ネットワーク管理コマンド

この章には、すべての製品別ネットワーク管理コマンドが含まれています。

- debug platform ip dhcp, 3 ページ
- debug platform snmp, 5 ページ
- monitor session, 6 ページ
- monitor session destination, 8 ページ
- monitor session filter, 13 ページ
- monitor session source, 15 ページ
- show monitor session, 18 ページ
- show platform snmp counters, 20 ページ
- snmp-server enable traps, 21 ページ
- snmp-server enable traps bridge, 25 ページ
- snmp-server enable traps call-home, 27 ページ
- snmp-server enable traps cef, 29 ページ
- snmp-server enable traps cpu, 31 ページ
- snmp-server enable traps dot1x, 33 ページ
- snmp-server enable traps energywise, 35 ページ
- snmp-server enable traps envmon, 37 ページ
- snmp-server enable traps errdisable, 39 ページ
- snmp-server enable traps flash, 41 ページ
- snmp-server enable traps ike, 43 ページ
- snmp-server enable traps ipsec, 45 ページ
- snmp-server enable traps license, 47 ページ

- snmp-server enable traps mac-notification, 49 ページ
- snmp-server enable traps ospf, 51 ページ
- snmp-server enable traps pim, 53 ページ
- snmp-server enable traps port-security, 55 ページ
- snmp-server enable traps power-ethernet, 57 ページ
- snmp-server enable traps snmp, 59 ページ
- snmp-server enable traps stackwise, 61 ページ
- snmp-server enable traps storm-control, 64 ページ
- snmp-server enable traps stpx, 66 ページ
- snmp-server enable traps transceiver, 68 ページ
- snmp-server enable traps vstack, 70 ページ
- snmp-server engineID, 72 ページ
- snmp-server host, 73 ページ

debug platform ip dhcp

DHCPイベントをデバッグするには、ユーザEXECモードまたは特権EXECモードで**debug platform ip dhcp** コマンドを使用します。 デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug platform ip dhcp {**all** | **error** | **event** | **packet** | **rpc**}

no debug platform ip dhcp {**all** | **error** | **event** | **packet** | **rpc**}

構文の説明

all	すべての DHCP デバッグ メッセージを表示します。
error	DHCP エラー デバッグ メッセージを表示します。
event	DHCP イベント デバッグ メッセージを表示します。
packet	DHCP パケット関連デバッグ メッセージを表示します。
rpc	DHCP リモート プロシージャ コール（RPC）要求デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

undebug platform ip dhcp コマンドは、**no debug platform ip dhcp** コマンドと同じです。

あるスイッチスタック上でデバッグをイネーブルにした場合、アクティブスイッチでのみイネーブルになります。 スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* EXEC コマンドでスタック マスターからセッションを開始してください。 次に、スタック メンバのコマンドラインプロンプトで**debug** コマンドを入力します。 最初にセッションを開始せずにメ

ンバ スイッチのデバッグをイネーブルにするには、アクティブ スイッチ上で **remote command** *stack-member-number LINE* EXEC コマンドを使用することもできます。

関連コマンド

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング情報を表示します。
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

debug platform snmp

プラットフォーム依存の簡易ネットワーク管理プロトコル（SNMP）ソフトウェアのデバッグをイネーブルにするには、ユーザ EXEC モードまたは特権 EXEC モードで **debug platform snmp** コマンドを使用します。 デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug platform snmp

no debug platform snmp

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

デバッグはディセーブルです。

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 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

undebug platform snmp コマンドは、**no debug platform snmp** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合、アクティブスイッチでのみイネーブルになります。 スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* EXEC コマンドを使用して、アクティブ スイッチからのセッションを開始できます。 次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。 最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、アクティブ スイッチ上で **remote command** *stack-member-number LINE* EXEC コマンドを使用することもできます。

関連コマンド

コマンド	説明
show debugging	イネーブルになっているデバッグ タイプに関する情報を表示します。

monitor session

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

monitor session *session-number* {**destination** | **filter** | **source**}

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

構文の説明

session-number	SPAN または RSPAN セッションで識別されるセッション番号。 範囲は 1 ～ 68 です。 ただし、このスイッチが Catalyst 2960-S とスタックされる場合、範囲は 1 ～ 66 になります。
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 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

4 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 68 の SPAN および RSPAN セッ

ションを保持できます。ただし、このスイッチがCatalyst 2960-Sスイッチとスタックされる場合、2個のローカルSPANセッションおよびRSPAN送信元セッションを組み合わせた最大値に限定され、範囲は1 ～ 66になります。

プライベートVLANポートは、SPAN宛先ポートには設定できません。

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。

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

```
Switch# 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。 範囲は 1 ～ 68 です。 ただし、このスイッチが Catalyst 2960-S とスタックされる場合、範囲は 1 ～ 66 になります。
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 メンバー、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。

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	（任意）入力トラフィック転送をイネーブルにします。
dot1q vlan *vlan-id*	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。
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。
untagged vlan *vlan-id*	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。
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。
remote vlan *vlan-id*	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。

all, **local**, **range**, and **remote**	**all**、**local**、**range** *session-range*、または **remote** を **no monitor session** コマンドとともに使用して、それぞれ SPAN と RSPAN セッションすべて、ローカル SPAN セッションすべて、一定範囲のセッション、RSPAN 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。

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。

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 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

4 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 68 の SPAN および RSPAN セッションを保持できます。 ただし、このスイッチが Catalyst 2960-S スイッチとスタックされる場合、2 個のローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値に限定され、範囲は 1 ～ 66 になります。

SPAN または RSPAN の宛先は物理ポートである必要があります。

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

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

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

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

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

EtherChannel ポートは、SPAN または RSPAN 宛先ポートとして設定することはできません。 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。

プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。

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。

- 他のキーワードなしで、**monitor session** *session_number* **destination interface** *interface-id* を入力した場合、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。
- その他のキーワードを指定せずに、**monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** 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、入力トラフィック転送はイネーブルにはなりません。 （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の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リング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、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。

```
Switch(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。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination remote vlan 900
Switch(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。

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

```
Switch(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。

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

monitor session filter

特定のVLANにフローベースSPAN（FSPAN）セッションまたはフローベース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* [**,** | **-**] | {**ip** | **ipv6** | **mac**} **access-group** *access-list*}

no monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] | {**ip** | **ipv6** | **mac**} **access-group** *access-list*}

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。 範囲は 1 ～ 68 です。 ただし、このスイッチが Catalyst 2960-S とスタックされる場合、範囲は 1 ～ 66 になります。
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 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

4 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 68 の SPAN および RSPAN セッションを保持できます。 ただし、このスイッチが Catalyst 2960-S スイッチとスタックされる場合、2 個のローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値に限定され、範囲は 1 ～ 66 になります。

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

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

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

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

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

例

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

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

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

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

monitor session source

スイッチド ポート アナライザ（SPAN）セッションまたはリモート SPAN（RSPAN）送信元セッションを開始する、または既存の SPAN または RSPAN セッションでインターフェイスを追加または削除するにはには、**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。 範囲は 1 ～ 68 です。 ただし、このスイッチが Catalyst 2960-S とスタックされる場合、範囲は 1 ～ 66 になります。
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 メンバー、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 vlan *vlan-id*	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 15.0(2)EX1	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。

4 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 68 の SPAN および RSPAN セッションを保持できます。 ただし、このスイッチが Catalyst 2960-S スイッチとスタックされる場合、2 個のローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値に限定され、範囲は 1 ～ 66 になります。

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リング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
```

show monitor session

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

show monitor session {*session_number* | **all** | **erspan-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。 範囲は 1 ～ 68 です。 ただし、このスイッチが Catalyst 2960-S スイッチとスタックされる場合、2 個のローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値に限定され、範囲は 1 ～ 66 になります。
all	すべての SPAN セッションを表示します。
erspan-destination	宛先 ERSPAN セッションだけを表示します。
erspan-source	送信元 ERSPAN セッションだけを表示します。
local	ローカル SPAN セッションだけを表示します。
range *list*	一定範囲の SPAN セッションを表示します。*list* は有効なセッションの範囲です。 range は単一のセッション、または2つの数字を小さい数字からハイフンで区切ったセッションの範囲です。 カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。 （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 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

SPAN送信元セッションの最大数：4（送信元およびローカルセッションに適用）ただし、このスイッチが Catalyst 2960-S スイッチとスタックされる場合、2 個のローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値に限定されます。

例

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 session** 特権 EXEC コマンドの出力を示します。

```
Switch# 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** 特権 EXEC コマンドの出力を示します。

```
Switch# 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 platform snmp counters

プラットフォーム依存の簡易ネットワーク管理プロトコル（SNMP）カウンタ情報を表示するには、**show platform snmp counters** 特権 EXEC コマンドを使用します。

show platform snmp counters

構文の説明

このコマンドには引数またはキーワードはありません。

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 15.0(2)EX1	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。

snmp-server enable traps

スイッチ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簡易ネットワーク管理プロトコル（SNMP）通知を送信可能にするには、**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** | **cef** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **eigrp** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **hsrp** | **ike** | **ipmulticast** | **ipsec** | **license** | **mac-notification** | **ospf** | **pim** | **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** | **bridge** | **call-home** | **cef** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **eigrp** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **hsrp** | **ike** | **ipmulticast** | **ipsec** | **license** | **mac-notification** | **ospf** | **pim** | **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。*
cef	（任意）クラスタ トラップをイネーブルにします。*
cluster	（任意）SNMP クラスタ トラップをイネーブルにします。
config	（任意）SNMP 設定トラップをイネーブルにします。
config-copy	（任意）SNMP 設定コピー トラップをイネーブルにします。
config-ctid	（任意）SNMP 設定 CTID トラップをイネーブルにします。
copy-config	（任意）SNMP コピー設定トラップをイネーブルにします。
cpu	（任意）CPU 通知トラップをイネーブルにします。*
dot1x	（任意）SNMP dot1x トラップをイネーブルにします。*

eigrp	（任意）SNMP EIGRP 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。スイッチスタックでは、このトラップはスタックにおけるスイッチの挿入/取り外しを意味します。
hsrp	（任意）SNMP HSRP トラップをイネーブルにします。
ike	（任意）SNMP IKE トラップをイネーブルにします。*
ipmulticast	（任意）IP マルチキャスト ルーティング トラップをイネーブルにします。
ipsec	（任意）SNMP IPsec トラップをイネーブルにします。*
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。*
ospf	（任意）OSPF トラップをイネーブルにします。*
pim	（任意）SNMP PIM 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 15.0(2)EX1	このコマンドが追加されました。

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。

snmp-server enable traps コマンドは、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します。

（注） コマンドラインのヘルプ ストリングに表示される場合でも、**fru-ctrl**、**insertion** および **removal** キーワードはスイッチでサポートされません。 **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。

```
Switch(config)# snmp-server enable traps cluster
Switch(config)# snmp-server enable traps config
Switch(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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps bridge newroot
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps call-home message-send-fail
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

snmp-server enable traps cef

SNMP シスコ エクスプレス フォワーディング 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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps cef inconsistency
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps cpu threshold
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

snmp-server enable traps dot1x

IEEE 802.1x 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 dot1x** 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 dot1x [**auth-fail-vlan**][**guest-vlan**][**no-auth-fail-vlan**][**no-guest-vlan**]

no snmp-server enable traps dot1x [**auth-fail-vlan**][**guest-vlan**][**no-auth-fail-vlan**][**no-guest-vlan**]

構文の説明

auth-fail-vlan	（任意）ポートが設定された制限 VLAN に移行する場合にトラップを生成します。
guest-vlan	（任意）ポートが設定されたゲスト VLAN に移行する場合にトラップを生成します。
no-auth-fail-vlan	（任意）制限 VLAN が設定されていないために、ポートが制限 VLAN に移行しようとしてもできなかった場合にトラップを生成します。
no-guest-vlan	（任意）ゲスト VLAN が設定されていないために、ポートがゲスト VLAN に移行しようとしてもできなかった場合にトラップを生成します。

コマンド デフォルト

IEEE 802.1x 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 15.0(2)EX1	このコマンドが追加されました。

使用上のガイドライン

キーワードを何も指定せずに **snmp-server enable traps dot1x** コマンドを入力すると、すべての IEEE 802.1x トラップがイネーブルになります。

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、ポートが設定済み制限 VLAN に移行する場合にトラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps dot1x auth-fail-vlan
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

snmp-server enable traps energywise

SNMP EnergyWise 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 energywise** 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 energywise [**event-occured**][**level-change**][**neighbor-added**][**neighbor-deleted**]

no snmp-server enable traps energywise [**event-occured**][**level-change**][**neighbor-added**][**neighbor-deleted**]

構文の説明

event-occured	（任意）EnergyWise のイベント発生トラップをイネーブルにします。
level-change	（任意）EnergyWise のエンティティ レベル変化トラップをイネーブルにします。
neighbor-added	（任意）EnergyWise のネイバー追加トラップをイネーブルにします。
neighbor-deleted	（任意）EnergyWise のネイバー削除トラップをイネーブルにします。

コマンド デフォルト

SNMP EnergyWise 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 15.0(2)EX1	このコマンドが導入されました。

使用上のガイドライン

キーワードを何も指定せずに **snmp-server enable traps energywise** コマンドを入力すると、すべての EnergyWise トラップがイネーブルになります。

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、EnergyWise イベントが発生したときにトラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps energywise event-occured
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps envmon fan
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 ～ 4294967295 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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps errdisable notification-rate 2
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps flash insertion
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

snmp-server enable traps ike

IKEの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 ike** 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 ike {**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}}

no snmp-server enable traps ike {**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}}

構文の説明

policy	（任意）IKE ポリシー トラップをイネーブルにします。
add	（任意）IKE ポリシー トラップを追加します。
delete	（任意）IKE ポリシー トラップを削除します。
tunnel	（任意）IKE トンネル トラップをイネーブルにします。
start	（任意）IKE トンネル開始トラップをイネーブルにします。
stop	（任意）IKE トンネル停止トラップをイネーブルにします。

コマンド デフォルト

IKE 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 15.0(2)EX1	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、IKE トンネル開始トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps ike tunnel start
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

snmp-server enable traps ipsec

IPsec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 ipsec** 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 ipsec {**cryptomap** {**add** | **attach** | **delete** | **detach**} | **too-many-sas** | **tunnel** {**start** | **stop**}}

no snmp-server enable traps ipsec {**cryptomap** {**add** | **attach** | **delete** | **detach**} | **too-many-sas** | **tunnel** {**start** | **stop**}}

構文の説明

cryptomap	IPsec クリプトマップ トラップをイネーブルにします。
add	IPsec クリプトマップ追加トラップをイネーブルにします。
attach	IPsec クリプトマップ適用トラップをイネーブルにします。
delete	IPsec クリプトマップ削除トラップをイネーブルにします。
detach	IPsec クリプトマップ解除トラップをイネーブルにします。
too-many-sas	IPsec SA 過多トラップをイネーブルにします。
tunnel	IPsec トンネル トラップをイネーブルにします。
start	IPsec トンネル開始トラップをイネーブルにします。
stop	IPsec トンネル停止トラップをイネーブルにします。

コマンド デフォルト

IPsec 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 15.0(2)EX1	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、IPsec トンネル開始トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps ipsec tunnel start
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps license deploy
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps mac-notification change
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps ospf lsa
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps pim invalid-pim-message
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps port-security trap-rate 200
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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** *name* | **police**}

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

構文の説明

group *name*	指定したグループ番号またはリストにインライン パワー グループベース トラップをイネーブルにします。
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 15.0(2)EX1	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 poe1 の Power over Ethernet（PoE）トラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps poower-over-ethernet group poe1
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps snmp warmstart
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

snmp-server enable traps stackwise

SNMP StackWise 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 stackwise** 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 stackwise [**GLS**][**ILS**][**SRLS**] [**insufficient-power**][**invalid-input-current**] [**invalid-output-current**][**member-removed**][**member-upgrade-notification**] [**new-master**][**new-member**] [**port-change**][**power-budget-warning**][**power-invalid-topology**] [**power-link-status-changed**][**power-oper-status-changed**] [**power-priority-conflict**][**power-version-mismatch**][**ring-redundant**] [**stack-mismatch**][**unbalanced-power-supplies**][**under-budget**][**under-voltage**]

no snmp-server enable traps stackwise [**GLS**][**ILS**][**SRLS**] [**insufficient-power**][**invalid-input-current**] [**invalid-output-current**][**member-removed**][**member-upgrade-notification**] [**new-master**][**new-member**] [**port-change**][**power-budget-warning**][**power-invalid-topology**] [**power-link-status-changed**][**power-oper-status-changed**] [**power-priority-conflict**][**power-version-mismatch**][**ring-redundant**] [**stack-mismatch**][**unbalanced-power-supplies**][**under-budget**][**under-voltage**]

構文の説明

GLS	（任意）StackWise スタック電源 GLS トラップをイネーブルにします。
ILS	（任意）StackWise スタック電源 ILS トラップをイネーブルにします。
SRLS	（任意）StackWise スタック電源 SRLS トラップをイネーブルにします。
insufficient-power	（任意）Stackwise スタック電源の不平衡電源トラップをイネーブルにします。
invalid-input-current	（任意）Stackwise スタック電源の無効入力電流トラップをイネーブルにします。
invalid-output-current	（任意）Stackwise スタック電源の無効出力電流トラップをイネーブルにします。
member-removed	（任意）StackWise スタック メンバ削除トラップをイネーブルにします。
member-upgrade-notification	（任意）StackWise メンバのアップグレード用リロード トラップをイネーブルにします。
new-master	（任意）StackWise の新規マスター トラップをイネーブルにします。

new-memberport-change	（任意）StackWise の新規メンバポート トラップをイネーブルにします。
power-budget-warning	（任意）StackWise スタック電源バジェット警告トラップをイネーブルにします。
power-invalid-topology	（任意）Stackwise スタック電源の無効トポロジ トラップをイネーブルにします。
power-link-status-changed	（任意）StackWise スタック電源リンク ステータス変更トラップをイネーブルにします。
power-oper-status-changed	（任意）StackWise スタック電源ポート動作ステータス変更トラップをイネーブルにします。
power-priority-conflict	（任意）Stackwise スタック電源のプライオリティ競合トラップをイネーブルにします。
power-version-mismatch	（任意）StackWise スタック電源のバージョン不一致トラップをイネーブルにします。
ring-redundant	（任意）StackWise のリング冗長トラップをイネーブルにします。
stack-mismatch	（任意）StackWise スタック不一致トラップをイネーブルにします。
unbalanced-power-supplies	（任意）Stackwise スタック電源の不平衡電源トラップをイネーブルにします。
under-budget	（任意）StackWise スタック電源の不足バジェット トラップをイネーブルにします。
under-voltage	（任意）Stackwise スタック電源の不足電圧トラップをイネーブルにします。

コマンド デフォルト

SNMP StackWise 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 15.0(2)EX1	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、StackWise スタック電源の GLS トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps stackwise GLS
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

snmp-server enable traps storm-control

SNMP ストーム制御トラップ パラメータをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps storm-control** コマンドを使用します。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps storm-control {**trap-rate** *number-of-minutes*}

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

構文の説明

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

コマンド デフォルト

SNMP ストーム制御トラップ パラメータの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps storm-control trap-rate 10
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps stpx inconsistency
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps transceiver all
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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 15.0(2)EX1	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。

```
Switch(config)# snmp-server enable traps vstack addition
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の受信者（ホスト）を指定します。

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

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.0(2)EX1	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。

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

snmp-server host

簡易ネットワーク管理プロトコル（SNMP）通知操作の受信者を指定するには、スイッチで **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。 指定され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 Secure Hash Algorithm（SHA）による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をイネーブルにします（privacy とも呼ばれます）。
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 設定コピー トラップを送信します。
- **config-ctid**：SNMP 設定 CTID トラップを送信します。
- **copy-config**：SNMP コピー設定トラップを送信します。
- **cpu**：CPU 通知トラップを送信します。
- **cpu threshold**：CPU しきい値通知トラップを送信します。
- **entity**：SNMP エンティティ 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 エラー ディセーブル通知トラップを送信します。
- **event-manager**：SNMP 組み込みイベント マネージャ トラップを送信します。
- **flash**：SNMP フラッシュ通知を送信します。
- **flowmon**：SNMP フロー モニタ通知トラップを送信します。
- **ipmulticast**：SNMP IP マルチキャスト ルーティング トラップを送信します。
- **ipsla**：SNMP IP SLA トラップを送信します。
- **license**：ライセンス トラップを送信します。
- **local-auth**：SNMP ローカル認証トラップを送信します。
- **mac-notification**：SNMP MAC 通知トラップを送信します。
- **msdp**：SNMP Multicast Source Discovery Protocol（MSDP）トラップを送信します。
- **pim**：プロトコル独立型マルチキャスト（PIM）トラップを送信します。
- **power-ethernet**：SNMP パワー イーサネット トラップを送信します。
- **rtr**：SNMP 応答時間リポーター 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 作成トラップを送信します。
- **vlandelete**：SNMP VLAN 削除トラップを送信します。
- **vrfmib**：SNMP vrfmib トラップを送信します。
- **vtp**：SNMP VLAN とランキング プロトコル（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ていますが、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 15.0(2)EX1	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。 送信と同時に廃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スイッチを設定するには、**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、スイッチは **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** 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 番め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。

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

```
Switch(config)# snmp-server enable traps
Switch(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 に送信するようにスイッチをイネーブルにする方法を示します。

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

関連コマンド

コマンド	説明
snmp-server enable traps	スイッチが NMS にインフォーム要求やさまざまなトラップの SNMP 通知を送れるようにします。