# ネットワーク管理コマンド

# destination（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元セッションの宛先を設定するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで **destination** コマンドを使用します。宛先セッ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。

**destination**
**no destination**

## 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

送信元セッションの宛先は設定されていません。

## コマンド モード

ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

## コマンド履歴

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

## 使用上のガイドライン

ERSPAN トラフィックは、GRE カプセル化された SPAN トラフィックで、ERSPAN 宛先セッションによってだけ処理されます。

すべての ERSPAN 送信元セッション（最大 8）の宛先 IP アドレスが同一である必要はありません。ERSPAN 宛先セッションに IP アドレスを設定するには、**ip address** コマンドを入力します。

ERSPAN 送信元セッションの宛先 IP アドレスが（宛先スイッチ上のインターフェイスで設定される）、ERSPAN 宛先セッションが宛先ポートに送信するトラフィックの送信元です。**ip address** コマンドを使用して、送信元セッションおよび宛先セッションの両方に同一のアドレスを設定します。

## 例

次に、ERSPAN 送信元セッションの宛先を設定し、ERSPAN モニタ宛先セッション コンフィギュレーション モードを開始して、宛先プロパティを指定する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)#ip address 10.1.1.1
Switch(config-mon-erspan-src-dst)#
```

次の **show monitor session all** の出力例には、送信元セッションの宛先の異なる IP アドレスが示されています。

```
Switch# show monitor session all

Session 1
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session1
```

```
Destination IP Address : 10.1.1.1


Session 2
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session2
Destination IP Address : 192.0.2.1


Session 3
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session3
Destination IP Address : 198.51.100.1

Session 4
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session4
Destination IP Address : 203.0.113.1


Session 5
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session5
Destination IP Address : 209.165.200.225
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **erspan-id** | ERSPAN トラフィックを識別するため、宛先セッションで使用される ID を設定します。 |
| **ip ttl** | ERSPAN トラフィックのパケットの TTL 値を設定します。 |
| **monitor session type erspan-source** | ローカルの ERSPAN 送信元セッションを設定します。 |
| **origin** | ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。 |

# event manager applet

Embedded Event Manager（EEM）にアプレットを登録してアプレット コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **event manager applet** コマンドを使用します。アプレットを登録解除するには、このコマンドの **no** 形式を使用します。

**event manager applet** *applet-name* [**authorization bypass**] [**class** *class-options*] [**trap**]
**no event manager applet** *applet-name* [**authorization bypass**] [**class** *class-options*] [**trap**]

## 構文の説明

| | |
|---|---|
| *applet-name* | アプレット ファイルの名前。 |
| **authorization** | （任意）アプレットの AAA 許可タイプを指定します。 |
| **bypass** | （任意）EEM の AAA 許可タイプのバイパスを指定します。 |
| **class** | （任意）EEM ポリシー クラスを指定します。 |
| *class-options* | （任意）EEM ポリシー クラス。次のいずれかを指定できます：<br>• *class-letter*： 各ポリシークラスを識別する A ～ Z の文字。任意の *class-letter* を 1 つ指定できます。<br>• **default** ：デフォルトクラスに登録されたポリシーを指定します。 |
| **trap** | （任意）ポリシーがトリガーされたときに簡易ネットワーク管理プロトコル（SNMP）トラップを生成します。 |

## コマンド デフォルト

EEM アプレットは登録されません。

## コマンド モード

グローバル コンフィギュレーション（config）

## コマンド履歴

## コマンド履歴

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

## 使用上のガイドライン

EEM アプレットは、イベント スクリーニング基準とイベント発生時に実行するアクションを定義する簡潔な方法です。

アプレット コンフィギュレーションでは、event コンフィギュレーション コマンドを 1 つだけ使用できます。アプレット コンフィギュレーション サブモードが終了し、event コマンドが存在しない場合は、アプレットにイベントが関連付けられていないことを示す警告が表示されます。イベントが指定されていない場合、このアプレットは登録されたと判断されないため、アプレットは表示されません。このアプレットにアクションが割り当てられない場合、イベントはトリガーされますが、アクションは実行されません。1 つのアプレット コンフィギュレーション内で複数の action アプレット コンフィギュレーション コマンドが使用できます。登録

済みのアプレットを表示するには、**show event manager policy registered** コマンドを使用します。

アプレット コンフィギュレーション モードを終了しないと既存のアプレットが置き換えられないため、EEM アプレットを変更する前に、このコマンドの **no** 形式を使用して登録を解除します。アプレット コンフィギュレーション モードでアプレットを修正中であっても、既存のアプレットを実行できます。アプレット コンフィギュレーション モードを終了すると、古いアプレットが登録解除され、新しいバージョンが登録されます。

（注） 部分的な変更は行わないでください。EEM は、すでに登録されているポリシーの部分的な変更をサポートしません。EEM ポリシーは、変更で再登録する前に、常に登録解除する必要があります。

action コンフィギュレーション コマンドは、*label* 引数を使用することで一意に識別できます。label 引数には任意の文字列値が使用できます。アクションは、*label* 引数をソートキーとして、英数字のキーの昇順にソートされ、この順序で実行されます。

EEM は、ポリシー自体に含まれているイベントの指定内容に基づいて、ポリシーをスケジューリングおよび実行します。アプレット コンフィギュレーション モードが終了するとき、EEM は、入力された event コマンドと action コマンドを検査し、指定されたイベントの発生時に実行されるようにアプレットを登録します。

EEM ポリシーは、登録されたときに **class** *class-letter* が指定されている場合はクラスに割り当てられます。クラスなしで登録された EEM ポリシーは、**default**クラスに割り当てられます。**default**をクラスとして保持するスレッドは、スレッドが作業に利用可能であるとき、デフォルトクラスにサービスを提供します。特定のクラス文字に割り当てられたスレッドは、スレッドが作業に利用可能であるとき、クラス文字が一致する任意のポリシーをサービスします。

EEM 実行スレッドが、指定されたクラスのポリシー実行に利用可能でない場合で、クラスのスケジューラルールが設定されている場合は、ポリシーは該当クラスのスレッドが実行可能になるまで待ちます。同じ入力イベントからトリガーされた同期ポリシーは、同一の実行スレッドにスケジュールされなければなりません。ポリシーは、queue_priority をキューイング順序として使用し、各クラスの別々のキューにキューイングされます。

ポリシーがトリガーされると、AAA が設定されている場合は、許可のために AAA サーバに接続します。**authorization bypass** キーワードの組み合わせを使用して、AAA サーバへの接続をスキップし、ポリシーをただちに実行することができます。EEM は、AAA バイパス ポリシー名をリストに保存します。このリストは、ポリシーがトリガーされたときに検査されます。一致が見つかった場合、AAA 許可はバイパスされます。

EEM ポリシーによって設定されたコマンドの許可を避けるために、EEM は AAA が提供する名前付き方式リストを使用します。これらの名前付き方式リストは、コマンド許可を持たないように設定できます。

次に、AAA の設定例を示します。

この設定は、192.168.10.1 のポート 10000 に TACACS+ サーバを想定しています。TACACS+ サーバがイネーブルでない場合、コンフィギュレーション コマンドは、コンソールで許可されます。ただし、EEM ポリシーとアプレット CLI の相互動作は失敗します。

```
enable password lab
aaa new-model
tacacs-server host 128.107.164.152 port 10000
tacacs-server key cisco
aaa authentication login consoleline none
aaa authorization exec consoleline none
aaa authorization commands 1 consoleline none
aaa authorization commands 15 consoleline none
line con 0
 exec-timeout 0 0
 login authentication consoleline
aaa authentication login default group tacacs+ enable
aaa authorization exec default group tacacs+
aaa authorization commands 1 default group tacacs+
aaa authorization commands 15 default group tacacs+
```

**authorization** キーワード、**class** キーワード、**trap** キーワードは任意の組み合わせで使用できます。

## 例

次に、IPSLAping1 という名前の EEM アプレットが登録され、指定された SNMP オブジェクト ID の値と完全一致する（正常な IP SLA ICMP エコー動作を表す）場合に実行される例を示します（これは**ping** コマンドに相当します）。エコー操作が失敗した場合は 4 つのアクションがトリガーされ、イベント モニタリングは 2 回目の失敗後までディセーブルにされます。サーバへの ICMP エコー動作が失敗したことを示すメッセージが syslog に送信され、SNMP トラップが生成され、EEM はアプリケーション固有のイベントをパブリッシュし、IPSLA1F というカウンタが値 1 で増分されます。

```
Router(config)# event manager applet IPSLAping1
Router(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.42.1.2.9.1.6.4 get-type exact
entry-op eq entry-val 1 exit-op eq exit-val 2 poll-interval 5
Router(config-applet)# action 1.0 syslog priority critical msg "Server IP echo failed:
OID=$_snmp_oid_val"
Router(config-applet)# action 1.1 snmp-trap strdata "EEM detected server reachability
failure to 10.1.88.9"
Router(config-applet)# action 1.2 publish-event sub-system 88000101 type 1 arg1 10.1.88.9
arg2 IPSLAEcho arg3 fail
Router(config-applet)# action 1.3 counter name _IPSLA1F value 1 op inc
```

次に、名前 one、クラス A でアプレットを登録し、タイマー イベント ディテクタが 10 秒ごとにイベントをトリガーするアプレット コンフィギュレーション モードを開始する例を示します。イベントがトリガーされると、**action syslog** コマンドにより、syslog にメッセージ「hello world」が書き込まれます。

```
Router(config)# event manager applet one class A
Router(config-applet)# event timer watchdog time 10
Router(config-applet)# action syslog syslog msg "hello world"
Router(config-applet)# exit
```

次に、名前 one、クラス A でアプレットを登録するときに、AAA 許可をバイパスする例を示します。

```
Router(config)# event manager applet one class A authorization bypass
Router(config-applet)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show event manager policy registered** | 登録されているEEMポリシーを表示します。 |

# filter（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元がトランクポートの場合に、ERSPAN 送信元 VLAN フィルタリングを設定するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで **filter** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

**filter** {**ip access-group** {*standard-access-list extended-access-list acl-name*} | **ipv6 access-group** *acl-name* | **mac access-group** *acl-name* | **vlan** *vlan-id*[{,}] [{-}]}
**no filter** {**ip** [{**access-group** | [{*standard-access-list extended-access-list acl-name*}]}] | **ipv6** [{**access-group**}] | **mac** [{**access-group**}] | **vlan** *vlan-id*[{,}] [{-}]}

## 構文の説明

| | |
|---|---|
| **ip** | IP アクセス制御ルールを指定します。 |
| **access-group** | アクセス制御グループを指定します。 |
| *standard-access-list* | 標準 IP アクセスリスト。 |
| *extended-access-list* | 拡張 IP アクセスリスト。 |
| *acl-name* | アクセスリスト名。 |
| **ipv6** | IPv6 アクセス制御ルールを指定します。 |
| **mac** | Media Access Control（MAC）ルールを指定します。 |
| **vlan** *vlan-ID* | ERSPAN 送信元 VLAN を指定します。有効な値は 1 ～ 4094 です。 |
| , | （任意）別の VLAN を指定します。 |
| - | （任意）VLAN の範囲を指定します。 |

## コマンド デフォルト

送信元 VLAN フィルタリングは設定されていません。

## コマンド モード

ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

## コマンド履歴

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

## 使用上のガイドライン

送信元 VLAN とフィルタ VLAN を同じセッションに含めることはできません。

モニタされたトランクインターフェイス上で **filter** コマンドを設定した場合、指定された VLAN セット上のトラフィックだけがモニタされます。

## 例

次に、送信元 VLAN フィルタリングを設定する例を示します。

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# filter vlan 3
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **monitor session type erspan-source** | ローカルのERSPAN送信元セッションを設定します。 |

# ip wccp

Web キャッシュサービスをイネーブルにし、アプリケーションエンジンで定義されたダイナミックサービスに対応するサービス番号を指定するには、device で **ip wccp** 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。サービ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。

**ip wccp** {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]
**no ip wccp** {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]

## 構文の説明

| | |
|---|---|
| **web-cache** | Web キャッシュ サービスを指定します（WCCP バージョン 1 とバージョン 2）。 |
| *service-number* | ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 の範囲で指定できます。サービスの最大数（**web-cache** キーワードで指定する Web キャッシュサービスを含む）は 256 です。 |
| **group-address** *groupaddress* | （任意）サービス グループに参加するために devices およびアプリケーションエンジンが使用するマルチキャスト グループ アドレスを指定します。 |
| **group-list** *access-list* | （任意）マルチキャスト グループ アドレスが使用されない場合、サービス グループに加入しているアプリケーション エンジンに対応する有効な IP アドレスのリストを指定します。 |
| **redirect-list** *access-list* | （任意）ホストから特定のホストまたは特定のパケットのリダイレクト サービスを指定します。 |
| **password** *encryption-number password* | （任意）暗号化番号を指定します。指定できる範囲は 0 ～ 7 です。暗号化しない場合は 0、独自の場合は 7 を使用します。また、7 文字以内でパスワード名を指定します。device は、パスワードと MD5 認証値を組み合わせて、device とアプリケーション エンジンとの接続にセキュリティを確保します。デフォルトでは、パスワードは設定されておらず、認証も実行されていません。 |

## コマンド デフォルト

WCCP サービスがデバイスでイネーブルにされていません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

シスコ エクスプレス フォワーディング スイッチングがイネーブルのとき、WCCP の透過的キャッシングはネットワーク アドレス変換（NAT）をバイパスします。この状況に対処するには、発信方向で WCCP 透過キャッシングを設定し、コンテンツ エンジン インターフェイスで Cisco Express Forwarding スイッチングを有効にし、**ip wccp web-cache redirect out** コマンドを指定します。キャッシュに面するルータ インターフェイスで **ip wccp redirect exclude in** コマンドを指定し、内部インターフェイスの着信方向に WCCP を設定します。この設定は、そのインターフェイスに到着したパケットのリダイレクションを回避します。

サービス グループを設定するときにリダイレクト リストを含めることもできます。指定されたリダイレクト リストは、NAT（送信元）IP アドレスを含むパケットを拒否して、リダイレクションを阻止します。

このコマンドは、指定されたサービス番号または Web キャッシュ サービス名のサポートをイネーブルまたはディセーブルにするよう device に指示します。サービス番号は 0 ～ 254 の範囲で指定できます。サービス番号または名前がイネーブルになると、ルータはサービス グループの確立に参加できます。

**no ip wccp** コマンドが入力されると、device はサービスグループへの参加を終了し、引き続きサービスが設定されているインターフェイスがなければ領域の割り当てを解除し、他のサービスが設定されていなければ WCCP タスクを終了します。

**web-cache** に続くキーワードと *service-number* 引数はオプションで、任意の順序で指定できますが、1 回しか指定できません。

### 例

次に、Web キャッシュ、アプリケーション エンジンまたはサーバに接続されたインターフェイス、およびクライアントに接続するインターフェイスを設定する例を示します。

```
デバイス(config)# ip wccp web-cache
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# no switchport
デバイス(config-if)# ip address 172.20.10.30 255.255.255.0
デバイス(config-if)# no shutdown
デバイス(config-if)# exit
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# no switchport
デバイス(config-if)#
*Dec  6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to
down

デバイス(config-if)# ip address 175.20.20.10 255.255.255.0
デバイス(config-if)# no shutdown
デバイス(config-if)# ip wccp web-cache redirect in
デバイス(config-if)# ip wccp web-cache group-listen
```

```
デバイス(config-if)# exit
```

# monitor session

ポート間のトラフィック分析のために、イーサネット スイッチド ポート アナライザ（SPAN）セッションまたはリモート スイッチド ポート アナライザ（RSPAN）セッションのコンフィギュレーションを新規作成するか、既存のセッションのコンフィギュレーションに追加するには、**monitor session** 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。SPAN セッションまたは RSPAN セッションをクリアするには、このコマンドの **no** 形式を使用します。

**monitor session** *session-number* {**destination** | **filter** | **source**}
**no monitor session** {*session-number* [**destination** | **filter** | **source**] | **all** | **local** | **range** *session-range* | **remote**}

## 構文の説明

| *session-number* | |
|---|---|
| **all** | すべてのモニタ セッションをクリアします。 |
| **local** | すべてのローカル モニタ セッションをクリアします。 |
| **range** *session-range* | 指定された範囲のモニタ セッションをクリアします。 |
| **remote** | すべてのリモート モニタ セッションをクリアします。 |

## コマンド デフォルト

モニタ セッションは設定されていません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

### 例

次に、ローカル SPAN セッション 1 を作成して Po13（EtherChannel ポート）のトラフィックをモニタし、セッションの SPAN トラフィックを VLAN 1281 のみに限定する例を示します。出力トラフィックは送信元を複製します。入力転送はイネーブルになりません。

```
デバイス(config)# monitor session 1 source interface Po13
デバイス(config)# monitor session 1 filter vlan 1281
デバイス(config)# monitor session 1 destination interface GigabitEthernet2/0/36
encapsulation replicate
デバイス(config)# monitor session 1 destination interface GigabitEthernet3/0/36
encapsulation replicate
```

次に、これらのセットアップ手順を完了した後の **show monitor session all** コマンドの出力を示します。

```
デバイス# show monitor session all

Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Po13
Destination Ports      : Gi2/0/36,Gi3/0/36
    Encapsulation      : Replicate
          Ingress      : Disabled
Filter VLANs           : 1281
...
```

# monitor session

ポート間のトラフィック分析のために、イーサネットスイッチドポートアナライザ（SPAN）セッション、リモートスイッチドポートアナライザ（RSPAN）セッション、またはEncapsulated Remote Switched Port Analyzer（ERSPAN）セッションのコンフィギュレーションを新規作成するか、既存のセッションのコンフィギュレーションに追加するには、**monitor session** 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。セッションをクリアするには、このコマンドの **no** 形式を使用します。

**monitor session** *session-number* {**destination** | **filter** | **source** | **type** {**erspan-destination** | **erspan-source**}}
**no monitor session** {*session-number* [**destination** | **filter** | **source** | **type** {**erspan-destination** | **erspan-source**}] | **all** | **local** | **range** *session-range* | **remote**}

## 構文の説明

| | |
|---|---|
| *session-number* | セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。 |
| **all** | すべてのモニタ セッションをクリアします。 |
| **local** | すべてのローカルモニタセッションをクリアします。 |
| **range** *session-range* | 指定された範囲のモニタ セッションをクリアします。 |
| **remote** | すべてのリモートモニタセッションをクリアします。 |

## コマンド デフォルト

モニタ セッションは設定されていません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| Cisco IOS XE Fuji 16.9.2 | このコマンドが導入されました。 |
| Cisco IOS XE Gibraltar 16.11.1 | **type** {**erspan-destination** | **erspan-source**} キーワードが導入されました。 |

## 使用上のガイドライン

2 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチスタック上で、合計 66 の SPAN、RSPAN、および ERSPAN セッションを保有できます。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、FRSPAN、および ERSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

### 例

次に、ローカル SPAN セッション 1 を作成して Po13（EtherChannel ポート）のトラフィックをモニタし、セッションの SPAN トラフィックを VLAN 1281 のみに限定する例を示します。出力トラフィックは送信元を複製します。入力転送はイネーブルになりません。

```
Device(config)# monitor session 1 source interface Po13
Device(config)# monitor session 1 filter vlan 1281
Device(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
 replicate
Device(config)# monitor session 1 destination interface GigabitEthernet3/0/36 encapsulation
 replicate
```

次に、これらのセットアップ手順を完了した後の **show monitor session all** コマンドの出力を示します。

```
Device# show monitor session all

Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Po13
Destination Ports      : Gi2/0/36,Gi3/0/36
    Encapsulation      : Replicate
          Ingress      : Disabled
Filter VLANs           : 1281
...
```

# monitor session destination

新規にスイッチドポートアナライザ（SPAN）セッションまたはリモート SPAN（RSPAN）宛先セッションを開始し、ネットワーク セキュリティ デバイス（Cisco IDS Sensor アプライアンスなど）の宛先ポート上の入力トラフィックをイネーブルにし、既存の SPAN または RSPAN セッションでインターフェイスを追加または削除するには、**monitor session destination** 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。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから宛先インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

**monitor session** *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**]} | {**remote**} **vlan** *vlan-id*
**no monitor session** *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**]} | {**remote**} **vlan** *vlan-id*

## 構文の説明

| | |
|---|---|
| *session-number* | |
| **interface** *interface-id* | SPAN または RSPAN セッションの宛先または送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポート チャネルも有効なインターフェイス タイプであり、指定できる範囲は 1 ～ 128 です。 |
| **,** | （任意）複数のインターフェイスまたはVLANを指定します。または、前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。 |
| **-** | （任意）インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。 |
| **encapsulation replicate** | （任意）宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。<br><br>次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。**encapsulation** オプションは、**no** 形式では無視されます。 |

| | |
|---|---|
| **encapsulation dot1q** | （任意）宛先インターフェイスが IEEE 802.1Q カプセル化の送信元インターフェイスの着信パケットを受け入れるように指定します。<br><br>次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。**encapsulation** オプションは、**no** 形式では無視されます。 |
| **ingress** | 入力トラフィック転送をイネーブルにします。 |
| **dot1q** | （任意）指定された VLAN をデフォルト VLAN として、IEEE 802.1Q カプセル化された着信パケットを受け入れます。 |
| **untagged** | （任意）指定された VLAN をデフォルト VLAN として、タグなしカプセル化された着信パケットを受け入れます。 |
| **isl** | ISL カプセル化を使用して入力トラフィックを転送するように指定します。 |
| **remote** | RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。<br><br>RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。 |
| **vlan** *vlan-id* | **ingress** キーワードとのみ使用された場合、入力トラフィックに対するデフォルトの VLAN を設定します。 |

## コマンド デフォルト

モニタ セッションは設定されていません。

ローカル SPAN の宛先ポートで **encapsulation replicate** が指定されなかった場合、パケットはカプセル化のタグなしのネイティブ形式で送信されます。

入力転送は宛先ポートではディセーブルになっています。

**all**、**local**、**range** *session-range*、**remote** を **no monitor session** コマンドに指定することで、すべての SPAN および RSPAN、すべてのローカル SPAN、範囲、すべての RSPAN セッションをクリアできます。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

SPAN または RSPAN の宛先は物理ポートである必要があります。

スイッチ上またはスイッチ スタック上で、最大 64 の宛先ポートを保有できます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1 つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN（VSPAN）を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1 つのポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。**[,|-]** オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ（,）の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

EtherChannel ポートは、SPAN または RSPAN 宛先ポートとして設定することは。EtherChannel グループのメンバである物理ポートは、宛先ポートとして使用できます。ただし、SPAN の宛先として機能する間は、EtherChannel グループに参加できません。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1X 認証をイネーブルにすることはできますが、ポートが SPAN 宛先として削除されるまで IEEE 802.1X 認証はディセーブルです。IEEE 802.1X 認証がポート上で使用できない場合、スイッチはエラー メッセージを返します。SPAN または RSPAN 送信元ポートでは IEEE 802.1X 認証をイネーブルにすることができます。

入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。

宛先ポートは次のような動作を設定できます。

- **monitor session** *session_number* **destination interface** *interface-id* を他のキーワードなしで入力すると、出力のカプセル化はタグなしとなり、入力転送はイネーブルになりません。
- **monitor session** *session_number* **destination interface** *interface-id* **ingress** を入力した場合は、出力カプセル化はタグなしで、入力カプセル化はそのあとに続くキーワードが **dot1q** と **untagged** のいずれであるかによって決まります。

- **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** を他のキーワードなしで入力すると、出力のカプセル化はソースインターフェイスのカプセル化を複製し、入力転送はイネーブルになりません（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。
- **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate ingress** を入力した場合は、出力カプセル化は送信元インターフェイスカプセル化を複製し、入力カプセル化はそのあとに続くキーワードが **dot1q** と **untagged** のいずれであるかによって決まります（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

### 例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
デバイス(config)# monitor session 1 source interface gigabitethernet1/0/1 both
デバイス(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、宛先ポートを既存のローカル SPAN セッションから削除する方法を示します。

```
デバイス(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

次の例では、ある送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
デバイス(config)# monitor session 1 source interface gigabitethernet1/0/1
デバイス(config)# monitor session 1 destination remote vlan 900
デバイス(config)# end
```

次の例では、モニタリングされたトラフィックを受信するスイッチに、RSPAN 宛先セッション 10 を設定する方法を示します。

```
デバイス(config)# monitor session 10 source remote vlan 900
デバイス(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。出力トラフィックは送信元のカプセル化を複製します。入力トラフィックは IEEE 802.1Q カプセル化を使用します。

```
デバイス(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 dot1q ingress dot1q vlan 5
```

次の例では、カプセル化をサポートしないセキュリティ デバイスを使用して、VLAN 5 上の入力トラフィックの宛先ポートを設定する方法を示します。出力トラフィックおよび入力トラフィックはタグなしです。

```
デバイス(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
untagged vlan 5
```

# monitor session filter

フローベース SPAN（FSPAN）セッションやフローベース RSPAN（FRSPAN）送信元または宛先セッションを新しく開始する、または特定の VLAN に対して SPAN 送信元トラフィックを制限（フィルタ処理）するには、**monitor session filter** 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。SPAN または RSPAN セッションからフィルタを削除するには、このコマンドの **no** 形式を使用します。

**monitor session** *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }
**no monitor session** *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }

## 構文の説明

| | |
|---|---|
| *session-number* | |
| **vlan** *vlan-id* | SPAN 送信元トラフィックを特定の VLAN に制限するため、トランクの送信元ポート上のフィルタとしてVLANのリストを指定します。*vlan-id* で指定できる範囲は 1 ～ 4094 です。 |
| , | 任意）複数の VLAN を指定します。または VLAN 範囲を前の範囲から区切ります。カンマの前後にスペースを入れます。 |
| - | （任意）VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。 |

## コマンド デフォルト

モニタ セッションは設定されていません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

1 つの VLAN、または複数のポートや VLAN、特定範囲のポートや VLAN でトラフィックをモニタできます。複数または一定範囲の VLAN を指定するには、[,|-] オプションを使用します。

複数の VLAN を指定するときは、カンマ（,）の前後にスペースが必要です。VLAN の範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

VLAN のフィルタリングは、トランクの送信元ポート上で選択された一連の VLAN のネットワーク トラフィック解析を参照します。デフォルトでは、すべての VLAN がトランクの送信元ポートでモニタリングされます。**monitor session** *session_number* **filter vlan** *vlan-id* コマンドを使用すると、トランク送信元ポートの SPAN トラフィックを指定された VLAN だけに限定できます。

VLAN のモニタリングおよび VLAN のフィルタリングは相互に排他的な関係です。VLAN が送信元の場合、VLANのフィルタリングはイネーブルにできません。VLANのフィルタリングが設定されている場合、VLAN は送信元になることができません。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

### 例

次の例では、既存のセッションの SPAN トラフィックを指定の VLAN だけに制限する方法を示します。

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

次に、ローカル SPAN セッション 1 を作成してスタック メンバ 1 の送信元ポート 1 とスタック メンバ 2 の宛先ポートの送受信両方のトラフィックをモニタし、FSPAN セッションでアクセス リスト番号 122 を使用して IPv4 トラフィックをフィルタする例を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 1 filter ip access-group 122
```

# monitor session source

スイッチドポートアナライザ（SPAN）セッションまたはリモートSPAN（RSPAN）送信元セッションを開始する、または既存のSPANまたはRSPANセッションでインターフェイスを追加または削除するには、**monitor session source** 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。SPANまたはRSPANセッションを削除したり、SPANまたはRSPANセッションから送信元インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

**monitor session** *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}
**no monitor session** *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}

## 構文の説明

*session_number*

| | |
|---|---|
| **interface** *interface-id* | SPANまたはRSPANセッションの送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポートチャネルも有効なインターフェイスタイプであり、指定できる範囲は1 ～ 48 です。 |
| **,** | （任意）複数のインターフェイスまたはVLANを指定します。または、前の範囲からインターフェイスまたはVLANの範囲を分離します。カンマの前後にスペースを入れます。 |
| **-** | （任意）インターフェイスまたはVLANの範囲を指定します。ハイフンの前後にスペースを入れます。 |
| **both** \| **rx** \| **tx** | （任意）モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。 |
| **remote** | （任意）RSPAN送信元または宛先セッションのリモートVLANを指定します。指定できる範囲は2 ～ 1001または1006 ～ 4094です。<br><br>RSPAN VLANはVLAN 1（デフォルトのVLAN）、またはVLAN ID 1002 ～ 1005（トークンリングおよびFDDI VLANに予約済）になることはできません。 |

| | |
|---|---|
| **vlan** *vlan-id* | **ingress** キーワードだけで使用された場合、入力トラフィックにデフォルトの VLAN を設定します。 |

**コマンド デフォルト**

モニタ セッションは設定されていません。

送信元インターフェイスのデフォルトでは、受信トラフィックと送信トラフィックの両方をモニタリングします。

送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。

**コマンド モード**

グローバル コンフィギュレーション

**コマンド履歴**

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

**使用上のガイドライン**

送信元ポートまたは送信元 VLAN を出入りするトラフィックは、SPAN または RSPAN を使用してモニタできます。送信元ポートまたは送信元 VLAN にルーティングされるトラフィックはモニタできません。

物理ポート、ポート チャネル、VLAN が送信元になることができます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1 つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN（VSPAN）を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1 つのポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。[,|-] オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ（,）の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

個々のポートはそれらが EtherChannel に参加している間もモニタリングすることができます。また、RSPAN 送信元インターフェイスとして **port-channel** 番号を指定することで EtherChannel バンドル全体をモニタリングすることができます。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 送信元ポートでは IEEE 802.1X 認証をイネーブルにすることができます。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

### 例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、複数の送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

# monitor session type erspan-source

ローカルの Encapsulated Remote Switched Port Analyzer（ERSPAN）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 **monitor session type erspan-source** コマンドを使用します。ERSPAN 設定を削除するには、このコマンドの **no** 形式を使用します。

**monitor session** *span-session-number* **type erspan-source**
**no monitor session** *span-session-number* **type erspan-source**

## 構文の説明

| | |
|---|---|
| *span-session-number* | ローカル ERSPAN セッションの番号。有効値は 1 ～ 66 です。 |

## コマンド デフォルト

ERSPAN 送信元セッションは設定されていません。

## コマンド モード

グローバル コンフィギュレーション（config）

## コマンド履歴

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

## 使用上のガイドライン

*span-session-number* およびセッション タイプ（*erspan-source* キーワードによって設定）は、設定後は変更できません。セッションを削除するには、このコマンドの **no** 形式を使用し、新しいセッション ID または新しいセッション タイプでセッションを再作成します。

ERSPAN 送信元セッションの宛先 IP アドレスが（宛先スイッチ上のインターフェイスで設定される必要がある）、ERSPAN宛先セッションが宛先ポートに送信するトラフィックの送信元です。ERSPAN モニタ宛先セッション コンフィギュレーション モードで **ip address** コマンドを使用して、送信元セッションと宛先セッションの両方に同じアドレスを設定できます。

ERSPAN ID により、同じ宛先 IP アドレスに着信する ERSPAN トラフィックと異なる ERSPAN 送信元セッションとが区別されます。

ローカル ERSPAN 送信元セッションの最大数は 8 に制限されています。

## 例

次に、ERSPAN 送信元セッション番号を設定する例を示します。

```
Switch(config)# monitor session 55 type erspan-source
Switch(config-mon-erspan-src)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **monitor session type** | ERSPAN 送信元セッション番号を作成するか、セッションに対して ERSPAN セッション コンフィギュレーション モードを開始します。 |
| **show capability feature monitor** | モニタ機能に関する情報を表示します。 |

| コマンド | 説明 |
| --- | --- |
| **show monitor session** | ERSPAN、SPAN、RSPAN のセッションに関する情報を表示します。 |

# show ip sla statistics

Cisco IOS IP サービスレベル契約（SLA）のすべての動作または指定された動作の現在または集約された動作ステータスおよび統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip sla statistics** コマンドを使用します。

**show ip sla statistics** ［ *operation-number* ［**details**］ | **aggregated** ［ *operation-number* | **details**］ | **details**］

## 構文の説明

| | |
|---|---|
| *operation-number* | （任意）動作ステータスおよび統計情報を表示する動作の番号。受け入れられる値の範囲は 1 ～ 2147483647 です。 |
| **details** | （任意）詳細出力を指定します。 |
| **aggregated** | （任意）IP SLA 集約統計を指定します。 |

## コマンド デフォルト

稼働しているすべての IP SLA 動作の出力を表示します。

## コマンド モード

ユーザ EXEC

特権 EXEC

## コマンド履歴

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

## 使用上のガイドライン

動作の残りの継続時間、動作がアクティブかどうか、完了時刻など、IP SLA 動作の現在の状態を表示するには、 **show ip sla statistics** を使用します。出力には、最後の（最近完了した）動作に対して返されたモニタリング データも含まれます。この生成された操作 ID は、基本マルチキャスト操作に対して、また操作全体の要約統計の一部として **show ip sla** コンフィギュレーション コマンドを使用すると表示されます。

あるレスポンダに対して詳細を表示するには、その特定の操作IDに**show**コマンドを入力します。

### 例

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

```
デバイス# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
```

```
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

# show monitor

すべてのスイッチドポートアナライザ（SPAN）およびリモート SPAN（RSPAN）セッションに関する情報を表示するには、EXEC モードで **show monitor** コマンドを使用します。

**show monitor** ［**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} ［**detail**］］

## 構文の説明

| | |
|---|---|
| **session** | （任意）指定された SPAN セッションの情報を表示します。 |
| *session_number* | |
| **all** | （任意）すべての SPAN セッションを表示します。 |
| **local** | （任意）ローカル SPAN セッションだけを表示します。 |
| **range** *list* | （任意）一定範囲の SPAN セッションを表示します。*list* は有効なセッションの範囲です。range は単一のセッション、または 2 つの数字を小さい数字からハイフンで区切ったセッションの範囲です。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。<br>（注） このキーワードは、特権 EXEC モードの場合だけ使用可能です。 |
| **remote** | （任意）リモート SPAN セッションだけを表示します。 |
| **detail** | （任意）指定されたセッションの詳細情報を表示します。 |

## コマンド モード

ユーザ EXEC

特権 EXEC

## コマンド履歴

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

## 使用上のガイドライン

**show monitor** コマンドと **show monitor session all** コマンドの出力は同じです。

### 例

次に、**show monitor** ユーザ EXEC コマンドの出力例を示します。

```
デバイス# show monitor
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

次の例では、ローカル SPAN 送信元セッション 1 に対する **show monitor** ユーザ EXEC コマンドの出力を示します。

```
デバイス# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次の例では、入力トラフィック転送をイネーブルにした場合の **show monitor session all** ユーザ EXEC コマンドの出力を示します。

```
デバイス# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
```

```
Ingress encap : Untagged
```

# show monitor session

すべてのスイッチドポートアナライザ（SPAN）およびリモート SPAN（RSPAN）セッションに関する情報を表示するには、EXEC モードで **show monitor session** コマンドを使用します。

**show monitor session** {*session_number* | **all** | **erspan-source** | **local** | **range** *list* | **remote**} [**detail**]

## 構文の説明

| | |
|---|---|
| *session_number* | SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 68 です。ただし、このスイッチが Catalyst 2960-S スイッチとスタックされる場合、2 個のローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値に限定され、範囲は 1 ～ 66 になります。 |
| **all** | すべての SPAN セッションを表示します。 |
| **erspan-source** | 送信元 ERSPAN セッションだけを表示します。 |
| **local** | ローカル SPAN セッションだけを表示します。 |
| **range** *list* | 一定範囲の SPAN セッションを表示します。*list* は有効なセッションの範囲です。range は単一のセッション、または 2 つの数字を小さい数字からハイフンで区切ったセッションの範囲です。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。<br>（注） このキーワードは、特権 EXEC モードの場合だけ使用可能です。 |
| **remote** | リモート SPAN セッションだけを表示します。 |
| **detail** | （任意）指定されたセッションの詳細情報を表示します。 |

## コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

## コマンド履歴

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

**使用上のガイドライン** ローカルの ERSPAN 送信元セッションの最大数は 8 です。

### 例

次に、ローカル SPAN 送信元セッション 1 に対する **show monitor session** コマンドの出力例を示します。

```
デバイス# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次に、入力トラフィックの転送が有効になっている場合の **show monitor session all** コマンドの出力例を示します。

```
デバイス# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

次に、**show monitor session erspan-source** コマンドの出力例を示します。

```
Switch# show monitor session erspan-source

Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
RX Only : Gi1/4/33
Destination IP Address : 20.20.163.20
Destination ERSPAN ID : 110
Origin IP Address : 10.10.10.216
IPv6 Flow Label : None
```

# show platform software fed switch ip wccp

プラットフォーム依存 Web Cache Communication Protocol（WCCP）情報を表示するには、**show platform software fed switch ip wccp** 特権 EXEC コマンドを使用します。

```
show platform software fed switch{switch-number|active|standby}ip
wccp{cache-engines |interfaces |service-groups}
```

## 構文の説明

| | |
|---|---|
| **switch**{*switch_num*\|**active**\|**standby**} | 情報を表示するデバイス。<br>• *switch_num*：スイッチ ID を入力します。指定されたスイッチに関する情報を表示します。<br>• **active**：アクティブスイッチの情報を表示します。<br>• **standby**：存在する場合、スタンバイスイッチの情報を表示します。 |
| **cache-engines** | WCCP キャッシュ エンジンを表示します。 |
| **interfaces** | WCCP インターフェイスを表示します。 |
| **service-groups** | WCCP サービス グループを表示します。 |

## コマンド モード

特権 EXEC

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

このコマンドは、deviceが IP サービス フィーチャ セットを実行している場合だけ使用可能です。

次に、WCCP インターフェイスを表示する例を示します。

```
デバイス# show platform software fed switch 1 ip wccp interfaces

WCCP Interface Info

=====================

**** WCCP Interface: Port-channel13 iif_id: 000000000000007c (#SG:3),  VRF: 0 Ingress
WCCP ****
port_handle:0x20000f9

List of Service Groups on this interface:
```

```
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority:
 35
Promiscuous mode (no ports).


* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority:
 35
Promiscuous mode (no ports).


* Service group id:60 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority:
 35
Promiscuous mode (no ports).



**** WCCP Interface: Port-channel14 iif_id: 000000000000007e (#SG:3),  VRF: 0 Ingress
WCCP ****
port_handle:0x880000fa

List of Service Groups on this interface:
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority:
 35
Promiscuous mode (no ports).


* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority:
 35
Promiscuous mode (no ports).
<output truncated>
```

# show platform software swspan

スイッチドポートアナライザ（SPAN）情報を表示するには、特権EXECモードで **show platform software swspan** コマンドを使用します。

**show platform software swspan** {**switch**} {{{**F0** | **FP active**} **counters**} | **R0** | **RP active**} {**destination sess-id** *session-ID* | **source sess-id** *session-ID*}

## 構文の説明

| | |
|---|---|
| **switch** | スイッチに関する情報を表示します。 |
| **F0** | Embedded Service Processor（ESP）スロット0に関する情報を表示します。 |
| **FP** | ESP に関する情報を表示します。 |
| **active** | ESP またはルート プロセッサ（RP）のアクティブ インスタンスに関する情報を表示します。 |
| **counters** | SWSPAN メッセージ カウンタを表示します。 |
| **R0** | RP スロット 0 に関する情報を表示します。 |
| **RP** | RP に関する情報を表示します。 |
| **destination sess-id** *session-ID* | 指定された宛先セッションに関する情報を表示します。 |
| **source sess-id** *session-ID* | 指定された送信元セッションに関する情報を表示します。 |

## コマンド モード

特権 EXEC（#）

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| Cisco IOS XE Denali 16.1.1 | このコマンドは、Cisco IOS Release 16.1.1 よりも前のリリースで導入されました。 |

## 使用上のガイドライン

セッション番号が存在しないか、SPAN セッションがリモート接続先セッションの場合、コマンド出力には「% Error: No Information Available」のメッセージが表示されます。

## 例

次に、**show platform software swspan FP active source** コマンドの出力例を示します。

```
Switch# show platform software swspan FP active source sess-id 0

Showing SPAN source detail info

Session ID : 0
Intf Type : PORT
Port dpidx : 30
PD Sess ID : 1
```

```
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 579
AOM Object Status : Done
Parent AOM object Id : 118
Parent AOM object Status : Done

Session ID : 9
Intf Type : PORT
Port dpidx : 8
PD Sess ID : 0
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 578
AOM Object Status : Done
Parent AOM object Id : 70
Parent AOM object Status : Done
```

次に、**show platform software swspan RP active destination** コマンドの出力例を示します。

```
Switch# show platform software swspan RP active destination

Showing SPAN destination table summary info

Sess-id IF-type IF-id Sess-type
---------------------------------------
1 PORT 19 Remote
```

# snmp ifmib ifindex persist

維持させる ifIndex 値をグローバルにイネーブルにし、リブート後も維持されるようにして、Simple Network Management Protocol（SNMP）で使用できるようにするには、グローバル コンフィギュレーション モードで **snmp ifmib ifindex persist** コマンドを使用します。ifIndex パーシステンスをグローバルに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。

**snmp ifmib ifindex persist**
**no snmp ifmib ifindex persist**

## 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

デバイスの ifIndex パーシステンスがディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション（config）

## 使用上のガイドライン

**snmp ifmib ifindex persist** コマンドは、インターフェイス固有の設定をオーバーライドしません。ifIndex パーシステンスのインターフェイス固有の設定は、インターフェイス コンフィギュレーション モードで **snmp ifindex persist** コマンドと **snmp ifindex clear** コマンドを使用して設定されます。

**snmp ifmib ifindex persist** コマンドは、インターフェイス MIB（IF-MIB）の ifIndex テーブル内の ifDescr エントリと ifIndex エントリを使用して、ルーティングデバイス上のすべてのインターフェイスの ifIndex パーシステンスをイネーブルにします。

ifIndex パーシステンスとは、リブート後も IF-MIB 内の ifIndex 値を存続させ、SNMP を使用する特定のインターフェイスの ID が維持されるようにします。

ifIndex パーシステンスが **no snmp ifindex persist** コマンドを使用して、特定のインターフェイスに対して以前にディセーブルされていた場合、ifIndex パーシステンスはそのインターフェイスではディセーブルのままとなります。

## 例

次に、すべてのインターフェイスの ifIndex パーシステンスをイネーブルにする例を示します。

```
Device(config)# snmp ifmib ifindex persist
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **snmp ifindex clear** | 以前に特定のインターフェイスに対してインターフェイス コンフィギュレーション モードで発行された設定済み **snmp ifIndex** コマンドをクリアします。 |
| **snmp ifindex persist** | IF-MIB でリブート後も維持する（ifIndex persistence）ifIndex 値をイネーブルにします。 |

# snmp-server enable traps

deviceでネットワーク管理システム（NMS）にインフォーム要求やさまざまなトラップのSimple Network Management Protocol（SNMP）通知を送信可能にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps** 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。

**snmp-server enable traps** ［**auth-framework** ［**sec-violation**］ | **bridge** | **call-home** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp** ］
**no snmp-server enable traps** ［**auth-framework** ［**sec-violation**］ | **bridge** | **call-home** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp** ］

## 構文の説明

| | |
|---|---|
| **auth-framework** | （任意）SNMP CISCO-AUTH-FRAMEWORK-MIB トラップをイネーブルにします。 |
| **sec-violation** | （任意）SNMP camSecurityViolationNotif 通知をイネーブルにします。 |
| **bridge** | （任意）SNMP STP ブリッジ MIB トラップをイネーブルにします。* |
| **call-home** | （任意）SNMP CISCO-CALLHOME-MIB トラップをイネーブルにします。* |
| **cluster** | （任意）SNMP クラスタ トラップをイネーブルにします。 |
| **config** | （任意）SNMP 設定トラップをイネーブルにします。 |
| **config-copy** | （任意）SNMP 設定コピー トラップをイネーブルにします。 |
| **config-ctid** | （任意）SNMP設定CTID トラップをイネーブルにします。 |
| **copy-config** | （任意）SNMPコピー設定トラップをイネーブルにします。 |
| **cpu** | （任意）CPU 通知トラップをイネーブルにします。* |
| **dot1x** | （任意）SNMP dot1x トラップをイネーブルにします。* |

| | |
|---|---|
| **energywise** | （任意）SNMP energywise トラップをイネーブルにします。* |
| **entity** | （任意）SNMP エンティティ トラップをイネーブルにします。 |
| **envmon** | （任意）SNMP 環境モニタ トラップをイネーブルにします。* |
| **errdisable** | （任意）SNMP エラーディセーブル トラップをイネーブルにします。* |
| **event-manager** | （任意）SNMP 組み込みイベント マネージャ トラップをイネーブルにします。 |
| **flash** | （任意）SNMP フラッシュ通知トラップをイネーブルにします。* |
| **fru-ctrl** | （任意）エンティティ現場交換可能ユニット（FRU）制御トラップを生成します。deviceスタックでは、このトラップはスタックにおけるdeviceの挿入/取り外しを意味します。 |
| **license** | （任意）ライセンス トラップをイネーブルにします。* |
| **mac-notification** | （任意）SNMP MAC 通知トラップをイネーブルにします。* |
| **port-security** | （任意）SNMP ポート セキュリティ トラップをイネーブルにします。* |
| **power-ethernet** | （任意）SNMP パワーイーサネット トラップをイネーブルにします。* |
| **rep** | （任意）SNMP レジリエント イーサネット プロトコル トラップをイネーブルにします。 |
| **snmp** | （任意）SNMP トラップをイネーブルにします。* |
| **stackwise** | （任意）SNMP StackWise トラップをイネーブルにします。* |
| **storm-control** | （任意）SNMP ストーム制御トラップ パラメータをイネーブルにします。 |
| **stpx** | （任意）SNMP STPX MIB トラップをイネーブルにします。* |
| **syslog** | （任意）SNMP syslog トラップをイネーブルにします。 |

| | |
|---|---|
| **transceiver** | （任意）SNMP トランシーバ トラップをイネーブルにします。* |
| **tty** | （任意）TCP接続トラップを送信します。この設定はデフォルトでイネーブルになっています。 |
| **vlan-membership** | （任意）SNMP VLAN メンバーシップ トラップをイネーブルにします。 |
| **vlancreate** | （任意）SNMP VLAN作成トラップをイネーブルにします。 |
| **vlandelete** | （任意）SNMP VLAN削除トラップをイネーブルにします。 |
| **vstack** | （任意）SNMP スマートインストール トラップをイネーブルにします。* |
| **vtp** | （任意）VLAN トランキング プロトコル（VTP）トラップをイネーブルにします。 |

**コマンド デフォルト**

SNMP トラップの送信をディセーブルにします。

**コマンド モード**

グローバル コンフィギュレーション

**コマンド履歴**

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

**使用上のガイドライン**

上記の表のアスタリスクが付いているコマンド オプションにはサブ コマンドがあります。これらのサブ コマンドの詳細については、関連コマンドの項を参照してください。

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

トラップまたは情報がサポートされている場合に、これらの送信をイネーブルにするには、**snmp-server enable traps** コマンドを使用します。

（注） **fru-ctrl, insertion** および **removal**キーワードは、コマンドラインのヘルプストリングに表示されますが、deviceでサポートされていません。**snmp-server enable informs** グローバル コンフィギュレーション コマンドは、サポートされていません。SNMP情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host** *host-addr* **informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、複数の SNMP トラップ タイプをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps cluster
デバイス(config)# snmp-server enable traps config
デバイス(config)# snmp-server enable traps vtp
```

# snmp-server enable traps bridge

STP ブリッジ MIB トラップを生成するには、グローバル コンフィギュレーション モードで **snmp-server enable traps bridge** 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。

**snmp-server enable traps bridge** ［**newroot**］［**topologychange**］
**no snmp-server enable traps bridge** ［**newroot**］［**topologychange**］

## 構文の説明

| | |
|---|---|
| **newroot** | （任意）SNMP STP ブリッジ MIB 新規ルート トラップをイネーブルにします。 |
| **topologychange** | （任意）SNMP STP ブリッジ MIB トポロジ変更トラップをイネーブルにします。 |

## コマンド デフォルト

ブリッジ SNMP トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次の例では、NMS にブリッジ新規ルート トラップを送信する方法を示します。

```
デバイス(config)# snmp-server enable traps bridge newroot
```

# snmp-server enable traps bulkstat

データ収集 MIB トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps bulkstat** 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。

**snmp-server enable traps bulkstat** ［**collection** | **transfer**］
**no snmp-server enable traps bulkstat** ［**collection** | **transfer**］

## 構文の説明

| | |
|---|---|
| **collection** | （任意）データ収集MIB収集トラップをイネーブルにします。 |
| **transfer** | （任意）データ収集MIB送信トラップをイネーブルにします。 |

## コマンド デフォルト

データ収集 MIB トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、データ収集 MIB 収集トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps bulkstat collection
```

# snmp-server enable traps call-home

SNMP CISCO-CALLHOME-MIB トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps call-home** 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。

**snmp-server enable traps call-home** ［**message-send-fail** | **server-fail**］
**no snmp-server enable traps call-home** ［**message-send-fail** | **server-fail**］

## 構文の説明

| | |
|---|---|
| **message-send-fail** | （任意）SNMP メッセージ送信失敗トラップをイネーブルにします。 |
| **server-fail** | （任意）SNMP サーバ障害トラップをイネーブルにします。 |

## コマンド デフォルト

SNMP CISCO-CALLHOME-MIB トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、SNMP メッセージ送信失敗トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps call-home message-send-fail
```

# snmp-server enable traps cef

SNMP Cisco Express Forwarding（CEF）トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps cef** 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。

**snmp-server enable traps cef** [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]
**no snmp-server enable traps cef** [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

## 構文の説明

| | |
|---|---|
| **inconsistency** | （任意）SNMP CEF 矛盾トラップをイネーブルにします。 |
| **peer-fib-state-change** | （任意）SNMP CEF ピア FIB ステート変更トラップをイネーブルにします。 |
| **peer-state-change** | （任意）SNMP CEF ピア ステート変更トラップをイネーブルにします。 |
| **resource-failure** | （任意）SNMP リソース障害トラップをイネーブルにします。 |

## コマンド デフォルト

SNMP CEF トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、SNMP CEF 矛盾トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps cef inconsistency
```

# snmp-server enable traps cpu

CPU通知をイネーブルにするには、グローバル コンフィギュレーション モードで**snmp-server enable traps cpu** 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。

**snmp-server enable traps cpu** ［**threshold**］
**no snmp-server enable traps cpu** ［**threshold**］

**構文の説明**

| | |
|---|---|
| **threshold** | （任意）CPU しきい値通知をイネーブルにします。 |

**コマンド デフォルト**

CPU 通知の送信はディセーブルになります。

**コマンド モード**

グローバル コンフィギュレーション

**コマンド履歴**

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

**使用上のガイドライン**

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

**例**

次に、CPU しきい値通知を生成する例を示します。

```
デバイス(config)# snmp-server enable traps cpu threshold
```

# snmp-server enable traps envmon

SNMP 環境トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps envmon** 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。

**snmp-server enable traps envmon** ［**fan**］［**shutdown**］［**status**］ ［**supply**］［**temperature**］
**no snmp-server enable traps envmon** ［**fan**］［**shutdown**］［**status**］ ［**supply**］［**temperature**］

## 構文の説明

| | |
|---|---|
| **fan** | （任意）ファン トラップをイネーブルにします。 |
| **shutdown** | （任意）環境シャットダウン モニタ トラップをイネーブルにします。 |
| **status** | （任意）SNMP 環境ステータス変更トラップをイネーブルにします。 |
| **supply** | （任意）環境電源モニタ トラップをイネーブルにします。 |
| **temperature** | （任意）環境温度モニタ トラップをイネーブルにします。 |

## コマンド デフォルト

環境 SNMP トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、ファン トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps envmon fan
```

# snmp-server enable traps errdisable

エラーディセーブルのSNMP通知をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps errdisable** 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。

**snmp-server enable traps errdisable** ［**notification-rate** *number-of-notifications*］
**no snmp-server enable traps errdisable** ［**notification-rate** *number-of-notifications*］

## 構文の説明

| | |
|---|---|
| **notification-rate** *number-of-notifications* | （任意）通知レートとして 1 分当たりの通知の数を指定します。受け入れられる値の範囲は 0 ～ 10000 です。 |

## コマンド デフォルト

エラー ディセーブルの SNMP 通知送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、エラー ディセーブルの SNMP 通知数を 2 に設定する例を示します。

```
デバイス(config)# snmp-server enable traps errdisable notification-rate 2
```

# snmp-server enable traps flash

SNMP フラッシュ通知をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps flash** 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。

**snmp-server enable traps flash** ［**insertion**］［**removal**］
**no snmp-server enable traps flash** ［**insertion**］［**removal**］

## 構文の説明

| | |
|---|---|
| **insertion** | （任意）SNMP フラッシュ挿入通知をイネーブルにします。 |
| **removal** | （任意）SNMP フラッシュ取り出し通知をイネーブルにします。 |

## コマンド デフォルト

SNMP フラッシュ通知の送信はディセーブルです。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、SNMP フラッシュ挿入通知を生成する例を示します。

```
デバイス(config)# snmp-server enable traps flash insertion
```

# snmp-server enable traps isis

Intermediate System-to-Intermediate System（IS-IS）リンクステート ルーティング プロトコル トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps isis** 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。

**snmp-server enable traps isis** ［**errors** | **state-change**］
**no snmp-server enable traps isis** ［**errors** | **state-change**］

**構文の説明**

| | |
|---|---|
| **errors** | （任意）IS-IS エラー トラップをイネーブルにします。 |
| **state-change** | （任意）IS-IS ステート変更トラップをイネーブルにします。 |

**コマンド デフォルト**

IS-IS のトラップ送信はディセーブルになります。

**コマンド モード**

グローバル コンフィギュレーション

**コマンド履歴**

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

**使用上のガイドライン**

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

**例**

次に、IS-IS エラー トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps isis errors
```

# snmp-server enable traps license

ライセンストラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps license** 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。

**snmp-server enable traps license** [**deploy**][**error**][**usage**]
**no snmp-server enable traps license** [**deploy**][**error**][**usage**]

## 構文の説明

| | |
|---|---|
| **deploy** | （任意）ライセンス導入トラップをイネーブルにします。 |
| **error** | （任意）ライセンスエラートラップをイネーブルにします。 |
| **usage** | （任意）ライセンス使用トラップをイネーブルにします。 |

## コマンド デフォルト

ライセンス トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、ライセンス導入トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps license deploy
```

# snmp-server enable traps mac-notification

SNMP MAC 通知トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps mac-notification** 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。

**snmp-server enable traps mac-notification** ［**change**］［**move**］［**threshold**］
**no snmp-server enable traps mac-notification** ［**change**］［**move**］［**threshold**］

## 構文の説明

| | |
|---|---|
| **change** | （任意）SNMP MAC 変更トラップをイネーブルにします。 |
| **move** | （任意）SNMP MAC 移動トラップをイネーブルにします。 |
| **threshold** | （任意）SNMP MAC しきい値トラップをイネーブルにします。 |

## コマンド デフォルト

SNMP MAC 通知トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、SNMP MAC 通知変更トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps mac-notification change
```

# snmp-server enable traps ospf

SNMP の Open Shortest Path First（OSPF）トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps ospf** 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。

**snmp-server enable traps ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]
**no snmp-server enable traps ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]

## 構文の説明

| | |
|---|---|
| **cisco-specific** | （任意）シスコ固有のトラップをイネーブルにします。 |
| **errors** | （任意）エラー トラップをイネーブルにします。 |
| **lsa** | （任意）リンクステート アドバタイズメント（LSA）トラップをイネーブルにします。 |
| **rate-limit** | （任意）レート制限トラップをイネーブルにします。 |
| *rate-limit-time* | （任意）レート制限トラップの時間の長さを秒数で指定します。指定できる値は 2 ～ 60 です。 |
| *max-number-of-traps* | （任意）設定した時間内に送信するレート制限トラップの最大数を指定します。 |
| **retransmit** | （任意）パケット再送信トラップをイネーブルにします。 |
| **state-change** | （任意）状態変更トラップをイネーブルにします。 |

## コマンド デフォルト

OSPF SNMP トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、LSA トラップをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps ospf lsa
```

# snmp-server enable traps pim

SNMP プロトコル独立型マルチキャスト（PIM）トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps pim** 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。

**snmp-server enable traps pim** ［**invalid-pim-message**］［**neighbor-change**］［**rp-mapping-change**］
**no snmp-server enable traps pim**
［**invalid-pim-message**］［**neighbor-change**］［**rp-mapping-change**］

## 構文の説明

| | |
|---|---|
| **invalid-pim-message** | （任意）無効な PIM メッセージ トラップをイネーブルにします。 |
| **neighbor-change** | （任意）PIM ネイバー変更トラップをイネーブルにします。 |
| **rp-mapping-change** | （任意）ランデブー ポイント（RP）マッピング変更トラップをイネーブルにします。 |

## コマンド デフォルト

PIM SNMP トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、無効な PIM メッセージ トラップをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps pim invalid-pim-message
```

# snmp-server enable traps port-security

SNMP ポートセキュリティトラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps port-security** 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。

**snmp-server enable traps port-security** ［**trap-rate** *value*］
**no snmp-server enable traps port-security** ［**trap-rate** *value*］

## 構文の説明

| | |
|---|---|
| **trap-rate** *value* | （任意）1 秒間に送信するポート セキュリティ トラップの最大数を設定します。指定できる範囲は 0 ～ 1000 です。デフォルトは 0 です（制限はなく、トラップは発生するたびに送信されます）。 |

## コマンド デフォルト

ポート セキュリティ SNMP トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、1 秒当たり 200 の速度でポート セキュリティ トラップをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps port-security trap-rate 200
```

# snmp-server enable traps power-ethernet

SNMP の Power over Ethernet（PoE）トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps power-ethernet** 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。

**snmp-server enable traps power-ethernet** {**group** *number* | **police**}
**no snmp-server enable traps power-ethernet** {**group** *number* | **police**}

## 構文の説明

| | |
|---|---|
| **group** *number* | 指定したグループ番号に対するインラインパワーグループベース トラップをイネーブルにします。受け入れられる値の範囲は 1 ～ 9 です。 |
| **police** | インライン パワー ポリシング トラップをイネーブルにします。 |

## コマンド デフォルト

Power over Ethernet の SNMP トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、グループ 1 の Power over Ethernet（PoE）トラップをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps poower-over-ethernet group 1
```

# snmp-server enable traps snmp

SNMP トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps snmp** 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。

**snmp-server enable traps snmp** ［**authentication** ］［**coldstart** ］［**linkdown** ］［**linkup** ］［**warmstart**］
**no snmp-server enable traps snmp** ［**authentication** ］［**coldstart** ］［**linkdown** ］［**linkup** ］［**warmstart**］

## 構文の説明

| | |
|---|---|
| **authentication** | （任意）認証トラップをイネーブルにします。 |
| **coldstart** | （任意）コールドスタート トラップをイネーブルにします。 |
| **linkdown** | （任意）リンクダウン トラップをイネーブルにします。 |
| **linkup** | （任意）リンクアップ トラップをイネーブルにします。 |
| **warmstart** | （任意）ウォームスタート トラップをイネーブルにします。 |

## コマンド デフォルト

SNMP トラップの送信をディセーブルにします。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、ウォーム スタートの SNMP トラップをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps snmp warmstart
```

# snmp-server enable traps storm-control

SNMP ストーム制御トラップパラメータをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps storm-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。

**snmp-server enable traps storm-control** {**trap-rate** *number-of-minutes*}
**no snmp-server enable traps storm-control** {**trap-rate**}

## 構文の説明

| | |
|---|---|
| **trap-rate** *number-of-minutes* | （任意）SNMP ストーム制御トラップ レートを分単位で指定します。受け入れられる値の範囲は 0 ～ 1000 です。 |

## コマンド デフォルト

SNMP ストーム制御トラップ パラメータの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、SNMP ストーム制御トラップレートを 1 分あたり 10 トラップに設定する例を示します。

```
デバイス(config)# snmp-server enable traps storm-control trap-rate 10
```

# snmp-server enable traps stpx

SNMP STPX MIB トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps stpx** 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。

**snmp-server enable traps stpx** [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]
**no snmp-server enable traps stpx** [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]

## 構文の説明

| | |
|---|---|
| **inconsistency** | （任意）SNMP STPX MIB 矛盾更新トラップをイネーブルにします。 |
| **loop-inconsistency** | （任意）SNMP STPX MIB ループ矛盾更新トラップをイネーブルにします。 |
| **root-inconsistency** | （任意）SNMP STPX MIB ルート矛盾更新トラップをイネーブルにします。 |

## コマンド デフォルト

SNMP STPX MIB トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、SNMP STPX MIB 矛盾更新トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps stpx inconsistency
```

# snmp-server enable traps transceiver

SNMP トランシーバトラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps transceiver** 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。

**snmp-server enable traps transceiver** {**all**}
**no snmp-server enable traps transceiver** {**all**}

**構文の説明**

| | |
|---|---|
| **all** | （任意）すべてのSNMPトランシーバ トラップをイネーブルにします。 |

**コマンド デフォルト**

SNMP トランシーバ トラップの送信はディセーブルになります。

**コマンド モード**

グローバル コンフィギュレーション

**コマンド履歴**

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

**使用上のガイドライン**

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

**例**

次に、すべての SNMP トランシーバ トラップを設定する例を示します。

```
デバイス(config)# snmp-server enable traps transceiver all
```

# snmp-server enable traps vrfmib

SNMP vrfmib トラップを許可するには、グローバル コンフィギュレーション モードで **snmp-server enable traps vrfmib** 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。

**snmp-server enable traps vrfmib** [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]
**no snmp-server enable traps vrfmib** [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

## 構文の説明

| | |
|---|---|
| **vnet-trunk-down** | （任意）vrfmib trunk ダウン トラップをイネーブルにします。 |
| **vnet-trunk-up** | （任意）vrfmib trunk アップ トラップをイネーブルにします。 |
| **vrf-down** | （任意）vrfmib vrf ダウン トラップをイネーブルにします。 |
| **vrf-up** | （任意）vrfmib vrf アップ トラップをイネーブルにします。 |

## コマンド デフォルト

SNMP vrfmib トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

この例は、vrfmib trunk ダウン トラップを生成する方法を示しています。

```
デバイス(config)# snmp-server enable traps vrfmib vnet-trunk-down
```

# snmp-server enable traps vstack

SNMP スマートインストール トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps vstack** 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。

**snmp-server enable traps vstack** [**addition**] [**failure**] [**lost**] [**operation**]
**no snmp-server enable traps vstack** [**addition**] [**failure**] [**lost**] [**operation**]

## 構文の説明

| | |
|---|---|
| **addition** | （任意）クライアントによって追加されたトラップをイネーブルにします。 |
| **failure** | （任意）ファイルのアップロードとダウンロード障害トラップをイネーブルにします。 |
| **lost** | （任意）クライアントの損失トラップをイネーブルにします。 |
| **operation** | （任意）動作モード変更トラップをイネーブルにします。 |

## コマンド デフォルト

SNMP スマート インストール トラップの送信はディセーブルになります。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

## 例

次に、SNMP スマートインストール クライアント追加トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps vstack addition
```

# snmp-server engineID

SNMP のローカルコピーまたはリモートコピーに名前を設定するには、グローバル コンフィギュレーション モードで **snmp-server engineID** コマンドを使用します。

**snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}

## 構文の説明

| | |
|---|---|
| **local** *engineid-string* | SNMP コピーの名前に 24 文字の ID 文字列を指定します。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジンIDのうちゼロのみが続く箇所を除いた部分だけです。 |
| **remote** *ip-address* | リモート SNMP コピーを指定します。SNMP のリモート コピーを含むデバイスの *ip-address* を指定します。 |
| **udp-port** *port-number* | （任意）リモートデバイスのユーザ データグラム プロトコル（UDP）ポートを指定します。デフォルトは 162 です。 |

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

なし

### 例

次の例では、ローカル エンジン ID 1234000000000000000000000 を設定します。

```
デバイス(config)# snmp-server engineID local 1234
```

# snmp-server host

Simple Network Management Protocol（SNMP）通知操作の受信者（ホスト）を指定するには、deviceで **snmp-server host** グローバル コンフィギュレーション コマンドを使用します。指定したホストを削除するには、このコマンドの **no** 形式を使用します。

**snmp-server host** {*host-addr*} [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }
**no snmp-server host** {*host-addr*} [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

## 構文の説明

| | |
|---|---|
| *host-addr* | ホスト（ターゲットとなる受信側）の名前またはインターネットアドレスです。 |
| **vrf** *vrf-instance* | （任意）仮想プライベート ネットワーク（VPN）ルーティング インスタンスとこのホストの名前を指定します。 |
| **informs** \| **traps** | （任意）このホストに SNMP トラップまたは情報を送信します。 |
| **version 1** \| **2c** \| **3** | （任意）トラップの送信に使用する SNMP のバージョンを指定します。<br>**1**：SNMPv1。情報の場合は、このオプションを使用できません。<br>**2c**：SNMPv2C。<br>**3**：SNMPv3。認証キーワードの 1 つ（次の表の行を参照）が、バージョン 3 キーワードに従っている必要があります。 |
| **auth** \| **noauth** \| **priv** | **auth**（任意）：Message Digest 5（MD5）およびセキュア ハッシュ アルゴリズム（SHA）パケット認証をイネーブルにします。<br>**noauth**（デフォルト）：noAuthNoPriv セキュリティ レベル。**auth** \| **noauth** \| **priv** キーワードの選択が指定されていない場合、これがデフォルトとなります。<br>**priv**（任意）：データ暗号規格（DES）によるパケット暗号化（「プライバシー」ともいう）をイネーブルにします。 |
| *community-string* | 通知処理にともなって送信される、パスワードと類似したコミュニティ ストリングです。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** 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から、**snmp-server host** コマンドを使用することを推奨します。<br>（注） コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。 |

*notification-type* （任意）ホストに送信される通知のタイプです。タイプが指定されていない場合、すべての通知が送信されます。通知タイプには、次のキーワードの 1 つまたは複数を指定できます。

- **auth-framework**：SNMP CISCO-AUTH-FRAMEWORK-MIB トラップを送信します。
- **bridge**：SNMP スパニング ツリー プロトコル（STP）ブリッジ MIB トラップを送信します。
- **bulkstat**：データ収集 MIB 収集通知トラップを送信します。
- **call-home**：SNMP CISCO-CALLHOME-MIB トラップを送信します。
- **cef**：SNMP CEF トラップを送信します。
- **config**：SNMP 設定トラップを送信します。
- **config-copy**：SNMP config-copy トラップを送信します。
- **config-ctid**：SNMP config-ctid トラップを送信します。
- **copy-config**：SNMP コピー設定トラップを送信します。
- **cpu**：CPU 通知トラップを送信します。
- **cpu threshold**：CPU しきい値通知トラップを送信します。
- **entity**：SNMP エントリ トラップを送信します。

- **envmon**：環境モニタ トラップを送信します。
- **errdisable**：SNMP errdisable 通知トラップを送信します。
- **event-manager**：SNMP Embedded Event Manager トラップを送信します。
- **flash**：SNMP FLASH 通知を送信します。
- **flowmon**：SNMP flowmon 通知トラップを送信します。
- **ipmulticast**：SNMP IP マルチキャスト ルーティング トラップを送信します。
- **ipsla**：SNMP IP SLA トラップを送信します。
- **license**：ライセンス トラップを送信します。
- **local-auth**：SNMP ローカル認証トラップを送信します。
- **mac-notification**：SNMP MAC 通知トラップを送信します。
- **pim**：SNMP プロトコル独立型マルチキャスト（PIM）トラップを送信します。
- **power-ethernet**：SNMP パワー イーサネット トラップを送信します。
- **snmp**：SNMP タイプ トラップを送信します。
- **storm-control**：SNMP ストーム制御トラップを送信します。
- **stpx**：SNMP STP 拡張 MIB トラップを送信します。
- **syslog**：SNMP syslog トラップを送信します。
- **transceiver**：SNMP トランシーバ トラップを送信します。
- **tty**：TCP 接続トラップを送信します。
- **vlan-membership**：SNMP VLAN メンバーシップ トラップを送信します。
- **vlancreate**：SNMP VLAN 作成のトラップを送信します。
- **vlandelete**：SNMP VLAN 削除トラップを送信します。
- **vrfmib**：SNMP vrfmib トラップを送信します。
- **vtp**：SNMP VLAN Trunking Protocol（VTP）トラップを送信します。

## コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。通知は送信されません。

キーワードを指定しないでこのコマンドを入力した場合は、デフォルトで、すべてのトラップタイプがホストに送信されます。情報はこのホストに送信されません。

**version** キーワードがない場合、デフォルトはバージョン 1 になります。

バージョン 3 を選択し、認証キーワードを入力しなかった場合は、デフォルトで **noauth**（noAuthNoPriv）セキュリティレベルになります。

（注） **fru-ctrl** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。

## コマンド モード

グローバル コンフィギュレーション

## コマンド履歴

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

## 使用上のガイドライン

SNMP通知は、トラップまたは情報要求として送信できます。トラップを受信しても受信側は確認応答を送信しないため、トラップは信頼できません。送信側では、トラップが受信されたかどうかを判別できません。ただし、情報要求を受信したSNMPエンティティは、SNMP応答PDUを使用してメッセージに確認応答します。送信側が応答を受信しない場合、インフォーム要求を再送信して、インフォームが目的の宛先に到達する可能性を向上できます。

ただし、情報はエージェントおよびネットワークのリソースをより多く消費します。送信と同時に破棄されるトラップと異なり、インフォーム要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持する必要があります。また、トラップの送信は1回限りですが、情報は数回にわたって再試行が可能です。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。

**snmp-server host** コマンドを入力しなかった場合は、通知が送信されません。SNMP 通知を送信するように device を設定するには、**snmp-server host** コマンドを少なくとも 1 つ入力する必要があります。キーワードを指定しないでこのコマンドを入力した場合、そのホストではすべてのトラップタイプがイネーブルになります。複数のホストをイネーブルにするには、ホストごとに **snmp-server host** コマンドを個別に入力する必要があります。コマンドには複数の通知タイプをホストごとに指定できます。

ローカルユーザがリモートホストと関連付けられていない場合、device は **auth**（authNoPriv）および **priv**（authPriv）の認証レベルの情報を送信しません。

同じホストおよび同じ種類の通知（トラップまたは情報）に対して複数の **snmp-server host** コマンドを指定した場合は、後に入力されたコマンドによって前のコマンドが上書きされます。最後の **snmp-server host** コマンドだけが有効です。たとえば、ホストに **snmp-server host inform** コマンドを入力してから、同じホストに別の **snmp-server host inform** コマンドを入力した場合は、2 番目のコマンドによって最初のコマンドが置き換えられます。

**snmp-server host** コマンドは、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと組み合わせて使用します。グローバルに送信される SNMP 通知を指定するには、**snmp-server enable traps** コマンドを使用します。1 つのホストでほとんどの通知を受信する場合は、このホストに対して、少なくとも 1 つの **snmp-server enable traps** コマンドと **snmp-server host** コマンドをイネーブルにする必要があります。一部の通知タイプは、**snmp-server enable traps** コマンドで制御できません。たとえば、ある通知タイプは常にイネーブルですが、別の通知タイプはそれぞれ異なるコマンドによってイネーブルになります。

キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** コマンドを使用してください。

## 例

次の例では、トラップに対して一意の SNMP コミュニティ ストリング comaccess を設定し、このストリングによる、アクセス リスト 10 を介した SNMP ポーリング アクセスを禁止します。

```
デバイス(config)# snmp-server community comaccess ro 10
デバイス(config)# snmp-server host 172.20.2.160 comaccess
デバイス(config)# access-list 10 deny any
```

次の例では、名前 myhost.cisco.com で指定されたホストに SNMP トラップを送信する方法を示します。コミュニティ ストリングは、comaccess として定義されています。

```
デバイス(config)# snmp-server enable traps
デバイス(config)# snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、コミュニティストリング public を使用して、すべてのトラップをホスト myhost.cisco.com に送信するように device をイネーブルにする方法を示します。

```
デバイス(config)# snmp-server enable traps
デバイス(config)# snmp-server host myhost.cisco.com public
```

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

# switchport mode access

トランキングなし、タグなしの単一VLANイーサネットインターフェイスとしてインターフェイスを設定するには、テンプレート コンフィギュレーション モードで **switchport mode access** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**switchport mode access**
**no switchport mode access**

## 構文の説明

| | |
|---|---|
| **switchport mode access** | トランキングなし、タグなしの単一VLANイーサネットインターフェイスとして、インターフェイスを設定します。 |

## コマンド デフォルト

アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。アクセス ポートは、デフォルトで、VLAN 1 のトラフィックを送受信します。

## コマンド モード

テンプレート コンフィギュレーション

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| | このコマンドが導入されました。 |

## 例

次に、単一 VLAN インターフェイスを設定する例を示します。

```
デバイス(config-template)# switchport mode access
```

# switchport voice vlan

指定された VLAN からのすべての音声トラフィックを転送するように指定するには、テンプレート コンフィギュレーション モードで **switchport voice 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。

**switchport voice vlan***vlan_id*
**no switchport voice vlan**

## 構文の説明

| | |
|---|---|
| **switchport voice vlan***vlan_id* | すべての音声トラフィックを指定された VLAN 経由で転送するように指定します。 |

## コマンド デフォルト

1 ～ 4094 の値を指定できます。

## コマンド モード

テンプレート コンフィギュレーション

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| | このコマンドが導入されました。 |

## 例

次に、指定された VLAN からのすべての音声トラフィックを転送するように指定する例を示します。

```
デバイス(config-template)# switchport voice vlan 20
```