# snmp-server enable traps ospf cisco-specific state-change through snmp-server enable traps voice poor-qov

# snmp-server enable traps ospf cisco-specific state-change

T o enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) transition state changes, use the **snmp-server enable traps ospf cisco-specific state-change**command in global configuration mode. To disable OSPF transition state change SNMP notifications, use the **no**form of this command.

**snmp-server enable traps ospf cisco-specific state-change** [{**nssa-trans-change** | **shamlink** [{**interface** | **interface-old** | **neighbor**}]}]
**no snmp-server enable traps ospf cisco-specific state-change** [{**nssa-trans-change** | **shamlink** [{**interface** | **interface-old** | **neighbor**}]}]

## Syntax Description

| | |
|---|---|
| **nssa-trans-change** | (Optional) Enables only not-so-stubby area (NSSA) translator state changes trap for the OSPF area. |
| **shamlink** | (Optional) Enables only the sham-link transition state changes trap for the OSPF area. |
| **interface** | (Optional) Enables only the sham-link interface state changes trap for the OSPF area. |
| **interface -old** | (Optional) Enables only the replaced interface transition state changes trap for the OSPF area. |
| **neighbor** | (Optional) Enables only the sham-link neighbor transition state changes trap for the OSPF area. |

## Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF transition state changes are not created.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(5) | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |
| 12.0(30)S | The **shamlink**, **interface-old**, and **neighbor** keywords were added. |
| 12.3(14)T | Support was added for the **shamlink**, **interface-old**, and **neighbor** keywords. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

You cannot enter both the **interface** and **interface-old** keywords because you cannot enable both the new and replaced sham-link interface transition state change traps. You can configure only one of the two traps, but not both.

## Examples

The following example enables the router to send OSPF sham-link transition state change notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps ospf cisco-specific errors config-error** | Enables SNMP notifications for OSPF nonvirtual interface mismatch errors. |
| **snmp-server enable traps ospf cisco-specific errors shamlink** | Enables SNMP notifications for OSPF sham-link errors. |
| **snmp-server enable traps ospf cisco-specific retransmit** | Enables SNMP notifications for OSPF retransmission errors. |

# snmp-server enable traps pim

To enable Protocol Independent Multicast (PIM) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pim**command in global configuration mode. To disable PIM-specific SNMP notifications, use the **no**form of this command.

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

## Syntax Description

| | |
|---|---|
| **neighbor-change** | (Optional) Enables notifications indicating when a router's PIM interface is disabled or enabled, or when a router's PIM neighbor adjacency expires. |
| **rp-mapping-change** | (Optional) Enables notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages. |
| **invalid-pim-message** | (Optional) Enables invalid PIM message traps. For example, an invalid PIM message could result when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group. |

## Command Default

SNMP notifications are disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(4)T | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files, available from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

## Examples

The following example shows how to configure a router to generate notifications indicating that a PIM interface on the router has been enabled:

```
! Configure PIM traps to be sent as SNMPv2c traps to host with IP address 10.0.0.1.
Router(config)# snmp-server host 10.0.0.1 traps version 2c public pim

! Configure router to send the neighbor-change class of notifications to host.
Router(config)# snmp-server enable traps pim neighbor-change

! Enable PIM sparse-dense mode on Ethernet interface 0/0.
```

```
Router(config)# interface ethernet0/0

Router(config-if)# ip pim sparse-dense-mode
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps** | Enables all available SNMP notifications on your system. |
| **snmp-server host** | Specifies the recipient of an SNMP notification operation. |
| **snmp-server trap-source** | Specifies the interface from which an SNMP trap should originate. |

# snmp-server enable traps power-ethernet group

To configure the group containing the slot that is connected to a power Ethernet power source entity (PSE), use the **snmp-server enable traps power-ethernet group** command in global configuration mode. To disable the group, use the **no** form of this command.

**snmp-server enable traps power-ethernet group** *slot-number*
**no snmp-server enable traps power-ethernet group** *slot-number*

## Syntax Description

| | |
|---|---|
| *slot-number* | Integer that specifies the number of the group that contains the slot that is connected to a power Ethernet PSE. The range is from 1 to 4. |

## Command Default

Groups containing a slot that is connected to a PSE are not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)SY | This command was introduced. |

## Usage Guidelines

Enable the trap for the group to receive the trap generated from the interface of the slot.

## Examples

The following example shows how to configure a group for the Ethernet PSE device:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server enable traps power-ethernet group 2
Device(config)# end
```

## Related Commands

| Command | Description |
|---|---|
| **power inline** | Determines how inline power is applied to a device on the specified switch port. |
| **show power inline** | Displays the power status for a specified port or for all ports. |
| **snmp-server trap-source** | Specifies the interface (and hence the corresponding IP address) from which an SNMP trap originates. |

# snmp-server enable traps pppoe

To enable Point-to-Point Protocol over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pppoe**command in global configuration mode. To disable PPPoE session count SNMP notifications, use the **no**form of this command.

**snmp-server enable traps pppoe**
**no snmp-server enable traps pppoe**

## Syntax Description

This command has no arguments or keywords.

## Command Default

SNMP notifications are disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(1)DC | This command was introduced. |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| Cisco IOS XE Release 2.5 | This command was implemented on Cisco ASR 1000 series routers. |

## Usage Guidelines

This command enables SNMP traps only. It does not support inform requests.

To configure the PPPoE session-count thresholds at which SNMP notifications will be sent, use the **pppoe limit max-sessions** or **pppoe max-sessions** commands.

For a complete description of the SNMP notifications and additional MIB functions, see the CISCO-PPPOE-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs

## Examples

The following example enables the router to send PPPoE session-count SNMP notifications to the host at the address 192.0.2.0:

```
snmp-server community public RW
snmp-server enable traps pppoe
snmp-server host 192.0.2.0 version 2c public udp-port 1717
```

## Related Commands

| Command | Description |
|---|---|
| **pppoe limit max-sessions** | Sets the maximum number of PPPoE sessions that will be permitted on a router, and sets the PPPoE session-count threshold at which an SNMP trap will be generated. |
| **pppoe max-sessions** | Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated. |
| **snmp-server host** | Specifies the recipient of an SNMP notification operation. |

| Command | Description |
|---|---|
| **snmp-server trap-source** | Specifies the interface from which an SNMP trap should originate. |

# snmp-server enable traps pppoe per-interface

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications on an interface trap, use the **snmp-server enable traps pppoe per-interface** command in global configuration mode. To disable PPPoE session count SNMP notifications on an interface trap, use the **no** form of this command.

**snmp-server enable traps pppoe per-interface [loss-percent | loss-threshold]**
**no snmp-server enable traps pppoe per-interface [loss-percent | loss-threshold]**

## Syntax Description

| | |
|---|---|
| **loss-percent** | (Optional) Enables the per-interface loss-percent trap. |
| **loss-threshold** | (Optional) Enables the per-interface loss-threshold trap. |

## Command Default

PPPoE session count SNMP notifications are disabled on an interface trap.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)S | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe per-interface** command enables traps and inform requests for the specified notification types. A notification for this command indicates that the percentage of PPPoE sessions lost has crossed the configured threshold value for a particular interface.

## Examples

The following example shows how to enable PPPoE session count SNMP notifications on a per-interace loss-percent trap:

```
Device(config)# snmp-server enable traps pppoe per-interface loss-percent
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps pppoe per-mac** | Enables PPPoE session count SNMP notifications for a node with MAC address traps. |
| **snmp-server enable traps pppoe per-vc** | Enables PPPoE session count SNMP notifications for a VC trap. |
| **snmp-server enable traps pppoe per-vlan** | Enables PPPoE session count SNMP notifications on a VLAN trap. |
| **snmp-server enable traps pppoe session** | Enables PPPoE session count SNMP notifications for a session trap. |
| **snmp-server enable traps pppoe vc** | Enables PPPoE session count SNMP notifications for all VC traps between nodes. |

# snmp-server enable traps pppoe per-mac

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications for a node with MAC address traps, use the **snmp-server enable traps pppoe per-mac** command in global configuration mode. To disable PPPoE session count SNMP notifications for a node with MAC address traps, use the **no** form of this command.

**snmp-server enable traps pppoe per-mac [limit | throttle]**
**no snmp-server enable traps pppoe per-mac [limit | throttle]**

## Syntax Description

| | |
|---|---|
| **limit** | (Optional) Enables the per-MAC limit trap. |
| **throttle** | (Optional) Enables the per-MAC throttle trap. |

## Command Default

PPPoE session count SNMP notifications are disabled for a node with MAC address traps.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)S | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe per-mac** command enables both traps and inform requests for the specified notification types. A notification for this command indicates that the number of active sessions from a particular client Ethernet MAC address has reached the configured per-MAC limit.

## Examples

The following example shows how to enable PPPoE session count SNMP notifications for a node with per-MAC limit traps:

```
Device(config)# snmp-server enable traps pppoe per-mac limit
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps pppoe per-interface** | Enables PPPoE session count SNMP notifications on an interface trap. |
| **snmp-server enable traps pppoe per-vc** | Enables PPPoE session count SNMP notifications for a VC trap. |
| **snmp-server enable traps pppoe per-vlan** | Enables PPPoE session count SNMP notifications on a VLAN trap. |
| **snmp-server enable traps pppoe session** | Enables PPPoE session count SNMP notifications for a session trap. |
| **snmp-server enable traps pppoe vc** | Enables PPPoE session count SNMP notifications for all VC traps between nodes. |

# snmp-server enable traps pppoe per-vc

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications for a virtual connection (VC) trap, use the **snmp-server enable traps pppoe per-vc** command in global configuration mode. To disable PPPoE session count SNMP notifications for a VC trap, use the **no** form of this command.

**snmp-server enable traps pppoe per-vc [limit | throttle]**
**no snmp-server enable traps pppoe per-vc [limit | throttle]**

## Syntax Description

| | |
|---|---|
| **limit** | (Optional) Enables a per-VC limit trap. |
| **throttle** | (Optional) Enables a per-VC throttle trap. |

## Command Default

PPPoE session count SNMP notifications are disabled for a VC trap.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)S | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe per-vc** command enables traps and inform requests for the specified notification types. A notification for this command indicates the number of active sessions for a ATM VCI/VPI that has crossed the configured maximum limit.

## Examples

The following example shows how to enable PPPoE session count SNMP notifications on a per-VC limit trap:

```
Device(config)# snmp-server enable traps pppoe per-vc limit
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps pppoe per-interface** | Enables PPPoE session count SNMP notifications on an interface trap. |
| **snmp-server enable traps pppoe per-mac** | Enables PPPoE session count SNMP notifications for a node with MAC address traps. |
| **snmp-server enable traps pppoe per-vlan** | Enables PPPoE session count SNMP notifications on a VLAN trap. |
| **snmp-server enable traps pppoe session** | Enables PPPoE session count SNMP notifications for a session trap. |
| **snmp-server enable traps pppoe vc** | Enables PPPoE session count SNMP notifications for all VC traps between nodes. |

# snmp-server enable traps pppoe per-vlan

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications on a VLAN trap, use the **snmp-server enable traps pppoe per-vlan** command in global configuration mode. To disable PPPoE session count SNMP notifications on a VLAN trap, use the **no** form of this command.

**snmp-server enable traps pppoe per-vlan [limit | throttle]**
**no snmp-server enable traps pppoe per-vlan [limit | throttle]**

## Syntax Description

| | |
|---|---|
| **limit** | (Optional) Enables a per-VLAN limit trap. |
| **throttle** | (Optional) Enables a per-VLAN throttle trap. |

## Command Default

PPPoE session count SNMP notifications are disabled on a VLAN trap.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)S | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe per-vlan** command enables traps and inform requests for the specified notification types. A notification for this command indicates the number of new PPPoE session requests coming on a particular VLAN over a configured time interval that has reached the rate limit.

## Examples

The following example shows how to enable PPPoE session count SNMP notifications on a per-VLAN limit trap:

```
Device(config)# snmp-server enable traps pppoe per-vlan limit
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps pppoe per-interface** | Enables PPPoE session count SNMP notifications on an interface trap. |
| **snmp-server enable traps pppoe per-mac** | Enables PPPoE session count SNMP notifications for a node with MAC address traps. |
| **snmp-server enable traps pppoe per-vc** | Enables PPPoE session count SNMP notifications for a VC trap. |
| **snmp-server enable traps pppoe session** | Enables PPPoE session count SNMP notifications for a system trap. |
| **snmp-server enable traps pppoe vc** | Enables PPPoE session count SNMP notifications for all VC traps between nodes. |

# snmp-server enable traps pppoe system

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications on a system trap, use the **snmp-server enable traps pppoe system** command in global configuration mode. To disable PPPoE session count SNMP notifications on a system trap, use the **no** form of this command.

**snmp-server enable traps pppoe system [loss-percent | loss-threshold | threshold]**
**no snmp-server enable traps pppoe system [loss-percent | loss-threshold | threshold]**

## Syntax Description

| | |
|---|---|
| **loss-percent** | (Optional) Enables the session loss-percent trap. |
| **loss-threshold** | (Optional) Enables the session loss-threshold trap. |
| **threshold** | (Optional) Enables the session threshold trap. |

## Command Default

PPPoE session count SNMP notifications are disabled on a system trap.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)S | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe system** command enables traps and inform requests for the specified notification types. A notification for this command indicates the percentage of PPPoE session lost globally over a period of time that has crossed the configured threshold.

## Examples

The following example shows how to enable PPPoE session count SNMP notifications on a system loss-percent trap:

```
Device(config)# snmp-server enable traps pppoe system loss-percent
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps pppoe per-interface** | Enables PPPoE session count SNMP notifications on an interface trap. |
| **snmp-server enable traps pppoe per-mac** | Enables PPPoE session count SNMP notifications for a node with MAC address traps. |
| **snmp-server enable traps pppoe per-vc** | Enables PPPoE session count SNMP notifications for a VC trap. |
| **snmp-server enable traps pppoe per-vlan** | Enables PPPoE session count SNMP notifications on a VLAN trap. |

| Command | Description |
| --- | --- |
| **snmp-server enable traps pppoe vc** | Enables PPPoE session count SNMP notifications for all VC traps between nodes. |

# snmp-server enable traps pppoe vc

To enable PPP over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications on all virtual connection (VC) traps between nodes, use the **snmp-server enable traps pppoe vc** command in global configuration mode. To disable PPPoE session count SNMP notifications on all VC traps between nodes, use the **no** form of this command.

**snmp-server enable traps pppoe vc [threshold]**
**no snmp-server enable traps pppoe vc [threshold]**

## Syntax Description

| | |
|---|---|
| **threshold** | (Optional) Enables a VC threshold trap. |

## Command Default

PPPoE session count SNMP notifications are disabled on all VC traps between nodes.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)S | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps pppoe vc** command enables traps and inform requests for the specified notification types. A notification for this command indicates the number of active sessions for a ATM VCI/VPI that has crossed the configured maximum limit on a VC interface.

## Examples

The following example shows how to enable PPPoE session count SNMP notifications on a VC threshold trap:

```
Device(config)# snmp-server enable traps pppoe vc threshold
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps pppoe per-interface** | Enables PPPoE session count SNMP notifications for an interface trap. |
| **snmp-server enable traps pppoe per-mac** | Enables PPPoE session count SNMP notifications for a node with MAC address traps. |
| **snmp-server enable traps pppoe per-vc** | Enables PPPoE session count SNMP notifications for a VC trap. |
| **snmp-server enable traps pppoe per-vlan** | Enables PPPoE session count SNMP notifications on a VLAN trap. |
| s**nmp-server enable traps pppoe per-system** | Enables PPPoE session count SNMP notifications for a session trap. |

# snmp-server enable traps repeater

To enable or disable standard repeater (hub) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps repeater**command in global configuration mode. To disable repeater notifications, use the **no**form of this command.

**snmp-server enable traps repeater** [**health**] [**reset**]
**no snmp-server enable traps repeater** [**health**] [**reset**]

## Syntax Description

| | |
|---|---|
| **health** | (Optional) Enables the rptrHealth trap, which conveys information related to the operational status of the repeater. |
| **reset** | (Optional) Sends the rptrResetEvent trap on completion of a repeater reset action (triggered by the transition to a START state by a manual command). |

## Command Default

SNMP notifications are disabled.

If no option keywords are specified when entering this command, all repeater notifications available on your system are enabled or disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables Repeater MIB notifications, as defined in RFC 1516. RFC 1516 defines objects for managing IEEE 802.3 10 Mbps baseband repeaters, also known as hubs.

Two sets of notifications are available for this command. The following notification is defined in the CISCO-REPEATER-MIB (enterprise 1.3.6.1.4.1.9.9.22.3):

- 1 ciscoRptrIllegalSrcAddrTrap (illegal source address trap)

The following notifications are defined in the CISCO-REPEATER-MIB-V1SMI (enterprise 1.3.6.1.2.1.22):

- 1 rptrHealth
- 2 rptrGroupChange
- 3 rptrResetEvent

For a complete description of the repeater notifications and additional MIB functions, refer to the CISCO-REPEATER-MIB.my and CISCO-REPEATER-MIB-V1SMI.my files, available on Cisco.com at

http://www.cisco.com/public/mibs/ .

When the optional **health** keyword is used, the rptrHealth trap is sent when the value of rptrOperStatus changes, or upon completion of a nondisruptive test.

The rptrOperStatus object indicates the operational state of the repeater. Status values are as follows:

- other(1)--undefined or unknown status
- ok(2)--no known failures
- rptrFailure(3)--repeater-related failure
- groupFailure(4)--group-related failure
- portFailure(5)--port-related failure
- generalFailure(6)--failure, unspecified type

When the optional **reset** keyword is used, the rptrResetEvent trap is not sent when the agent restarts and sends an SNMP coldStart or warmStart trap.

The **snmp-server enable traps repeater**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

## Examples

The following example shows how to enable the router to send repeater inform notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps repeater
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server host** | Specifies the recipient of an SNMP notification operation. |
| **snmp-server trap-source** | Specifies the interface that an SNMP trap should originate from. |

# snmp-server enable traps resource-policy

To enable Embedded Resource Manager (ERM)-MIB notification traps, use the **snmp-server enable traps resource-policy** command in global configuration mode. To disable the ERM-MIB notification traps, use the **no** form of this command.

**snmp-server enable traps resource-policy**
**no snmp-server enable traps resource-policy**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Notification traps will be sent to the host that is configured to receive traps.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |
| 12.4(15)T | This command was integrated into Cisco IOS Release 12.4(15)T. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |

## Examples

The following example shows how to configure the router to send SNMP notifications for ERM to a host:

```
Router(config)# snmp-server enable traps resource policy
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server community** | Permits access to SNMP by setting up the community access string. |
| **snmp-server host** | Specifies the recipient of an SNMP notification message. |

# snmp-server enable traps rtr

To enable the sending of Cisco IOS IP Service Level Agreements (SLAs) Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server enable traps rtr**command in global configuration mode. To disable IP SLAs SNMP notifications, use the **no**form of this command.

**snmp-server enable traps rtr**
**no snmp-server enable traps rtr**

## Syntax Description

This command has no arguments or keywords.

## Command Default

SNMP notifications are disabled by default.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command controls (enables or disables) Cisco IOS IP SLAs notifications, as defined in the Response Time Monitor MIB (CISCO-RTTMON-MIB).

The **snmp-server enable traps rtr**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

## Examples

The following example shows how to enable the router to send IP SLAs SNMP traps to the host at the address myhost.cisco.com using the community string defined as public:

```
snmp-server enable traps rtr
snmp-server host myhost.cisco.com informs version 2c public rtr
```

## Related Commands

| Command | Description |
|---|---|
| **ip sla monitor** | Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode. |
| **ip sla** | Begins configuration for an IP SLAs operation and enters IP SLA configuration mode. |
| **snmp-server host** | Specifies the destination NMS and transfer parameters for SNMP notifications. |
| **snmp-server trap-source** | Specifies the interface that an SNMP trap should originate from. |

# snmp-server enable traps snmp

To enable the RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps snmp**command in global configuration mode. To disable RFC 1157 SNMP notifications, use the **no**form of this command.

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

## Syntax Description

| | |
|---|---|
| **authentication** | (Optional) Controls the sending of SNMP authentication failure notifications. |
| **linkup** | (Optional) Controls the sending of SNMP linkUp notifications. |
| **linkdown** | (Optional) Controls the sending of SNMP linkDown notifications. |
| **coldstart** | (Optional) Controls the sending of SNMP coldStart notifications. |
| **warmstart** | (Optional) Controls the sending of SNMP warmStart notifications. |

## Command Default

SNMP notifications are disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 11.3 | The **snmp-server enable traps snmp authentication** command was introduced. This command replaced the **snmp-server trap-authentication** command. |
| 12.1(3)T | The following keywords were added:<br>• **linkup**<br>• **linkdown**<br>• **coldstart** |
| 12.1(5)T | The **warmstart** keyword was added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

If you do not enter an **snmp-server enable traps snmp**command, no notifications controlled by this command are sent. To configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps snmp**command. When you enter the command with no keywords, all notification types are enabled. When you enter the command with a keyword, only the types of notifications related to that keyword are enabled.

When you use the optional **authentication**keyword, the authenticationFailure(4) trap signifies that the sending device is the addressee of a protocol message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs for packets with an incorrect community string and the SNMP traps are generated. For SNMPv3, authentication failure occurs for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside the authoritative SNMP engine's window (for example, packets that are configured outside access lists or time ranges) and a report PDU is generated, however authentication failure traps are not generated.

When you use the optional **linkup**keyword, the linkUp(3) trap signifies that the sending device recognizes one of the communication links represented in the agent's configuration coming up.

When you use the optional **linkdown**keyword, the linkDown(2) trap signifies that the sending device recognizes a failure in one of the communication links represented in the agent's configuration.

The **snmp-server enable traps snmp** [**linkup**] [**linkdown**] form of this command globally enables or disables SNMP linkUp and linkDown traps. After enabling either of these traps globally, you can disable them on specific interfaces using the **no snmp trap link-status** command in interface configuration mode. On the interface level, linkUp and linkDown traps are enabled by default, which means that these notifications do not have to be enabled on a per-interface basis. However, linkUp and linkDown notifications will not be sent unless you enable them globally using the **snmp-server enable traps snmp** command.

When you use the optional **coldstart**keyword, the coldStart(0) trap signifies that the sending device is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.

When you use the optional **warmstart**keyword, the warmStart(1) trap signifies that the sending device is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.

The **snmp-server enable traps snmp**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host**command.

For a host to receive a notification controlled by this command, you must enable both the **snmp-server enable traps** command and the **snmp-server host**command for that host. If the notification type is not controlled by this command, you must enable the appropriate **snmp-server host** command only.

## Examples

The following example shows how to enable the router to send all traps to the host myhost.cisco.com, using the community string public:

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

The following example shows how to enable the router to send all inform notifications to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public snmp
```

The following example shows how to enable all SNMP trap types, and then disable only the linkUp and linkDown traps:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps snmp
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
Router# configure terminal
Router(config)# no snmp-server enable traps snmp linkup linkdown
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication coldstart warmstart
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps** | Enables all available SNMP notifications on your system. |
| **snmp-server host** | Specifies the recipient of an SNMP notification operation. |
| **snmp-server informs** | Specifies inform request options. |
| **snmp-server trap authentication vrf** | Disables or reenables SNMP authentication notifications specific to VPN context mismatches. |
| **snmp-server trap-source** | Specifies the interface that an SNMP trap should originate from. |

# snmp-server enable traps srp

To enable the sending of Intelligent Protection Switching (IPS) Spatial Reuse Protocol (SRP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps srp** command in global configuration mode. To disable SRP notifications, use the **no** form of this command.

**snmp-server enable traps srp**
**no snmp-server enable traps srp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced to support DPT-OC12 Port Adapters. |

## Usage Guidelines

The Cisco SRP MIB module (CISCO-SRP-MIB.my) provides objects for monitoring IP-over-SONET IPS SRP traffic using the SNMP. When IPS is enabled, if a node or fiber facility failure is detected, traffic going toward or coming from the failure direction is wrapped (looped) back to go in opposite direction on the other ring.

The **snmp-server enable traps srp** command enables SRP state change notifications (traps or informs). SRP state change notifications are generated whenever one of the two sides of an SRP interface ring enters or leaves the wrapped state (when a ring wraps, or when a ring is restored).

Specifically, the srpMACIpsWrapCounter object in the CISCO-SRP-MIB increments when a Ring wraps, and the value of the rpMACIpsLastUnWrapTimeStamp object changes when a ring unwraps. (An “unwrap” event happens when the original ring is restored.)

The **snmp-server enable traps srp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

## Examples

In the following example, SRP-specific informs are enabled and will be sent to the host “myhost.cisco.com” using the community string defined as public:

```
Router(config)# snmp-server enable traps srp

Router(config)# snmp-server host myhost.cisco.com informs version 2c public srp
```

# snmp-server enable traps storm-control

To enable Simple Network Management Protocol (SNMP) storm-control trap notifications, use the **snmp-server enable traps storm-control**command in privileged EXEC mode. To disable storm-control trap notifications, use the **no**form of this command.

**snmp-server enable traps storm-control traps-rate num**
**no snmp-server enable traps storm-control traps-rate num**

## Syntax Description

| | | |
|---|---|---|
| **traps-rate** | *num* | Number of traps per minute; valid values are 0 through 1000. |

## Command Default

Storm-control traps are disabled.

## Command Modes

Configuration mode (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXJ | This command was introduced. |

## Examples

This example shows how to enable the storm-control trap notification trap rate to 250:

```
Router# snmp-server enable traps storm control traps-rate 250
Router#
```

## Related Commands

| Command | Description |
|---|---|
| snmp-server enable traps storm-control | Enables SNMP storm-control trap notifications. |
| **snmp-server host** | Specifies the recipient of an SNMP notification operation. |
| test snmp trap storm-control | Tests the SNMP CISCO-PORT-STORM-CONTROL-MIB traps. |

# snmp-server enable traps syslog

To enable the sending of system logging message Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps syslog**command in global configuration mode. To disable system logging message SNMP notifications, use the **no**form of this command.

**snmp-server enable traps syslog**
**no snmp-server enable traps syslog**

## Syntax Description

This command has no arguments or keywords.

## Command Default

SNMP notifications are disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) system logging message notifications. System logging messages (also called system error messages, or syslog messages) are status notification messages that are generated by the routing device during operation. These messages are typically logged to a destination (such as the terminal screen, to a system buffer, or to a remote “syslog” host).

If your software image supports the Cisco Syslog MIB, these messages can also be sent via SNMP to a network management station (NMS). To determine which software images support the Cisco Syslog MIB, used the Cisco MIB Locator tool at http://www.cisco.com/go/mibs/ .(At the time of writing, the Cisco Syslog MIB is only supported in “Enterprise” images.)

Unlike other logging processes on the system, debug messages (enabled using CLI debug commands) are not included with the logging messages sent via SNMP.

To specify the severity level at which notifications should be generated, use the **logging history** global configuration command. For additional information about the system logging process and severity levels, see the description of the **logging** commands.

The syslog notification is defined by the clogMessageGenerated NOTIFICATION-TYPE object in the Cisco Syslog MIB (CISCO-SYSLOG-MIB.my). When a syslog message is generated by the device a clogMessageGenerated notification is sent to the designated NMS. The clogMessageGenerated notification includes the following objects: clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp.

For a complete description of these objects and additional MIB information, see the text of CISCO-SYSLOG-MIB.my, available on Cisco.com using the SNMP Object Navigator tool at http://www.cisco.com/go/mibs . See also the CISCO-SYSLOG-EXT-MIB and the CISCO-SYSLOG-EVENT-EXT-MIB.

The **snmp-server enable traps syslog**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

## Examples

The following example enables the router to send system logging messages at severity levels 0 (emergencies) through 2 (critical) to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps syslog

Router(config)# logging history 2

Router(config)# snmp-server host myhost.cisco.com traps version 2c public
```

## Related Commands

| Command | Description |
|---|---|
| **logging history** | Limits syslog messages sent to the router's history table and to an SNMP NMS based on severity. |
| **snmp-server host** | Specifies the destination NMS and transfer parameters for SNMP notifications. |
| **snmp-server trap-source** | Specifies the interface that an SNMP trap should originate from. |

# snmp-server enable traps transceiver all

To enable all supported SNMP transceiver traps for all transceiver types in the global configuration mode, use the **snmp-server enable traps transceiver all**command. Use the **no** form of this command to disable the transceiver SNMP trap notifications.

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

## Syntax Description

The command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE | Support for this command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The **snmp-server enable traps**command is used with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

## Examples

This example shows how to enable all supported SNMP transceiver traps for all transceiver types:

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

## Related Commands

| Command | Description |
|---|---|
| **show interfaces transceiver** | Displays information about the optical transceivers that have DOM enabled. |

# snmp-server enable traps trustsec

To enable CISCO-TRUSTSEC-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps trustsec** command in global configuration mode. To disable trustsec notifications, use the **no** form of this command.

```
snmp-server enable traps trustsec [{authz-file-error|cache-file-error|
keystore-file-error|keystore-sync-fail|random-number-fail|
src-entropy-fail}]

no snmp-server enable traps trustsec [{authz-file-error|cache-file-error
|keystore-file-error|keystore-sync-fail|random-number-fail|
src-entropy-fail}]
```

## Syntax Description

| | |
|---|---|
| **authz-file-error** | (Optional) Enables SNMP ctsAuthzCacheFileErrNotif notifications. |
| **cache-file-error** | (Optional) Enables SNMP ctsCacheFileAccessErrNotif notifications. |
| **keystore-file-error** | (Optional) Enables SNMP ctsSwKeystoreFileErrNotif notifications. |
| **keystore-sync-fail** | (Optional) Enables SNMP ctsSwKeystoreSyncFailNotif notifications. |
| **random-number-fail** | (Optional) Enables SNMP ctsSapRandomNumberFailNotif notifications. |
| **src-entropy-fail** | (Optional) Enables SNMP ctsSrcEntropyFailNotif notifications. |

## Command Default

SNMP notifications are disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)SY | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps trustsec** command enables both traps and inform requests.

This command enables or disables CISCO-TRUSTSEC-MIB notifications.

## Examples

This example shows how to enable SNMP ctsAuthzCacheFileErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec authz-file-error
```

This example shows how to enable SNMP ctsCacheFileAccessErrNotif notifications;

```
Device(config)# snmp-server enable traps trustsec cache-file-error
```

This example shows how to enable SNMP ctsSwKeystoreFileErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec keystore-file-error
```

This example shows how to enable SNMP ctsSwKeystoreSyncFailNotif notifications;

```
Device(config)# snmp-server enable traps trustsec keystore-sync-fail
```

This example shows how to enable SNMP ctsSapRandomNumberFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec random-number-fail
```

This example shows how to enable SNMP ctsSrcEntropyFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec src-entropy-fail
```

## Related Commands

| Command | Description |
|---|---|
| **test snmp trap trustsec** | Tests SNMP trustsec notification traps and informs. |

# snmp-server enable traps trustsec-interface

To enable CISCO-TRUSTSEC-INTERFACE-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps trustsec-interface** command in global configuration mode. To disable trustsec-interface notifications, use the **no** form of this command.

```
snmp-server enable traps trustsec-interface [{authc-fail| authz-fail|
sap-fail| supplicant-fail| unauthorized}]

no snmp-server enable traps trustsec-interface [{authc-fail| authz-fail|
sap-fail| supplicant-fail| unauthorized}]
```

## Syntax Description

| | |
|---|---|
| **authc-fail** | (Optional) Enables SNMP ctsiIfAuthenticationFailNotif notifications. |
| **authz-fail** | (Optional) Enables SNMP ctsiAuthorizationFailNotif notifications. |
| **sap-fail** | (Optional) Enables SNMP ctsiIfSapNegotiationFailNotif notifications. |
| **supplicant-fail** | (Optional) Enables SNMP ctsiIfAddSupplicantFailNotif notifications. |
| **unauthorized** | (Optional) Enables SNMP ctsiIfUnauthorizedNotifEnable notifications. |

## Command Default

SNMP notifications are disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)SY | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps trustsec-interface** command enables both traps and inform requests.

This command enables or disables CISCO-TRUSTSEC-INTERFACE-MIB notifications.

## Examples

This example shows how to enable SNMP ctsiIfAuthenticationFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-interface authc-fail
```

This example shows how to enable SNMP ctsiAuthorizationFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-interface authz-fail
```

This example shows how to enable SNMP ctsiIfSapNegotiationFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-interface sap-fail
```

This example shows how to enable SNMP ctsiIfAddSupplicantFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-interface supplicant-fail
```

This example shows how to enable SNMP ctsiIfUnauthorizedNotifEnable notifications:

```
Device(config)# snmp-server enable traps trustsec-interface unauthorized
```

## Related Commands

| Command | Description |
|---|---|
| **test snmp trap trustsec-interface** | Tests SNMP trustsec-interface notification traps and informs. |

# snmp-server enable traps trustsec-policy

To enable CISCO-TRUSTSEC-POLICY-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps trustsec-policy** command in global configuration mode. To disable trustsec-policy notifications, use the **no** form of this command.

```
snmp-server enable traps trustsec-policy [{authz-sgacl-fail|
peer-policy-updated}]

no snmp-server enable traps trustsec-policy [{authz-sgacl-fail|
peer-policy-updated}]
```

## Syntax Description

| | |
|---|---|
| **authz-sgacl-fail** | (Optional) Enables SNMP ctspAuthorizationSgaclFailNotif notifications. |
| **peer-policy-updated** | (Optional) Enables SNMP ctspPeerPolicyUpdatedNotif notifications. |

## Command Default

SNMP notifications are disabled.

## Command Modes

Global configuration(config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)SY | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps trustsec-policy** command enables both traps and inform requests.

This command enables or disables CISCO-TRUSTSEC-POLICY-MIB notifications.

## Examples

This example shows how to enable SNMP ctspAuthorizationSgaclFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-policy authz-sgacl-fail
```

This example shows how to enable SNMP ctspPeerPolicyUpdatedNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-policy peer-policy-updated
```

## Related Commands

| Command | Description |
|---|---|
| **test snmp trap trustsec-policy** | Tests SNMP trustsec-policy notification traps and informs. |

# snmp-server enable traps trustsec-server

To enable CISCO-TRUSTSEC-SERVER-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps trustsec-server** command in global configuration mode. To disable trustsec-server notifications, use the **no** form of this command.

```
snmp-server enable traps trustsec-server [{provision-secret|radius-server}]

no snmp-server enable traps trustsec-server [{provision-secret|
radius-server}]
```

## Syntax Description

| | |
|---|---|
| **provision-secret** | (Optional) Enables SNMP ctsvNoProvisionSecretNotif notifications. |
| **radius-server** | (Optional) Enables SNMP ctsvNoRadiusServerNotif notifications. |

## Command Default

SNMP notifications are disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)SY | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps trustsec-server** command enables both traps and inform requests.

This command enables or disables CISCO-TRUSTSEC-SERVER-MIB notifications.

## Examples

This example shows how to enable SNMP ctsvNoProvisionSecretNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-server provision-secret
```

This example shows how to enable SNMP ctsvNoRadiusServerNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-server radius-server
```

## Related Commands

| Command | Description |
|---|---|
| **test snmp trap trustsec-server** | Tests SNMP trustsec-server notification traps and informs. |

# snmp-server enable traps trustsec-sxp

To enable CISCO-TRUSTSEC-SXP-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps trustsec-sxp** command in global configuration mode. To disable trustsec-sxp notifications, use the **no** form of this command.

```
snmp-server enable traps trustsec-sxp [{binding-conflict|binding-err|
binding-expn-fail|conn-config-err|conn-down|conn-srcaddr-err|conn-up|
msg-parse-err|oper-nodeid-change}]

no snmp-server enable traps trustsec-sxp [{binding-conflict|binding-err|
binding-expn-fail|conn-config-err|conn-down|conn-srcaddr-err|conn-up|
msg-parse-err|oper-nodeid-change}]
```

## Syntax Description

| | |
|---|---|
| **binding-conflict** | (Optional) Enables SNMP ctsxSxpBindingConflictNotif notifications. |
| **binding-err** | (Optional) Enables SNMP ctsxSxpBindingErrNotif notifications. |
| **binding-expn-fail** | (Optional) Enables SNMP ctsxSxpBindingExpnFailNotif notifications. |
| **conn-config-err** | (Optional) Enables SNMP ctsxSxpConnConfigErrNotif notifications. |
| **conn-down** | (Optional) Enables SNMP ctsxSxpConnDownNotif notifications. |
| **conn-srcaddr-err** | (Optional) Enables SNMP ctsxSxpConnSourceAddrErrNotif notifications. |
| **conn-up** | (Optional) Enables SNMP ctsxSxpConnUpNotif notifications. |
| **msg-parse-err** | (Optional) Enables SNMP ctsxSxpMsgParseErrNotif notifications. |
| **oper-nodeid-change** | (Optional) Enables SNMP ctsxSxpOperNodeIdChangeNotif notifications. |

## Command Default

SNMP notifications are disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)SY | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps trustsec-sxp** command enables both traps and inform requests.

This command enables or disables CISCO-TRUSTSEC-SXP-MIB notifications.

## Examples

This example shows how to enable SNMP ctsxSxpBindingConflictNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp binding-conflict
```

This example shows how to enable SNMP ctsxSxpBindingErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp binding-err
```

This example shows how to enable SNMP ctsxSxpBindingExpnFailNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp binding-expn-fail
```

This example shows how to enable SNMP ctsxSxpConnConfigErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp conn-config-err
```

This example shows how to enable SNMP ctsxSxpConnDownNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp conn-down
```

This example shows how to enable SNMP ctsxSxpConnSourceAddrErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp conn-srcaddr-err
```

This example shows how to enable SNMP ctsxSxpConnUpNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp conn-up
```

This example shows how to enable SNMP ctsxSxpMsgParseErrNotif notifications:

```
Device(config)# snmp-server enable traps trustsec-sxp msg-parse-err
```

This example shows how to enable SNMP ctsxSxpOperNodeIdChangeNotif notifications:

```
Device(config)# snmp-server enable traps trustsec oper-nodeid-change
```

## Related Commands

| Command | Description |
|---|---|
| **test snmp trap trustsec-sxp** | Tests SNMP trustsec-sxp notification traps and informs. |

# snmp-server enable traps voice

To enable Simple Network Management Protocol (SNMP) voice notifications, use the **snmp-server enable traps voice**command in global configuration mode. To disable SNMP voice notifications, use the **no**form of this command.

**snmp-server enable traps voice** [**poor-qov**] [**fallback**]
**no snmp-server enable traps voice**

## Syntax Description

| | |
|---|---|
| **poor-qov** | (Optional) Enables poor-quality-of-voice SNMP notifications. |
| **fallback** | (Optional) Enables SNMP fallback voice notifications. |

## Command Default

If you enter this command without any of the optional keywords, both available notifications are enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |
| 12.3(14)T | The **fallback** keyword was added. |

## Usage Guidelines

SNMP notifications can be sent as traps (notifications) or inform requests. This command enables both traps and inform requests.

The **poor-qov** keyword enables or disables poor-quality-of-voice notifications. The poor quality-of-voice notification is defined in CISCO-VOICE-DIAL-CONTROL-MIB as follows:

enterprise 1.3.6.1.4.1.9.9.63.2

(1) cvdcPoorQoVNotification

The **fallback** keyword enables or disables public switched telephone network (PSTN) fallback notifications. The fallback notification is defined in CISCO-VOICE-DIAL-CONTROL-MIB as follows:

(1) cvVoIPCallHistoryConnectionId

(2) cvVoIPCallHistoryFallbackIcpif

(2) cvVoIPCallHistoryFallbackLoss

(3) cvVoIPCallHistoryFallbackDelay

(4) cvVoIPCallHistoryRemSigIPAddrT

(5) cvVoIPCallHistoryRemSigIPAddr

(6) cvVoIPCallHistoryRemMediaIPAddrT

(7) cvVoIPCallHistoryRemMediaIPAddr

(8) cCallHistoryCallOrigin

(9) cvCommonDcCallHistoryCoderTypeRate

For a complete description of these notifications and additional MIB functions, see the CISCO-VOICE-DIAL-CONTROL-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs .

The **snmp-server enable traps voice**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

## Examples

The following example shows how to enable the router to send poor-quality-of-voice informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps voice poor-qov
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to enable the router to send PSTN fallback messages at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps voice fallback
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps voice poor-qov** | Enables poor quality-of-voice SNMP notifications. |
| **snmp-server host** | Specifies the recipient of an SNMP notification operation. |
| **snmp-server trap-source** | Specifies the interface which an SNMP trap should originate from. |

# snmp-server enable traps voice poor-qov

The **snmp-server enable traps voice poor-qov** command is replaced by the **snmp-server enable traps voice** command. See the **snmp-server enable traps voice** command for more information.

# snmp-server enable traps vswitch dual-active

To enable the CISCO-VIRTUAL-SWITCH-MIB Simple Network Management Protocol (SNMP) notification (trap) when the dual-active state is detected, use the **snmp-server enable traps vswitch dual-active** command in global configuration mode. To disable the CISCO-VIRTUAL-SWITCH-MIB SNMP notification (trap), use the **no** form of this command.

**snmp-server enable traps vswitch dual-active**
**no snmp-server enable traps vswitch dual-active**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The CISCO-VIRTUAL-SWITCH-MIB SNMP notification is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)SY | This command was introduced. |

## Usage Guidelines

The virtual switch link (VSL) is a special link that carries control and data traffic between the two chassis of a virtual switching system (VSS). The VSL is implemented as an EtherChannel with up to eight links. The VSL gives control traffic higher priority than data traffic so that control messages are never discarded. The SNMP agent runs on the VSS active supervisor engine. CISCO-VIRTUAL-SWITCH-MIB is the MIB for virtual switch mode.

If the VSL fails, the VSS standby chassis cannot determine the state of the VSS active chassis. To ensure that switchover occurs without delay, the VSS standby chassis assumes that the VSS active chassis has failed and initiates switchover to take over the VSS active role.

If the original VSS active chassis is still operational, both chassis are now VSS active. This situation is called a dual-active scenario. A dual-active scenario can have adverse effects on network stability because both chassis use the same IP addresses, Secure Shell (SSH) keys, and Spanning Tree Protocol (STP) bridge ID. The VSS must detect a dual-active scenario and take recovery action.

The **snmp-server enable traps vswitch dual-active** command enables the dual-active state change notification. When the VSS changes state to dual-active, SNMP sends the cvsDualActiveDetectionNotif notification. To receive this message from SNMP, enable this command.

This command enables both trap and inform requests.

## Examples

The following example shows how to enable the cvsDualActiveDetectionNotif notification:

```
Device(config)# snmp-server enable traps vswitch dual-active
Device(config)# exit
Device# test snmp trap vswitch dual-active

cvsDualActiveDetectionNotif notification was sent.
Device# show running-config all

.
.
```

```
.
snmp-server enable traps vswitch dual-active
.
.
.
```

The following example shows how to disable the cvsDualActiveDetectionNotif notification:

```
Device(config)# no snmp-server enable traps vswitch dual-active
Device(config)# exit
Device# test snmp trap vswitch dual-active

cvsDualActiveDetectionNotif notification is disabled.
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config all** | Displays the contents of the current running configuration file for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class configuration file of SNMP trap in dual-active state. |
| **test snmp trap vswitch dual-active** | Tests the CISCO-VIRTUAL-SWITCH-MIB SNMP notification (trap and inform) in the dual-active state. |