。デバッグ出力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 sw-vlan vtp {**events** | **packets** | **pruning** [**packets** | **xmit**] | **xmit**}

no debug sw-vlan vtp {**events** | **packets** | **pruning** [**packets** | **xmit**] | **xmit**}

構文の説明

events	VTP コード内の VTP_LOG_RUNTIME マクロによって生成された汎用の論理フローおよび詳細な VTP デバッグ メッセージを表示します。
packets	プルーニング パケットを除く Cisco IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信 VTP パケットの内容を表示します。
pruning	VTP プロトコル コードのプルーニング セグメントによって生成されるデバッグ メッセージをイネーブルにします。
packets	（任意）Cisco IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信 VTP プルーニング パケットの内容を表示します。
xmit	（任意）VTP コードが Cisco IOS VTP プラットフォーム依存層に送信するように要求するすべての発信 VTP パケットの内容を表示します。
xmit	VTP コードが Cisco IOS VTP プラットフォーム依存層に送信するように要求するすべての発信 VTP パケットの内容が表示されます。プルーニング パケットは含まれません。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

pruning を入力した後にパラメータを入力しない場合は、VTP プルーニング デバッグ メッセージが表示されます。

例

次の例では、ソフトウェア VLAN 発信 VTP パケットをデバッグする方法を示します。

```
Switch# debug sw-vlan vtp xmit
vtp xmit debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug sw-vlan vtp（no debug sw-vlan vtp と同じ）	デバッグ出力をディセーブルにします。

debug udld

UDLD アクティビティのデバッグをイネーブルにするには、**debug udld** コマンドを使用します。デバッグ出力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 udld {**events** | **packets** | **registries**}

no debug udld {**events** | **packets** | **registries**}

構文の説明

events	UDLD プロセス イベントが発生したときに、このイベントのデバッグをイネーブルにします。
packets	UDLD プロセスがパケット キューからパケットを受信し、UDLD プロトコル コードの要求に応答してパケットを送信しようとするときの、プロセスのデバッグをイネーブルにします。
registries	UDLD プロセスが、このプロセスに依存するモジュールおよびその他のフィーチャ モジュールからのレジストリ アップコールを処理するときの、プロセスのデバッグをイネーブルにします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、スーパーバイザ エンジンだけでサポートされ、スイッチ コンソールからだけ入力できます。

例

次の例では、UDLD イベントをデバッグする方法を示します。

```
Switch# debug udld events
UDLD events debugging is on
Switch#
```

次の例では、UDLD パケットをデバッグする方法を示します。

```
Switch# debug udld packets
UDLD packets debugging is on
Switch#
```

次の例では、UDLD レジストリ イベントをデバッグする方法を示します。

```
Switch# debug udld registries
UDLD registries debugging is on
Switch#
```

関連コマンド

コマンド	説明
undebug udld（no debug udld と同じ）	デバッグ出力をディセーブルにします。

debug vqpc

VLAN Query Protocol（VQP）をデバッグするには、**debug vqpc** コマンドを使用します。デバッグ出力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 vqpc [**all** | **cli** | **events** | **learn** | **packet**]

no debug vqpc [**all** | **cli** | **events** | **learn** | **packet**]

構文の説明

all	（任意）すべての VQP イベントをデバッグします。
cli	（任意）VQP コマンドライン インターフェイスをデバッグします。
events	（任意）VQP イベントをデバッグします。
learn	（任意）VQP アドレス ラーニングをデバッグします。
packet	（任意）VQP パケットをデバッグします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、すべての VQP デバッグをイネーブルにする方法を示します。

```
Switch# debug vqpc all
Switch#
```

関連コマンド

コマンド	説明
vmps reconfirm（特権 EXEC）	VLAN Query Protocol（VQP）クエリーをただちに送信し、VLAN Membership Policy Server（VMPS; VLAN メンバーシップ ポリシー サーバ）を使用してすべてのダイナミック VLAN 割り当てを再確認します。

define interface-range

インターフェイスのマクロを作成するには、**define interface-range** コマンドを使用します。

define interface-range *macro-name interface-range*

構文の説明

macro-name	インターフェイス範囲マクロの名前（最大 32 文字）。
interface-range	インターフェイスを指定する場合の有効範囲のリスト。「使用上のガイドライン」を参照してください。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

マクロ名は最大 32 文字の文字列です。

マクロには、最大 5 つの範囲を含めることができます。インターフェイス範囲はモジュールをまたがることはできません。

interface-range を入力する場合は、次のフォーマットを使用します。

- *interface-type* {*mod*}/{*first-interface*} - {*last-interface*}
- *interface-type* {*mod*}/{*first-interface*} - {*last-interface*}

interface-type の有効値は、次のとおりです。

- **FastEthernet**
- **GigabitEthernet**
- **Vlan** *vlan_id*

例

次の例では、複数インターフェイスのマクロを作成する方法を示します。

```
Switch(config)# define interface-range macro1 gigabitethernet 4/1-6, fastethernet 2/1-5
Switch(config)#
```

関連コマンド

コマンド	説明
interface range	複数のポートで 1 つのコマンドを同時に実行します。

deny

DHCP バインディングと一致した ARP パケットを拒否するには、**deny** コマンドを使用します。指定した ACE をアクセス リストから削除するには、このコマンドの **no** 形式を使用します。

deny {[**request**] **ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} | **response ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} [{**any** | **host** *target-ip* | *target-ip target-ip-mask*}] **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [{**any** | **host** *target-mac* | *target-mac target-mac-mask*}]} [**log**]

no deny {[**request**] **ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} | **response ip** {**any** | **host** *sender-ip* | *sender-ip sender-ip-mask*} [{**any** | **host** *target-ip* | *target-ip target-ip-mask*}] **mac** {**any** | **host** *sender-mac* | *sender-mac sender-mac-mask*} [{**any** | **host** *target-mac* | *target-mac target-mac-mask*}]} [**log**]

構文の説明

request	（任意）ARP 要求の照合を要求します。**request** を指定しない場合は、すべての ARP パケットに対して照合が行われます。
ip	送信元 IP アドレスを指定します。
any	任意の IP アドレスまたは MAC アドレスを許可するように指定します。
host *sender-ip*	特定の送信元 IP アドレスだけを許可するように指定します。
sender-ip sender-ip-mask	特定の範囲の送信元 IP アドレスを許可するように指定します。
mac	送信元 MAC アドレスを指定します。
host *sender-mac*	特定の送信元 MAC アドレスだけを許可するように指定します。
sender-mac sender-mac-mask	特定の範囲の送信元 MAC アドレスを許可するように指定します。
response	ARP 応答の一致条件を指定します。
ip	ARP 応答の IP アドレス値を指定します。
host *target-ip*	（任意）特定の宛先 IP アドレスだけを許可するように指定します。
target-ip target-ip-mask	（任意）特定の範囲の宛先 IP アドレスを許可するように指定します。
mac	ARP 応答の MAC アドレス値を指定します。
host *target-mac*	（任意）特定の宛先 MAC アドレスだけを許可するように指定します。
target-mac target-mac-mask	（任意）特定の範囲の宛先 MAC アドレスを許可するように指定します。
log	（任意）Access Control Entry（ACE; アクセス コントロール エントリ）に一致するパケットを記録します。

デフォルト

ARP アクセス リストの末尾に暗黙的な **deny ip any mac any** コマンドが指定されています。

コマンド モード

arp-nacl コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

deny 句を追加すると、一致基準に基づいて ARP パケットを転送またはドロップできます。

例

次の例に示すホストの MAC アドレスは 0000.0000.abcd、IP アドレスは 1.1.1.1 です。次の例では、このホストからの要求と応答をどちらも拒否する方法を示します。

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
Switch# show arp access-list

ARP access list static-hosts
    deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

関連コマンド

コマンド	説明
arp access-list	ARP アクセス リストを定義したり、定義済みリストの最後に句を追加したりします。
ip arp inspection filter vlan	DAI がイネーブルの場合にスタティック IP が設定されたホストからの ARP を許可したり、ARP アクセス リストを定義して VLAN に適用したりします。
permit	DHCP バインディングとの一致に基づいて ARP パケットを許可します。

destination（netflow-lite エクスポータ サブモード）

（注）　NetFlow-lite は Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチでのみサポートされます。

netflow-lite サブモードで宛先アドレスを指定するには、**destination** コマンドを使用します。エクスポ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。

destination *destination-address*

no destination *destination-address*

構文の説明

destination-address	NetFlow-lite コレクタの宛先アドレスを指定します。

デフォルト

なし

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)SG	このコマンドが Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチに追加されました。

使用上のガイドライン

最小構成のエクスポータ、送信元レイヤ 3 インターフェイス、およびコレクタの UDP 宛先ポートの必須パラメータの 1 つ。

例

次の例では、netflow-lite サブモードで宛先アドレスを指定する方法を示します。

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

```
Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite  Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address:   5.5.5.6
    Source IP Address:        5.5.5.5
    VRF label:
    DSCP:                     0x20
    TTL:                      128
    COS:                      7
  Transport Protocol Configuration:
    Transport Protocol:       UDP
    Destination Port:         8188
    Source Port:              61670
  Export Protocol Configuration:
    Export Protocol:                  netflow-v9
    Template data timeout:            60
    Options sampler-table timeout:    1800
    Options interface-table timeout:  1800
  Exporter Statistics:
    Packets Exported:         0
```

show netflow-lite exporter 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
cos（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの CoS 値を指定します。
source（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの送信元レイヤ 3 インターフェイスを指定します。
transport udp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの UDP トランスポート宛先ポートを指定します。
ttl（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの TTL 値を指定します。
dscp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの CoS 値を指定します。
template data timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのテンプレート データ タイムアウトを指定します。
options timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのオプションのタイムアウトを指定します。
export-protocol（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのエクスポート プロトコルを指定します。

destination address

Call Home メッセージの送信先となる宛先電子メール アドレスまたは URL を設定するには、**destination address** コマンドを使用します。

destination address {**email** *email-address* | **http** *url*}

構文の説明

email *email-address*	宛先電子メール アドレスを 1 ～ 200 文字で指定します。
http *url*	宛先 HTTP URL を 2 ～ 200 文字で指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

cfg-call-home-profile

コマンド履歴

リリース	変更箇所
12.2(52)SG	Catalyst 4500 シリーズ スイッチでサポートされるようになりました。

使用上のガイドライン

プロファイル call-home コンフィギュレーション サブモードを開始するには、call-home コンフィギュレーション モードで **profile** コマンドを使用します。

セキュア サーバに https:// *destination* URL を入力する場合は、トラストポイント CA も設定する必要があります。

例

次の例では、電子メール アドレス **callhome@cisco.com** に宛先を設定する方法を示します。

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination address email callhome@cisco.com
```

関連コマンド

コマンド	説明
destination message-size-limit bytes	宛先プロファイルの最大宛先メッセージ サイズを設定します。
destination preferred-msg-format	優先するメッセージ形式を設定します。
destination transport-method	メッセージの転送形式をイネーブルにします。
profile	プロファイル call-home コンフィギュレーション サブモードを開始します
subscribe-to-alert-group all	使用可能なすべてのアラート グループに登録します。
subscribe-to-alert-group configuration	この宛先プロファイルを Configuration アラート グループに登録します。
subscribe-to-alert-group diagnostic	この宛先プロファイルを Diagnostic アラート グループに登録します。

コマンド	説明
subscribe-to-alert-group environment	この宛先プロファイルを Environment アラート グループに登録します。
subscribe-to-alert-group inventory	この宛先プロファイルを Inventory アラート グループに登録します。
subscribe-to-alert-group syslog	この宛先プロファイルを Syslog アラート グループに登録します。

destination message-size-limit bytes

宛先プロファイルの最大宛先メッセージ サイズを設定するには、**destination message-size-limit bytes** コマンドを使用します。

destination message-size-limit bytes

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。

デフォルト

3145728 バイト

コマンド モード

cfg-call-home-profile

コマンド履歴

リリース	変更箇所
12.2(52)SG	Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

プロファイル call-home コンフィギュレーション サブモードを開始するには、call-home コンフィギュレーション モードで **profile** コマンドを使用します。

例

次の例では、宛先プロファイルの最大メッセージ サイズを 3000000 に設定する方法を示します。

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination message-size-limit 3000000
Switch(cfg-call-home-profile)#
```

関連コマンド

コマンド	説明
destination address	Call Home メッセージが送信される宛先電子メール アドレスまたは URL を設定します。
destination preferred-msg-format	優先するメッセージ形式を設定します。
destination transport-method	メッセージの転送形式をイネーブルにします。
profile	プロファイル call-home コンフィギュレーション サブモードを開始します
subscribe-to-alert-group all	使用可能なすべてのアラート グループに登録します。
subscribe-to-alert-group configuration	この宛先プロファイルを Configuration アラート グループに登録します。
subscribe-to-alert-group diagnostic	この宛先プロファイルを Diagnostic アラート グループに登録します。
subscribe-to-alert-group environment	この宛先プロファイルを Environment アラート グループに登録します。

コマンド	説明
subscribe-to-alert-group inventory	この宛先プロファイルを Inventory アラート グループに登録します。
subscribe-to-alert-group syslog	この宛先プロファイルを Syslog アラート グループに登録します。

destination preferred-msg-format

使用するメッセージ形式を設定するには、**destination preferred-msg-format** コマンドを使用します。

destination preferred-msg-format {**long-text** | **short-text** | **xml**}

構文の説明

long-text	ロングテキスト形式でメッセージを送信します。
short-text	ショートテキスト形式でメッセージを送信します。
xml	XML 形式でメッセージを送信します。

デフォルト

xml

コマンド モード

cfg-call-home-profile

コマンド履歴

リリース	変更箇所
12.2(52)SG	Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

プロファイル call-home コンフィギュレーション サブモードを開始するには、call-home コンフィギュレーション モードで **profile** コマンドを使用します。

例

次の例では、使用するメッセージ形式をロング テキストに設定する方法を示します。

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination preferred-msg-format long-text
Switch(cfg-call-home-profile)#
```

関連コマンド

コマンド	説明
destination address	Call Home メッセージが送信される宛先電子メール アドレスまたは URL を設定します。
destination message-size-limit bytes	宛先プロファイルの最大宛先メッセージ サイズを設定します。
destination transport-method	メッセージの転送形式をイネーブルにします。
profile	プロファイル call-home コンフィギュレーション サブモードを開始します
subscribe-to-alert-group all	使用可能なすべてのアラート グループに登録します。
subscribe-to-alert-group configuration	この宛先プロファイルを Configuration アラート グループに登録します。
subscribe-to-alert-group diagnostic	この宛先プロファイルを Diagnostic アラート グループに登録します。

コマンド	説明
subscribe-to-alert-group environment	この宛先プロファイルを Environment アラート グループに登録します。
subscribe-to-alert-group inventory	この宛先プロファイルを Inventory アラート グループに登録します。
subscribe-to-alert-group syslog	この宛先プロファイルを Syslog アラート グループに登録します。

destination transport-method

メッセージ転送方式をイネーブルにするには、**destination transport-method** コマンドを使用します。

destination transport-method {**email** | **http**}

構文の説明

email	転送方式として電子メールをイネーブルにします。
http	転送方式として HTTP をイネーブルにします。

デフォルト

e-mail

コマンド モード

cfg-call-home-profile

コマンド履歴

リリース	変更箇所
12.2(52)SG	Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

プロファイル call-home コンフィギュレーション サブモードを開始するには、call-home コンフィギュレーション モードで **profile** コマンドを使用します。

例

次の例では、転送方式を HTTP に設定する方法を示します。

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination transport-method http
```

関連コマンド

コマンド	説明
destination address	Call Home メッセージが送信される宛先電子メール アドレスまたは URL を設定します。
destination message-size-limit bytes	宛先プロファイルの最大宛先メッセージ サイズを設定します。
destination preferred-msg-format	優先するメッセージ形式を設定します。
profile	プロファイル call-home コンフィギュレーション サブモードを開始します
subscribe-to-alert-group all	使用可能なすべてのアラート グループに登録します。
subscribe-to-alert-group configuration	この宛先プロファイルを Configuration アラート グループに登録します。
subscribe-to-alert-group diagnostic	この宛先プロファイルを Diagnostic アラート グループに登録します。
subscribe-to-alert-group environment	この宛先プロファイルを Environment アラート グループに登録します。

コマンド	説明
subscribe-to-alert-group inventory	この宛先プロファイルを Inventory アラート グループに登録します。
subscribe-to-alert-group syslog	この宛先プロファイルを Syslog アラート グループに登録します。

device-sensor filter-list

センサー デバイスの出力に追加または除外される CDP または Link Layer Discovery Protocol（LLPD）フィルタ リスト（Type-Length-Value（TLV）フィールドのリストを含む）を作成するには、グローバル コンフィギュレーション モードで、**device-sensor filter-list** コマンドを使用します。フィルタ リストを削除するには、このコマンドの **no** 形式を使用します。

device-sensor filter-list cdp | lldp list *list-name*

no device-sensor filter-list cdp | lldp list *list-name*

構文の説明

list	ディスカバリ プロトコル フィルタ リストが含まれます。
list-name	フィルタ リストの名前。

デフォルト

プロトコル TLV フィールドのフィルタ リストは使用できません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
IOS XE 3.4.0SG and IOS 15.1(2)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

プロトコル フィルタ リストの名前を設定し、Discovery Protocol センサー コンフィギュレーション モードを開始するには、**device-sensor filter-list** コマンドを使用します。**tlv** {**name** *tlv-name* | **number** *tlv-number*} コマンドを使用して、Discovery Protocol センサー コンフィギュレーション モードで TLV のリストを設定できます。**name** *tlv-name* のキーワードと引数のペアを使用して、TLV の名前を指定します。使用可能な TLV の名前を調べるには、**?** を入力するか、次の表を参照してください。

表 2-1　CDP TLV 名

CDP TLV 名	説明
グローバル コンフィギュレーション モード	
app	アプリケーション TLV をイネーブルにします
forward	別のインターフェイスに CDP パケットを転送します
location	ロケーション情報をイネーブルにします
インターフェイス コンフィギュレーション モード	
app	アプリケーション TLV をイネーブルにします
location	ロケーション情報をイネーブルにします
server-location	インターフェイス上で CDP ロケーション サーバをイネーブルにします

表 2-2　LLDP TLV

LLPP TLV 名	説明
グローバル コンフィギュレーション モード	
4-wire-power-management	MDI TLV の Cisco 4-wire 電源
mac-phy-cfg	IEEE 802.3 MAC/PHY コンフィギュレーション ステータス TLV
management-address	管理アドレス TLV
port-description	ポート記述 TLV
port-vlan	ポート VLAN ID TLV
power-management	MDI TLV の IEEE 802.3 DTE 電源
system-capabilities	システム機能 TLV
system-description	システム記述 TLV
system-name	システム名 TLV
インターフェイス コンフィギュレーション モード	
inventory-management	LLDP Media Endpoint Devices（MED）のインベントリ管理 TLV
location	LLDP-MED ロケーション TLV
network-policy	LLDP-MED ネットワーク ポリシー TLV

number *tlv-name* のキーワードと引数のペアを使用して、TLV フィルタ リストに追加する TLV 番号を指定します。

no tlv {**name** *tlv-name* | **number** *tlv-number*} コマンドを使用して、TLV フィルタ リストから個々の TLV を削除します。

no device-sensor filter-list lldp list *tlv-list-name* コマンドを使用して、すべての TLV を含む TLV リスト全体を削除します。

次に、TLV のリストを含む LLDP フィルタを作成する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-list lldp list lldp-list
Switch(config-sensor-lldplist)# tlv name mac-phy-config
Switch(config-sensor-lldplist)# tlv name system-name
Switch(config-sensor-lldplist)# end
```

例

次に、TLV のリストを含む LLDP フィルタを作成する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-list lldp list lldp-list
Switch(config-sensor-lldplist)# tlv name mac-phy-config
Switch(config-sensor-lldplist)# tlv name system-name
Switch(config-sensor-lldplist)# end
```

関連コマンド

コマンド	説明
debug device-sensor	デバイス センサーのデバッグをイネーブルにします。
device-sensor accounting	新しいセンサー データの検出時に、デバイス センサー プロトコル データをアカウンティング レコードに追加し、追加のアカウンティング イベントを生成します。
device-sensor filter-list dhcp	デバイス センサー出力に含めるまたは除外することができるオプションのリストを含む DHCP フィルタを作成します。
show device-sensor cache	デバイス センサーのキャッシュ エントリを表示します。

device-sensor filter-list dhcp

デバイス センサー出力に含めるまたは除外することができるオプションのリストを含む DHCP フィルタを作成するには、グローバル コンフィギュレーション モードで **device-sensor filter-list dhcp** コマンドを使用します。オプションのリストを含む DHCP フィルタを削除するには、このコマンドの **no** 形式を使用します。

device-sensor filter-list dhcp list *option-list-name*

no device-sensor filter-list dhcp list *option-list-name*

構文の説明

list	DHCP オプション フィルタ リストが含まれます。
option-list-name	DHCP オプション フィルタ リスト名。

デフォルト

DHCP オプション フィルタ リストは使用できません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
IOS XE 3.4.0SG and IOS 15.1(2)SG)	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

device-sensor filter-list dhcp コマンドを使用して DHCP オプション フィルタ リストの名前を設定し、DHCP センサー コンフィギュレーション モードを開始します。**option** {**name** *option-name* | **number** *option-number*} コマンドを使用して、DHCP センサー コンフィギュレーション モードでオプションのリストを設定できます。**name** *option-name* のキーワードと引数のペアを使用して、DHCP オプションの名前を指定します。**number** *option-number* のキーワードと引数のペアを使用して、DHCP オプション フィルタ リストに追加する TLV 番号を指定します。

no option {**name** *option-name* | **number** *option-number*} コマンドを使用して、DHCP オプション フィルタ リストから個々のオプションを削除します。

オプション フィルタ リスト全体を削除するには、**no device-sensor filter-list dhcp list** *option-list-name* コマンドを使用します。

例

次に、オプションのリストを含む DHCP フィルタを作成する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-list dhcp list dhcp-list
Switch(config-sensor-dhcplist)# option name domain-name
Switch(config-sensor-dhcplist)# option name host-name
Switch(config-sensor-dhcplist)# option number 50
Switch(config-sensor-dhcplist)# end
```

関連コマンド

コマンド	説明
debug device-sensor	デバイス センサーのデバッグをイネーブルにします。
device-sensor accounting	新しいセンサー データの検出時に、デバイス センサー プロトコル データをアカウンティング レコードに追加し、追加のアカウンティング イベントを生成します。
device-sensor filter-list	デバイス センサー出力に含めるまたは除外することができるオプションのリストを含む CDP または LLDP フィルタを作成します。
show device-sensor cache	デバイス センサーのキャッシュ エントリを表示します。

device-sensor filter-spec

センサー デバイスの出力にプロトコル フィルタ リストを適用するには、グローバル コンフィギュレーション モードで **device-sensor filter-spec** コマンドを使用します。デバイス センサー出力からプロトコル フィルタ リストを削除するには、このコマンドの **no** 形式を使用します。

device-sensor filter-spec {cdp | lldp | dhcp} {exclude {all | list *list-name***} | include list** *list-name***}**

構文の説明

cdp	デバイス センサー出力に CDP TLV フィルタ リストを適用します。
lldp	デバイス センサー出力に LLDP TLV フィルタ リストを適用します。
dhcp	デバイス センサー出力に DHCP オプション フィルタ リストを適用します。
exclude	デバイス センサーの出力から除外するプロトコル TLV または DHCP オプションを指定します。
all	関連するプロトコル用のすべての通知をディセーブルにします。
list *list-name*	フィルタ リストの名前を指定します。
include	デバイス センサー出力に含める必要がある TLV または DHCP オプションを指定します。

デフォルト

すべての TLV または DHCP オプションは通知に含まれ、通知をトリガーします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
IOS XE 3.4.0SG and IOS 15.1(2)SG)	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

センサー デバイスの出力に含まれる CDP または LLDP の TLV フィールドや、DHCP オプションのリストを指定するには、**device-sensor filter-spec** コマンドを使用します。

DISCOVER、OFFER、REQUEST、ACK および IP アドレスなど、特定の TLV およびメッセージ タイプは、無条件に除外されます。除外される TLV およびメッセージ タイプは、上位層プロトコルの転送に使用されます。これらは、頻繁に変更され、エンドポイントに関する有益な情報をほとんど伝送しません。OFFER メッセージも、複数のサーバかで受信されることがあり、エンドポイントに関する有益な情報を伝送しないため、除外されます。

例

次に、CDP TLV フィルタ リストをデバイス センサー出力に適用する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor filter-spec cdp include cdp-list1
```

関連コマンド

コマンド	説明
debug device-sensor	デバイス センサーのデバッグをイネーブルにします。
device-sensor accounting	新しいセンサー データの検出時に、デバイス センサー プロトコル データをアカウンティング レコードに追加し、追加のアカウンティング イベントを生成します。
device-sensor filter-list	デバイス センサー出力に含めるまたは除外することができるオプションのリストを含む CDP または LLDP フィルタを作成します。
device-sensor filter-list dhcp	デバイス センサー出力に含めるまたは除外することができるオプションのリストを含む DHCP フィルタを作成します。
show device-sensor cache	デバイス センサーのキャッシュ エントリを表示します。

device-sensor notify

TLV 変更に関するクライアント通知およびイベント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 **device-sensor notify** コマンドを使用します。TLV 変更に関するクライアント通知およびアカウンティング イベント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。

device-sensor notify all-changes | new-tlvs

no device-sensor notify all-changes | new-tlvs

構文の説明

all-changes	すべての TLV 変更に関するクライアント通知およびアカウンティング イベントをイネーブルにします。
new-tlvs	新しい TLV 変更のみに関するクライアント通知およびアカウンティング イベントをイネーブルにします。

デフォルト

クライアント通知とアカウンティング イベントは新しい TLV に関してのみ生成されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
IOS XE 3.4.0SG and IOS 15.1(2)SG)	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

デフォルトでは、サポートされている各ピア プロトコルに関して、特定のセッションのコンテキストで以前受信されなかった TLV が着信パケットに含まれている場合にのみクライアント通知とアカウンティング イベントが生成されます。

すべての TLV 変更に関するクライアント通知とアカウンティング イベントをイネーブルにして、新しい TLV が受信され、以前受信された TLV は異なる値で受信されるようにするには、**device-sensor notify all-changes** コマンドを使用します。

デフォルトの動作に戻すには、**device-sensor notify new-tlvs** または **default device-sensor notify** コマンドを使用します。

例

次に、すべての TLV 変更のクライアント通知およびアカウンティング イベントをイネーブルにする例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# device-sensor notify all-changes
```

関連コマンド

コマンド	説明
debug device-sensor	デバイス センサーのデバッグをイネーブルにします。
device-sensor filter-list	デバイス センサー出力に含めるまたは除外することができるオプションのリストを含む CDP または LLDP フィルタを作成します。

コマンド	説明
device-sensor filter-list dhcp	デバイス センサー出力に含めるまたは除外することができるオプションのリストを含む DHCP フィルタを作成します。
show device-sensor cache	デバイス センサーのキャッシュ エントリを表示します。

diagnostic fpga soft-error recover

SEU の動作を設定するには、**diagnostic fpga soft-error recover** 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。

diagnostic fpga soft-error recover {conservative | aggressive}

no diagnostic fpga soft-error recover

構文の説明

conservative	スーパーバイザ エンジンがリロードするのではなく、コンソール エラー メッセージを 1 時間に 1 回発行するように指定します。 次のメンテナンス ウィンドウでスーパーバイザ エンジンをリロードする必要があります。
aggressive	スーパーバイザ エンジンがすぐに、自動的にリロードするように指定します。クラッシュダンプが生成され、リロードの原因として SEU イベントを識別できます。

デフォルト

このコマンドが設定されていない場合、スイッチはデフォルトの SEU の動作を示します。SSO に達した冗長スイッチでは、デフォルトの動作は aggressive です。その他のすべてのスイッチでは、デフォルトの動作は conservative です。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(53)SG3、 12.2(54)SG、 15.0(2)SG XE 3.1.1SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(53)SG6 15.0(2)SG2 XE 3.3.0SG	**conservative** オプションのサポートが追加されました。

使用上のガイドライン

システムの FPGA の SEU イベントにより、スイッチが不安定になるおそれがあります。唯一の回復方法は、影響を受けるスーパーバイザ エンジンをリロードすることです。ただし、SEU イベントは無害であるので、ユーザに影響を与えることを防ぐためにメンテナンス ウィンドウまでリロードを遅らせることができます。または、SEU が原因でスイッチがクラッシュしたり、トラフィックをドロップしたりするのを避けるために即座にリロードを強制することもできます。

例

次の例では、SEU の動作 を conservative に設定する方法を示します。

```
Switch(config)# diagnostic fpga soft-error recover conservative
```

次の例では、デフォルトの動作に戻す方法を示します。

```
Switch(config)# no diagnositc fpga soft-error recover
```

diagnostic monitor action

スイッチがパケット メモリの障害を検出したときのスイッチのアクションを指示するには、**diagnostic monitor action** コマンドを使用します。

diagnostic monitor action [**conservative** | **normal** | **aggressive**]

構文の説明

conservative	（任意）起動時 SRAM 診断はすべての障害を記録し、ハードウェアの動作から影響を受けるすべてのバッファを削除することを指定します。進行中の SRAM の診断はイベントを記録しますが、他のアクションは行いません。
normal	（任意）継続的な障害がスーパーバイザ エンジンをリセットすることを除いて、SRAM の診断が conservative モードで動作することを指定します。ブート アップ テストにより影響を受けるメモリをマッピングすることができます。
aggressive	（任意）起動時の障害は障害を記録するだけで、スーパーバイザ エンジンがオンラインにならないことを除いて、SRAM の診断が通常モードで動作することを指定します。冗長スーパーバイザ エンジンまたはネットワーク レベルの冗長性が引き継ぐことができます。

デフォルト

通常モード

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

問題を解決するのにスイッチを再起動しない場合は、**conservative** キーワードを使用します。

冗長スーパーバイザ エンジンがあるか、またはネットワーク レベルで冗長性が確保されている場合は、**aggressive** キーワードを使用します。

例

次の例では、継続的な障害が発生した場合に RPR のスイッチオーバーを開始するようにスイッチを設定する方法を示します。

```
Switch# configure terminal
Switch (config)# diagnostic monitor action normal
```

関連コマンド

コマンド	説明
show diagnostic result module test 2	モジュールベースの診断テスト結果を表示します。
show diagnostic result module test 3	モジュールベースの診断テスト結果を表示します。

diagnostic start

指定した診断テストを実行するには、**diagnostic start** コマンドを使用します。

diagnostic start {**module** *num*} {**test** *test-id*} [**port** *num*]

構文の説明

module *num*	モジュール番号。
test	実行するテストを指定します。
test-id	実行するテストの ID 番号を指定します。ケーブル診断の *test-id*、または **cable-tdr** キーワードを使用できます。
port *num*	（任意）インターフェイスのポート番号を指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(25)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、指定したモジュールで、指定した診断テストを実行する方法を示します。

```
This exec command starts the TDR test on specified interface
Switch# diagnostic start module 1 test cable-tdr port 3
diagnostic start module 1 test cable-tdr port 3
module 1: Running test(s) 5 Run interface level cable diags
module 1: Running test(s) 5 may disrupt normal system operation
Do you want to continue? [no]: yes
yes
Switch#
2d16h: %DIAG-6-TEST_RUNNING: module 1: Running online-diag-tdr{ID=5} ...
2d16h: %DIAG-6-TEST_OK: module 1: online-diag-tdr{ID=5} has completed successfully

Switch#
```

（注） TDR テストの結果を表示するには、**show cable-diagnostic tdr** コマンドを使用します。テスト結果は、テストの開始から約 1 分が経過するまで表示されません。テスト開始から 1 分以内に **show cable-diagnostic tdr** コマンドを入力すると、「TDR test is in progress on interface...」というメッセージが表示される場合があります。

関連コマンド

コマンド	説明
show diagnostic content	診断内容に関する情報を表示します。

dot1x auth-fail max-attempts コマンド

ポートが Auth-fail VLAN（認証失敗 VLAN）に移行する前の最大試行回数を設定するには、**dot1x auth-fail max-attempts** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x auth-fail max-attempts *max-attempts*

no dot1x auth-fail max-attempts *max-attempts*

構文の説明

max-attempts	ポートが Auth-fail VLAN（認証失敗 VLAN）に移行する前の最大試行回数を 1 ～ 10 の範囲で指定します。

デフォルト

デフォルト値は 3 です。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(25)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、ファスト イーサネット インターフェイス 4/3 でポートが Auth-fail VLAN（認証失敗 VLAN）に移行する前の最大試行回数を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x auth-fail max-attempts 5
Switch(config-if)# end
Switch#
```

関連コマンド

コマンド	説明
dot1x max-reauth-req	認証プロセスを再開する前に、スイッチが EAP-Request/Identity フレームをクライアントに再送信する最大回数を設定します。
show dot1x	802.1X 情報を表示します。

dot1x auth-fail vlan

ポートで Auth-fail VLAN（認証失敗 VLAN）をイネーブルにするには、**dot1x auth-fail 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。

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan *vlan-id*

構文の説明

vlan-id	VLAN を 1 ～ 4094 の範囲で指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(25)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、ファスト イーサネット インターフェイス 4/3 上で Auth-fail VLAN（認証失敗 VLAN）を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch#
```

関連コマンド

コマンド	説明
dot1x max-reauth-req	認証プロセスを再開する前に、スイッチが EAP-Request/Identity フレームをクライアントに再送信する最大回数を設定します。
show dot1x	dot1x 情報を表示します。

dot1x control-direction

スイッチのポート単位で単方向ポート制御をイネーブルにするには、**dot1x control-direction** コマンドを使用します。単方向ポート制御をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

dot1x control-direction [**in** | **both**]

no dot1x control-direction

構文の説明

in	（任意）ポートで着信トラフィックを制御するように指定します。
both	（任意）ポートで着信トラフィックと発信トラフィックの両方を制御するように指定します。

デフォルト

着信トラフィックと発信トラフィックの両方が制御されます。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

単方向制御を使用して、リモート システムを管理できます。単方向制御を使用すると、マジック パケットと呼ばれる特定のイーサネット パケットを使用して、システムの電源をリモートでオンにできます。

単方向制御を使用すると、802.1X ポートからシステムをリモート管理できます。これまでは、システムを終了させると、ポートが無許可ステートになっていました。この状態のポートでは、EAPoL パケットの送受信しか許可されません。したがって、単方向制御のマジック パケットがホストに到達する方法がなく、システムが起動していないかぎり、ポートを認証して開くことができませんでした。

例

次の例では、着信パケットに対して単方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x control-direction in
Switch(config-if)#
```

関連コマンド

コマンド	説明
show dot1x	dot1x 情報を表示します。

dot1x credentials（グローバル コンフィギュレーション）

dot1x credentials 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、サプリカント スイッチでプロファイルを設定します。

dot1x credentials *profile*

no dot1x credentials *profile*

構文の説明

profile	サプリカント スイッチのプロファイルを指定します。

デフォルト

スイッチにプロファイルは設定されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(54)SG	このコマンドが追加されました。

使用上のガイドライン

このスイッチをサプリカントにするには、オーセンティケータとして別のスイッチをセットアップしてある必要があります。

例

次の例では、スイッチをサプリカントとして設定する方法を示します。

```
Switch(config)# dot1x credentials profile
```

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
cisp enable	Client Information Signalling Protocol（CISP）をイネーブルにします。
show cisp	指定されたインターフェイスの CISP 情報を表示します。

dot1x critical

ポートで 802.1X クリティカル認証をイネーブルにするには、**dot1x critical** 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 critical

no dot1x critical

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

クリティカル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 モード

コマンド履歴

リリース	変更箇所
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、802.1X クリティカル認証をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x critical
Switch(config-if)#
```

関連コマンド

コマンド	説明
dot1x critical eapol	EAP 交換の途中でポートがクリティカル認証を受けた場合の EAPOL 成功パケットの送信をイネーブルにします。
dot1x critical recovery delay	ポートの再初期化が行われる時間間隔を設定します。
dot1x critical vlan	クリティカル認証を受けたポートを特定の VLAN に割り当てます。
show dot1x	dot1x 情報を表示します。

dot1x critical eapol

EAP 交換の途中でポートがクリティカル認証を受けた場合の EAPOL 成功パケットの送信をイネーブルにするには、**dot1x critical eapol** 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 critical eapol

no dot1x critical eapol

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトでは EAPOL 成功パケットは送信されません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、EAPOL 成功パケットの送信をイネーブルにする方法を示します。

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

関連コマンド

コマンド	説明
dot1x critical	ポートで 802.1X クリティカル認証をイネーブルにします。
dot1x critical recovery delay	ポートの再初期化が行われる時間間隔を設定します。
dot1x critical vlan	クリティカル認証を受けたポートを特定の VLAN に割り当てます。
show dot1x	dot1x 情報を表示します。

dot1x critical recovery delay

ポートの再初期化が行われる時間間隔を設定するには、**dot1x critical recovery delay** 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 critical recovery delay *delay-time*

no dot1x critical recovery delay

構文の説明

delay-time	AAA 遷移が発生した場合のポート再初期化の時間間隔を指定します。有効値の範囲は 1 ～ 10,000 ミリ秒です。

デフォルト

遅延時間は 100 ミリ秒に設定されています。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、802.1X クリティカル回復の遅延時間を 500 に設定する方法を示します。

```
Switch(config-if)# dot1x critical recovery delay 500
Switch(config-if)#
```

関連コマンド

コマンド	説明
dot1x critical	ポートで 802.1X クリティカル認証をイネーブルにします。
dot1x critical eapol	EAP 交換の途中でポートがクリティカル認証を受けた場合の EAPOL 成功パケットの送信をイネーブルにします。
dot1x critical vlan	クリティカル認証を受けたポートを特定の VLAN に割り当てます。
show dot1x	dot1x 情報を表示します。

dot1x critical vlan

クリティカル認証を受けたポートを特定の VLAN に割り当てるには、**dot1x critical 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。

dot1x critical vlan *vlan-id*

no dot1x critical *vlan-id*

構文の説明

vlan-id	（任意）VLAN を指定します。有効値の範囲は 1 ～ 4094 です。

デフォルト

ポートの VLAN でクリティカル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 モード

コマンド履歴

リリース	変更箇所
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

指定した VLAN のタイプはポートのタイプと一致している必要があります。ポートがアクセス ポートの場合、VLAN は通常の VLAN である必要があります。ポートがプライベート VLAN のホスト ポートの場合、VLAN は有効なプライベート VLAN ドメインのセカンダリ VLAN である必要があります。ポートがルーテッド ポートの場合、VLAN は指定できません。

このコマンドは、クリティカル認証 VLAN サブシステムを含まないプラットフォーム（レイヤ 3 スイッチなど）ではサポートされません。

例

次の例では、ポート VLAN で 802.1X クリティカル認証をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x critical vlan 350
Switch(config-if)#
```

関連コマンド

コマンド	説明
dot1x critical	ポートで 802.1X クリティカル認証をイネーブルにします。
dot1x critical eapol	EAP 交換の途中でポートがクリティカル認証を受けた場合の EAPOL 成功パケットの送信をイネーブルにします。
dot1x critical recovery delay	ポートの再初期化が行われる時間間隔を設定します。
show dot1x	dot1x 情報を表示します。

dot1x guest-vlan

ポート単位でゲスト VLAN をイネーブルにするには、**dot1x guest-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。

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan *vlan-id*

構文の説明

vlan-id	VLAN を 1 ～ 4094 の範囲で指定します。

デフォルト

このコマンドにデフォルト設定はありません。ゲスト VLAN 機能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 モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(25)EWA	設定済みゲスト VLAN ID としてセカンダリ VLAN のサポートが追加されました。

使用上のガイドライン

ゲスト VLAN は、アクセス ポートまたはプライベート VLAN ホスト ポートとしてスタティックに設定されたポートのみで設定可能です。スタティックに設定されたアクセス ポートでは、通常の VLAN をゲスト VLAN として設定可能です。スタティックに設定されたプライベート VLAN ホスト ポートでは、セカンダリ プライベート VLAN をゲスト VLAN として設定可能です。

例

次の例では、ファスト イーサネット インターフェイス 4/3 でゲスト VLAN をイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 26
Switch(config-if)# end
Switch(config)# end
Switch#
```

関連コマンド

コマンド	説明
dot1x max-reauth-req	認証プロセスを再開する前に、スイッチが EAP-Request/Identity フレームをクライアントに再送信する最大回数を設定します。
show dot1x	dot1x 情報を表示します。

dot1x guest-vlan supplicant

802.1X 対応サプリカント（ホスト）をゲスト VLAN に登録するには、**dot1x guest-vlan supplicant** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x quest-vlan supplicant

no dot1x quest-vlan supplicant

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。

デフォルト

802.1X 対応ホストはゲスト VLAN に登録されていません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(25)EWA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

Cisco Release 12.2(25) EWA では、**dot1x guest-vlan supplicant** コマンドを使用して、802.1X 対応ホストをゲスト VLAN に登録できます。Cisco Release 12.2(25)EWA よりも前のリリースでは、ゲスト VLAN に登録できるのは 802.1X 非対応ホストだけでした。

ゲスト VLAN サプリカントの動作をイネーブルにした場合、Catalyst 4500 シリーズ スイッチは EAPOL パケットの履歴を維持しません。このスイッチでは、インターフェイスで EAPOL パケットが検出されたかどうかに関係なく、802.1X 認証に失敗したクライアントのゲスト VLAN へのアクセスを許可します。

例

次の例では、802.1X 対応サプリカント（ホスト）をゲスト VLAN に登録する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# end
Switch#
```

関連コマンド

コマンド	説明
dot1x system-auth-control	スイッチで 802.1X 認証をイネーブルにします。
show dot1x	dot1x 情報を表示します。

dot1x host-mode

IEEE 802.1X 許可ポートで単一ホスト（クライアント）または複数ホストを許可するには、スイッチ スタックまたはスタンドアロン スイッチで **dot1x host-mode** インターフェイス コンフィギュレーション コマンドを使用します。IEEE802.1x 許可ポート上で、Multidomain Authentication（MDA; マルチドメイン認証）をイネーブルにするには、**multi-domain** キーワードを使用します。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 host-mode {**multi-host** | **single-host** | **multi-domain**}

no dot1x host-mode [**multi-host** | **single-host** | **multi-domain**}

構文の説明

multi-host	スイッチ上で複数のホストをイネーブルにします。
single-host	スイッチ上で単一のホストをイネーブルにします。
multi-domain	スイッチ ポート上で MDA をイネーブルにします。

デフォルト

デフォルト設定は、シングルホスト モードです。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(20)EWA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(37)SG	複数ドメインのサポートが追加されました。

使用上のガイドライン

このコマンドを使用すると、IEEE 802.1X 対応ポートを単一のクライアントに限定したり、複数のクライアントを IEEE 802.1X 対応ポートに接続したりすることができます。マルチホスト モードでは、接続されたホストのうち 1 つだけが許可されれば、すべてのホストのネットワーク アクセスが許可されます。ポートが無許可ステートになった場合（再認証が失敗した場合、または Extensible Authentication Protocol over LAN（EAPOL）-Logoff メッセージを受信した場合）には、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

ポートで MDA をイネーブルにするには、**multi-domain** キーワードを使用します。MDA はポートをデータ ドメインと音声ドメインの両方に分割します。MDA により、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が同じ IEEE 802.1x 対応ポート上で許可されます。

このコマンドを入力する前に、指定のポートで **dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認します。

音声 VLAN およびデータ VLAN は、どちらも ACS サーバからダイナミックに割り当てることができます。スイッチでダイナミック VLAN 割り当てをイネーブルにするのに、追加設定は必要ありません。VLAN 割り当てをイネーブルにするには、Cisco ACS サーバを設定する必要があります。ACS サーバを設定して音声 VLAN を割り当てる方法の詳細については、『Catalyst 4500 Series Switch Software Configuration Guide-Release, 12.2(52)SG』の「Cisco ACS Configuration for VLAN Assignment」を参照してください。

例

次の例では、IEEE 802.1X 認証および multiple-host モードをイネーブルにする方法を示します。

```
Switch# configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet6/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
Switch#
```

次に、MDA をイネーブルにして、ポートでホストおよび音声デバイスの両方を許可する例を示します。

```
Switch# configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet6/1
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

設定を確認するには、**show dot1x** [**interface** *interface-id*] 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
show dot1x	dot1x 情報を表示します。

dot1x initialize

802.1X を再初期化する前にインターフェイスを無許可にするには、**dot1x initialize** コマンドを使用します。

dot1x initialize *interface*

構文の説明

interface	インターフェイスの番号。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ステート マシンを初期化して、新しい認証環境を設定するには、このコマンドを使用します。

例

次の例では、インターフェイスで 802.1X ステート マシンを初期化する方法を示します。

```
Switch# dot1x initialize
Switch#
```

関連コマンド

コマンド	説明
show dot1x	dot1x 情報を表示します。

dot1x mac-auth-bypass

スイッチで 802.1X MAC アドレス バイパスをイネーブルにするには、**dot1x mac-auth-bypass** コマンドを使用します。MAC アドレス バイパスをディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x mac-auth-bypass [**eap**]

no dot1x mac-auth-bypass [**eap**]

構文の説明

eap	（任意）EAP MAC アドレス認証の使用を指定します。

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

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

dot1x mac-auth-bypass 設定をポートから削除しても、ポートの許可ステートまたは認証ステートに影響はありません。ポートが未認証ステートの場合、そのポートは未認証ステートのままです。また、MAB がアクティブの場合、認証は 802.1X オーセンティケータに戻ります。ポートが MAC アドレスで許可されている場合に MAB 設定を削除すると、このポートの許可された状態は、再認証が実行されるまで維持されます。再認証が実行されると、回線上で検出された 802.1X サプリカントが優先されて、MAC アドレスが削除されます。

例

次の例では、EAP MAC アドレス認証をイネーブルにする方法を示します。

```
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)#
```

dot1x max-reauth-req

認証プロセスを再開する前に、スイッチが EAP-Request/Identity フレームをクライアントに再送信する最大回数を設定するには、**dot1x max-reauth-req** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x max-reauth-req *count*

no dot1x max-reauth-req

構文の説明

count	認証プロセスを再開する前に、スイッチが EAP-Request/Identity フレームを再送信する回数。有効値の範囲は 1 ～ 10 です。

デフォルト

スイッチは再送信を最大 2 回行います。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

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。この設定は、dot1x 非対応クライアントが設定されている場合に、このクライアントがゲスト VLAN に登録されるまでの待機時間に影響します。

設定を確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

例

次の例では、認証プロセスを再開する前に、スイッチが EAP-Request/Identity フレームを再送信する回数を 5 回に設定する方法を示します。

```
Switch(config-if)# dot1x max-reauth-req 5
Switch(config-if)#
```

関連コマンド

コマンド	説明
show dot1x	dot1x 情報を表示します。

dot1x max-req

認証プロセスを再開する前に、スイッチが Extensible Authentication Protocol（EAP; 拡張認証プロトコル）-Request/Identity 以外のタイプの EAP-Request フレームをクライアントに再送信する最大回数を設定するには、**dot1x max-req** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x max-req *count*

no dot1x max-req

構文の説明

count	認証プロセスを再開する前に、スイッチが EAP-Request/Identity 以外のタイプの EAP-Request フレームを再送信する回数。有効値の範囲は 1 ～ 10 です。

デフォルト

スイッチは再送信を最大 2 回行います。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(19)EW	このコマンドは EAP-Request/Identity 再送信制限を制御するように変更されました。

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。

設定を確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

例

次の例では、認証プロセスを再開する前に、スイッチが EAP-Request フレームを再送信する回数を 5 回に設定する方法を示します。

```
Switch(config-if)# dot1x max-req 5
Switch(config-if)#
```

次の例では、デフォルト設定に戻す方法を示します。

```
Switch(config-if)# no dot1x max-req
Switch(config-if)#
```

関連コマンド

コマンド	説明
dot1x initialize	802.1X を再初期化する前にインターフェイスを無許可にします。
dot1x max-reauth-req	認証プロセスを再開する前に、スイッチが EAP-Request/Identity フレームをクライアントに再送信する最大回数を設定します。
show dot1x	dot1x 情報を表示します。

dot1x port-control

ポートの許可ステートの手動制御をイネーブルにするには、**dot1x port-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

構文の説明

auto	インターフェイスで 802.1X 認証をイネーブルにし、スイッチおよびクライアント間の 802.1X 認証交換に基づきポートを許可または無許可ステートに移行します。
force-authorized	インターフェイスで 802.1X 認証をディセーブルにし、認証交換を必要とせずにポートを許可ステートに移行します。ポートはクライアントの 802.1x ベース認証なしで通常のトラフィックを送受信します。
force-unauthorized	ポートを強制的に無許可ステートに移行することで、指定したインターフェイスを経由するすべてのアクセスを拒否し、クライアントからの認証試行をすべて無視します。スイッチはインターフェイス経由でクライアントに認証サービスを提供できません。

デフォルト

ポート 802.1X 許可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 モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

802.1X プロトコルは、レイヤ 2 スタティック アクセス ポートおよびレイヤ 3 ルーテッド ポートの両方でサポートされています。

ポートが次のポートとして設定されていない場合のみ、**auto** キーワードを使用できます。

- トランク ポート：トランク ポートで 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、802.1X はイネーブルになりません。802.1X をイネーブルにしたポートをトランク モードに変更しようとしても、ポートのモードは変更されません。
- ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、802.1X はイネーブルになりません。802.1X 対応ポートをダイナミック モードに変更しようとしても、ポートのモードは変更されません。
- EtherChannel ポート：ポート上で 802.1X をイネーブルにする前に、EtherChannel から 802.1X を削除する必要があります。EtherChannel または EtherChannel 内のアクティブなポート上で 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。非アクティブな EtherChannel のポートで 802.1X をイネーブルにしても、そのポートは EtherChannel に加入しません。

- スイッチド ポート アナライザ（SPAN）宛先ポート：SPAN 宛先ポートで 802.1X をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、802.1X はディセーブルに設定されます。SPAN 送信元ポートでは 802.1X をイネーブルにすることができます。

スイッチで 802.1X をグローバルにディセーブルにするには、各ポートで 802.1X をディセーブルにする必要があります。このタスクのグローバル コンフィギュレーション コマンドはありません。

例

次の例では、ギガビット イーサネット 1/1 で 802.1X をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# dot1x port-control auto
Switch#
```

show dot1x all または **show dot1x interface** *int* コマンドを使用してポート制御ステータスを表示すると、設定を確認できます。ステータスがイネーブルの場合は、ポート制御値が **auto** または **force-unauthorized** に設定されていることを示します。

関連コマンド

コマンド	説明
show dot1x	dot1x 情報を表示します。

dot1x re-authenticate

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

dot1x re-authenticate [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）インターフェイスのモジュール番号およびポート番号。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドを使用すると、再認証試行（re-authperiod）と自動再認証の間に設定された期間（秒）を待機することなく、クライアントを再認証できます。

例

次の例では、ギガビット イーサネット インターフェイス 1/1 に接続されたデバイスを手動で再認証する方法を示します。

```
Switch# dot1x re-authenticate interface gigabitethernet1/1
Starting reauthentication on gigabitethernet1/1
Switch#
```

dot1x re-authentication

クライアントの定期的な再認証をイネーブルにするには、**dot1x re-authentication** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x re-authentication

no dot1x re-authentication

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。

デフォルト

定期的な再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 モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

定期的な再認証試行が行われる時間間隔を設定するには、**dot1x timeout re-authperiod** 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。

例

次の例では、クライアントの定期的な再認証をディセーブルにする方法を示します。

```
Switch(config-if)# no dot1x re-authentication
Switch(config-if)#
```

次の例では、定期的な再認証をイネーブルにして、再認証を試行する間隔（秒）を 4000 秒に設定する方法を示します。

```
Switch(config-if)# dot1x re-authentication
Switch(config-if)# dot1x timeout re-authperiod 4000
Switch#
```

設定を確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x timeout	再認証タイマーを設定します。
show dot1x	dot1x 情報を表示します。

dot1x system-auth-control

スイッチで 802.1X 認証をイネーブルにするには、**dot1x system-auth-control** コマンドを使用します。システムで 802.1X 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。

dot1x system-auth-control

no dot1x system-auth-control

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。

デフォルト

802.1X 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 モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

スイッチの任意のポートで 802.1X アクセス コントロールを使用する場合は、**dot1x system-auth-control** をイネーブルにする必要があります。次に、802.1X アクセス コントロールを使用する特定ポートごとに **dot1x port-control auto** コマンドを使用してください。

例

次の例では、802.1X 認証をイネーブルにする方法を示します。

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

関連コマンド

コマンド	説明
dot1x initialize	802.1X を再初期化する前にインターフェイスを無許可にします。
show dot1x	dot1x 情報を表示します。

dot1x timeout

再認証タイマーを設定するには、**dot1x timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout {**reauth-period** {*seconds* | **server**} | **quiet-period** *seconds* | **tx-period** *seconds* |
supp-timeout *seconds* | **server-timeout** *seconds*}

no dot1x timeout {**reauth-period** | **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout**}

構文の説明

reauth-period *seconds*	再認証試行の間隔（秒）。有効値の範囲は 1 ～ 65535 です。詳細については、「使用上のガイドライン」の項を参照してください。
reauth-period server	再認証試行の間隔（秒）。有効値の範囲は 1 ～ 65535 で、Session-Timeout RADIUS 属性に従います。詳細については、「使用上のガイドライン」の項を参照してください。
quiet-period *seconds*	スイッチがクライアントとの認証情報の交換に失敗したあと、待機状態を続ける期間（秒）。有効値の範囲は 0 ～ 65535 秒です。
tx-period *seconds*	要求を再送信するまで、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待機する期間（秒）。有効値の範囲は 1 ～ 65535 秒です。
supp-timeout *seconds*	スイッチが EAP-Request パケットの再送信を待機する期間（秒）。有効値の範囲は 30 ～ 65535 秒です。
server-timeout *seconds*	バックエンド オーセンティケータが認証サーバにパケットを再送信するのをスイッチが待機する期間（秒）。有効値の範囲は 30 ～ 65535 秒です。

デフォルト

デフォルト設定は、次のとおりです。

- 再認証期間は 3600 秒です。
- 待機時間は 60 秒です。
- 送信間隔は 30 秒です。
- サプリカントのタイムアウトは 30 秒です。
- サーバのタイムアウトは 30 秒です。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(12)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(25)EWA	「サーバ」からの再認証タイマー選択のサポートが追加されました。

使用上のガイドライン

dot1x timeout re-authperiod コマンドを入力する前に、定期的な再認証をイネーブルにしておく必要があります。定期的な再認証をイネーブルにするには、**dot1x re-authentication** コマンドを入力します。

例

次の例では、要求を再送信する前に、スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待機する秒数を 60 秒に設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# end
Switch#
```

設定を確認するには、**show dot1x** 特権 EXEC コマンドを入力します。

次の例では、Session-Timeout 属性から得られる再認証タイムアウトを使用するように、スイッチを設定する方法を示します。この属性は、ホストが 802.1X 経由で認証に成功したときに受信する RADIUS Access-Accept メッセージから取得します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet4/3
Switch(config-if)# dot1x timeout reauth-period server
Switch(config-if)# end
Switch#
```

関連コマンド

コマンド	説明
dot1x initialize	802.1X を再初期化する前にインターフェイスを無許可にします。
show dot1x	dot1x 情報を表示します。

dscp（netflow-lite エクスポータ サブモード）

NetFlow-lite コレクタの CoS 値を指定するには、**dscp** コマンドを使用します。この値を削除するには、このコマンドの **no** 形式を使用します。

（注）　NetFlow-lite は Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチでのみサポートされます。

dscp *dscp-value*

no dscp *dscp-value*

構文の説明

dscp-value	NetFlow-lite コレクタの DSCP 値を指定します。有効な値は 0 ～ 63 です。

デフォルト

0

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)SG	このコマンドが Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチに追加されました。

例

次の例では、NetFlow-lite コレクタの CoS 値を指定する方法を示します。

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#

Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite  Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address:   5.5.5.6
    Source IP Address:        5.5.5.5
    VRF label:
```

```
    DSCP:                       0x20
    TTL:                        128
    COS:                        7
  Transport Protocol Configuration:
    Transport Protocol:         UDP
    Destination Port:           8188
    Source Port:                61670
  Export Protocol Configuration:
    Export Protocol:                    netflow-v9
    Template data timeout:              60
    Options sampler-table timeout:      1800
    Options interface-table timeout:    1800
  Exporter Statistics:
    Packets Exported:           0
```

show netflow-lite exporter 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
cos（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの CoS 値を指定します。
source（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの送信元レイヤ 3 インターフェイスを指定します。
transport udp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの UDP トランスポート宛先ポートを指定します。
ttl（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの TTL 値を指定します。
destination（netflow-lite エクスポータ サブモード）	netflow-lite サブモードでの宛先アドレスを指定します。
template data timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのテンプレート データ タイムアウトを指定します。
options timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのオプションのタイムアウトを指定します。
export-protocol（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのエクスポート プロトコルを指定します。

dual-active detection（仮想スイッチ）

デュアル アクティブ検出をイネーブルにして設定するには、仮想スイッチのコンフィギュレーション サブモードで **dual-active detection** コマンドを使用します。デュアル アクティブ検出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。

dual-active detection {**pagp** [**trust channel-group** *num*]}

no dual-active detection {**pagp**}

構文の説明

pagp	デュアル アクティブ検出方法として、ポート集約プロトコル（PAgP）を設定します。デフォルトではイネーブルになっています。
trust channel-group *num*	（任意）PAgP デュアル アクティブ検出に使用する EtherChannel/ポート バンドルを指定します。範囲：1 ～ 256。デフォルトではディセーブルになっています。

デフォルト

bfd および **pagp** はイネーブルになっています。

trust はディセーブルになっています。

コマンド モード

仮想スイッチ コンフィギュレーション サブモード（config-vs-domain）

コマンド履歴

リリース	変更箇所
Cisco IOS XE 3.4.0SG および 15.1(2)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

PAgP が VSS とそのアクセス スイッチの間の MEC 上で実行されている場合、VSS は拡張 PAgP メッセージングを使用してデュアル アクティブ シナリオを検出できます。MEC は VSS の両方のシャーシにアクセス スイッチへのリンクがある必要があります。デフォルトでは、PAgP デュアル アクティブ検出はイネーブルです。ただし、拡張メッセージは、信頼モードがイネーブルになっているチャネル グループ上でのみ送信されます

fast hello デュアル アクティブ検出メカニズムを設定する場合は、デュアル アクティブ インターフェイス ペアも fast hello デュアル アクティブ メッセージング リンクとして動作するように設定する必要があります。

オプションのキーワードおよび引数である trust channel-group num を入力すると、次が適用されます。

- ポート チャネルにインターフェイスがない場合でも、またはポート チャネルが PAgP 以外のプロトコル タイプである場合でも、ポート チャネルで信頼モードを設定できます。**show pagp dual-active** コマンドの出力には、信頼モード ステータスは表示されますが、インターフェイスは表示されません。
- 信頼モードを設定するには、ポート チャネルが存在する必要があります。ポート チャネルが存在しない場合は、次のエラー メッセージが表示されます。

```
Router(config-vs-domain)# dual-active trust pagp channel-group 30
Port-channel 30 not configured
```

- 信頼できるポートが削除されると、信頼モードの設定が削除され、次の警告メッセージが表示されます。

```
Port-channel num is a trusted port-channel for PAgP
  dual-active detection. Restricting this
  port-channel has deleted the dual-active trust
  channel-group configuration associated with it.
```

- 信頼できるポートが仮想スイッチ ポートに変更された場合、ポートが制限されると信頼モードの設定が削除され、次の警告メッセージが表示されます。

```
Port-channel num is a trusted port-channel for PAgP
  dual-active detection. Deletion of this
  port-channel has deleted the dual-active trust
  channel-group configuration associated with it.
```

- 仮想スイッチ ポート チャネルで dual-active detection pagp trust port-channel コマンドを入力すると、次のエラー メッセージが表示されます。

```
Cannot configure dual-active trust mode on a virtual switch port-channel
```

例

次に、PAgP デュアル アクティブ検出用のインターフェイスを設定する例を示します。

```
Router(config)# switch virtual domain domain-id
Router (config-vs-domain)# dual-active detection pagp
Router (config-vs-domain)#
```

次に、PAgP デュアル アクティブ検出に使用する EtherChannel/ ポート バンドルを指定する例を示します。

```
Router(config)# switch virtual domain domain-id
Router (config-vs-domain)# dual-active detection pagp trust port-channel 20
Router (config-vs-domain)#
```

次に、fast hello デュアル アクティブ検出用にインターフェイスを設定する例を示します。

```
Router(config)# switch virtual domain domain-id
Router (config-vs-domain)# dual-active detection
Router (config-vs-domain)# exit
Router(config)# interface fastethernet 1/2/40
Router(config-if)# dual-active
WARNING: Interface FastEthernet1/2/40 placed in restricted config mode. All extraneous
configs removed!
Router(config-if)# no shutdown
```

関連コマンド

コマンド	説明
show switch virtual（仮想スイッチ）	デュアル アクティブ検出の設定とステータスに関する情報を表示します。

dual-active recovery ip address

スイッチが回復モードのときに管理インターフェイスの IP アドレスを設定するには、仮想スイッチ コンフィギュレーション サブモードで **dual-active recovery ip address** コマンドを使用します。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。

dual-active recovery [switch *num***] ip address** *ip-address ip-mask*

no dual-active recovery ip address *ip-address ip-mask*

構文の説明

switch *num*	（任意）IP アドレスを使用する必要があるシャーシの仮想スイッチの番号。指定しない場合、両方のスイッチに同じ IP アドレスが使用されます。
ip-address	IP アドレスを指定します。
ip-mask	IP アドレス マスクを指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

仮想スイッチ コンフィギュレーション サブモード（config-vs-domain）

コマンド履歴

リリース	変更箇所
Cisco IOS XE 3.4.0SG および 15.1(2)SG	Catalyst 4500 シリーズ スイッチでこのコマンドがサポートされるようになりました。

使用上のガイドライン

このコマンドは最大 3 つの IP アドレスを使用できます。スイッチ 1、スイッチ 2、グローバル IP アドレスに 1 つずつ使用します。スイッチが回復モードを開始すると、管理インターフェイス用に設定されたスイッチ固有の回復 IP アドレスが選択されます。スイッチ固有の IP アドレスが未設定の場合、グローバル回復 IP アドレスが使用されます。スイッチ固有の回復 IP アドレスもグローバル回復 IP アドレスも設定されていない場合は、スイッチが回復モードを開始しても、スイッチ上の fastEthernet1 管理インターフェイスにアクティブな IP アドレスがない状態になります。

インターフェイス コンフィギュレーション モードで fastEthernet1 に設定された通常の IP アドレスは、設定が保持されます。

例

次に、グローバル回復 IP アドレスを設定する例を示します。

```
Switch(config)# switch virtual domain domain-id
Switch(config-vs-domain)# dual-acti
ve recovery ip address 192.168.1.5 255.255.255.0
Switch(config-vs-domain)# exit
```

関連コマンド

コマンド	説明
dual-active detection（仮想スイッチ）	仮想スイッチのデュアル アクティブ検出を設定します。
show switch virtual（仮想スイッチ）	デュアル アクティブ検出の設定とステータスに関する情報を表示します。

duplex

インターフェイスでデュプレックス動作を設定するには、**duplex** 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。

duplex {**auto** | **full** | **half**}

no duplex

構文の説明

auto	自動ネゴシエーション動作を指定します。
full	全二重動作を指定します。
half	半二重動作を指定します。

デフォルト

半二重動作

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

表 2-1 に、サポートされているコマンド オプションをインターフェイス別に示します。

表 2-1　サポートされている duplex コマンド オプション

インターフェイス タイプ	サポートされている構文	デフォルト設定	注意事項
10/100 Mbps モジュール	**duplex** [**half** | **full**]	**half**	速度が **auto** に設定されている場合は、**duplex** モードを設定できません。 速度が **10** または **100** に設定されている場合にデュプレックス設定を行わないと、デュプレックス モードは**半二重**に設定されます。
100 Mbps ファイバ モジュール	**duplex** [**half** | **full**]	**half**	

表 2-1　サポートされている duplex コマンド オプション

インターフェイス タイプ	サポートされている構文	デフォルト設定	注意事項
ギガビット イーサネット インターフェイス	サポートされていません。	サポートされていません。	ギガビット イーサネット インターフェイスは **全二重**に設定されます。
10/100/1000	**duplex** [**half** | **full**]		速度が **auto** または **1000** に設定されている場合は、**duplex** を設定できません。 速度が **10** または **100** に設定されている場合にデュプレックス設定を行わないと、デュプレックス モードは **半二重**に設定されます。

16 ポート RJ-45 ギガビット イーサネット ポートの送信速度が **1000** に設定されている場合、デュプレックス モードは **full** に設定されます。送信速度が **10** または **100** に変更された場合でも、デュプレックス モードは **full** のままです。送信速度が 1000 Mbps から **10** または **100** に変更された場合は、スイッチのデュプレックス モードを正しく設定する必要があります。

注意　インターフェイス速度およびデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

表 2-2 に、デュプレックス モードおよび速度モードをさまざまに組み合わせた場合のシステム パフォーマンスを示します。指定した **duplex** コマンドと **speed** コマンドの設定の組み合わせによって、表に示す動作が行われます。

表 2-2　duplex コマンドと speed コマンドの関係

duplex コマンド	speed コマンド	システムの動作
duplex half または **duplex full**	**speed auto**	速度モードとデュプレックス モードの両方を自動ネゴシエーションします。
duplex half	**speed 10**	強制的に 10 Mbps および半二重になります。
duplex full	**speed 10**	強制的に 10 Mbps および全二重になります。
duplex half	**speed 100**	強制的に 100 Mbps および半二重になります。
duplex full	**speed 100**	強制的に 100 Mbps および全二重になります。
duplex full	**speed 1000**	強制的に 1000 Mbps および全二重になります。

例

次の例では、インターフェイスを全二重動作に設定する方法を示します。

```
Switch(config-if)# duplex full
Switch(config-if)#
```

関連コマンド

コマンド	説明
speed	インターフェイス速度を設定します。
interface（Cisco IOS のマニュアルを参照）	インターフェイスを設定します。

コマンド	説明
show controllers（Cisco IOS のマニュアルを参照）	コントローラ情報を表示します。
show interfaces	インターフェイス情報を表示します。

energywise（グローバル コンフィギュレーション）

エンティティで EnergyWise をイネーブルにして設定するには **energywise** 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。エンティティ上で EnergyWise をディセーブルにしたり、EnergyWise 設定を削除したりするには、このコマンドの **no** 形式を使用します。

energywise {**importance** *importance* | **keywords** *word,word,...* | **level** *level* | **management** *tcp-port-number* | **name** *name* | **neighbor** *hostname* | *ip-address udp-port-number* | **role** *role*}

no energywise {**importance** | **keywords** | **level** | **management** | **name** | **neighbor** | **role**}

構文の説明

importance *importance*	エンティティの重要度を設定します。 範囲は 1 ～ 100 です。
keywords *word,word,...*	エンティティのキーワードを 1 つ以上割り当てます。 複数のキーワードを割り当てる場合は、各キーワードをカンマで区切ります。キーワードの区切り文字としてスペースを使用しないでください。 *word* 値についての注意点は、次のとおりです。 • 英数字と、#、(、%、!、& などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
level *level*	エンティティの電力レベルを設定します。 有効な値は 10 のみです。
management *tcp-port-number*	管理ステーションに接続する TCP ポートを指定します。 指定できる範囲は 1 ～ 65000 です。
name *name*	EnergyWise 固有のエンティティ名を指定します。 *name* 値についての注意点は、次のとおりです。 • 英数字と、#、(、%、!、& などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
neighbor *hostname* | *ip-address udp-port-number*	スタティック ネイバーを割り当てます。 • ホスト名（*hostname*）または IP アドレス（*ip-address*）。 • クエリーを送受信する UDP ポート（*udp-port-number*）。指定できる範囲は 1 ～ 65000 です。
role *role*	EnergyWise ドメインでのエンティティのロールを指定します。たとえば、lobby.b20 とします。 *role* 値についての注意点は、次のとおりです。 • 英数字と、#、(、%、!、& などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。

デフォルト

重要度は 1 です。

キーワードは定義されません。

電力レベルは 10 です。

tcp-port-number は 43440 です。

名前はホスト名です。

ネイバーは割り当てられません。

ロールはモデル番号です。

コマンド モード

設定

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

エンティティをドメインに追加すると、エンティティおよびその PoE ポートで EnergyWise がイネーブルにされます。

例

次の例では、EnergyWise をイネーブルにし、エンティティをドメインに割り当ててパスワードを設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
Switch(config)# energywise importance 50
Switch(config)# energywise keywords lab1,devlab
Switch(config)# energywise management 60500
Switch(config)# energywise name Entity01
Switch(config)# energywise neighbor 4500-21 43440
Switch(config)# energywise role role.lobbyaccess
Switch(config)# end
```

関連コマンド

コマンド	説明
show energywise	EnergyWise の設定とステータスを表示します。

energywise（インターフェイス コンフィギュレーション）

Power over Ethernet（PoE）ポートで EnergyWise を設定するには、**energywise** 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。ポート上で EnergyWise をディセーブルにしたり、EnergyWise 設定を削除したりするには、このコマンドの **no** 形式を使用します。

energywise [**importance** *importance* | **keywords** *word,word,...* | **level** *level* [**recurrence at** *minute hour day_of_month month day_of_week*] | **name** *name* | **role** *role*]

no energywise

構文の説明

importance *importance*	（任意）ポートの重要度を設定します。 範囲は 1 ～ 100 です。
keywords *word,word,...*	（任意）ポートに少なくとも 1 つのキーワードを割り当てます。 複数のキーワードを割り当てる場合は、各キーワードをカンマで区切ります。キーワードの区切り文字としてスペースを使用しないでください。 *word* 値についての注意点は、次のとおりです。 • 英数字と、#、(、%、!、& などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
level *level*	（任意）ポートの電力レベルを設定します。 有効な値は 0 および 10 のみです。

recurrence importance *importance* **at** *minute hour day_of_month month day_of_week*	（任意）電源オンまたは電源オフの繰り返しをスケジューリングします。 • **importance** *importance*：ドメイン内のポートの重要度を設定します。範囲は 1 ～ 100 です。 • *minute*：指定できる範囲は 0 ～ 59 です。***** をワイルドカードとして使用します。 • *hour*：指定できる範囲は 0 ～ 23 です。***** をワイルドカードとして使用します。 • *day_of_month*：指定できる範囲は 1 ～ 31 です。* をワイルドカードとして使用します。 • *month*：有効値の範囲は 1 ～ 12 です。**jan**、**feb**、**mar**、**apr** などと入力することもできます。***** をワイルドカードとして使用します。 • *day_of_week*：有効値の範囲は 0 ～ 7 です（0 と 7 はどちらも日曜日を表します）。***** をワイルドカードとして使用します。 **（注）** 指定する時刻は、PoE エンティティの時間帯に基づく現地時間です。 **（注）** 日にちと曜日をどちらも指定すると（つまり、ワイルドカードではない）、いずれかのフィールドが現在時刻に一致したときに繰り返しが実行されます。 **（注）** 繰り返しは、指定した分きっかりではなく、そこから 1 分以内に実行されます。したがって、60 秒ほど遅れて行われる場合があります。
name *name*	（任意）EnergyWise 固有のポート名を指定します。 *name* 値についての注意点は、次のとおりです。 • 英数字と、#、(、%、!、& などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
role *role*	（任意）ドメインでのポートのロールを指定します。たとえば、lobbyport とします。 *role* 値についての注意点は、次のとおりです。 • 英数字と、#、(、%、!、& などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。

デフォルト

重要度は 1 です。

キーワードは定義されません。

電力レベルは 10 です。

この名前は、インターフェイス名の短縮バージョンです。たとえば、ギガビット イーサネット 1/2 の場合は Gi1.2 となります。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが追加されました。

使用上のガイドライン

importance 値および **level** 値をデフォルト設定に戻すには、**default energywise importance** コマンドおよび **default energywise level** コマンドを使用します。

例

次の例では、PoE ポートで EnergyWise をイネーブルにして設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
Switch(config)# interface Gi1.2
Switch(config-if)# energywise level 10 recurrence importance 90 at 0 8 * * *
Switch(config-if)# energywise level 0 recurrence importance 90 at 0 20 * * *
Switch(config-if)# energywise inportance 50
Switch(config-if)# energywise name lobbyInterface.3
Switch(config-if)# energywise role role.lobbyaccess
Switch(config-if)# end
```

（注） 繰り返しは、指定した分きっかりではなく、そこから 1 分以内に実行されます。したがって、60 秒ほど遅れて行われる場合があります。

関連コマンド

コマンド	説明
show energywise	EnergyWise の設定とステータスを表示します。

energywise domain

エンティティで EnergyWise をイネーブルにし、そのエンティティをドメインに割り当て、ドメイン内のエンティティ間の通信を保護するパスワードを設定するには、**energywise domain** 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。エンティティ上で EnergyWise をディセーブルにしたり、EnergyWise 設定を削除したりするには、このコマンドの **no** 形式を使用します。

energywise domain *domain-name* **secret** [**0** | **7**] *password* [**protocol udp port** *udp-port-number* [**interface** *interface-id* | **ip** *ip-address*]]

no energywise domain

構文の説明

domain *domain-name*	指定した *domain-name* を持つドメインにエンティティを割り当てます。 • 英数字と、#、(、%、!、& などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
secret [**0** | **7**] ***password***	ドメイン内のエンティティ間の通信を保護する *password* を設定します。 • （任意）**0**：暗号化されていないパスワードを使用します。 • （任意）**7**：非表示パスワードを使用します。この場合は、service password-encryption をイネーブルにする必要があります。 **0** も **7** も入力しなかった場合、エンティティでは、デフォルト値の 0 を使用します。 *password* 値についての注意点は、次のとおりです。 • 英数字と、#、(、%、!、& などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
port *udp-port-number*	（任意）クエリーを送受信する UDP ポートを指定します。 指定できる範囲は 1 ～ 65000 です。
interface *interface-id*	（任意）ブリッジ型ネットワークで他の EnergyWise スイッチと通信するインターフェイスを、スイッチが選択するのではなく（デフォルト）、自分で指定します。
ip *ip-address*	（任意）ルーテッド ネットワークで、EnergyWise ピアとの通信で使用する IP アドレスを指定します。システムが選択したデフォルト値は使用しません。 **interface** オプションおよび **ip** オプションは相互に排他的な関係です。

デフォルト

エンティティはドメインに割り当てられていません。

パスワードは設定されていません。

udp-port-number は 43440 です。

コマンド モード

設定

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが追加されました。

使用上のガイドライン

energywise domain *domain-name* **secret** [**0** | **7**] *password* コマンドを入力すると、エンティティでは、ネットワークとの通信および管理アプリケーションとの通信に使用可能な最初のインターフェイスを選択します。

例

次の例では、EnergyWise をイネーブルにし、*domain-name* および *password* の値を設定する方法を示します。

```
Switch(config)# energywise domain cisco secret cisco protocol udp port 43440 ip 2.2.4.30
```

次の例では、EnergyWise をイネーブルにし、管理アプリケーションへのルートを指定する方法を示します。

```
Switch(config)# energywise domain cisco secret 0 cisco protocol udp port 43440 ip
192.168.1.2
```

関連コマンド

コマンド	説明
show energywise	EnergyWise の設定とステータスを表示します。

energywise query

クエリーを実行して、電力情報を表示したり、エンティティまたは PoE ポートに電力を供給したりするには、**energywise query** 特権 EXEC コマンドを使用します。

energywise query importance *importance* {**keywords** *word,word,...* | **name** *name*} **collect** {**delta** | **usage**}

energywise query importance *importance* {**keywords** *word,word,...* | **name** *name*} **set level** *level*

energywise query importance *importance* {**keywords** *word,word,...* | **name** *name*} **sum** {**delta** | **usage**}

構文の説明

importance ***importance***	エンティティまたはポートの重要度を設定します。 範囲は 1 ～ 100 です。
keywords *word,word,...*	クエリーで使用する 1 つまたは複数のキーワードを指定します。 複数のキーワードを指定するときは、各キーワードをカンマで区切ります。キーワード間にスペースを使用しないでください。 *word* 値についての注意点は、次のとおりです。 • 英数字と、#、(、%、!、& などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
name ***name***	クエリーで使用する名前。 ワイルドカードの場合は、* を使用するか、または name の終わりにアスタリスクを付けて *name** とします。 *name* 値についての注意点は、次のとおりです。 • 英数字と、#、(、%、!、& などの記号を入力できます。 • 文字や記号の間にアスタリスク（*）や空白を使用しないでください。
collect {**delta** | **usage**}	エンティティまたは PoE ポートの delta 値または usage 値を表示します。 • **delta**：現行の電力レベルと使用可能な電力レベルの差異だけを表示します。 • **usage**：現行の消費電力だけを表示します。
set level *level*	エンティティまたは PoE ポートの電力レベルを設定します。 エンティティの場合、有効な値は 10 だけです。 ポートの場合、有効な値は 0 および 10 です。
sum {**delta** | **usage**}	エンティティまたは PoE ポートの delta 値または usage 値の合計を表示します。 • **delta**：現行の電力レベルと使用可能な電力レベルの差異の合計だけを表示します。 • **usage**：現行の消費電力の合計だけを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ポートを電源オンまたは電源オフにするには、**energywise query** {**keywords** *word,word,...* | **name** *name*} **set level** *level* コマンドを入力します。

注意　このクエリーは、コマンドを入力したエンティティおよびクエリー基準と一致するドメイン内の他のデバイスに影響するため、使用する場合は注意が必要です。

例

次の例では、エンティティ名をフィルタリングする方法をいくつか示します。

```
Switch# energywise query importance 100 name phone* collect usage
EnergyWise query, timeout is 3 seconds:

Host            Name            Usage
----            ----            -----
2.2.2.21        phone           0.0 (W)
2.2.2.21        phone           15.4 (W)
2.2.2.21        phone           0.0 (W)
2.2.2.22        phone           0.0 (W)
2.2.2.21        phone           0.0 (W)
2.2.2.22        phone           15.4 (W)
2.2.2.21        phone           0.0 (W)
2.2.2.23        phone           15.4 (W)
2.2.2.21        phone           0.0 (W)

Queried:  9    Responded:  9      Time:  0.26 seconds

Switch# energywise query importance 100 name * sum usage
EnergyWise query, timeout is 3 seconds:

Total Usage
-----------
346.3 (W)

Queried:  147    Responded:  147      Time:  0.121 seconds

Switch# energywise query importance 100 name lobby* collect usage

EnergyWise query, timeout is 3 seconds:

Host            Name              Usage
----            ----              -----
2.2.4.30        lobbyInterface.17 10.0 (W)

Queried:  1    Responded:  1      Time:  0.7 seconds

Switch# energywise query importance 100 name Fa1.0.4* sum usage

EnergyWise query, timeout is 3 seconds:

Total Usage
-----------
12.9 (W)

Queried:  10    Responded:  10      Time:  0.6 seconds
```

次の例では、delta 値の合計およびドメイン内の潜在的な電力変化を示します。

```
Switch# energywise query importance 100 name * sum delta
EnergyWise query, timeout is 3 seconds:

Level   Label       Delta Power (W)
-----   -----       -----------
0       Shut        -12.9
1       Hibernate   +723.8
2       Sleep       +723.8
3       Standby     +723.8
4       Ready       +723.8
5       Low         +723.8
6       Frugal      +723.8
7       Medium      +723.8
8       Reduced     +723.8
9       High        +723.8
10      Full        +723.8

Queried:  48    Responded:  48      Time:  0.15 seconds
```

次の例では、ドメイン内の消費レベルを示します。

```
Switch# show energywise children
Interface   Role              Name                  Usage      Lvl   Imp  Type
---------   ----              ----                  -----      ---   ---  ----
            control           SwitchA               86.0  (W)  10    100  parent
Gi1/0/1     interface         Gi1.0.1               0.0   (W)  10    20   child
.
.
.
Gi1/0/6     interface         Gi1.0.6               0.0   (W)  10    20   child
Gi1/0/7     role.lobbyaccess  lobbyInterface.7      0.0   (W)  10    50   child
Gi1/0/8     interface         Gi1.0.8               0.0   (W)  10    20   child
<output truncated>

Switch# energywise query importance 100 name * set level 0
EnergyWise query, timeout is 3 seconds:

Success rate is (0/0) setting entities

Queried:  0    Responded:  0      Time:  0.996 seconds

Switch# energywise query importance 100 name * set level 10
EnergyWise query, timeout is 3 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!
Success rate is (48/48) setting entities
```

次の例では、エンティティでキーワードを割り当てる方法を示します。

```
Switch(config)# interface Gi1/2
Switch(config-if)# energywise keywords lobby,sattelite
Switch(config-if)# energywise keywords public
Switch(config-if)# end
Switch# show running-config interface gigabitethernet1/0/2
!
interface GigabitEthernet1/2
energywise level 0 recurrence importance 90 at 0 8 * * *
 energywise level 10 recurrence importance 90 at 0 20 * * *
 energywise importance 50
 energywise role role.lobbyaccess
 energywise keywords lobby,sattelite,public
 energywise name lobbyInterface.2
```

```
end

Switch# energywise query keyword lobby collect usage
EnergyWise query, timeout is 3 seconds:

Host            Name              Usage
----            ----              -----
2.2.4.30        lobbyInterface.17 15.4 (W)

Queried:  1    Responded:  1      Time:  0.0 seconds


Switch# energywise query keyword satellite sum usage
EnergyWise query, timeout is 3 seconds:

Total Usage
-----------
15.4 (W)

Queried:  1    Responded:  1      Time:  0.11 seconds
```

epm access control

アクセス コントロールを設定するには、**epm access control [open | default]** コマンドを使用します。

epm access control [open | default]

構文の説明

open	オープン アクセス コントロールを指定します。
default	デフォルトのアクセス コントロールを指定します。

デフォルト

epm access control コマンドが設定されていない場合、動作は **epm access control default** コマンドにデフォルト設定されます。NVGEN に格納されるものはありません。

コマンド モード

コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(54)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

epm access control コマンドを入力すると、NVGEN に格納されます。

ホストの認証時に ACL が ACS サーバからダウンロードされていない場合、ホストはポート ACL により制限され、追加の許可を受信しません。このような場合は、**epm access control open** コマンドを入力すると、認証後、ホストに対して **permit ip** *host* の任意のエントリが作成されます。このエントリは、ACL が ACS からダウンロードされない場合にだけ作成されます。

epm access control open コマンドは認証オープン モードで特に役立ちます。ホストが認証される前でも、ホストからのトラフィックは通過を許可されます。このトラフィックは、ポート ACL によって制限されます。このような場合は、ACL が ACS からダウンロードされない場合、そのホストは追加の許可を受信しません。認証の後でも、ホストは引き続きポート ACL によって制限されます。**epm access control open** が設定されている場合、認証後に完全なアクセスが与えられます。

epm access control default が設定され、ACL がダウンロードされない場合、ポート ACL がポート上の唯一の ACL です。これが、Cisco IOS Release 12.2(54) SG 以前のアクセス コントロールの機能です。

例

次の例では、オープン アクセス コントロールをイネーブルにする方法を示します。

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

次の例では、デフォルトのアクセス コントロールをイネーブルにする方法を示します。

```
Switch(config)# epm access control default
```

関連コマンド

コマンド	説明
show ipv6 snooping counters	RA ガードによってポートごとにドロップされたパケットの数を表示します。

erase

ファイル システムを消去するには、**erase** コマンドを使用します。

erase {**/all** [**non-default** | **nvram:**] | **cat4000_flash** | **nvram:** | **startup-config**}

構文の説明

/all nvram:	NVRAM 内のすべての内容を消去します。
/all non-default	NVRAM、ブートフラッシュ、cat4000_flash、crashinfo など、ローカル スーパーバイザ エンジンの不揮発性ストレージ内にあるファイルおよび設定を消去します。Catalyst 4500 シリーズ スイッチは、工場出荷時設定にリセットされます。 **（注）** このコマンド オプションは、スタンドアロンのスーパーバイザ エンジンのみが対象です。
cat4000_flash:	VLAN データベースのコンフィギュレーション ファイルを消去します。
nvram:	NVRAM 内の startup-config ファイルおよび private-config ファイルを消去します。
startup-config:	NVRAM 内の startup-config ファイルおよび private-config ファイルを消去します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
12.2(25)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

注意 **erase** コマンドを使用してファイル システムを消去すると、そのファイル システム内のファイルは回復できません。

デュアル スーパーバイザ エンジンを搭載している冗長構成スイッチのコマンド ヘルプ メッセージには、上記のコマンド オプションの他に、slave というプレフィックスの付いたオプションが表示されます。このオプションは、NVRAM およびフラッシュ（slavenvram: や slavecat4000_flash: など）の識別に使用されます。

erase nvram: コマンドは、**write erase** コマンドおよび **erase startup-confg** コマンドに替わるコマンドです。このコマンドは、startup-config ファイルおよび private-config ファイルを両方とも消去します。

erase /all nvram: コマンドは、startup-config ファイルおよび private-config ファイルの他に、NVRAM 内のすべてのファイルを消去します。

erase cat4000_flash: コマンドは、VLAN データベース コンフィギュレーション ファイルを消去します。

erase /all non-default コマンドは、製造工場および修理センターで作業の効率化に役立ちます。このコマンドは、不揮発性ストレージに格納された設定および状態を消去し、Catalyst 4500 シリーズ スイッチを工場出荷時設定にリセットします。デフォルト設定には、Cisco IOS ライブラリの説明にある設定と、**erase /all non-default** コマンド（vtp mode=transparent、ROMMON 変数 ConfigReg=0x2101、PS1= "rommon ! >" および EnableAutoConfig=1）によって行われた設定が含まれています。

デフォルト設定については、次のガイドを参照してください。

- 『*Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4*』（次の URL）
  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_4/cf_12_4_book.html
- 『*Cisco IOS Configuration Fundamentals Configuration Command Reference, Release 12.2*』（次の URL）
  http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/ffun_r.html

注意　**erase /all non-default** コマンドを実行すると、ブートフラッシュ内にある Cisco IOS イメージが消去されます。（アクセス可能な TFTP サーバや、ほとんどのシャーシ モデルに用意されている slot0 に挿入されたフラッシュ カードなどから）Cisco IOS イメージをブートフラッシュに再コピーできること、またはアクセス可能なネットワーク サーバに格納されたイメージからスイッチを起動できることを確認してください。

例

次の例では、非揮発性ストレージ内のファイルおよび設定を消去し、スイッチを工場出荷時設定にリセットする方法を示します。

```
Switch# erase /all non-default
Switch#
Erase and format operation will destroy all data in non-volatile storage.  Continue?
[confirm]
Formatting bootflash: ...

Format of bootflash complete
Erasing nvram:
Erasing cat4000_flash:
Clearing crashinfo:data
Clearing the last power failure timestamp
Clearing all ROMMON variables
Setting default ROMMON variables:
     ConfigReg=0x2101
     PS1=rommon ! >
     EnableAutoConfig=1
Setting vtp mode to transparent
%WARNING! Please reboot the system for the changes to take effect
Switch#
00:01:48: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

次の例では、NVRAM の内容を消去する方法を示します。

```
Switch# erase /all nvram:
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
00:38:10: %SYS-7-NV_BLOCK_INIT: Initalized the geometry of nvram
```

```
Switch#
```

次の例では、ファイル システム cat4000_flash を消去する方法を示します。

```
Switch# erase cat4000_flash:
Erasing the cat4000_flash filesystem will remove all files! Continue? [confirm]
[OK]
Erase of cat4000_flash:complete
Switch#
```

関連コマンド

コマンド	説明
boot config（Cisco IOS のマニュアルを参照）	コンフィギュレーション ファイルのデバイスおよびファイル名を指定します。
delete（Cisco IOS のマニュアルを参照）	フラッシュ メモリ デバイスまたは NVRAM からファイルを削除します。
show bootvar	BOOT 環境変数情報を表示します。
undelete（Cisco IOS のマニュアルを参照）	クラス A フラッシュ ファイル システムで「削除」マークが付いたファイルを回復します。

errdisable detect

errdisable 検出をイネーブルにするには、**errdisable detect** コマンドを使用します。errdisable 検出機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

errdisable detect cause {**all** | **arp-inspection** [**action shutdown vlan**] | **bpduguard shutdown vlan** | **dhcp-rate-limit** [**action shutdown vlan**] | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap**}

no errdisable detect cause {**all** | **arp-inspection** [**action shutdown vlan**] | **bpduguard shutdown vlan** | **dhcp-rate-limit** [**action shutdown vlan**] | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap**}

構文の説明

cause	errdisable 検出を指定して、特定の原因の検出を行います。
all	すべての errdisable 原因の errdisable 検出を指定します。
arp-inspection	ARP インスペクション errdisable 原因の検出を指定します。
action shutdown vlan	（任意）ARP インスペクションおよび DHCP レート制限で VLAN ごとに errdisable を指定します。
bpduguard shutdown vlan	BPDU ガードで VLAN ごとに errdisable を指定します。
dhcp-rate-limit	DHCP レート制限 errdisable 原因の検出を指定します。
dtp-flap	DTP フラップ errdisable 原因の検出を指定します。
gbic-invalid	GBIC 無効 errdisable 原因の検出を指定します。
l2ptguard	レイヤ 2 プロトコル トンネル errdisable 原因の検出を指定します。
link-flap	リンク フラップ errdisable 原因の検出を指定します。
pagp-flap	PAgP フラップ errdisable 原因の検出を指定します。

デフォルト

すべての errdisable 原因が検出されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(52)SG	VLAN 単位の errdisable 検出のサポートが追加されました。

使用上のガイドライン

原因（dtp-flap、link-flap、pagp-flap）は、errdisable ステートが発生する理由として定義されます。インターフェイスで原因が検出されると、そのインターフェイスは errdisable ステート（リンクダウンステートに類似した動作ステート）になります。

インターフェイスを errdisable ステートから手動で回復するには、**shutdown** コマンドを入力してから **no shutdown** コマンドを入力する必要があります。

ポートがシャットダウンされないようにするために、**shutdown vlan** オプションを使用して、違反が発生したポートで問題の VLAN だけをシャットダウンできます。このオプションは、bpduguard、arp-inspection、および dhcp-rate-limit の 3 つの原因に対して使用できます。**clear errdisable** コマンドを使用すると、ポートでディセーブルになっている VLAN を回復できます。

例

次の例では、リンクフラップ errdisable 原因の errdisable 検出をイネーブルにする方法を示します。

```
Switch(config)# errdisable detect cause link-flap
Switch(config)#
```

次の例では、BPDU ガードで VLAN ごとに errdisable 検出をイネーブルにする方法を示します。

```
Switch(config)# errdisable detect cause bpduguard shutdown vlan
Switch(config)#
```

次の例では、DAI で errdisable 検出をディセーブルにする方法を示します。

```
Switch(config)# no errdisable detect cause arp-inspection
Switch(config)# end
Switch# show errdisable detect
ErrDisable Reason    Detection   Mode
-----------------    ----------  ------
arp-inspection       Enabled     port
bpduguard            Enabled     vlan
channel-misconfig    Enabled     port
dhcp-rate-limit      Enabled     port
dtp-flap             Enabled     port
gbic-invalid         Enabled     port
psecure-violation    Enabled     port/vlan
Switch#
```

関連コマンド

コマンド	説明
show errdisable detect	errdisable 検出ステータスを表示します。
show interfaces status	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

errdisable recovery

回復メカニズム変数を設定するには、**errdisable recovery** 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。

errdisable recovery [**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **pesecure-violation** | **security-violation** | **storm-control** | **udld** | **unicastflood** | **vmps**} [**arp-inspection**] [**interval** {*interval*}]]

no errdisable recovery [**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **pesecure-violation** | **security-violation** | **storm-control** | **udld** | **unicastflood** | **vmps**} [**arp-inspection**] [**interval** {*interval*}]]

構文の説明

cause	（任意）errdisable 回復をイネーブルにして特定の原因から回復します。
all	（任意）すべての errdisable 原因の回復タイマーをイネーブルにします。
arp-inspection	（任意）ARP インスペクション原因の回復タイマーをイネーブルにします。
bpduguard	（任意）BPDU ガード errdisable 原因の回復タイマーをイネーブルにします。
channel-misconfig	（任意）チャネル設定ミス errdisable 原因の回復タイマーをイネーブルにします。
dhcp-rate-limit	（任意）DHCP レート制限 errdisable 原因の回復タイマーをイネーブルにします。
dtp-flap	（任意）DTP フラップ errdisable 原因の回復タイマーをイネーブルにします。
gbic-invalid	（任意）GBIC 無効 errdisable 原因の回復タイマーをイネーブルにします。
l2ptguard	（任意）レイヤ 2 プロトコル トンネル errdisable 原因の回復タイマーをイネーブルにします。
link-flap	（任意）リンク フラップ errdisable 原因の回復タイマーをイネーブルにします。
pagp-flap	（任意）PAgP フラップ errdisable 原因の回復タイマーをイネーブルにします。
pesecure-violation	（任意）pesecure 違反 errdisable 原因の回復タイマーをイネーブルにします。
security-violation	（任意）802.1X セキュリティ違反によりディセーブルになったポートの自動回復をイネーブルにします。
storm-control	（任意）ストーム制御 errdisable ステートから回復するタイマーをイネーブルにします。
udld	（任意）UDLD errdisable 原因の回復タイマーをイネーブルにします。
unicastflood	（任意）ユニキャスト フラッド errdisable 原因の回復タイマーをイネーブルにします。
vmps	（任意）VMPS errdisable 原因の回復タイマーをイネーブルにします。
arp-inspection	（任意）ARP インスペクション原因および回復タイムアウトをイネーブルにします。
interval *interval*	（任意）指定した errdisable 原因から回復する時間を指定します。有効値の範囲は 30 ～ 86400 秒です。

デフォルト

errdisable 回復はディセーブルです。

回復間隔は 300 秒に設定されています。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(19)EW	ストーム制御機能のサポート。

使用上のガイドライン

原因（bpduguard、dtp-flap、link-flap、pagp-flap、udld）は、errdisable ステートが発生する理由として定義されます。インターフェイスで原因が検出されると、そのインターフェイスは errdisable ステート（リンクダウン ステートに類似した動作ステート）になります。原因に対する errdisable 回復をイネーブルにしない場合、インターフェイスは shutdown および no shutdown が実行されるまで errdisable ステートのままです。原因の回復をイネーブルにした場合、インターフェイスは errdisable ステートから回復し、すべての原因がタイムアウトになったときに処理を再開できるようになります。

インターフェイスを errdisable から手動で回復するには、**shutdown** コマンドを入力してから **no shutdown** コマンドを入力する必要があります。

例

次の例では、BPDU ガード errdisable 原因の回復タイマーをイネーブルにする方法を示します。

```
Switch(config)# errdisable recovery cause bpduguard
Switch(config)#
```

次に、タイマーを 300 秒に設定する例を示します。

```
Switch(config)# errdisable recovery interval 300
Switch(config)#
```

次の例では、ARP インスペクションの errdisable 回復をイネーブルにする方法を示します。

```
Switch(config)# errdisable recovery cause arp-inspection
Switch(config)# end
Switch# show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Enabled

Timer interval: 300 seconds
```

```
Interfaces that will be enabled at the next timeout:

Switch#
```

関連コマンド

コマンド	説明
show errdisable detect	errdisable 検出ステータスを表示します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

export-protocol（netflow-lite エクスポータ サブモード）

（注）　NetFlow-lite は Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチでのみサポートされます。

NetFlow-lite コレクタのエクスポート プロトコルを指定するには、**export-protocol** コマンドを使用します。この値を削除するには、このコマンドの **no** 形式を使用します。

export-protocol {**netflow-v9** | **ipfix**}

no export-protocol {**netflow-v9** | **ipfix**}

構文の説明

netflow-v9	Netflow V9 のエクスポート フォーマットを指定します。
ipfix	Netflow V10 または IPFIX のエクスポート フォーマットを指定します。

デフォルト

netflow-v9

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)SG	このコマンドが Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチに追加されました。

使用上のガイドライン

デフォルトでは、エクスポート プロトコルは Netflow V9 です。IPFIX または Netflow V10 は新しいエクスポート フォーマットです。これらは、元のサンプリング パケットから抽出される実際のパケット セクション バイトに従ってサンプル パケットのより効率的なパッケージングを可能にする可変長符号化をサポートします。

例

次の例では、NetFlow-lite コレクタのエクスポート プロトコルを指定する方法を示します。

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
```

```
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#

Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite  Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address:   5.5.5.6
    Source IP Address:        5.5.5.5
    VRF label:
    DSCP:                     0x20
    TTL:                      128
    COS:                      7
  Transport Protocol Configuration:
    Transport Protocol:       UDP
    Destination Port:         8188
    Source Port:              61670
  Export Protocol Configuration:
    Export Protocol:                  netflow-v9
    Template data timeout:            60
    Options sampler-table timeout:    1800
    Options interface-table timeout:  1800
  Exporter Statistics:
    Packets Exported:         0
```

show netflow-lite exporter 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
netflow-lite exporter	エクスポータを定義し、NetFlow-lite エクスポータ サブモードを開始します。
destination（netflow-lite エクスポータ サブモード）	netflow-lite サブモードでの宛先アドレスを指定します。
source（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの送信元レイヤ 3 インターフェイスを指定します。
transport udp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの UDP トランスポート宛先ポートを指定します。
ttl（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの TTL 値を指定します。
cos（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの CoS 値を指定します。
dscp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの CoS 値を指定します。
template data timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのテンプレート データ タイムアウトを指定します。
options timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのオプションのタイムアウトを指定します。

exporter（netflow-lite モニタ サブモード）

（注）　NetFlow-lite は Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチでのみサポートされます。

netflow-lite モニタ サブモードのエクスポータを割り当てるには、**exporter** コマンドを使用します。サンプラを削除するには、このコマンドの **no** 形式を使用します。

exporter *exporter-name*

no exporter *exporter-name*

構文の説明

exporter-name	エクスポータを指定します。

デフォルト

なし

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)SG	このコマンドが Catalyst 4948E および Catalyst 4948E-F イーサネット スイッチに追加されました。

使用上のガイドライン

物理ポート インターフェイス モード、ポート チャネル インターフェイス モード、または config VLAN モードでこのコマンドを入力できます。

例

次の例では、ポートのギガビット インターフェイス 1/3 のモニタを設定する方法を示します。

```
Switch# config terminal
Switch(config)# int GigabitEthernet1/3
Switch(config-if)# netflow-lite monitor 1
Switch(config-netflow-lite-monitor)# sampler sampler1
Switch(config-netflow-lite-monitor)# average-packet-size 128
Switch(config-netflow-lite-monitor)# exporter exporter1
Switch(config-netflow-lite-monitor)# exit
Switch(config-if)# exit
Switch(config)# exit
Switch# show netflow-lite monitor 1 interface gi1/3
Interface GigabitEthernet1/3:
  Netflow-lite  Monitor-1:
    Active:               TRUE
    Sampler:              sampler1
    Exporter:             exporter1
    Average Packet Size:  0
  Statistics:
    Packets exported:     0
```

```
Packets observed:      0
Packets dropped:       0
Average Packet Size observed: 64
Average Packet Size used: 64
```

show netflow-lite exporter 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
sampler（netflow-lite モニタ サブモード）	netflow-lite モニタ サブモードのインターフェイスでサンプリングをアクティブにします。
average-packet-size（netflow-lite モニタ サブモード）	観測ポイントでの平均パケット サイズを指定します。
exporter（netflow-lite モニタ サブモード）	netflow-lite モニタ サブモードのエクスポータを割り当てます。

flowcontrol

ポーズ フレームを送受信するようにギガビット イーサネット インターフェイスを設定するには、**flowcontrol** コマンドを使用します。フロー制御設定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。

flowcontrol {**receive** | **send**} {**off** | **on** | **desired**}

no flowcontrol {**receive** | **send**} {**off** | **on** | **desired**}

構文の説明

receive	インターフェイスがポーズ フレームを処理するように指定します。
send	インターフェイスがポーズ フレームを送信するように指定します。
off	ローカル ポートがリモート ポートからポーズ フレームを受信して処理したり、リモート ポートにポーズ フレームを送信したりできないようにします。
on	ローカル ポートがリモート ポートからポーズ フレームを受信して処理したり、リモート ポートにポーズ フレームを送信したりできるようにします。
desired	リモート ポートが on、off、または desired のいずれに設定されていても、予測可能な結果が得られます。

デフォルト

ギガビット イーサネット インターフェイスのデフォルト設定は、次のとおりです。

- ポーズ フレームの送信は off です（非オーバーサブスクライブ ギガビット イーサネット インターフェイス）。
- ポーズ フレームの受信は desired です（非オーバーサブスクライブ ギガビット イーサネット インターフェイス）。
- ポーズ フレームの送信が on である：オーバーサブスクライブされたギガビット イーサネット インターフェイス
- ポーズ フレームの受信は desired です（オーバーサブスクライブ ギガビット イーサネット インターフェイス）。

表 2-3 に、モジュールのデフォルト設定を示します。

表 2-3　モジュールのデフォルト設定

モジュール	ポート	送信
WS-X4418-GB および WS-X4416-2GB-TX 以外のすべてのモジュール	オーバーサブスクライブ ポート以外のすべてのポート	Off
WS-X4418-GB	アップリンク ポート（1 ～ 2）	Off
WS-X4418-GB	オーバーサブスクライブ ポート（3 ～ 18）	On
WS-X4412-2GB-TX	アップリンク ポート（13 ～ 14）	Off

表 2-3　モジュールのデフォルト設定

モジュール	ポート	送信
WS-X4412-2GB-TX	オーバーサブスクライブ ポート（1 ～ 12）	On
WS-X4416-2GB-TX	アップリンク ポート（17 ～ 18）	Off

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ポーズ フレームは、バッファが一杯であるために、一定期間、フレームを送信停止する信号を送信元に送る特殊なパケットです。

表 2-4 に、**flowcontrol** コマンドで **send** および **receive** キーワードをさまざまに設定して使用する場合の注意事項を示します。

表 2-4　send および receive キーワードの設定

設定	説明
send on	ローカル ポートからリモート ポートへのポーズ フレームの送信をイネーブルにします。予測可能な結果を得るには、**send on** の使用を、リモート ポートが **receive on** または **receive desired** に設定されている場合だけにします。
send off	ローカル ポートがポーズ フレームをリモート ポートに送信するのを防止します。予測可能な結果を得るには、**send off** の使用を、リモート ポートが **receive off** または **receive desired** に設定されている場合だけにします。
send desired	リモート ポートが **receive on**、**receive off**、または **receive desired** のいずれに設定されていても、予測可能な結果が得られます。
receive on	リモート ポートが送信するポーズ フレームを、ローカル ポートが処理できるようにします。予測可能な結果を得るには、**receive on** の使用を、リモート ポートが **send on** または **send desired** に設定されている場合だけにします。
receive off	リモート ポートからローカル ポートにポーズ フレームを送信しないようにします。予測可能な結果を得るには、**send off** の使用を、リモート ポートが **receive off** または **receive desired** に設定されている場合だけにします。
receive desired	リモート ポートが **send on**、**send off**、または **send desired** のいずれに設定されていても、予測可能な結果が得られます。

表 2-5 に、速度設定に基づいて、ギガビット イーサネット インターフェイスでフロー制御がどのように強制またはネゴシエートされるかを示します。

表 2-5　スイッチ タイプ、モジュール、およびポートごとの送信機能

インターフェイス タイプ	設定速度	アドバタイズされたフロー制御
10/100/1000BASE-TX	速度 1000	常にフロー制御される設定
1000BASE-T	常にネゴシエーションがイネーブル	常にフロー制御がネゴシエートされる設定
1000BASE-X	速度非ネゴシエーションなし	フロー制御がネゴシエートされる設定
1000BASE-X	速度非ネゴシエーション	フロー制御が強制される設定

例

次の例では、送信フロー制御をイネーブルにする方法を示します。

```
Switch(config-if)# flowcontrol receive on
Switch(config-if)#
```

次の例では、送信フロー制御をディセーブルにする方法を示します。

```
Switch(config-if)# flowcontrol send off
Switch(config-if)#
```

次の例では、受信フロー制御を desired に設定する方法を示します。

```
Switch(config-if)# flowcontrol receive desired
Switch(config-if)#
```

関連コマンド

コマンド	説明
interface port-channel	ポートチャネル インターフェイスへのアクセスまたはポートチャネル インターフェイスの作成を行います。
interface range	複数のポートで 1 つのコマンドを同時に実行します。
show flowcontrol	フロー制御に関連するステータスおよび統計情報をインターフェイスごとに表示します。
show running-config	スイッチの実行コンフィギュレーションを表示します。
speed	インターフェイス速度を設定します。

hardware statistics

ACL で TCAM ハードウェア統計情報をイネーブルにするには、**hardware statistics** コマンドを使用します。TCAM ハードウェア統計情報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。

hardware statistics

no hardware 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。

デフォルト

ハードウェア統計情報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 モード

コマンド履歴

リリース	変更箇所
12.2(40)SG	Supervisor Engine 6-E および Catalyst 4900M でサポートされるようになりました。

使用上のガイドライン

Supervisor Engine 6-E および Catalyst 4900 M シャーシの TCAM ハードウェアには、すべての分類/QoS CAM エントリを格納する十分なハードウェア統計情報エントリがありません。したがって、各 CAM エントリの統計情報は、必要に応じてイネーブルにする必要があります。

例

次の例では、ACL の ACE で TCAM ハードウェア統計情報をイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip access-list extended myv4
Switch(config-ext-nacl)#permit ip any any
Switch(config-ext-nacl)#hardware statistics
Switch(config-ext-nacl)#end
```

関連コマンド

コマンド	説明
ip access list（Cisco IOS のマニュアルを参照）	IP Access Control List（ACL; アクセス コントロール リスト）を作成します。
ipv6 access list（Cisco IOS のマニュアルを参照）	IPv6 ACL を作成します。
mac access-list extended	拡張 MAC アクセス リストを定義します。

hw-module beacon

（注）　**hw-module beacon** コマンドは WS-C4500X-32 のアップリンク モジュール上でだけイネーブルになります。

ビーコン ボタンとともにビーコン LED を制御するには、**hw-module beacon** コマンドを入力します。

hw-module beacon [on | off]

構文の説明

on	LED を点灯します。
off	LED を消灯します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
IOS-XE 3.3.0SG（15.1(1)SG）	このコマンドが WS-C4500X-32 に追加されました。

使用上のガイドライン

スイッチの前面のビーコン ボタンを押すか、**hw mod beacon** コマンドを入力します。そのため、オペレータがスイッチの背面側にいるときでもスイッチを確認できます。（複数の装置がある場合、LED および CLI はスイッチ ID として機能します）。

青色のビーコン LED スイッチを押すと、ビーコン LED の状態が切り替わります。

例

複数の WS-C4500X-32 シャーシが近くにあり、1 台のシャーシのポート 11 からトランシーバを取り外す場合、**hw-module beacon on** コマンドでスイッチを識別できます。

```
Switch# hw-module beacon on
Switch#
*Feb 16 13:12:24.418: %C4K_IOSMODPORTMAN-6-BEACONTURNEDON: Beacon has been turned on
```

ビーコンが点灯している WS-C4500X-32 が探しているスイッチです。

ビーコン LED が点灯しているスイッチで必要なサービスが完了したら、ビーコン ボタンを押すか、**hw-module beacon off** コマンドを入力してビーコン LED を消灯します。

```
Switch# hw-module beacon off
Switch#
*Feb 16 13:12:18.083: %C4K_IOSMODPORTMAN-6-BEACONTURNEDOFF: Beacon has been turned off
```

hw-module module start

（注）　**hw-module module start** コマンドは WS-C4500X-32 のアップリンク モジュール上でだけイネーブルになります。

モジュールが停止した後に起動するには、**hw-module module start** コマンドを使用します。

hw-module module *number* **start**

構文の説明

number	アップリンク モジュール ID。WS-C4500 に唯一適用される値は 2 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
IOS-XE 3.3.0SG（15.1(1)SG）	このコマンドが WS-C4500X-32 に追加されました。

使用上のガイドライン

hw-module module *number* **stop** コマンドを使用するか **OIR ボタン**を押して停止したモジュールを起動するには、**hw-module module** *number* **start** コマンドを入力するか、物理的に取り外してから再挿入します。

例

次の例は、モジュールが停止している場合にこのコマンドを入力した結果を示しています。

```
Switch# hw-module module 2 start
Switch#
*Feb  5 16:36:27.352: %C4K_IOSMODPORTMAN-6-MODULEINSERTED: Module 2 is inserted
*Feb  5 16:37:15.902: %C4K_IOSMODPORTMAN-6-MODULEONLINE: Module 2 (WS-X4908X-10G-TIM S/N:
JAE15340C0J Hw: 0.1) is online
Switch#show module
Chassis Type : WS-C4500X-32

Power consumed by backplane : 0 Watts

Mod Ports Card Type                                  Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 1    32  4500X-32 10GE (SFP+)                    WS-C4900X-32P-10G  JAE153505E9
 2     8  10GE SFP+                               WS-X4908X-10G-TIM  JAE15340C0J

 M MAC addresses                    Hw  Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
 1 0022.bde2.1061 to 0022.bde2.1080 0.2 15.0(1r)SG(0 0.DEV-0          Ok
 2 0022.bde2.1579 to 0022.bde2.1580 0.1                               Ok
```

```
Switch#
```

次の例は、モジュールが停止していない場合にこのコマンドを入力した結果を示しています。

```
Switch# hw-module module 2 start
% Module 2 not stopped
```

関連コマンド

コマンド	説明
hw-module module stop	モジュールをシャットダウンして、安全に取り外せるようにします。

hw-module module stop

（注）　**hw-module module stop** コマンドは WS-C4500X-32 のアップリンク モジュール上でだけイネーブルになります。

モジュールをシャット ダウンして、安全に取り外せるようにするには、**hw-module module stop** コマンドを入力します。

hw-module module *number* **stop**

構文の説明

number	アップリンク モジュール ID。WS-C4500 に唯一適用される値は 2 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
IOS-XE 3.3.0SG（15.1(1)SG）	このコマンドが WS-C4500X-32 に追加されました。

使用上のガイドライン

OIR ボタンを押すことなく、アップリンク モジュールの OIR を開始します。

例

次の例は、モジュールが動作している場合に **hw-module module stop** コマンドを入力した結果を示しています。

```
Switch# hw-module module 2 stop
Proceed with module stop? [confirm]
Switch#
*Feb  5 16:34:37.325: %C4K_IOSMODPORTMAN-6-MODULEOFFLINE: Module 2 is offline
Switch#show module
Chassis Type : WS-C4500X-32

Power consumed by backplane : 0 Watts

Mod Ports Card Type                                  Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 1    32  4500X-32 10GE (SFP+)                    WS-C4900X-32P-10G  JAE153505E9
 2     8  Module being held in reset               WS-X4908X-10G-TIM  JAE15340C0J

 M MAC addresses                     Hw  Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
 1 0022.bde2.1061 to 0022.bde2.1080 0.2 15.0(1r)SG(0 0.DEV-0           Ok
 2 0022.bde2.1579 to 0022.bde2.1580 0.1                                In Reset

Switch#
```

次の例は、モジュールがすでに停止している場合に **hw-module module stop** コマンドを入力した結果を示しています。

```
Switch# hw-module module 2 stop
% Module 2 stopped
```

関連コマンド

コマンド	説明
hw-module module start	停止されているモジュールを起動します。

hw-module port-group

モジュールでギガビット イーサネット インターフェイスまたは 10 ギガビット イーサネット インターフェイスを選択するには、**hw-module port-group** コマンドを使用します。

hw-module module *number* **port-group** *number* **select** [**gigabitethernet** | **tengigabitethernet**]

構文の説明

module	回線モジュールを指定します。
number	TwinGig コンバータをサポートするモジュールを指定します。
port-group *number*	スイッチのポート グループ番号。
select	インターフェイス タイプを指定します。有効な値はギガビット イーサネットおよび 10 ギガビット イーサネットです。
gigabitethernet	（任意）ギガビット イーサネットを指定します。
tengigabitethernet	（任意）10 ギガビット イーサネットを指定します。

デフォルト

10 ギガビット。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(40)SG	TwinGig コンバータ モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E や WS-X4606-10GE-E など、TwinGig コンバータ モジュールをサポートする Cisco Catalyst 4500 モジュールでサポートされています。

例

次の例では、TwinGig コンバータを使用する WS-X4606-10GE-E でギガビット イーサネット インターフェイスを選択する方法を示します。

```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hw-module module 1 port-group 1 select gigabitethernet
Switch(config)# exit
```

設定を表示するには、**show interfaces status** コマンドを使用します。

関連コマンド

コマンド	説明
show hw-module port-group	モジュールの X2 ホールがどのようにグループ化されているかを表示します。
show interfaces status	インターフェイスのステータスまたは errdisable ステートにあるインターフェイスのリストを表示します。

hw-module power

スロットまたは回線モジュールの電源をオフにするには、**no hw-module power** コマンドを使用します。電源をオンに戻すには、**hw-module power** コマンドを使用します。

hw-module [**slot** | **module**] *number* **power**

no hw-module [**slot** | **module**] *number* **power**

構文の説明

slot	（任意）シャーシのスロットを指定します。
module	（任意）回線モジュールを指定します。
number	スロット番号またはモジュール番号。

デフォルト

起動後に電源がオンになります。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(18)EW	slot キーワードおよび module キーワードが追加されました。

使用上のガイドライン

no hw-mod mod x power コマンドを入力し、ラインカードの OIR を行った後、コンフィギュレーションは維持され、適用されるシャーシ内のスロットに対して有効です。

例

次の例では、スロット 5 にあるモジュールの電源をオフにする方法を示します。

```
Switch# no hw-module slot 5 power
Switch#
```

関連コマンド

コマンド	説明
clear hw-module slot password	インテリジェント回線モジュールのパスワードをクリアします。

hw-module system max-queue-limit

ユーザがすべてのインターフェイスのキュー制限をグローバルに変更できるようにするには、**hw-module system max-queue-limit** コマンドを使用します。グローバル設定を取り消すには、このコマンドの **no** 形式を使用します。

hw-module system max-queue-limit *max-queue-limit*

no hw-module system max-queue-limit *max-queue-limit*

構文の説明

max-queue-limit	すべてのインターフェイスのキュー制限を指定します。有効な値は 1024 ～ 8184 です。このパラメータは 8 の倍数にする必要があります。

デフォルト

デフォルトでは使用不可

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
15.0(2)SG1 と 3.2.1SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドを使用すると、すべてのインターフェイスにキュー制限を含むポリシーを適用するのではなく、すべてのインターフェイスのキュー制限をグローバルに変更することができます。

これはグローバル コンフィギュレーション コマンドです。これはポート単位、クラス単位 **queue-limit** コマンドで無効にすることができます。

スタンドアロン スーパーバイザ エンジンに対して、このコマンドを適用すると、エンジンを再起動する必要があります。冗長スーパーバイザ エンジンでは、両方のスーパーバイザ エンジンの再起動を強制するには **redundancy reload shelf** コマンドを入力する必要があります。

例

次の例では、キュー制限を 1024 にグローバルに設定する方法を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# hw-module system max-queue-limit 1024
Need to reboot to take effect max queue limit
Switch(config)# exit
Switch# reload  (for standalone supervisors)
Switch# redundancy reload shelf (for reduandancy supervisors in SSO mode)
or
Switch# redundancy force-switchover (followed by another redundancy force-switchover, for
reduandancy supervisors in RPR mode
```

hw-module uplink mode

共有バックプレーンまたは tengigabitethernet モードを使用できるようにアップリンク モードを変更します。共有バックプレーン アップリンク モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

hw-module uplink mode [**shared-backplane** | **tengigabitethernet**]

no hw-module uplink mode [**shared-backplane** | **tengigabitethernet**]

構文の説明

shared-backplane	（任意）冗長モードで動作する場合、Supervisor Engine 6-E および Catalyst 4900 M シャーシのブロッキング ポートとして 4 個の 10 ギガビット イーサネット アップリンクを指定します。
tengigabitethernet	（任意）WS-X4640-CSFP-E ラインカードを備えた Supervisor Engine 6-E で 2 個の 10 ギガビット イーサネット アップリンクを指定します。

デフォルト

2 つの 10 ギガビット イーサネット ポートまたは 4 つの 1 ギガビット イーサネット ポートだけをスーパーバイザ エンジンで使用できます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(44)SG	**shared-backplane** キーワードが、Catalyst 4500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0SG（15.1(1)SG）	**tengigabitethernet** キーワードが、Supervisor Engine 6-E に追加されました。

使用上のガイドライン

hw-module uplink mode shared-backplane コマンドを使用してアップリンク モードを変更する場合は、システムをリロードする必要があります。コンソールには、リロードを示すメッセージが表示されます。

6 または 7 スロット シャーシ（Catalyst 4506-E、4507R-E、および 4507R+E）の Supervisor Engine 6-E の場合、ハードウェアの制限によりデフォルトのアップリンク モードでは WS-X4640-CSFP-E ラインカードは最後のスロットで起動できません。TenGig モードを有効にするには、**hw-module uplink mode tengigabitethernet** コマンドの入力後にシステムをリロードする必要があります。実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存後、設定は NVGEN に格納されます。システムをリロードする前に、**show run | incl uplink** コマンドを使用してアップリンク設定を確認できます。さらに、**show hw-module uplink** コマンドを入力してアップリンク モードを表示できます。これは、現在のアップリンク モードおよびシステムのリロード後のモードをレポートします。

アップリンク TenGig モードでは、アップリンクは非冗長モードと冗長モードの 2 つの 10 ギガビット イーサネット インターフェイスに制限されます。ギガビット イーサネット インターフェイスはサポートされていません。WS-X4640-CSFP-E ラインカードは 6 および 7 スロット シャーシの最後のスロットで起動します。デフォルト モードに戻すには、tengigabitethernet モードでシステムをリロードします。SharedBackplane モードは、システムのリロードが必要なデフォルト モードから選択できます。

hw-module module x port-group x select gigabitethernet コマンドは、gigabitethernet モードを選択しないようにするためにアップリンク TenGig モードでブロックされます。

例

次の例では、共有バックプレーン アップリンク モードをイネーブルにする方法を示します。

```
Switch(config)# hw-module uplink mode shared-backplane
A reload of the active supervisor is required to apply the new configuration.
Switch(config)# exit
Switch#
```

次の例では、共有バックプレーン アップリンク モードをディセーブルにする方法を示します。

```
Switch(config)# no hw-module uplink mode shared-backplane
A reload of the active supervisor is required to apply the new configuration.
Switch(config)# exit
Switch#
```

次の例では、アップリンク モードの現在の状態を表示する方法を示します。

```
Switch# show hw-module uplink
Active uplink mode configuration is Default
(will be Shared-backplane after next reload)

A reload of active supervisor is required to apply the new configuration.
```

関連コマンド

コマンド	説明
show hw-module uplink	ハードウェア モジュールのアップリンク情報を表示します。

hw-module uplink select

WS-C4510R シャーシの Supervisor Engine V-10GE または WS-C4507R シャーシの Supervisor 7L-E で 10 ギガビット イーサネットまたはギガビット イーサネット アップリンクを選択するには、**hw-module uplink select** コマンドを使用します。

（注）　Supervisor Engine 7L-E は 10 スロット シャーシ（WS-C4510R）ではサポートされません。

hw-module uplink select {**tengigabitethernet** | **gigabitethernet** | **all**}

hw-module uplink select {**tengigabitethernet** | **gigabitethernet**} (Sup-7L-E のみ)

（注）　オプション **all** は Supervisor Engine 7L-E ではサポートされません。

構文の説明

tengigabitethernet	（任意）10 ギガビット イーサネット アップリンクを指定します。
gigabitethernet	（任意）ギガビット イーサネット アップリンクを指定します。
all	（任意）すべてのアップリンクを指定します（10 ギガビット イーサネットおよびギガビット イーサネット）。

デフォルト

tengigabitethernet

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(25)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(25)SG	**all** キーワードのサポートが追加されました。
15.0(2)XO	WS-C4507R のシャーシ内の Supervisor Engine 7L-E 用のアップリンク ポートの数は、スーパーバイザ エンジンのモード（単一または冗長）およびアップリンク モードの設定（1 ギガビットまたは 10 ギガビット）によって決まります。

使用上のガイドライン

10 個のスロットを搭載しているシャーシ（Catalyst 4510R および 4510R-E）に取り付けた Supervisor Engine V-10GE（WS-X4516-10GE）では、アップリンク モードを変更したスタートアップ コンフィギュレーションをフラッシュ メモリにコピーしてシステムを再起動しても、システムは新しいアップリンク モードで起動しません。アップリンク モードを変更したスタートアップ コンフィギュレーションをフラッシュ メモリにコピーしたあと、コマンド インターフェイス経由で新しいアップリンク モードに変更してから、システムを再起動する必要があります。この操作により、システムが新しいアップリンク モードで起動します。

Supervisor Engine V-10GE および Supervisor Engine II+10GE は、10 ギガビット イーサネットおよびギガビット イーサネットのアップリンク ポートをサポートしています。Supervisor Engine II+10GE では、常にすべてのアップリンク ポートを使用可能です。同様に、Supervisor Engine V-10GE を W-C4503、W-4506、または W-4507R シャーシに接続すると、すべてのアップリンク ポートが常に使

用可能となります。Supervisor Engine V-10GE を W-4510R シャーシに接続した場合は、10 ギガビット イーサネット アップリンク ポート、ギガビット イーサネット アップリンク ポート、またはすべてのアップリンク ポートの使用を選択できます。すべてのアップリンク ポートの使用を選択する場合、10 番目のスロットは WS-X4302-GB スイッチング ラインカードだけをサポートします。このコマンドが有効になるのは、リロード後にかぎられることに注意してください（**redundancy reload shelf** コマンドの実行後）。

アップリンクの選択は初期化時にハードウェアにプログラムされるため、アクティブなアップリンクを変更するには、コンフィギュレーションを保存してスイッチをリロードする必要があります。アップリンクの設定を変更すると、システムの応答としてスイッチをリロードする必要があることを通知するメッセージが表示され、（冗長モードに従って）スイッチをリロードする適切なコマンドが示されます。

all キーワードを選択する場合は、10 番目のスロットが空であるか、または WS-X4302-GB スイッチング モジュールが取り付けられていることを確認してください。

このコマンドに **no** 形式はありません。設定を取り消すには、アップリンクを設定する必要があります。

WS-C4507R のシャーシ内の Supervisor Engine 7L-E では、アップリンク オプションの数はスーパーバイザ エンジンのモード（単一または冗長）およびアップリンク モードの設定（1 ギガビットまたは 10 ギガビット）によって決まります。

単一スーパーバイザ モード

単一スーパーバイザ モードでは、Supervisor Engine 7L-E は最大 2 個の 10 ギガビットまたは 4 個の 1 ギガビット ポートでアップリンク設定をサポートします（表 2-6）。

表 2-6　単一スーパーバイザ モードのアップリンク オプション

スロット 1	スロット 2	スロット 3	スロット 4	この着脱可能モジュールの組み合わせで達成可能な速度（帯域幅）
コマンドライン インターフェイスから 10 ギガビット動作を選択します。				
SFP+	SFP+	—	—	20 Gbps
SFP+	SFP	—	—	11 Gbps
SFP	SFP+	—	—	11 Gbps
SFP	SFP	—	—	2 Gbps
コマンドライン インターフェイスから 1 ギガビット動作を選択します。				
SFP	SFP	SFP	SFP	4 Gbps

冗長スーパーバイザ モード

冗長スーパーバイザ モードでは、Supervisor Engine 7L-E は 1+1（10 ギガビット モードで）および 2+2（1 ギガビット モードで）をサポートします（表 2-7）。

（注） 冗長性のサポートはスロット 3 と 4 にはありません。

表 2-7　冗長スーパーバイザ モードのアップリンク オプション

アクティブ スーパーバイザ アップリンク ポート				スタンバイ スーパーバイザ アップリンク ポート				
A1	A2	A3	A4	B1	B2	B3	B4	この着脱可能モジュールの組み合わせで達成可能な速度
コマンドライン インターフェイスから 10 ギガビット動作を選択します。								
SFP+	—	—	—	SFP+	—	—	—	20 Gbps
SFP+	—	—	—	SFP	—	—	—	11 Gbps
SFP	—	—	—	SFP+	—	—	—	11 Gbps
SFP	—	—	—	SFP	—	—	—	2 Gbps
コマンドライン インターフェイスから 1 ギガビット動作を選択します。								
SFP	SFP	—	—	SFP	SFP	—	—	4 Gbps

例

次の例では、ギガビット イーサネット アップリンクを選択する方法を示します。

```
Switch(config)# hw-module uplink select gigabitethernet
A reload of the active supervisor is required to apply the new configuration.
Switch(config)# exit
Switch#
```

（注） ギガビット イーサネット アップリンクは、次にリロードしたあとにアクティブになります。

次の例では、SSO モードの冗長システムでギガビット イーサネット アップリンクを選択する方法を示します。

```
Switch(config)# hw-module uplink select gigabitethernet
A 'redundancy reload shelf' or power-cycle of chassis is required to apply the new
configuration
Switch(config)# exit
Switch#
```

（注） ギガビット イーサネット アップリンクは、次にシャーシ/シェルフをリロードしたあとにアクティブになります。シャーシ/シェルフをリロードするには、**redundancy reload shelf** コマンドを使用します。

次の例では、RPR モードの冗長システムでギガビット イーサネット アップリンクを選択する方法を示します。

```
Switch(config)# hw-module uplink select gigabitethernet
A reload of the active supervisor is required to apply the new configuration.
Switch(config)# exit
Switch#
```

（注） ギガビット イーサネット アップリンクは、アクティブ スーパーバイザ エンジンのスイッチオーバーまたはリロード時にアクティブになります。

次の例では、SSO モードの冗長システムですべてのアップリンクを選択する方法を示します。

```
Switch(config)# hw-module uplink select all
Warning: This configuration mode may disable slot10.
```

```
A 'redundancy reload shelf' or power-cycle of chassis is required to apply the new
configuration.
Switch(config)# exit
Switch#
```

（注）　**all** キーワードを選択する場合、スーパーバイザ エンジンの 10 番目のスロットでサポートされるのは Drome ボードだけです。

関連コマンド

コマンド	説明
show hw-module uplink	ハードウェア モジュールのアップリンク情報を表示します。

instance

VLAN または VLAN のセットを MST インスタンスにマッピングするには、**instance** コマンドを使用します。VLAN を共通インスタンスのデフォルトに戻すには、このコマンドの **no** 形式を使用します。

instance *instance-id* {**vlans** *vlan-range*}

no instance *instance-id*

構文の説明

instance-id	指定した VLAN のマッピング先となる MST インスタンス。有効値の範囲は 0 ～ 15 です。
vlans *vlan-range*	指定したインスタンスにマッピングする VLAN の番号を指定します。この番号には、1 つの値または範囲を入力します。有効値の範囲は 1 ～ 4094 です。

デフォルト

マッピングはディセーブルです。

コマンド モード

MST コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

マッピングは、絶対的ではなく差分的に行われます。VLAN の範囲を入力した場合、この範囲は既存の VLAN に追加されるか、または既存の VLAN から削除されます。

マッピングされていない VLAN は、CIST インスタンスにマッピングされます。

例

次の例では、VLAN の範囲をインスタンス 2 にマッピングする方法を示します。

```
Switch(config-mst)# instance 2 vlans 1-100
Switch(config-mst)#
```

次の例では、VLAN をインスタンス 5 にマッピングする方法を示します。

```
Switch(config-mst)# instance 5 vlans 1100
Switch(config-mst)#
```

次の例では、インスタンス 2 から CIST インスタンスに VLAN の範囲を移動する方法を示します。

```
Switch(config-mst)# no instance 2 vlans 40-60
Switch(config-mst)#
```

次の例では、インスタンス 2 にマッピングされたすべての VLAN を CIST インスタンスに戻す方法を示します。

```
Switch(config-mst)# no instance 2
Switch(config-mst)#
```

関連コマンド

コマンド	説明
name	MST リージョン名を設定します。
revision	MST コンフィギュレーションのリビジョン番号を設定します。
show spanning-tree mst	MST プロトコル情報を表示します。
spanning-tree mst configuration	MST コンフィギュレーション サブモードを開始します。