ネットワーク管理コマンド

- clear snmp stats hosts （3 ページ）
- description（ERSPAN） （4 ページ）
- destination（ERSPAN） （5 ページ）
- event manager applet （11 ページ）
- filter（ERSPAN） （15 ページ）
- header-type （17 ページ）
- ip wccp （18 ページ）
- map platform-type （20 ページ）
- match platform-type （21 ページ）
- monitor capture (interface/control plane) （22 ページ）
- monitor capture buffer （24 ページ）
- monitor capture clear （25 ページ）
- monitor capture export （26 ページ）
- monitor capture file （27 ページ）
- monitor capture limit （29 ページ）
- monitor capture match （30 ページ）
- monitor capture start （31 ページ）
- monitor capture stop （32 ページ）
- monitor session （33 ページ）
- monitor session destination （35 ページ）
- monitor session filter （40 ページ）
- monitor session source （42 ページ）
- monitor session type （45 ページ）
- show capability feature monitor （47 ページ）
- show class-map type control subscriber （48 ページ）
- show ip sla statistics （49 ページ）
- show monitor （51 ページ）
- show monitor capture （54 ページ）
- show monitor session （56 ページ）

- show parameter-map type subscriber attribute-to-service （59 ページ）
- show platform software fed switch ip wccp （60 ページ）
- show platform software swspan （62 ページ）
- show snmp stats （64 ページ）
- shutdown（モニタセッション） （66 ページ）
- snmp ifmib ifindex persist （67 ページ）
- snmp-server community （68 ページ）
- snmp-server enable traps （70 ページ）
- snmp-server enable traps bridge （74 ページ）
- snmp-server enable traps bulkstat （75 ページ）
- snmp-server enable traps call-home （76 ページ）
- snmp-server enable traps cef （77 ページ）
- snmp-server enable traps cpu （78 ページ）
- snmp-server enable traps envmon （79 ページ）
- snmp-server enable traps errdisable （80 ページ）
- snmp-server enable traps flash （81 ページ）
- snmp-server enable traps isis （82 ページ）
- snmp-server enable traps license （83 ページ）
- snmp-server enable traps mac-notification （84 ページ）
- snmp-server enable traps ospf （85 ページ）
- snmp-server enable traps pim （87 ページ）
- snmp-server enable traps port-security （88 ページ）
- snmp-server enable traps power-ethernet （89 ページ）
- snmp-server enable traps snmp （90 ページ）
- snmp-server enable traps storm-control （91 ページ）
- snmp-server enable traps stpx （92 ページ）
- snmp-server enable traps transceiver （93 ページ）
- snmp-server enable traps vrfmib （94 ページ）
- snmp-server enable traps vstack （95 ページ）
- snmp-server engineID （96 ページ）
- snmp-server group （97 ページ）
- snmp-server host （101 ページ）
- snmp-server manager （106 ページ）
- snmp-server user （107 ページ）
- snmp-server view （112 ページ）
- source（ERSPAN） （114 ページ）
- switchport mode access （115 ページ）
- switchport voice vlan （116 ページ）

clear snmp stats hosts

NMS の IP アドレス、NMS がエージェントをポーリングした回数、およびポーリングのタイムスタンプをクリアするには、特権 EXEC モードで **clear snmp stats hosts** コマンドを使用します。

clear snmp stats hosts

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

SNMPエージェントにポーリングされたSNMPマネージャの詳細がシステムに保存されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

clear snmp stats hosts コマンドは、SNMP エージェントにポーリングされたすべてのエントリを削除するために使用します。

次に、**clear snmp stats hosts** コマンドの出力例を示します。

```
Device# clear snmp stats hosts
Request Count                   Last Timestamp              Address
```

description（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元セッションを説明するには、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 **description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description *description*
no description

構文の説明

description	このセッションのプロパティについて説明します。

コマンド デフォルト

説明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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

description 引数は 240 文字以内で指定します。

例

次に、ERSPAN 送信元セッションを説明する例を示します。

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# description source1
```

関連コマンド

コマンド	説明
monitor session type	ローカルの ERSPAN 送信元または宛先セッションを設定します。

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 Everest 16.5.1a	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.1.1	IPv6 ERSPAN のサポートとして、送信元セッション宛先コンフィギュレーション モードに **ipv6** キーワードが追加されました。

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。

destination コマンドを入力すると、コマンドモードが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）から送信元セッション宛先コンフィギュレーション モード（config-mon-erspan-src-dst）に切り替わります。このモードで使用できるコマンドの一覧を表示するには、システムプロンプトで疑問符（?）を入力します。

erspan-id *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。有効な値の範囲は 1 ～ 1023 です。
exit	モニタ ERSPAN 宛先セッション送信元プロパティモードを終了します。

ip { **address** *ipv4-address* | **dscp** *dscp-value* | **ttl** *ttl-value* }	IP プロパティを指定します。次のオプションを設定できます。 • **address** *ipv4-address*：ERSPAN 宛先セッションの IP アドレスを設定します。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 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。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。 • **dscp** *dscp-value*：ERSPAN トラフィックのパケットの DiffServ コードポイント（DSCP）値を設定します。有効値は 0 ～ 63 です。 DSCP 値を削除するには、このコマンドの **no** 形式を使用します。 • **ttl** *ttl-value*：ERSPAN トラフィックのパケットの存続可能時間（TTL）値を設定します。有効値は 2 ～ 255 です。 TTL 値を削除するには、このコマンドの **no** 形式を使用します。

ipv6 { **address** *ipv6-address* | **dscp** *dscp-value* | **flow-label** | **ttl** *ttl-value* }	IPv6プロパティを指定します。次のオプションを設定できます。 • **address** *ipv6-address*：ERSPAN宛先セッションのIPv6アドレスを設定します。すべてのERSPAN送信元セッション（最大8）の宛先IPv6アドレスが同一である必要はありません。 ERSPAN送信元セッションの宛先IPv6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。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。 • **dscp** *dscp-value*：ERSPANトラフィックのパケットのDiffServコードポイント（DSCP）値を設定します。有効値は0～63です。 DSCP値を削除するには、このコマンドの **no** 形式を使用します。 • **flow-label**：フローラベルを設定します。有効な値は0～1048575です。 • **ttl** *ttl-value*：ERSPANトラフィックのパケットの存続可能時間（TTL）値を設定します。有効値は2～255です。 TTL値を削除するには、このコマンドの **no** 形式を使用します。
mtu*bytes*	ERSPANの切り捨ての最大伝送ユニット（MTU）サイズを指定します。デフォルト値は9000バイトです。
origin { **ip address** *ip-address* | **ipv6 address***ipv6-address*}	ERSPANトラフィックの送信元を設定します。IPv4アドレスまたはIPv6アドレスを入力できます。
vrf*vrf-id*	宛先セッションのVirtual Routing and Forwarding（VRF）を設定します。VRF IDを入力します。

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。

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、各種プロパティを設定する例を示します。

次の例では、宛先プロパティ **ip** を指定します。

```
Device(config)# monitor session 2 type erspan-source
```

```
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)#ip address 10.1.1.1
Device(config-mon-erspan-src-dst)#
```

次に、宛先セッションの ERSPAN ID を設定する例を示します。

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 3
```

次に、ERSPAN トラフィックの DSCP 値を設定する例を示します。

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ip dscp 15
```

次に、ERSPAN トラフィックの TTL 値を設定する例を示します。

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ip ttl 32
```

次の例では、宛先プロパティ **ipv6** を指定します。

```
Device(config)# monitor session 3 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)#ipv6 address 2001:DB8::1
Device(config-mon-erspan-src-dst)#
```

次に、ERSPAN トラフィック IPv6 の DSCP 値を設定する例を示します。

```
Device(config)# monitor session 3 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ipv6 dscp 10
```

次に、ERSPAN トラフィック IPv6 のフローラベル値を設定する例を示します。

```
Device(config)# monitor session 3 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ipv6 flow-label 6
```

次に、ERSPAN トラフィック IPv6 の TTL 値を設定する例を示します。

```
Device(config)# monitor session 3 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ipv6 ttl 32
```

次に、1000 バイトの MTU を指定する例を示します。

```
Device(config)# monitor session 2 type erspan-source
```

```
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# mtu 1000
```

次に、ERSPAN 送信元セッションの IP アドレスを設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)# origin ip address 192.0.2.1
```

次に、ERSPAN 送信元セッションの IPv6 アドレスを設定する例を示します。

```
Switch(config)# monitor session 3 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# origin ipv6 address 2001:DB8:1::1
```

次に、宛先セッションの VRF を設定する例を示します。

```
Switch(config)# monitor session 3 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# vrf vrfexample
```

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。

```
Device# show monitor session all

Session 1
---------
Type                   : ERSPAN Source Session
Status                 : Admin Disabled


Session 2
----------
Type                   : ERSPAN Source Session
Status                 : Admin Disabled
Source VLANs           :
    RX Only            : 400
Destination IP Address   : 10.1.1.1
Destination ERSPAN ID    : 220
Origin IP Address        : 192.0.2.1
IP TTL                   : 10
ERSPAN header-type       : 3


Session 3
----------
Type                   : ERSPAN Source Session
Status                 : Admin Enabled
Source Ports           :
    Both               : Fo1/0/2
Destination IP Address   : 10.1.1.2
Destination ERSPAN ID    : 251
Origin IP Address        : 192.0.2.2
ERSPAN header-type       : 3


Session 4
----------
Type                   : ERSPAN Source Session
```

```
Status                   : Admin Disabled
Source VLANs             :
    Both                 : 30
Destination IP Address   : 10.1.1.3
Destination ERSPAN ID    : 260
Origin IP Address        : 192.0.2.3


Session 5
----------
Type                     : ERSPAN Source Session
Status                   : Admin Enabled
Source VLANs             :
    Both                 : 500
Destination IP Address   : 10.1.1.4
Destination ERSPAN ID    : 100
Origin IP Address        : 192.0.2.4
```

関連コマンド

コマンド	説明
monitorsession type	ローカルのERSPAN送信元または宛先セッションを設定します。

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： • *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。 • **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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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* ｜ **sgt** *sgt-id* [**,**] [**-**] ｜ **vlan** *vlan-id*[**,**] [**-**]
no filter ip [**access-group** ｜[*standard-access-list extended-access-list acl-name*]] ｜ **ipv6** [**access-group**] ｜ **mac** [**access-group**] ｜ **sgt** *sgt-id* [**,**] [**-**] ｜ **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。
sgt *sgt-ID*	セキュリティグループタグ（SGT）を指定します。有効値は 1 ～ 65535 です。
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 Everest 16.5.1a	このコマンドが導入されました。
Cisco IOS XE Fuji 16.9.1	**sgt** キーワードが導入されました。 Cisco Catalyst 9500 シリーズ ハイ パフォーマンス スイッチに導入されました。

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	**sgt** キーワードが導入されました。 Cisco Catalyst 9500 シリーズ スイッチに導入されました。

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	ローカルの ERSPAN 送信元または宛先セッションを設定します。

header-type

カプセル化の ERSPAN ヘッダータイプを設定するには、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 **header-type** 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。

header-type *header-type*
no header-type *header-type*

構文の説明

header-type	ERSPAN ヘッダータイプ。有効なヘッダータイプは 2 および 3 です。

コマンド デフォルト

ERSPAN ヘッダータイプは 2 に設定されています。

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 Fuji 16.9.1	このコマンドが導入されました。 Cisco Catalyst 9500 シリーズ ハイ パフォーマンス スイッチに導入されました。
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。 Cisco Catalyst 9500 シリーズスイッチに導入されました。

例

次に、ERSPAN ヘッダータイプを 3 に変更する例を示します。

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

関連コマンド

コマンド	説明
monitor session type	ローカルの ERSPAN 送信元または宛先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、デバイスで **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デバイス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。デバイスは、パスワードと MD5 認証値を組み合わせて、デバイス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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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デバイスに指示します。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、デバイス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。

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

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

map platform-type

パラメータマップ属性フィルタ基準をプラットフォームタイプに設定するには、パラメータマップ フィルタ モードで **map platform-type** コマンドを使用します。この基準を削除するには、このコマンドの **no** 形式を使用します。

map-number **map platform-type** {**eq** | **not-eq** | **regex** *platform-type*}
no *map-number* **map platform-type** {**eq** | **not-eq** | **regex** *platform-type*}

構文の説明

map-number	パラメータマップ番号。
eq	フィルタタイプ名がプラットフォームタイプ名と同じであることを指定します。
not-eq	フィルタタイプ名がプラットフォームタイプ名と同じでないことを指定します。
regex	フィルタタイプ名が正規表現であることを指定します。
platform-type	パラメータマップ属性フィルタ基準のプラットフォームタイプ。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

パラメータマップフィルタ（config-parameter-map-filter）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、パラメータマップ属性フィルタ基準をプラットフォームタイプに設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para
Device(config-parameter-map-filter)# 10 map platform-type eq C9xxx
```

関連コマンド

コマンド	説明
parameter-map type subscriber attribute-to-service	サブスクライバ パラメータ マップを設定し、パラメータマップ フィルタ コンフィギュレーション モードを開始します。

match platform-type

プラットフォームタイプに基づいて制御クラスを評価するには、コントロール クラスマップ フィルタ モードで **match platform-type** コマンドを使用します。この条件を削除するには、このコマンドの **no** 形式を使用します。

match platform-type *platform-name*
no match platform-type *platform-name*

構文の説明

platform-name	プラットフォームの名前。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コントロール クラスマップ フィルタ （config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、クラスマップフィルタでプラットフォームタイプを照合するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT
Device(config-filter-control-classmap)# match platform-type C9xxx
```

関連コマンド

コマンド	説明
class-map type control subscriber	制御クラスを作成し、制御クラスマップ フィルタ モードを開始します。

monitor capture (interface/control plane)

接続ポイントおよびパケットフロー方向を指定してモニタキャプチャポイントを設定する、またはキャプチャポイントに接続ポイントを追加するには、特権 EXEC モードで **monitor capture** コマンドを使用します。指定した接続ポイントおよびパケットフロー方向でモニタキャプチャを無効にする、またはキャプチャポイント上の複数の接続ポイントのいずれかを無効にするには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*}{**interface** *interface-type interface-id* | **control-plane**}{**in** | **out** | **both**}
no monitor capture {*capture-name*}{**interface** *interface-type interface-id* | **control-plane**}{**in** | **out** | **both**}

構文の説明

capture-name	定義するキャプチャの名前。
interface *interface-type interface-id*	*interface-type* および *interface-id* とのインターフェイスを接続ポイントとして指定します。引数の意味は次のとおりです。 • **GigabitEthernet** *interface-id*：ギガビット イーサネット IEEE 802.3z インターフェイス。 • **vlan** *vlan-id*：VLAN。*vlan-id*の範囲は 1 ～ 4095 です。
control-plane	コントロール プレーンを接続ポイントとして指定します。
in | **out** | **both**	キャプチャするトラフィックの方向を指定します。

コマンド デフォルト

Wireshark キャプチャは設定されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

接続ポイントがこのコマンドを使用してキャプチャポイントに関連付けられると、方向を変更する唯一の方法は、このコマンドの **no** 形式を使用して接続ポイントを削除し、新しい方向に接続ポイントを再接続することです。接続ポイントの方向は上書きできません。

接続ポイントがキャプチャ ポイントから削除され、1つの接続ポイントのみが関連付けられている場合、キャプチャ ポイントは効率的に削除されます。

このコマンドを別の接続ポイントで再実行することで、複数の接続ポイントをキャプチャ ポイントと関連付けることができます。次に例を示します。

インターフェイスの出力方向にキャプチャされたパケットは、スイッチの書き換えによって行われた変更（TTL、VLAN タグ CoS、チェックサム、および MAC アドレス、DSCP、プレシデント、UP など）が反映されないこともあります。

特定の順序はキャプチャ ポイントを定義する場合には適用されません。任意の順序でキャプチャ ポイント パラメータを定義できます。Wireshark CLI では、単一行のパラメータ数に制限はありません。これはキャプチャ ポイントを定義するために必要なコマンドの数を制限します。

VRF、管理ポート、プライベート VLAN はいずれも接続ポイントとして使用することはできません。

Wireshark は宛先 SPAN ポートでパケットをキャプチャできません。

VLAN が Wireshark の接続ポイントとして使用されている場合、パケットは、入力方向でのみキャプチャされます。

例

物理インターフェイスを接続ポイントとして使用してキャプチャ ポイントを定義するには次を実行します。

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```

（注） 2 つ目のコマンドは、キャプチャ ポイントのコア フィルタを定義します。これは、キャプチャポイントが機能するために必要です。

複数の接続ポイントを持つキャプチャ ポイントを定義するには次を実行します。

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap control-plane in
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
```

複数の接続ポイントで定義されたキャプチャ ポイントから接続ポイントを削除するには次を実行します。

```
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
Device# no monitor capture mycap control-plane
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
```

monitor capture buffer

モニタキャプチャ（WireShark）のバッファを設定するには、特権 EXEC モードで **monitor capture buffer** コマンドを使用します。モニタキャプチャバッファを無効にする、またはバッファを循環バッファからデフォルトの線形バッファに戻すには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **buffer** {**circular** [**size** *buffer-size*] | **size** *buffer-size*}
no monitor capture {*capture-name*} **buffer** [**circular**]

構文の説明

capture-name	バッファが設定されるキャプチャの名前。
circular	バッファが循環タイプであることを指定します。循環タイプのバッファは、バッファが消費された後も以前にキャプチャされたデータを上書きすることでデータのキャプチャを継続します。
size *buffer-size*	（任意）バッファのサイズを指定します。範囲は 1 ～ 100 MB です。

コマンド デフォルト

線形バッファが設定されます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

最初に WireShark のキャプチャを設定すると、小規模の循環バッファが提案されます。

例

1 MB のサイズの循環バッファを設定する場合は次を実行します。

```
Device# monitor capture mycap buffer circular size 1
```

monitor capture clear

モニタキャプチャ（WireShark）バッファをクリアするには、特権 EXEC モードで **monitor capture clear** コマンドを使用します。

monitor capture {*capture-name*} **clear**

構文の説明

capture-name	バッファがクリアされるキャプチャの名前。

コマンド デフォルト

バッファのコンテンツはクリアされません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

キャプチャ中、または 1 つ以上の最終条件が満たされたか **monitor capture stop** コマンドを入力したためにキャプチャが停止された後に、**monitor capture clear** コマンドを使用します。キャプチャが停止した後に **monitor capture clear** コマンドを入力した場合、バッファにキャプチャされたパケットがないため、ファイルへのキャプチャされたパケットのコンテンツの保存に使用された **monitor capture export** コマンドには影響はありません。

パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。

例

mycap をキャプチャするためにバッファ コンテンツをクリアするには次を実行します。

```
Device#  monitor capture mycap clear
```

monitor capture export

ファイルにモニタキャプチャ（WireShark）をエクスポートするには、特権 EXEC モードで **monitor capture export** コマンドを使用します。

monitor capture {*capture-name*} **export** *file-location* **:** *file-name*

構文の説明

capture-name	エクスポートするキャプチャの名前。
file-location : *file-name*	（任意）キャプチャ ストレージ ファイルの場所およびファイル名を指定します。*file-location* に使用可能な値は次のとおりです。 • flash：オンボード フラッシュ ストレージ • ：USB ドライブ

コマンド デフォルト

キャプチャされたパケットは保存されません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

使用上のガイドライン

ストレージの宛先がキャプチャバッファである場合にのみ **monitor capture export** コマンドを使用します。ファイルはリモートにもローカルにも保存できます。キャプチャ中またはパケットキャプチャ停止後にこのコマンドを使用します。パケットキャプチャは、1つ以上の終了条件が満たされた場合、または **monitor capture stop** コマンドを入力すると停止します。

WireSharkがスタック内のスイッチで使用される場合、パケットキャプチャは前述の *file-location* で指定されたアクティブスイッチに接続されるデバイス上にのみ保存されます。例：flash1 はアクティブなスイッチに接続されています。flash2はセカンダリスイッチに接続されています。この場合、パケット キャプチャの保存に使用できるのは flash1 だけです。

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

例

キャプチャ バッファの内容を flash ドライブの mycap.pcap にエクスポートするには次を実行します。

monitor capture file

モニタキャプチャ（WireShark）ストレージファイル属性を設定するには、特権 EXEC モードで **monitor capture file** コマンドを使用します。ストレージファイル属性を削除するには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **file**{ [**buffer-size** *temp-buffer-size*] [**location** *file-location* **:** *file-name*] [**ring** *number-of-ring-files*] [**size** *total-size*] }
no monitor capture {*capture-name*} **file**{ [**buffer-size**] [**location**] [**ring**] [**size**] }

構文の説明

capture-name	変更するキャプチャの名前。
buffer-size *temp-buffer-size*	（任意）一時バッファのサイズを指定します。*temp-buffer-size* の範囲は 1 ～ 100 MB です。これはパケット損失を削減するために指定されます。
location *file-location* : *file-name*	（任意）キャプチャ ストレージ ファイルの場所およびファイル名を指定します。*file-location* に使用可能な値は次のとおりです。 • flash：オンボード フラッシュ ストレージ • ：USB ドライブ
ring *number-of-ring-files*	（任意）キャプチャが循環ファイルチェーンに保存されること、およびファイル リング内のファイル数を指定します。
size *total-size*	（任意）キャプチャ ファイルの合計サイズを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ストレージの宛先がファイルである場合にのみ **monitor capture file** コマンドを使用します。ファイルはリモートにもローカルにも保存できます。パケット キャプチャの停止後にこのコマンドを使用します。パケットキャプチャは、1 つ以上の終了条件が満たされた場合、または **monitor capture stop** コマンドを入力すると停止します。

WireShark がスタック内のスイッチで使用される場合、パケットキャプチャは前述の *file-location* で指定されたアクティブスイッチに接続されるデバイス上にのみ保存されます。例：flash1 はアクティブなスイッチに接続されています。flash2 はセカンダリスイッチに接続されています。この場合、パケット キャプチャの保存に使用できるのは flash1 だけです。

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

例

フラッシュ ドライブに保管されているファイル名が mycap.pcap であることを指定するには次を実行します。

```
Device# monitor capture mycap file location flash:mycap.pcap
```

monitor capture limit

キャプチャ制限を設定するには、特権 EXEC モードで **monitor capture limit** コマンドを使用します。キャプチャ制限を削除するには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **limit** {[**duration** *seconds*][**packet-length** *size*][**packets** *num*]}
no monitor capture {*capture-name*} **limit** [**duration**][**packet-length**][**packets**]

構文の説明

capture-name	キャプチャ制限を割り当てられるキャプチャの名前。
duration *seconds*	（任意）キャプチャ期間（秒）を指定します。範囲は 1 ～ 1000000 です。
packet-length *size*	（任意）パケット長（バイト）を指定します。実際のパケットが特定の長さより長い場合、数がバイト引数によって示される最初のセットのバイトのみが保存されます。
packets *num*	（任意）キャプチャに対して処理されるパケット数を指定します。

コマンド デフォルト

キャプチャ制限は設定されません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

60 秒のセッション制限および 400 バイトのパケット セグメント長を設定するには次を実行します。

```
Device# monitor capture mycap limit duration 60 packet-len 400
```

monitor capture match

モニタ（Wireshark）キャプチャに対して明示的にインラインコアフィルタを定義するには、特権 EXEC モードで **monitor capture match** コマンドを使用します。この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 capture {*capture-name*} **match** {**any** | **mac** *mac-match-string* | **ipv4** {**any** | **host** | **protocol**}{**any** | **host**} | **ipv6** {**any** | **host** | **protocol**}{**any** | **host**}}
no monitor capture {*capture-name*} **match**

構文の説明

capture-name	コア フィルタを割り当てられるキャプチャの名前。
any	すべてのパケットを指定します。
mac *mac-match-string*	レイヤ 2 パケットを指定します。
ipv4	IPv4 パケットを指定します。
host	ホストを指定します。
protocol	プロトコルを指定します。
ipv6	IPv6 パケットを指定します。

コマンド デフォルト

コア フィルタは設定されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

ソースまたは宛先上の任意の IP バージョン 4 パケットに一致するキャプチャ ポイントに対してキャプチャ ポイントおよびコア フィルタを定義するには、次を実行します。

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```

monitor capture start

トラフィック トレース ポイントでパケットデータのバッファへのキャプチャを開始するには、特権 EXEC モードで **monitor capture start** コマンドを使用します。

monitor capture {*capture-name*} **start**

構文の説明

capture-name	開始するキャプチャの名前。

コマンド デフォルト

バッファのコンテンツはクリアされません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

キャプチャポイントが定義された後にパケットデータキャプチャを有効にするには、**monitor capture clear** コマンドを使用します。パケットデータのキャプチャを停止するには、**monitor capture stop** コマンドを使用します。

CPU およびメモリなどのシステム リソースがキャプチャの開始前に使用可能であることを確認します。

例

バッファ コンテンツのキャプチャを開始するには次を実行します。

```
Device#  monitor capture mycap start
```

monitor capture stop

トラフィック トレース ポイントでパケットデータのキャプチャを停止するには、特権 EXEC モードで **monitor capture stop** コマンドを使用します。

monitor capture {*capture-name*} **stop**

構文の説明

capture-name	停止するキャプチャの名前。

コマンド デフォルト

パケット データ キャプチャが進行中です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

monitor capture stop コマンドを使用して、**monitor capture start** コマンドによって開始したパケットデータのキャプチャを停止します。線形および循環の 2 つのタイプのキャプチャ バッファを設定できます。線形バッファがいっぱいになった場合、データ キャプチャは自動的に停止します。循環バッファがいっぱいになると、データ キャプチャは最初から開始し、データは上書きされます。

例

バッファ コンテンツのキャプチャを停止するには次を実行します。

```
Device#  monitor capture mycap stop
```

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 Everest 16.5.1a	このコマンドが導入されました。
Cisco IOS XE Fuji 16.9.1	**type** {**erspan-destination** | **erspan-source**} キーワードが導入されました。 Cisco Catalyst 9500 シリーズ ハイ パフォーマンス スイッチに導入されました。

リリース	変更内容
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。 Cisco Catalyst 9500 シリーズ スイッチに導入されました。

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	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 ～ 66 です。
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。 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。 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。 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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

8 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 および RSPAN セッションを保有できます。

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 ポートを SPAN または RSPAN 宛先ポートとして設定できます。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。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(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。

```
Device(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。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
```

```
Device(config)# monitor session 1 destination remote vlan 900
Device(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。

```
Device(config)# monitor session 10 source remote vlan 900
Device(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。

```
Device(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。

```
Device(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	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 ～ 66 です。
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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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 および RSPAN セッションを保有できます。

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。

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
Device(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	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 ～ 66 です。
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。 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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

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 および RSPAN セッションを保有できます。

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

ローカルの Encapsulated Remote Switched Port Analyzer（ERSPAN）セッションを設定するには、グローバル コンフィギュレーション モードで **monitor session type** 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-destination** | **erspan-source**
no monitor session *span-session-number* **type erspan-destination** | **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 送信元または宛先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 Everest 16.5.1a	このコマンドが導入されました。
Cisco IOS XE Fuji 16.9.1	**erspan-destination** キーワードが導入されました。 Cisco Catalyst 9500 シリーズ ハイ パフォーマンス スイッチに導入されました。
Cisco IOS XE Gibraltar 16.11.1	**erspan-destination** キーワードが導入されました。 Cisco Catalyst 9500 シリーズ スイッチに導入されました。

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。

新しく設定されたERSPANセッションは、デフォルトで**shutdown**の状態になります。ERSPANセッションは、送信元インターフェイス、ERSPAN ID、ERSPAN IP アドレスなどの他の必須設定とともに **no shutdown** コマンドが設定されるまで非アクティブのままです。

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。

```
Device(config)# monitor session 55 type erspan-source
Device(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または宛先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。
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 capability feature monitor

モニタ機能に関する情報を表示するには、特権 EXEC モードで **show capability feature monitor** コマンドを使用します。

show capability feature monitor erspan-destination | **erspan-source**

構文の説明

erspan-destination	設定済みの Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元セッションに関する情報を表示します。
erspan-source	すべての設定済みのグローバル組み込みテンプレートを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

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

```
Switch# show capability feature monitor erspan-source

ERSPAN Source Session Supported: true
No of Rx ERSPAN source session: 8
No of Tx ERSPAN source session: 8
ERSPAN Header Type supported: II
ACL filter Supported: true
Fragmentation Supported: true
Truncation Supported: false
Sequence number Supported: false
QOS Supported: true
```

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

```
Switch# show capability feature monitor erspan-destination

ERSPAN Destination Session Supported: false
```

関連コマンド

コマンド	説明
monitor session type erspan-source	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 class-map type control subscriber

設定されている制御ポリシーのクラスマップ統計情報を表示するには、特権 EXEC モードで **show class-map type control subscriber** コマンドを使用します。

show class-map type control subscriber {all | **name** *control-class-name***}**

構文の説明

all	すべての制御ポリシーのクラスマップ統計情報を表示します。
name *control-class-name*	指定した制御ポリシーのクラスマップ統計情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、**show class-map type control subscriber name** *control-class-name* コマンドの出力例を示します。

```
Device# show class-map type control subscriber name platform

Class-map                 Action                       Exec  Hit  Miss  Comp
---------                 ------                       ----  ---  ----  ----
match-all platform        match platform-type C9xxx    0     0    0     0
Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
       condition without a need to continue on to the end
```

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device# 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	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 ～ 66 です。
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。 （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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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

SPAN 送信元セッションの最大数：2（送信元およびローカル セッションに適用）

例

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

```
Device# 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。

```
Device# 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。

```
Device# 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 capture

モニタキャプチャ（WireShark）の内容を表示するには、特権 EXEC モードで **show monitor capture file** コマンドを使用します。

show monitor capture [*capture-name* [**buffer**] | **file** *file-location* **:** *file-name*][**brief** | **detailed** | **display-filter** *display-filter-string*]

構文の説明

capture-name	（任意）表示するキャプチャの名前を指定します。
buffer	（任意）指定されたキャプチャに関連するバッファが表示されることを指定します。
file *file-location* : *file-name*	（任意）表示するキャプチャ ストレージ ファイルのファイル位置と名前を指定します。
brief	（任意）表示内容の概要を指定します。
detailed	（任意）詳細な表示内容を指定します。
display-filter *display-filter-string*	*display-filter-string* に従って表示内容をフィルタ処理します。

コマンド デフォルト

すべてのキャプチャの内容を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

none

例

mycap という名前のキャプチャのキャプチャを表示するには次を実行します。

```
Device# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
    Capture all packets
  Buffer Details:
```

```
 Buffer Type: LINEAR (default)
File Details:
 Associated file name: flash:mycap.pcap
 Size of buffer(in MB): 1
Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Packets per second: 0 (no limit)
 Packet sampling rate: 0 (no sampling)
```

show monitor session

スイッチドポートアナライザ（SPAN）、リモート SPAN（RSPAN）、および Encapsulated Remote Switched Port Analyzer（ERSPAN）の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-destination** | **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 ～ 66 です。
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。
erspan-destination	宛先 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。 （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 Everest 16.5.1a	このコマンドが導入されました。

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	**erspan-destination** キーワードが導入されました。 Cisco Catalyst 9500 シリーズ ハイ パフォーマンス スイッチに導入されました。
Cisco IOS XE Gibraltar 16.11.1	**erspan-destination** キーワードが導入されました。 Cisco Catalyst 9500 シリーズ スイッチに導入されました。

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。

```
Device# 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。

```
Device# 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。

```
Device# 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
```

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

```
Device# show monitor session erspan-destination

Type                    : ERSPAN Destination Session
Status                  : Admin Enabled
Source IP Address       : 10.10.10.210
Source ERSPAN ID        : 40
```

show parameter-map type subscriber attribute-to-service

パラメータマップの統計を表示するには、特権 EXEC モードで **show parameter-map type subscriber attribute-to-service** コマンドを使用します。

show parameter-map type subscriber attribute-to-service {all | name *parameter-map-name***}**

構文の説明

all	すべてのパラメータマップの統計を表示します。
name *parameter-map-name*	指定したパラメータマップの統計を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、**show parameter-map type subscriber attribute-to-service name** *parameter-map-name* コマンドの出力例を示します。

```
Device# show parameter-map type subscriber attribute-to-service name platform


Parameter-map name: platform
 Map: 10 platform-type regex "C9xxx"
  Action(s):
     10 interface-template critical
```

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 switchswitch-number | active | standbyip
wccpcache-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。 • *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。 • **active**：アクティブスイッチの情報を表示します。 • **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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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、デバイスが 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。

```
Device# 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 Everest 16.5.1a	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
```

show snmp stats

SNMP の統計を表示するには、特権 EXEC モードで **show snmp stats** コマンドを使用します。

show snmp stats { **hosts** | **oid**}

構文の説明

hosts	SNMPエージェントにポーリングされたSNMPサーバの詳細を表示します。
oid	最近要求されたオブジェクト識別子（OID）を表示します。

コマンド デフォルト

SNMP エージェントにポーリングされた SNMP マネージャエントリを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

show snmp stats hosts コマンドは、NMS の IP アドレス、NMS がエージェントをポーリングした回数、およびポーリングのタイムスタンプを一覧表示するために使用します。SNMP エージェントにポーリングされたエントリを削除するには、**clear snmp stats hosts** コマンドを使用します。

show snmp stats oid コマンドを実行する前に、デバイスを NMS に接続します。コマンド出力には、NMSから最近要求されたOIDのリストが表示されます。また、オブジェクトIDがNMSから要求された回数も示します。この情報は、NMS が照会している MIB に関する情報がほとんどない場合に、メモリリークやネットワーク障害のトラブルシューティングに役立ちます。**show snmp stats oid** コマンドを使用すると、NMS から最近要求された OID をいつでも確認できます。

次に、**show snmp stats hosts** コマンドの出力例を示します。

```
Device# show snmp stats hosts
Request Count                   Last Timestamp              Address
2                               00:00:01 ago                3.3.3.3
1                               1w2d ago                    2.2.2.2
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *1 : show snmp stats hosts* のフィールドの説明

フィールド	説明
`Request Count`	SNMPマネージャからSNMPエージェントに要求が送信された回数が表示されます。

フィールド	説明
Last Timestamp	SNMP マネージャから SNMP エージェントに要求が送信された時刻が表示されます。
アドレス（Address）	要求を送信した SNMP マネージャの IP アドレスが表示されます。

次に、**show snmp stats oid** コマンドの出力例を示します。

```
Device# show snmp stats oid

time-stamp                      #of times requested        OID
15:30:01 UTC Dec 2 2019                   6             ifPhysAddress
15:30:01 UTC Dec 2 2019                  10             system.2
15:30:01 UTC Dec 2 2019                   9             system.1
09:39:39 UTC Nov 26 2019                  3             system.5
09:39:39 UTC Nov 26 2019                  3             stem.4
09:39:39 UTC Nov 26 2019                  3             system.7
09:39:39 UTC Nov 26 2019                  2             system.6
09:39:39 UTC Nov 26 2019                 10             ceemEventMapEntry.2
09:39:39 UTC Nov 26 2019                  6             ipAddrEntry.4
09:39:39 UTC Nov 26 2019                  3             ipAddrEntry.5
09:39:39 UTC Nov 26 2019                 10             ipAddrEntry.3
09:39:39 UTC Nov 26 2019                  7             ipAddrEntry.2
09:39:39 UTC Nov 26 2019                  4             ipAddrEntry.1
09:39:39 UTC Nov 26 2019                  1             lsystem.3
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *2 : show snmp stats oid* のフィールドの説明

フィールド	説明
time-stamp	NMS からオブジェクト識別子が要求された日時が表示されます。
#of times requested	オブジェクト ID が要求された回数を表示します。
OID	NMS から最近要求されたオブジェクト識別子が表示されます。

shutdown（モニタセッション）

設定された ERSPAN セッションをディセーブルにするには、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 **shutdown** コマンドを使用します。設定された ERSPAN セッションをイネーブルにするには、このコマンドの **no** 形式を使用します。

shutdown
no shutdown

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

新しく設定された ERSPAN セッションは、シャットダウンの状態になります。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ERSPAN セッションは、**no shutdown** コマンドが設定されるまで非アクティブのままです。

例

次に、**no shutdown** コマンドを使用して ERSPAN セッションをアクティブにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# description source1
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 100
Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)# ip address 10.1.0.2
Device(config-mon-erspan-src-dst)# ip dscp 10
Device(config-mon-erspan-src-dst)# ip ttl 32
Device(config-mon-erspan-src-dst)# mtu 512
Device(config-mon-erspan-src-dst)# vrf monitoring
Device(config-mon-erspan-src-dst)# exit
Device(config-mon-erspan-src)# no shutdown
Device(config-mon-erspan-src)# end
```

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と宛先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。

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 community

Simple Network Management Protocol（SNMP）へのアクセスを許可するコミュニティ アクセス ストリングを設定するには、グローバル コンフィギュレーション モードで **snmp-server community** コマンドを使用します。指定したコミュニティストリングを削除するには、このコマンドの **no** 形式を使用します。

snmp-server community [**clear** | **encrypted**] *community-string* [**view** *view-name*] [**RO** | **RW**] [**SDROwner** | **SystemOwner**] [*access-list-name*]
no snmp-server community *community-string*

構文の説明

clear	（任意）入力された community-string がクリアテキストで、**show running** コマンドで表示されるときに暗号化されるように指定します。
encrypted	（任意）入力された *community-string* が暗号化テキストで、**show running** コマンドの実行時に暗号化されて表示されるように指定します。
community-string	パスワードのように動作し、SNMP プロトコルへのアクセスを許可します。*community-string* 引数の最大長は 32 文字の英字です。 **clear** キーワードが使用された場合、*community-string* はクリアテキストと見なされます。**encrypted** キーワードが使用された場合、*community-string* は暗号化テキストと見なされます。どちらも使用されなかった場合、*community-string* はクリアテキストと見なされます。
view*view-name*	（任意）事前に定義したビューの名前を指定します。ビューには、コミュニティで使用できるオブジェクトが定義されています。
RO	（任意）読み取り専用アクセス権を指定します。許可された管理ステーションは、MIB オブジェクトの取得だけを実行できます。
RW	（任意）読み取り/書き込みアクセス権を指定します。許可された管理ステーションは、MIB オブジェクトの取得と修正の両方を実行できます。
SDROwner	（任意）オーナー Service Domain Router（SDR）へのアクセスを制限します。
SystemOwner	（任意）オーナー以外のすべての SDR へのアクセスを含むシステム全体へのアクセスを提供します。
access-list-name	（任意）SNMP エージェントへアクセスするためにコミュニティ ストリングの使用を許可された IP アドレスのアクセス リスト名。

コマンド デフォルト

SNMP コミュニティ ストリングは、デフォルトで、すべての MIB オブジェクトへの読み取り専用アクセスを許可しています。コミュニティ ストリングは、デフォルトで、SDR オーナーに割り当てられます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てが原因でコマンドを使用できない場合、AAA 管理者に連絡してください。

コミュニティ アクセス ストリングを設定して SNMP へのアクセスを許可するには、**snmp-server community** コマンドを使用します。

指定したコミュニティ ストリングを削除するには、このコマンドの **no** 形式を使用します。

クリアテキストで入力したコミュニティ ストリングを **show running** コマンドの出力で暗号化して表示するには、**clear** キーワードを使用します。暗号化されたストリングを入力するには、**encrypted** キーワードを使用します。クリア テキストでコミュニティ ストリングを入力し、それがシステムによって暗号化されないようにするには、どちらのキーワードも使用しないようにします。

SDROwner キーワードを指定して **snmp-server community** コマンドを入力すると、オーナー SDR 内の MIB オブジェクト インスタンスに対してのみ SNMP アクセスが許可されます。**SystemOwner** キーワードを指定して **snmp-server community** コマンドを入力すると、システム内のすべての SDR に SNMP アクセスが許可されます。

（注） オーナー以外の SDR では、コミュニティ名は、そのコミュニティ名に割り当てられたアクセス権限に関係なく、その SDR に属するオブジェクト インスタンスだけにアクセスを許可します。オーナー SDR へのアクセスおよびシステム全体のアクセス特権は、オーナー SDR からだけ使用できます。

例

次に、comaccess ストリングを SNMP に割り当てて読み取り専用アクセスを許可する方法、および IP アクセス リスト 4 がコミュニティ ストリングを使用できるように指定する例を示します。

```
RP/0/RP0/CPU0:router(config)# snmp-server community comaccess ro 4
```

次に、mgr ストリングを SNMP に割り当てて、制限ビューのオブジェクトへの読み取りと書き込みアクセスを許可する例を示します。

```
RP/0/RP0/CPU0:router(config)# snmp-server community mgr view restricted rw
```

次に、comaccess コミュニティを削除する例を示します。

```
RP/0/RP0/CPU0:router(config)# no snmp-server community comaccess
```

関連コマンド

コマンド	説明
snmp-server view	SNMP のビュー エントリを作成または更新します。

snmp-server enable traps

デバイス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** | **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** | **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。*
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。デバイススタックでは、このトラップはスタックにおけるデバイスの挿入/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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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、デバイス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。

```
Device(config)# snmp-server enable traps config
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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。デフォルトは 0 です。 値 0 は、制限が適用されず、発生するたびにトラップが送信されることを示します。設定すると、**show run all** コマンド出力に `no snmp-server enable traps storm-control` が表示されます。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

```
Device(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 デフォルト

SNMP のエンジン ID は自動的に生成されますが、実行コンフィギュレーションには表示または保存されません。デフォルトまたは設定されたエンジン ID を表示するには、show snmp engineID コマンドを使用します。

一般的なシナリオでは、SNMP の設定後、この自動生成されたエンジン ID を使用します。ただし、スイッチが StackWise Virtual で実行されている場合はアクティブスイッチの MAC アドレスに基づきます。

スタックがリロードされ、スタックの別のスイッチが初回起動時にスタンバイとして選出されると、別の SNMPv3 エンジン ID が割り当てられます。これは SNMP 環境で障害の原因となりますが、snmp-server engineID local engineid-string を定義することで回避できます。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

なし

例

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

```
Device(config)# snmp-server engineID local 1234
```

snmp-server group

新しい Simple Network Management Protocol（SNMP）グループを設定するには、グローバル コンフィギュレーション モードで **snmp-server group** コマンドを使用します。指定した SNMP グループを削除するには、このコマンドの **no** 形式を使用します。

snmp-server group *group-name* **v1** | **v2c** | **v3** **auth** | **noauth** | **priv** [**context** *context-name*] [**match exact** | **prefix**] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-numberacl-name*]]
no snmp-server group *group-name* **v1** | **v2c** | **v3** **auth** | **noauth** | **priv** [**context** *context-name*]

構文の説明

group-name	グループの名前。
v1	グループが SNMPv1 セキュリティ モデルを使用していることを指定します。SNMPv1 は、最も安全性の低い SNMP セキュリティ モデルです。
v2c	グループが SNMPv2c セキュリティ モデルを使用していることを指定します。 SNMPv2c セキュリティ モデルでは、インフォームを送信でき、64 文字の文字列がサポートされています。
v3	グループが SNMPv3 セキュリティ モデルを使用していることを指定します。 SMNPv3 は、サポートされているセキュリティ モデルの中で最も安全です。SMNPv3 では、認証特性を明示的に設定できます。
auth	暗号化を行わないパケットの認証を指定します。
noauth	パケットの認証を行わないことを指定します。
priv	暗号化を行うパケットの認証を指定します。
context	（任意）この SNMP グループとそのビューと関連付ける SNMP コンテキストを指定します。
context-name	（任意）コンテキスト名。
match	（任意）正確なコンテキスト マッチを指定するか、またはコンテキスト プレフィックスのみを照合します。
exact	（任意）正確なコンテキストを照合します。
prefix	（任意）コンテキスト プレフィックスのみを照合します。
read	（任意）SNMP グループの読み取りビューを指定します。このビューでは、エージェントのコンテンツのみを表示できます。

read-view	（任意）ビューの名前である最大 64 文字の文字列。 デフォルトでは、**read** オプションを使用してこの状態を上書きしない限り、読み取りビューはインターネットオブジェクト識別子（OID）のスペース（1.3.6.1）に属するすべてのオブジェクトであるとみなされます。
write	（任意）SNMP グループの書き込みビューを指定します。このビューでは、データを入力してエージェントのコンテンツを設定できます。
write-view	（任意）ビューの名前である最大 64 文字の文字列。 デフォルトでは、書き込みビュー（つまり、ヌル OID）には何も定義されていません。書き込みアクセスを設定する必要があります。
notify	（任意）SNMP グループの通知ビューを指定します。このビューでは、通知、インフォーム、またはトラップを指定できます。
notify-view	（任意）ビューの名前である最大 64 文字の文字列。 デフォルトでは、**snmp-server host** コマンドが設定されるまで、通知ビュー（つまり、ヌル OID）には何も定義されていません。ビューを **snmp-server group** コマンドで指定した場合、生成されるそのビューのすべての通知は、グループに関連付けられているすべてのユーザに送信されます（そのユーザに対して SNMP サーバホストの設定が存在する場合）。 シスコでは、ソフトウェアに通知ビューを自動生成させることを推奨しています。このドキュメントの「通知ビューの設定」の項を参照してください。
access	（任意）グループに関連付ける標準アクセス コントロール リスト（ACL）を指定します。
ipv6	（任意）IPv6 名前付きアクセス リストを指定します。IPv6 と IPv4 の両方のアクセス リストが示されている場合は、IPv6 名前付きアクセス リストがリストの最初に表示されている必要があります。
named-access-list	（任意）IPv6 アクセス リストの名前。
acl-number	（任意）*acl-number* 引数は、以前に設定された標準アクセス リストを識別する 1 ～ 99 の整数です。
acl-name	（任意）*acl-name* 引数は、以前に設定された標準アクセス リストの名前である最大 64 文字の文字列です。

コマンド デフォルト　SNMP サーバ グループは設定されていません。

コマンド モード　グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

コミュニティ ストリングが内部的に設定されている場合、public という名前の 2 つのグループが自動生成されます。1 つは v1 セキュリティ モデル用、もう 1 つは v2c セキュリティ モデル用です。同様に、コミュニティ ストリングを削除すると、public という名前の v1 グループと public という名前の v2c グループが削除されます。

snmp-server group コマンドを設定する際、認証やプライバシーアルゴリズムにはデフォルト値はありません。また、デフォルトのパスワードも存在しません。Message Digest 5（MD5）パスワードの指定については、**snmp-server user** コマンドのドキュメントを参照してください。

通知ビューの設定

notify view オプションは、2 つの目的に使用できます。

- グループにSNMPを使用して設定された通知ビューがあり、その通知ビューを変更する必要がある。
- **snmp-server host** コマンドは、**snmp-server group** コマンドの前に設定されている可能性があります。この場合、**snmp-server host** コマンドを再設定するか、または適切な通知ビューを指定する必要があります。

次の理由から、SNMP グループを設定する際に通知ビューを指定することは推奨されていません。

- **snmp-server host** コマンドによってユーザに対して自動生成された通知ビューを、そのユーザに関連付けられているグループに追加する。
- グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。

snmp-server group コマンドの一部としてグループの通知ビューを指定する代わりに、指定された順序で次のコマンドを使用します。

1. **snmp-server user**：SNMP ユーザを設定します。
2. **snmp-server group**：通知ビューを追加しないで SNMP グループを設定します。
3. **snmp-server host**：トラップ操作の受信者を指定して、通知ビューを自動生成します。

SNMP コンテキスト

SNMP コンテキストによって、MIB データにアクセスする安全な方法が VPN ユーザに提供されます。VPN がコンテキストに関連付けられると、VPN 固有の MIB データがそのコンテキストに存在します。VPN をコンテキストに関連付けると、サービス プロバイダーが、複数 VPN でネットワークを管理できます。コンテキストを作成してVPNに関連付けることにより、サービス プロバイダーは、ある VPN のユーザが同じネットワーキング デバイス上で他の VPN のユーザに関する情報にアクセスするのを防ぐことができます。

読み取り、書き込み、または通知 SNMP ビューを SNMP コンテキストに関連付けるには、**context** *context-name* キーワードおよび引数とともにこのコマンドを使用します。

SNMP グループの作成

次の例は、SNMP サーバグループ「public」を作成して、すべてのオブジェクトに対して標準名前付きアクセスリスト「lmnop」のメンバへの読み取り専用アクセスを許可する方法を示しています。

```
Device(config)# snmp-server group public v2c access lmnop
```

SNMP サーバグループの削除

次の例に、設定から SNMP サーバグループ「public」を削除する方法を示します。

```
Device(config)# no snmp-server group public v2c
```

SNMP サバ グループと指定されたビューとの関連付け

次の例に、SNMPv2c グループ「GROUP1」のビューに関連付けられた SNMP コンテキスト「A」を示します。

```
Device(config)# snmp-server context A
Device(config)# snmp mib community commA
Device(config)# snmp mib community-map commA context A target-list commAVpn
Device(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify
viewB
```

関連コマンド

Command	Description
show snmp group	デバイス上のグループの名前、セキュリティモデル、各種ビューのステータス、および各グループのストレージタイプを表示します。
snmp mib community-map	SNMP コミュニティを SNMP コンテキスト、エンジン ID、セキュリティ名、または VPN ターゲットリストに関連付けます。
snmp-server host	SNMP 通知動作の受信者を指定します。
snmp-server user	SNMP グループに新しいユーザを設定します。

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、デバイスで **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。 **1**：SNMPv1。情報の場合は、このオプションを使用できません。 **2c**：SNMPv2C。 **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。 **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。 **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。 （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。
- **eigrp**：SNMP EIGRP 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。
- **isis**：SNMP IS-IS 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。
- **ospf**：Open Shortest Path First（OSPF）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。
- **port-security**：SNMP ポートセキュリティ 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。
- **vstack**SNMP スマート インストール 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。
- **wireless**：ワイヤレス 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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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デバイスを設定するには、**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、デバイスは **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。

```
Device(config)# snmp-server community comaccess ro 10
Device(config)# snmp-server host 172.20.2.160 comaccess
Device(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。

```
Device(config)# snmp-server enable traps
Device(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 に送信するようにデバイスをイネーブルにする方法を示します。

```
Device(config)# snmp-server enable traps
Device(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。

snmp-server manager

Simple Network Management Protocol（SNMP）マネージャプロセスを起動するには、グローバル コンフィギュレーション モードで **snmp-server manager** コマンドを使用します。SNMP マネージャプロセスを停止するには、このコマンドの **no** 形式を使用します。

snmp-server manager
no snmp-server manager

コマンド デフォルト

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが追加されました。

使用上のガイドライン

SNMP マネージャ プロセスは SNMP 要求をエージェントに送信し、エージェントから SNMP 応答と通知を受け取ります。SNMP マネージャ プロセスがイネーブルになっているときには、ルータはその他の SNMP エージェントに問い合わせて、送信されてきた SNMP トラップを処理できます。

ほとんどのネットワーク セキュリティ ポリシーでは、ルータが SNMP 要求を受け付け、SNMP 応答を送信し、SNMP 通知を送信するものと想定されています。SNMP マネージャ機能がイネーブルになっている状態では、ルータは、SNMP 要求の送信、SNMP 応答の受信、および SNMP 通知の受信も行います。場合によっては、この機能をイネーブルにする前にセキュリティ ポリシーの実装を更新する必要がある場合もあります。

通常、SNMP 要求は UDP ポート 161 に送信されます。通常、SNMP 応答は UDP ポート 161 から送信されます。通常、SNMP 通知は UDP ポート 162 に送信されます。

次に、SNMP マネージャ プロセスをイネーブルにする例を示します。

```
Router(config)# snmp-server manager
```

関連コマンド

Command	Description
show running-config	現在実行中のコンフィギュレーション ファイルまたは特定のインターフェイスのコンフィギュレーションの内容、またはマップ クラス情報を表示します。
show snmp user	グループ ユーザ名テーブルの各 SNMP ユーザ名に関する情報を表示します。
snmp-server engineID	デバイスで設定されたローカル SNMP エンジンおよびすべてのリモート エンジンの ID を表示します。

snmp-server user

Simple Network Management Protocol（SNMP）グループに新しいユーザを設定するには、グローバル コンフィギュレーション モードで**snmp-server user** コマンドを使用します。SNMP グループからユーザを削除するには、このコマンドの **no** 形式を使用します。

snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] **v1** | **v2c** | **v3** [**encrypted**] [**auth md5** | **sha** *auth-password*] [**access** [**ipv6** *nacl*] [**priv des** | **3des** | **aes 128** | **192** | **256** *privpassword*] *acl-numberacl-name*]
no snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] **v1** | **v2c** | **v3** [**encrypted**] [**auth md5** | **sha** *auth-password*] [**access** [**ipv6** *nacl*] [**priv des** | **3des** | **aes 128** | **192** | **256** *privpassword*] *acl-numberacl-name*]

構文の説明

username	エージェントに接続する、ホスト上のユーザの名前。
group-name	エントリが属する ACL（アクセス コントロール リスト）名
remote	（任意）ユーザが属するリモート SNMP エンティティ、およびそのエンティティのホスト名または IPv6 アドレスまたは IPv4 IP アドレスを指定します。IPv6 アドレスおよび IPv4 IP アドレスの両方を指定すると、IPv6 ホストが最初に表示されます。
host	（任意）リモート SNMP ホストの名前または IP アドレス。
udp-port	（任意）リモート ホストのユーザ データグラム プロトコル（UDP）ポート番号を指定します。
port	（任意）UDP ポートを識別する整数値。デフォルトは 162 です。
vrf	（任意）ルーティング テーブルのインスタンスを指定します。
vrf-name	（任意）データの格納に使用するバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）テーブルの名前。
v1	SNMPv1 を使用することを指定します。
v2c	SNMPv2c を使用することを指定します。
v3	SNMPv3 セキュリティ モデルを使用することを指定します。**encrypted** キーワードまたは **auth** キーワード、あるいはその両方の使用を許可します。
encrypted	（任意）パスワードが暗号化された形式で表示されるかどうかを指定します。
auth	（任意）使用する認証レベルを指定します。
md5	（任意）HMAC-MD5-96 認証レベルを指定します。
sha	（任意）HMAC-SHA-96 認証レベルを指定します。

auth-password	（任意）エージェントがホストからパケットを受信できるようにするストリング（64 文字以下）。
access	（任意）このSNMPユーザと関連付けるアクセスコントロールリスト（ACL）を指定します。
ipv6	（任意）この SNMP ユーザと関連付ける IPv6 名前付きアクセス リストを指定します。
nacl	（任意）ACL の名前です。IPv4、IPv6、または IPv4 と IPv6 の両方のアクセス リストを指定できます。両方を指定した場合は、IPv6名前付きアクセスリストがステートメントの最初に表示されます。
priv	（任意）SNMP メッセージ レベルの安全性のための SNMP バージョン 3 のユーザベース セキュリティ モデル（USM）の使用を指定します。
des	（任意）暗号化について 56 ビット Digital Encryption Standard（DES）アルゴリズムの使用を指定します。
3des	（任意）暗号化について168 ビット3DESアルゴリズムの使用を指定します。
aes	（任意）暗号化について Advanced Encryption Standard（AES）アルゴリズムの使用を指定します。
128	（任意）暗号化について 128 ビット AES アルゴリズムの使用を指定します。
192	（任意）暗号化について 192 ビット AES アルゴリズムの使用を指定します。
256	（任意）暗号化について 256 ビット AES アルゴリズムの使用を指定します。
privpassword	（任意）プライバシーユーザパスワードを指定する文字列（64 文字以下）。
acl-number	（任意）IPアドレスの標準アクセスリストを指定する1～99の範囲の整数。
acl-name	（任意）IP アドレスの標準アクセス リストの名前である文字列（64 文字以下）。

コマンド デフォルト

暗号化、パスワード、およびアクセスリストのデフォルト動作については、「使用上のガイドライン」の項にある表を参照してください。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

リモート ユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応するIPアドレスまたはポート番号を指定します。また、特定のエージェントにリモー

トユーザを設定する前に、**snmp-server engineID** コマンドに **remote** キーワードを指定して SNMP エンジン ID を設定します。リモート エージェントの SNMP エンジン ID は、パスワードから認証とプライバシー ダイジェストを計算する際に必要です。最初にリモート エンジン ID が設定されていない場合、コンフィギュレーション コマンドは失敗します。

privpassword 引数と *auth-password* 引数については、最小の長さが 1 文字で、推奨される長さは 8 文字以上であり、文字と数字の両方を含める必要があります。推奨される最大長は 64 文字です。

次の表に、暗号化、パスワード、およびアクセス リストのデフォルトのユーザ特性を示します。

表 *3 : snmp-server user* のデフォルトの説明

特性	デフォルト
アクセス リスト	すべての IP アクセス リストからのアクセスが許可されます。
暗号化	デフォルトでは存在しません。**encrypted** キーワードは、パスワードがメッセージ ダイジェスト アルゴリズム 5（MD5）ダイジェストであり、テキストパスワードではないことを指定するために使用されます。
パスワード	テキスト文字列と見なされます。
リモート ユーザ	すべてのユーザは、**remote** キーワードを使用してリモートであることを指定しないかぎり、この SNMP エンジンに対してローカルであると見なされます。

SNMP パスワードは、権威 SNMP エンジンの SNMP ID を使用してローカライズされます。インフォームの場合、正規の SNMP エージェントはリモート エンジンです。プロキシ要求またはインフォームを送信できるようにするには、SNMP データベース内のリモート エンジンの SNMP エンジン ID を設定する必要があります。

（注） SNMP ユーザ設定後にエンジン ID を変更すると、ユーザを削除できません。ユーザを削除するには、まず、SNMP ユーザを再設定する必要があります。

パスワードおよびダイジェストの取り扱い

コマンドを設定する際、認証やプライバシーアルゴリズムにはデフォルト値はありません。また、デフォルトのパスワードも存在しません。パスワードの最小の長さは 1 文字ですが、シスコではセキュリティのために 8 文字以上にすることを推奨しています。パスワードの推奨される最大長は 64 文字です。パスワードを忘れた場合は回復できないため、ユーザを再設定する必要があります。プレーン テキストのパスワードとローカライズされた MD5 ダイジェストの、どちらも指定できます。

ローカライズされた MD5 またはセキュア ハッシュ アルゴリズム（SHA）ダイジェストを持っている場合は、プレーン テキストのパスワードではなく、その文字列を指定できます。ダイ

ジェストは aa:bb:cc:dd の形式にする必要があります。aa、bb、および cc は 16 進値です。また、ダイジェストは正確に 16 個のオクテットであることが必要です。

例

次の例は、ユーザ abcd を public という名前の SNMP サーバ グループに追加する方法を示しています。この例では、ユーザにアクセス リストが指定されていないため、グループに適用されている標準の名前付きアクセス リストがユーザに適用されます。

```
Device(config)# snmp-server user abcd public v2c
```

次の例は、ユーザ abcd を public という名前の SNMP サーバ グループに追加する方法を示しています。この例では、標準の名前付きアクセス リスト qrst からのアクセス ルールがユーザに適用されます。

```
Device(config)# snmp-server user abcd public v2c access qrst
```

次の例では、プレーン テキストのパスワード cisco123 が、public という名前の SNMP サーバ グループのユーザ abcd に対して設定されています。

```
Device(config)# snmp-server user abcd public v3 auth md5 cisco123
```

show running-config コマンドを入力すると、このユーザの行が表示されます。このユーザが設定に追加されたことを確認するには、show snmp user コマンドを使用します。

（注） **show running-config** コマンドは、noAuthNoPriv モードで作成されたユーザを表示しますが、authPriv モードまたは authNoPriv モードで作成されたアクティブな SNMP ユーザは表示しません。authPriv、authNoPrv、または noAuthNoPriv モードで作成したアクティブな SNMPv3 ユーザを表示するには、**show snmp user** コマンドを使用します。

ローカライズされた MD5 または SHA ダイジェストを持っている場合は、プレーン テキストのパスワードではなく、その文字列を指定できます。ダイジェストは aa:bb:cc:dd の形式にする必要があります。aa、bb、および cc は 16 進値です。また、ダイジェストは正確に 16 個のオクテットであることが必要です。

次の例では、プレーン テキストのパスワードの代わりに MD5 ダイジェスト文字列が使用されています。

```
Device(config)# snmp-server user abcd public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

次の例では、ユーザ abcd が public という名前の SNMP サーバ グループから削除されます。

```
Device(config)# no snmp-server user abcd public v2c
```

次の例では、publicという名前のSNMPサーバグループからのユーザabcdが、secure3desをパスワードとして使用してプライバシーの暗号化のために168ビット3DESアルゴリズムを使用することを指定しています。

```
Device(config)# snmp-server user abcd public priv v2c 3des secure3des
```

関連コマンド

Command	Description
show running-config	現在実行中のコンフィギュレーションファイルまたは特定のインターフェイスのコンフィギュレーションの内容、またはマップ クラス情報を表示します。
show snmp user	グループ ユーザ名テーブルの各 SNMP ユーザ名に関する情報を表示します。
snmp-server engineID	デバイスで設定されたローカルSNMPエンジンおよびすべてのリモート エンジンの ID を表示します。

snmp-server view

ビューエントリを作成または更新するには、グローバル コンフィギュレーション モードで **snmp-server view** コマンドを使用します。指定された Simple Network Management Protocol（SNMP）サーバビューエントリを削除するには、このコマンドの **no** 形式を使用します。

snmp-server view *view-name oid-tree* **included** | **excluded**
no snmp-server view *view-name*

構文の説明

view-name	更新または作成しているビュー レコードのラベル。レコードはこの名前で参照されます。
oid-tree	ビューに含める、またはビューから除外する ASN.1 サブツリーのオブジェクト識別子。サブツリーを識別するために、1.3.6.2.4 などの数字や system などの単語で構成されるテキスト文字列を指定します。サブツリーファミリを指定するには、サブ ID の 1 文字をアスタリスク（*）ワイルドカードに変えます。たとえば、1.3.*.4 です。
included	*oid-tree* 引数に指定されている OID（およびサブツリー OID）を SNMP ビューに含めるように設定します。
excluded	*oid-tree* 引数に指定されている OID（およびサブツリー OID）を SNMP ビューから明示的に除外するように設定します。

コマンド デフォルト

ビュー エントリは存在しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

他の SNMP コマンドでは、引数として SMP ビューが必要です。このコマンドを使用して、他のコマンドの引数として使用するビューを作成します。

ビューを定義する代わりに、ビューが必要なときに 2 つの標準の定義済みビューを使用できます。1 つは *everything* で、ユーザがすべてのオブジェクトを表示することができることを示します。もう 1 つは *restricted* で、ユーザが system、snmpStats、snmpParties の 3 つのグループを表示できることを示します。定義済みビューは、RFC 1447 で説明されています。

最初に入力する **snmp-server** コマンドは、ルーティングデバイス上で SNMP をイネーブルにします。

例

次に、MIB-II サブツリー内のすべてのオブジェクトを含むビューを作成する例を示します。

```
snmp-server view mib2 mib-2 included
```

次に、MIB-II システム グループのすべてのオブジェクトおよび Cisco エンタープライズ MIB のすべてのオブジェクトを含むビューを作成する例を示します。

```
snmp-server view root_view system included
snmp-server view root_view cisco included
```

次に、sysServices（System 7）と MIB-II インターフェイス グループ内のインターフェイス 1 のすべてのオブジェクトを除く、MIB-II システム グループのすべてのオブジェクトを含むビューを作成する例を示します。

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
snmp-server view agon ifEntry.*.1 included
```

次の例では、USM、VACM、およびコミュニティ MIB は、ルート親「internet」の下にある他のすべての MIB とともにビュー「test」に明示的に含まれています。

```
! -- include all MIBs under the parent tree "internet"
snmp-server view test internet included
! -- include snmpUsmMIB
snmp-server view test 1.3.6.1.6.3.15 included
! -- include snmpVacmMIB
snmp-server view test 1.3.6.1.6.3.16 included
! -- exclude snmpCommunityMIB
snmp-server view test 1.3.6.1.6.3.18 excluded
```

関連コマンド

Command	Description
snmp-server community	SNMP プロトコルへのアクセスを許可するようにコミュニティ アクセス ストリングを設定します。
snmp-server manager	SNMP マネージャ プロセスを開始します。

source（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元インターフェイスまたはVLAN、およびモニタするトラフィックの方向を設定するには、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 **source** コマンドを使用します。この設定を無効にするには、このコマンドの **no** 形式を使用します。

source interface *type number* | **vlan** *vlan-ID*[**,** | **-** | **both** | **rx** | **tx**]

構文の説明

interface *type number*	インターフェイスのタイプおよび番号を指定します。
vlan *vlan-ID*	ERSPAN 送信元セッション番号と VLAN を関連付けます。有効な値は 1 ～ 4094 です。
,	（任意）別のインターフェイスを指定します。
-	（任意）インターフェイスの範囲を指定します。
both	（任意）ERSPAN の送受信トラフィックをモニタします。
rx	（任意）受信トラフィックのみモニタします。
tx	（任意）送信トラフィックのみモニタします。

コマンド デフォルト

送信元インターフェイスまたは VLAN が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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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。

例

次に、ERSPAN 送信元セッションのプロパティの設定例を示します。

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# source interface fastethernet 0/1 rx
```

関連コマンド

コマンド	説明
monitor session type	ローカルのERSPAN送信元または宛先セッションを設定します。

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
Cisco IOS XE Everest 16.5.1a	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。

```
Device(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
Cisco IOS XE Everest 16.5.1a Cisco IOS XE Fuji 16.9.1	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。

```
Device(config-template)# switchport voice vlan 20
```