



CHAPTER 2

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

この章には、Catalyst 4500 シリーズ スイッチの Cisco IOS コマンドのリストがアルファベット順に記載されています。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

マクロ キーワードのヘルプ 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、デフォルト設定はありません。

コマンドモード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
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かった場合、そのマクロは無効と見なされ、適用しようとしてもエラーとなります。**#macro keywords** コマンドを入力すると、構文を有効にするために必要なキーワード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た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トリ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。アカウントリ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

アカウントリ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	変更内容
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 アカウントリングには、RADIUS サーバが必要です。

このコマンドを使用すると、Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントリング) クライアントのアカウントリング機能によって、802.1X サブリカント (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 のアップデート パケットおよびウォッチドッグ パケットを転送できます (ウォッチドッグ パケットは、EAPOL-LOGON、EAPOL-LOGOFF、および EAPOL-INTERIM の各メッセージとして定義されています)。サブリカントが認証サーバによって正しく認証および許可されている場合にかぎり、これらのパケットが有効と見なされて転送されます。クライアントが再認証されると、暫定アップデート アカウントリング通知がアカウントリング サーバに送信されます。

例

次の例では、802.1X アカウントリ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 クライアントからの更新またはウォッチドッグ パケットを受け入れてロギングするように、適切に設定されている必要があります。

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。アカウント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

アカウント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	変更内容
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。

このコマンドを使用すると、AAA クライアントのアカウントング機能によって、802.1X サブリカント（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 のアップデートパケットおよびウォッチドッグパケットを転送できます（ウォッチドッグパケットは、EAPOL-LOGON、EAPOL-LOGOFF、および EAPOL-INTERIM の各メッセージとして定義されています）。サブリカントが認証サーバによって正しく認証および許可されている場合にかぎり、これらのパケットが有効と見なされて転送されます。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トング通知がアカウント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 クライアントからの更新またはウォッチドッグパケットを受け入れてロギングするように、適切に設定されている必要があります。

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トングをイネーブルにします。

access-group mode

オーバーライド モード (VACL を PACL よりも優先させる場合など) および非オーバーライド モード (merge モードや strict モードなど) 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は PACL モードが優先するように指定します。ポートに PACL 機能が設定されていない場合は、インターフェイスに適用可能なその他の機能がマージされ、インターフェイスに適用されます。
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 オーバーライド 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	変更内容
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、各方向に 1 つずつ IP ACL を適用できます (着信方向に 1 つと発信方向に 1 つ)。

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 機能をマージ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 でグローバルに制御パケットをキャプチャするよう指定します。
vlan	特定の VLAN で制御パケットをキャプチャするよう指定します。

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	変更内容
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、DHCP スヌーピングや IGMP スヌーピングなどの機能をグローバル レベルでディセーブルにして、代わりにこれらの機能が特定の VLAN 上でイネーブルになるよう設定を確認および変更する必要があります。

パス管理モードに変更すると、ハードウェアに VLAN 単位の CAM エントリがプログラムされるまでは、制御トラフィックがハードウェアでブリッジングされたり、最初はドロップされたりする場合があります。

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と、特定の機能が動作しません。

例

次の例では、制御パケットのキャプチャがイネーブルに設定されている VLAN 上で、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 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別の方法を示します。

```
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、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（マスクなし）。

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	変更内容
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 のプログラム時には、エントリとマスクの 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いずれかを使い切った場合は、ハードウェアに ACL を新しくプログラムすることができなくなります。マスクを使い切ってもエントリに空きがある場合は、プログラミング アルゴリズムを **packed** から **scattered** に変更して、マスクを使用可能にします。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。

この目的は、ACL エントリごとのマスク数をできるだけ少なくして、TCAM のリソースをより効率的に使用することです。 **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、ハードウェアにプログラムする ACL を packed アルゴリズムにする方法を示します。ACL がプログラムされると、わずか 49% の ACL エントリをプログラムするのに 89% のマスクが必要になります。

```
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#

```

次の例では、ハードウェアの ACL エントリ間のスペース（分散）を確保する方法を示します。49% のエントリをプログラムするために必要なマスク数は 49% に減少します。

```

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

ハードウェアにおける TCAM 領域間のバランスを修正するには、**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	変更内容
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つ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アクションを設定します。
forward	パケットを宛先に転送するアクションを設定します。

デフォルト

このコマンドには、デフォルト設定はありません。

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	変更内容
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 packets 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 packets タイプのデフォルトアクションは **drop** (拒否) です。

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

特定の packets 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 packets 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) #
```

関連コマンド

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、デフォルト設定はありません。

コマンドモード

cfg-call-home-profile

コマンド履歴

リリース	変更内容
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。

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、および管理ドメイン全体への設定番号の伝播を実行するには、**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、デフォルト設定はありません。

コマンドモード

VLAN コンフィギュレーション モード

コマンド履歴

リリース	変更内容
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)	スイッチをログオフして、アクティブな端末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、定義済みリストの最後に句を追加したりするには、**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、デフォルト設定はありません。

コマンドモード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
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 バインディングと一致した 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 バインディングと一致した 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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	変更内容
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 標準には、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おり、無許可のデバイスが公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します。

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 コントロールにより、デバイスが認証されるまでは Extensible Authentication Protocol (EAP; 拡張認証プロトコル) over LAN (EAPOL) トラフィックだけがそのデバイスの接続ポートを通過できます。認証に成功すると、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。このホストはネットワークの他のデバイスとトラフィックをやり取りできません。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ホストが接続されている場合、そのホストは、ネットワークの他のデバイスからトラフィックを受信することしかできません。

- 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。

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

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	変更内容
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*

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

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]}

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。デフォルト値は 2 です。
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。
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 Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントリング) サーバのアライブ アクションを設定します。
dead action authorize	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 アクションを設定します。
vlan vlan no-response action authorize	(任意) 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 (失敗するたびに) 無制限に再試行されます。

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	変更内容
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 **dot1x** 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、dot1x で認証エラーを伝えることです。デフォルトでは、このタイプのエラーが発生すると認証方式が再試行されます。設定済みの VLAN で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。このアクションを実行する前に認証を再試行する回数を任意で指定できます。

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 dot1x 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。

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

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 dot1x 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され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

<i>profile</i>	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 プロファイル名 (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	変更内容
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を使用すると、802.1X サブリカントが存在せず、管理対象デバイスではないクライアントを WebAuth 方式にフォールバックできます。

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

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	変更内容
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。スイッチング環境におけるドメインとは VLAN のことで、データ ドメインおよび音声ドメインの 2 つのドメインがサポー

トされています。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。両クライアントの認証には、異なる方式 (PC の場合は 802.1X、IP Phone の場合は MAB、またはその逆など) を使用できます。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 デバイスには dACL を使用し、音声デバイスには使用しない場合、ユーザのデータが WebAuth にフォールバックすると、フォールバック ポリシーに基づいて適用される ACL が音声トラフィックに影響します。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、サブ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。

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

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

特定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	変更内容
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 アクセスを使用すると、認証の実行前にクライアントまたはデバイスがネットワークにアクセスできます。

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

このコマンドは、このポートでのみ **authentication host-mode session-type open** グローバル コンフィギュレーション モード コマンドに優先します。

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

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

<i>method1</i>	試行する認証方式。有効な値は次のとおりです。 <ul style="list-style-type: none"> • 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。
<i>method2</i>	(任意) 試行する認証方式。有効な値は次のとおりです。
<i>method3</i>	<ul style="list-style-type: none"> • 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	変更内容
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、明示的にリスト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、認証が成功するまで、設定した（またはデフォルトの）順序で適用されます。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。

設定を確認するには、**show authentication** 特権 EXEC 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

特定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	変更内容
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

再認証期間は、**authentication timer** コマンドを使用して設定できます。

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

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て、ポートの最初のステータスを無許可ステータスにします。
force-authorized	(任意) インターフェイスで 802.1X をディセーブルにして、認証交換を必要とせずにポートを許可ステータスに変更します。ポートはクライアントとの 802.1X ベース認証を行わずに、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タスに変更して、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	変更内容
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、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：ポートで 802.1X をイネーブルにする前に、EtherChannel からポートを削除しておく必要があります。EtherChannel または EtherChannel のアクティブ ポートで 802.1X をイネーブルにしようとする、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、そのポートは EtherChannel に加入しません。

- Switch Port Analyzer (SPAN; スイッチ ポート アナライザ) 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。ただし、ポートが SPAN 宛先から削除されるまで 802.1X はディセーブルです。802.1X は SPAN 送信元ポートでイネーブルにできます。

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。このタスクにグローバル コンフィギュレーション コマンドはありません。

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

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 ステータス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。ネットワークにアクセスしようとする各クライアントは、クライアントの MAC アドレスを使用して一意に識別されます。

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

<i>method1</i>	試行する認証方式。有効な値は次のとおりです。 <ul style="list-style-type: none"> • 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。
<i>method2</i>	(任意) 試行する認証方式。有効な値は次のとおりです。
<i>method3</i>	<ul style="list-style-type: none"> • 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	変更内容
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 プライオリティは設定された順序と同じ順序になります。

設定を確認するには、**show authentication** 特権 EXEC 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。デフォルト値はオフです。 (注) 非アクティブ値は再認証タイマーの値より小さくする必要がありますが、非アクティブ値を再認証タイマーの値より大きく設定してもエラーとは見なされません。
reauthenticate server	Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントティング) サーバから、クライアントの再認証期間の値を Session-Timeout (RADIUS 属性 27) として取得するように指定します。
reauthenticate value	自動再認証が開始されるまでの時間（秒）を指定します。有効値の範囲は 1 ～ 65535 です。デフォルト値は 3600 です。
restart value	無許可ポートの認証試行が行われるまでの時間（秒）を指定します。有効値の範囲は 1 ～ 65535 です。デフォルト値はオフです。

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	変更内容
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または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かぎって変更してください。

非アクティビティ期間中、イーサネット スイッチ ネットワーク モジュールは、認証要求の受け付けまたは開始を行いません。デフォルトよりも小さい値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、Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントिंग) サーバから、クライアントの再認証期間の値を Session-Timeout (RADIUS 属性 27) として取得するように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。

auto qos voip

QoS ドメイン内に Voice over IP (VoIP) 用の Quality of Service を自動設定するには (Auto-QoS)、**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 コンフィギュレーションを標準 QoS のデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

cisco-phone	このインターフェイスを Cisco IP Phone に接続し、VoIP 用の QoS を自動設定します。着信パケットの CoS ラベルが信頼されるのは、IP Phone が検知される場合にかぎります。
trust	この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、VoIP 用の QoS を自動設定します。着信パケットの CoS ラベルおよび 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	変更内容
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

QoS ドメイン内の VoIP トラフィックに適切な QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、スイッチ、ネットワーク内部、QoS の着信トラフィックを分類できるエッジデバイスなどが含まれます。

cisco-phone キーワードは、Cisco IP Phone に接続された、ネットワークのエッジにあるポートで使用します。スイッチは、Cisco Discovery Protocol (CDP; シスコ検出プロトコル) 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。

trust キーワードは、ネットワーク内部に接続されたポートで使用します。トラフィックは他のエッジデバイスで分類済みと見なされるため、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; シスコ検出プロトコル) を使用して、Cisco IP Phone が存在するかどうかを検出します。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、受信したパケットの 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 がマークされないためです。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受信したパケットの 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)。

スタティック ポート、ダイナミック アクセス ポート、音声 VLAN アクセス ポート、およびトランク ポートで Auto-QoS を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 の設定を表示するには、Auto-QoS をイネーブルにする前にデバッグをイネーブルにします。Auto-QoS のデバッグをイネーブルにするには、**debug auto qos** 特権 EXEC コマンドを使用します。

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、標準 QoS がイネーブルになり、Auto-QoS 設定はそのインターフェイスの標準 QoS のデフォルト設定に変更されます。Auto-QoS によって実行されたグローバル コンフィギュレーションが、このアクションで変更されることはありません。グローバル コンフィギュレーションは維持されます。

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、受信した着信パケットの CoS ラベルおよび 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 として検出された場合に、Auto-QoS をイネーブルにし、受信した着信パケットの 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 以外のスーパーバイザ エンジン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# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
Switch(config-if)#
00:00:56:qos
00:00:57:qos map cos 3 to dscp 26
00:00:57:qos map cos 5 to dscp 46
00:00:58:qos map dscp 32 to tx-queue 1
00:00:58:qos dbl
00:01:00:policy-map autoqos-voip-policy
00:01:00: class class-default
00:01:00:   dbl
00:01:00:interface GigabitEthernet1/1
00:01:00: qos trust cos
00:01:00: tx-queue 3
00:01:00: priority high
00:01:00: shape percent 33
00:01:00: service-policy output autoqos-voip-policy
Switchconfig-if)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-phone
Switch(config-if)#
00:00:55:qos
```

■ auto qos voip

```

00:00:56:qos map cos 3 to dscp 26
00:00:57:qos map cos 5 to dscp 46
00:00:58:qos map dscp 32 to tx-queue 1
00:00:58:qos dbl
00:00:59:policy-map autoqos-voip-policy
00:00:59: class class-default
00:00:59:   dbl
00:00:59:interface GigabitEthernet1/1
00:00:59: qos trust device cisco-phone
00:00:59: qos trust cos
00:00:59: tx-queue 3
00:00:59:   priority high
00:00:59:   shape percent 33
00:00:59:   bandwidth percent 33
00:00:59:   service-policy output autoqos-voip-policy

```

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)#interface 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)	Auto-QoS をデバッグします。
qos map cos	信頼できるインターフェイスの入力 CoS/DSCP マッピングを定義します。
qos trust	インターフェイスの信頼状態を設定します。
show auto qos	適用されている 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-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	変更内容
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。

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

<i>bandwidth-kbps</i>	クラスに割り当てる帯域幅の量 (kbps 単位)。有効値の範囲は 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、優先キューイング クラスが設定されていて、そのクラスがレート制限されていない場合にのみサポートされます。

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	変更内容
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。

新しいキューに使用する未割り当ての帯域幅がない場合、または未割り当ての帯域幅が不十分で、明示的な帯域幅の指定がないすべてのキューに対して最小限の割合も設定できない場合、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、1 つのポリシー マップに含まれるクラス帯域幅の割合の合計は 100% 以下とします。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。
- 十分な大きさの帯域幅を設定し、レイヤ 2 のオーバーヘッドに対応する必要があります。
- ポリシー マップでは、すべてのクラスの帯域幅を **kbps** または割合のいずれかで指定できますが、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 つのクラスを含むポリシー マップが作成され、物理ポートに適用されます。

```
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、*voicel* 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 voicel
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	完全優先キュー (Low-Latency Queueing (LLQ; 低遅延キューイング)) 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 Quality of Service (QoS) 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 サブ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、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチ、Supervisor Engine 6-E、および Catalyst 4900M シャーシに追加されました。

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またはディセーブにします。 **alert-group** コマンドを参照してください。
- **contact-email-addr email-address** : システム接点の電子メール 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 用のカスタマー契約 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、エントリを二重引用符 (" ") 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*) と同じ設定の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、エントリを二重引用符 (" ") 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 モードを終了して、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 Fully Qualified Domain Name (FQDN; 完全修飾ドメイン名) を入力できます。プライオリティには、1 (最高) ~ 100 (最低) を割り当てることができます。

バックアップ用の電子メール サーバを定義するには、異なる **priority** 番号を指定して **mail-server** コマンドを再度入力します。

- **no** : コマンドを無効にするか、またはデフォルト値を設定します。

- **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、エントリを二重引用符 (" ") 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、エントリを二重引用符 (" ") 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、エントリを二重引用符 (" ") 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 メッセージの転送先 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 " <i>show-command</i> "	指定した CLI show コマンドの出力を送信して分析します。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 <i>name</i>	(任意) 要求の送信先とす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 <i>user-id</i>	(任意) 登録済み Smart Call Home ユーザの ID を指定します。 <i>user-id</i> を指定した場合、生成される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。 <i>user-id</i> 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチ、Supervisor Engine 6-E、および Catalyst 4900M シャーシに追加されました。

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。プロファイルには、転送ゲートウェイが設定されている電子メールアドレスを指定する必要があります。この場合、要求メッセージが Cisco TAC に転送され、ユーザは Smart Call Home サービスから応答を受信することができます。

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

次の例では、ユーザ指定の show コマンドを分析する要求を示します。

```
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 コマンドを送信して、コマンド出力を電子メールで受け取ります。
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 コマンドを実行して、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"	実行される 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 <i>email-addr</i>	CLI コマンド出力の送信先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 <i>SR</i>	コマンド出力の関連先となるアクティブな TAC ケース番号を指定します。この番号が必要となるのは、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のみです。この番号は電子メールの件名に表示されます。

コマンド デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチ、Supervisor Engine 6-E、および Catalyst 4900M シャーシに追加されました。

使用上のガイドライン

このコマンドにより、指定した CLI コマンドがシステムで実行されます。指定した CLI コマンドは、二重引用符 (" ") で囲む必要があります。また、すべてのモジュールのコマンドを含む、任意の run または show コマンドを指定できます。

コマンド出力は電子メールで送信され、指定した電子メール アドレスに届けられます。電子メール アドレスを指定しない場合、コマンド出力は Cisco TAC (attach@cisco.com) に送信されます。この電子メールは、件名にサービス番号（指定されている場合）が含まれるロング 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、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチ、Supervisor Engine 6-E、および Catalyst 4900M シャーシに追加されました。

使用上のガイドライン

モジュール番号を入力すると、モジュールの番号を指定できます。

profile profile-name を指定しなかった場合は、登録されている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、および目録の各アラート グループだけです。宛先プロファイルをアラート グループに登録する必要はありません。

例

次の例では、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する方法を示します。

```
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 Ciscotacl
```

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 をイネーブ爾またはディセーブ爾にします。
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 <i>profile-name</i>	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、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチ、Supervisor Engine 6-E、および Catalyst 4900M シャーシに追加されました。

使用上のガイドライン

このコマンドは、指定した宛先プロファイルにテスト メッセージを送信します。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ときはそのテキストを二重引用符 (" ") で囲む必要があります。メッセージを入力しない場合は、デフォルト メッセージが送信されます。

例

次の例では、Call Home テスト メッセージを手動で送信する方法を示します。

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

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ンネル 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	チャンネル 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 を使用せずにポートを強制的にチャンネル化します。
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、ポートは受信した 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) 他のデバイスからトラフィックが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します。
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 パケットを送信して、他のポートとのネゴシエーションを開始します。

デフォルト

チャンネル グループは割り当てられません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
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ンネル グループに割り当てる前にポートチャンネル インターフェイスを作成する必要はありません。ポートチャンネル 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ンネル 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。

チャンネル 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ン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ンネルの設定には、同じチャン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ンネル 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。

チャンネル 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。

ポートチャンネル インターフェイスで設定または属性を変更すると、その変更は、同じチャンネル グループ内のすべてのインターフェイスにポート チャネルとして伝播されます（たとえば、設定の変更は、ポート チャネルには含まれないがチャンネル グループには含まれている物理インターフェイスにも伝播されます）。

on モードで 2 つのポート グループを接続すると、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	ポートチャンネル 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。これらの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	変更内容
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

このコマンドは、Supervisor Engine I を搭載しているシステムではサポートされません。

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ン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。両方ともチャン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
<code>channel-group</code>	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。
<code>show etherchannel</code>	チャンネルの EtherChannel 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。このクラスは、**class-map** *class-map-name* グローバル コンフィギュレーション コマンドを使用して事前に作成されています。

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	変更内容
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、ポリシー マップ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る最小帯域幅を指定または変更します。詳細については、**bandwidth** 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 シャーシで使用できます。
- **dbl** : このクラスに届くトラフィックのダイナミック バッファ制限をイネーブルにします。この **dbl** の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 レート)** および **police (パーセント)** コマンドを参照してください。2 レート トラフィック ポリサーは、Supervisor Engine 6-E および Catalyst 4900M シャーシでサポートされています。
- **priority** : トラフィックのクラスの完全優先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。このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシでサポートされています。
- **service-policy (ポリシーマップ クラス)** : ポリシー マップ内に Quality of Service (QoS) 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 Class of Service (CoS; サービス クラス)、Differentiated Services Code Point (DSCP; DiffServ コード ポイント)、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。このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシでサポートされています。
- **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、デフォルトのクラスを含め、ポリシー マップで最大 256 のクラスをサポートしています。一致基準のいずれにも該当しないパケットは、デフォルト 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。このポリシーを入力ポートに適用すると、**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 に設定して、平均伝送速度 1 Mbps およびバースト 20 KB 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 (パーセント)	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	完全優先キュー (Low-Latency Queueing (LLQ; 低遅延キューイング)) 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)	インターフェイスにポリシー マップを適用します。
service-policy (ポリシーマップ クラス)	ポリシー マップ内に Quality of Service (QoS) 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 Class of Service (CoS; サービス クラス)、Differentiated Services Code Point (DSCP; DiffServ コードポイント)、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

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、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。
<i>class-map-name</i>	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	変更内容
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したい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 マップに対して設定された一致基準と照合され、そのクラスにパケットが属す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 Quality of Service (QoS) 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 コマンドを使用できるようになります。

- **description** : クラス マップの説明を入力します (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
<code>class</code>	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。
<code>match</code> (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。
<code>policy-map</code>	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。
<code>show class-map</code>	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) チャンネル 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、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 を使用して取得したカウンタをクリアせず、**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	変更内容
12.2(52)SG	このコマンドが追加されました。

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
```

show energywise neighbors 特権 EXEC コマンドを入力することによって、テーブルが削除されたことを確認できます。



(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	EnergyWise の設定およびエンティティと PoE ポートのスレ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	回復対象の VLAN のインターフェイスを指定します。
vlan	インターフェイス上の回復対象のすべての 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、デフォルト設定はありません。

コマンドモード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
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 範囲が指定されなかった場合は、指定したインターフェイス上のすべての VLAN が再度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 ステータスは変更されず、物理ポートの他の VLAN ポートには影響しません。STP に対してイベントを通知しないため、スパンニングツリーの処理は通常どおり行われ、VLAN ポートが適切なブロッキング ステータスまたはフォワーディング ステータスになります。

例

次の例では、インターフェイス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 ステータス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	変更内容
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)

Catalyst 4500 シリーズ スイッチの場合は、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 モジュールおよびポートの番号。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 リストの番号です。有効値の範囲は 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 統計情報をクリアして、削除の状態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 アドレスです。
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 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 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 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。
<i>mod/port</i>	(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。
<i>host_name</i>	(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。
<i>group_address</i>	(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。有効値の範囲は 0 ~ 2,147,483,647 です。
null interface_number	(任意) スル 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) チャンネル 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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ています。

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、Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) 経由で学習されたレシーバー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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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

明示的ホスト トラッキング データベースには、デフォルトで最大 1 KB のエントリを格納できます。この制限に達すると、データベースに新規エントリを作成できなくなります。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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、すべてのアクティブ 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 パケットが到着すると、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を示します。

clear lacp counters

特定のチャンネル 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) チャンネル 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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

このコマンドは、Supervisor Engine I を搭載しているシステムではサポートされません。

channel-group を指定しない場合は、すべてのチャンネル 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ンネル 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 エントリの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、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 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

<i>group-number</i>	チャンネル 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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イッキ 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

使用上のガイドライン

clear port-security all コマンドを入力すると、スイッチは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。



(注)

ステイ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	変更内容
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	ステイッキ 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 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) チャンネル 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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



(注)

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。

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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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

「system-cpp-policy」という名前のデフォルト サービス ポリシー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	変更内容
12.2(31)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。

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 Access Control List (ACL; アクセス コントロール リスト) 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)	インターフェイスにポリシー マップを適用します。
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。

counter

スイッチ ポートにカウンタ セットを割り当てるには、**counter** 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

no counter

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	変更内容
12.2(40)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

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシでサポートされています。送信カウンタおよび受信カウンタを設定できるスイッチ ポートの合計数は 4096 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 ポートに変更するか削除すると、ハードウェアカウンタが解放されます。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、スイッチ ポートにカウンタ セットを割り当てる方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface vlan 20
Switch(config-if)# counter
Switch(config-if)# end
Switch#
```

db1

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、**db1** 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。

db1

no db1

構文の説明

このコマンドには、キーワードまたは引数はありません。

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	変更内容
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 6E のサポートが追加されました。

使用上のガイドライン

DBL 設定のセマンティックスは、(W) RED アルゴリズムと類似しています。**db1** 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 **db1** 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)# db1
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
<code>policy-map</code>	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。
<code>service-policy</code> (ポリシーマップ クラス)	ポリシー マップ内に Quality of Service (QoS) ポリシーとして サービス ポリシーを作成します。
<code>show policy-map</code>	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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 <i>mod/port</i>	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。 モジュールおよびポートの番号。
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。有効値の範囲は 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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。
<i>mod/port</i>	モジュールおよびポートの番号。
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 <i>interface_num</i>	ポートチャンネルインターフェイスにデバッグ出力を制限します。有効値の範囲は 1 ~ 64 です。
vlan <i>vlan_id</i>	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。
<i>group-number</i>	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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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

条件セットが 1 つだけの場合にこの条件セットを削除しようとする、削除操作の中断を確認するメッセージとともにプロンプトが表示されます。**n** を押して削除を中断するか、または **y** を押して削除を実行できます。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場合があります。

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#
```

次の例では、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

特定の 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。有効値の範囲は 1 ～ 4096 です。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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

VLAN 条件セットが 1 つだけの場合にこの条件セットを削除しようとする、削除操作の中断を確認するメッセージとともにプロンプトが表示されます。**n** を押して削除を中断するか、または **y** を押して削除を実行できます。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
<code>undebg condition vlan</code> (no <code>debug condition vlan</code> と同じ)	デバッグ出力をディセーブルにします。

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	変更内容
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) モジュールへの 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	変更内容
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_attr: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#
```

■ debug etherchnl

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 <i>mod/port</i>	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。 モジュールおよびポートの番号。
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 <i>interface-num</i>	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。有効値の範囲は 1 ~ 64 です。
vlan <i>vlan_id</i>	VLAN インターフェイス番号を指定します。有効値の範囲は 1 ~ 4094 です。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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	変更内容
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	変更内容
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	変更内容
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	変更内容
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 コンソールからにかぎられます。

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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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

Port Manager (PM; ポート マネージャ) 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 クッキーの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、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 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	キーブアライブ 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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#
```

■ debug spanning-tree

関連コマンド

コマンド	説明
undebg 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 コンソールからにかぎられます。

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
undebg 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 シムの 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 ポートで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 シムのデコード済み送信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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、スイッチ コンソールからにかぎられます。

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
undebg 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

スパンニング 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、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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、スイッチ コンソールからにかぎられます。

例

次の例では、スパンニング 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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; IOS ファイル システム) 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 ファイルオープン動作のエラーの 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指定します。使用時の詳細については、「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時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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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
undebg 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 | allowedvlanfcgchange | fwdchange |
linkchange | modechange | pruningfcgchange | statechange}
```

```
no debug sw-vlan notification {accfwdchange | allowedvlanfcgchange | fwdchange |
linkchange | modechange | pruningfcgchange | 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。
allowedvlanfcgchange	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。
pruningfcgchange	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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 のプロトコル 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る汎用論理フローのデバッグ メッセージおよび詳細な VTP デバッグ メッセージを表示します。
packets	Cisco IOS VTP プラットフォーム依存レイヤから VTP コードに渡される、すべての着信 VTP パケット（プルーニング パケットを除く）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レイヤから VTP コードに渡される、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レイヤに送信を要求する、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レイヤに送信を要求する、すべての発信 VTP パケット（プルーニング パケットを除く）の内容を表示します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 の入力後、さら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 の発信 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#
```

■ debug sw-vlan vtp

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 udlld

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 udlld** 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 udlld {events | packets | registries}
```

```
no debug udlld {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、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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 コンソールからにかぎられます。

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 udlld 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 udlld 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 udlld registries
UDLD registries debugging is on
Switch#
```

■ debug udd

関連コマンド

コマンド	説明
undebug udd (no debug udd 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 アドレス学習をデバッグします。
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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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

<i>macro-name</i>	インターフェイス範囲マクロの名前（最大 32 文字）。
<i>interface-range</i>	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、デフォルト設定はありません。

コマンドモード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
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。モジュールをまたがったインターフェイス範囲の指定はできません。

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 に指定できる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 要求の照合条件を指定します。 request を指定しないと、すべての ARP パケットに対して照合が実行されます。
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 リストの最後には、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	変更内容
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 バインディングと一致した ARP パケットを許可します。

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 <i>email-address</i>	宛先電子メールアドレスを 1 ～ 200 文字で指定します。
http <i>url</i>	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、デフォルト設定はありません。

コマンドモード

cfg-call-home-profile

コマンド履歴

リリース	変更内容
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。

セキュア サーバに **https://** 宛先 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。

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	変更内容
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。

destination preferred-msg-format

優先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	変更内容
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、優先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。

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

電子メール

コマンドモード

cfg-call-home-profile

コマンド履歴

リリース	変更内容
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。

diagnostic monitor action

スイッチでパケット メモリ障害が検出された場合のアクションを指定するには、**diagnostic monitor action** コマンドを使用します。

diagnostic monitor action [conservative | normal | aggressive]

構文の説明	保守的	標準	攻撃的
	(任意) 起動時 SRAM 診断によってすべての障害を記録し、影響を受けるすべてのバッファをハードウェアで操作しないように指定します。実行中の SRAM 診断はイベントを記録しますが、その他のアクションは実行しません。	(任意) 継続的な障害によってスーパーバイザ エンジンがリセットされること以外は、SRAM 診断が保守モードで動作するように指定します。これにより、起動時テストで影響を受けるメモリを特定できます。	(任意) 起動時障害が障害のみを記録し、スーパーバイザ エンジンがオンラインになるのを許可しないこと以外は、SRAM 診断が通常モードで動作するように指定します。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のいずれかで引き継ぎが可能です。

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	変更内容
	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、継続的な障害の発生時に RPR 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 <i>test-id</i> 、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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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

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

<i>max-attempts</i>	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	変更内容
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	dot1x 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	変更内容
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	変更内容
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 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、キーワードまたは変数はありません。

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	変更内容
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、キーワードまたは変数はありません。

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	変更内容
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	変更内容
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	変更内容
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	変更内容
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 対応サブリカント (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 guest-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	変更内容
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 サブ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 対応サブリカント (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。IEEE 802.1x 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、single-host 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	変更内容
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タスになった場合（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。

ポート上で 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 により、ポートがデータ ドメインと音声ドメインに振り分けられます。MDA では、同じ IEEE 802.1x 対応ポート上でデータ デバイスと IP Phone などの音声デバイス（シスコ製または他社製）を同時に使用できません。

このコマンドを入力する前に、指定のポートに対して **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#
```

次の例では、MDA をイネーブルにして、ポートでホスト デバイスおよび音声デバイスの両方を許可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 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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	変更内容
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 サブ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	変更内容
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のみ変更してください。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	変更内容
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タス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タスに移行します。
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タスに移行します。ポートはクライアントとの 802.1X ベース認証を行わずに、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タスに移行することで、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	変更内容
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、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、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**：ポートで 802.1X をイネーブルにする前に、EtherChannel からポートを削除しておく必要があります。EtherChannel または EtherChannel のアクティブ ポートで 802.1X をイネーブルにしようとする、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。

- Switch Port Analyzer (SPAN; スイッチ ポート アナライザ) 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。ただし、ポートが SPAN 宛先から削除されるまで 802.1X はディセーブルです。802.1X は SPAN 送信元ポートでイネーブルにできます。

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。このタスクにグローバル 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、デフォルト設定はありません。

コマンドモード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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	変更内容
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	変更内容
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」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」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	変更内容
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。

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	変更内容
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 (続き)

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	サポートされません。	サポートされません。	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。
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 <i>importance</i>	エンティティの重要度を設定します。 指定できる範囲は 1 ~ 100 です。
keywords <i>word,word,...</i>	エンティティのキーワードを 1 つ以上割り当てます。 キーワードを複数割り当てる場合は、キーワードをカンマで区切るようにし、キーワード間にスペースを入れないでください。 <i>word</i> 値についての注意点は、次のとおりです。 <ul style="list-style-type: none"> 英数字、および #、(、%、!、& 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 <i>level</i>	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 <i>tcp-port-number</i>	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 <i>name</i>	EnergyWise 固有のエンティティ名を指定します。 <i>name</i> 値についての注意点は、次のとおりです。 <ul style="list-style-type: none"> 英数字、および #、(、%、!、& 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 <i>hostname</i> <i>ip-address</i> <i>udp-port-number</i>	スタティック ネイバーを割り当てます。 <ul style="list-style-type: none"> ホスト名 (<i>hostname</i>) または IP アドレス (<i>ip-address</i>)。 クエリーを送受信する UDP ポート (<i>udp-port-number</i>)。指定できる範囲は 1 ~ 65000 です。
role <i>role</i>	EnergyWise ドメインにおけるエンティティのロールを指定します。たとえば、lobby.b20。 <i>role</i> 値についての注意点は、次のとおりです。 <ul style="list-style-type: none"> 英数字、および #、(、%、!、& 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。

energywise (グローバル コンフィギュレーション)

デフォルト

重要度は 1 です。
 キーワードは定義されていません。
 電力レベルは 10 です。
tcp-port-number は 43440 です。
name はホスト名です。
 ネイバーは割り当てることができません。
role は、モデル番号です。

コマンド モード

コンフィギュレーション

コマンド履歴

リリース	変更内容
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

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 の設定および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。

指定できる範囲は 1 ~ 100 です。

keywords *word,word,...* (任意) ポートのキーワードを 1 つ以上割り当てます。

キーワードを複数割り当てる場合は、キーワードをカンマで区切るようにし、キーワード間にスペースを入れないでください。

word 値についての注意点は、次のとおりです。

- 英数字、および #、(、%、!、& 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 (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 at minute
hour day_of_month
month day_of_week*

- **importance** *importance* : ドメイン内のポートの重要度を設定します。指定できる範囲は 1 ~ 100 です。
- **minute** : 指定できる範囲は 0 ~ 59 です。ワイルドカードには * を使用してください。
- **hour** : 指定できる範囲は 0 ~ 23 です。ワイルドカードには * を使用してください。
- **day_of_month** : 指定できる範囲は 1 ~ 31 です。ワイルドカードには * を使用してください。
- **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。ワイルドカードには * を使用してください。
- **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)。ワイルドカードには * を使用してください。

(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行われます。

(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 <i>name</i>	(任意) EnergyWise 固有のポート名を指定します。 <i>name</i> 値についての注意点は、次のとおりです。 <ul style="list-style-type: none"> 英数字、および #、(、%、!、& 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 <i>role</i>	(任意) ドメインにおけるポートのロールを指定します。たとえば、lobbyport。 <i>role</i> 値についての注意点は、次のとおりです。 <ul style="list-style-type: none"> 英数字、および #、(、%、!、& 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ていません。

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	変更内容
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 importance 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 の設定および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 <i>domain-name</i>	指定した <i>domain-name</i> を持つドメインにエンティティを割り当てます。 <ul style="list-style-type: none"> 英数字、および #、(、%、!、& 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] <i>password</i>	ドメイン内のエンティティ間の通信を保護する <i>password</i> を設定します。 <ul style="list-style-type: none"> (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。 <p>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。</p> <p><i>password</i> 値についての注意点は、次のとおりです。</p> <ul style="list-style-type: none"> 英数字、および #、(、%、!、& 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 <i>udp-port-number</i>	(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 <i>interface-id</i>	(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 <i>ip-address</i>	(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

コンフィギュレーション

コマンド履歴

リリース	変更内容
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 の設定および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。 指定できる範囲は 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。 キーワードを複数指定する場合は、キーワードをカンマで区切るようにし、キーワード間にスペースを入れないでください。 <i>word</i> 値についての注意点は、次のとおりです。 <ul style="list-style-type: none"> 英数字、および #、(、%、!、& 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。 <i>name</i> 値についての注意点は、次のとおりです。 <ul style="list-style-type: none"> 英数字、および #、(、%、!、& 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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	変更内容
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

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
Gil/0/1	control	SwitchA	86.0 (W)	10	100	parent
.	interface	Gil.0.1	0.0 (W)	10	20	child
.						
Gil/0/6	interface	Gil.0.6	0.0 (W)	10	20	child
Gil/0/7	role.lobbyaccess	lobbyInterface.7	0.0 (W)	10	50	child
Gil/0/8	interface	Gil.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
```

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、デフォルト設定はありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
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-config** 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 12.2』 (次の URL)
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fun_c/index.htm
- 『Cisco IOS Configuration Fundamentals Configuration Command Reference, Release 12.2』 (次の URL)
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fun_r/index.htm



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	変更内容
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 |
peseure-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 |
peseure-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спек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) チャンネル設定ミス 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。
peseure-violation	(任意) peseure 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спек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	変更内容
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)#
```

次の例では、タイマーを 300 秒に設定する方法を示します。

```
Switch(config)# errdisable recovery interval 300
Switch(config)#
```

次の例では、ARP インспек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
vmmps                  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。

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 のいずれか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 フレームの送信は **on** 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）。
- 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
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	変更内容
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 ポートからリモート 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。
send desired	リモート ポートが receive on 、 receive off 、または receive desired のいずれか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 ポートから送信されるポーズ フレームの処理をローカル ポートでイネーブルにします。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 のいずれか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	変更内容
12.2(40)SG	Supervisor Engine 6-E および Catalyst 4900M シャーシのサポートが追加されました。

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 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 <i>number</i>	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	変更内容
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	変更内容
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。

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 uplink mode shared-backplane

アップリンク モードを変更して、冗長モードで動作している Supervisor Engine 6-E および Catalyst 4900 M シャーシの 4 つの 10 ギガビットイーサネットポートをすべてブロッキングポートとして使用できるようにするには、**hw-module uplink mode shared-backplane** コマンドを使用します。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

no hw-module uplink mode shared-backplane

構文の説明

このコマンドには、キーワードまたは引数はありません。

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	変更内容
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

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。

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

W-C4510R シャーシ内の Supervisor Engine V-10GE で 10 ギガビット イーサネットまたはギガビット イーサネットの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。

hw-module uplink select {tengigabitethernet | gigabitethernet | all}

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	変更内容
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。

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) に取り付けられた 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。

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 {vlan vlan-range}
```

```
no instance instance-id
```

構文の説明

<i>instance-id</i>	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。
vlan <i>vlan-range</i>	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	変更内容
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

マッピングは増分値であり、絶対値ではありません。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 はすべて 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 インスタンスに移動する方法を示します。

```
Switch(config-mst)# no instance 2
Switch(config-mst)#
```

関連コマンド

コマンド	説明
name	MST 領域名を設定します。
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。

■ instance