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

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notification types that are available on your system, use the **snmp-server enable traps**command in global configuration mode. To disable all available SNMP notifications, use the **no**form of this command.

snmp-server enable traps [*notification-type*] **[vrrp]**

no snmp-server enable traps [*notification-type*] **[vrrp]**

Syntax Description

notification-type	(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled (if the **no** form is used). The notification type can be one of the following keywords: **alarms** --Enables alarm filtering to limit the number of syslog messages generated. Alarms are generated for the severity configured as well as for the higher severity values. • The *severity*argument is an integer or string value that identifies the severity of an alarm. Integer values are from 1 to 4. String values are critical, major, minor, and informational. The default is 4 (informational). Severity levels are defined as follows: • 1--Critical. The condition affects service. • 2--Major. Immediate action is needed. • 3--Minor. Minor warning conditions. • 4--Informational. No action is required. This is the default.
	• **auth-framework** [**sec-violation**]--Enables the SNMP CISCO-AUTH-FRAMEWORK-MIB traps. The optional **sec-violation** keyword enables the SNMP camSecurityViolationNotif notification. 1
	• **config** --Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is (1) ciscoConfigManEvent.

	• **dot1x** --Enables IEEE 802.1X traps. This notification type is defined in the CISCO PAE MIB. **Catalyst 6500 Series Switches** The following keywords are available under the **dot1x** keyword: • • **auth-fail-vlan** --Enables the SNMP cpaeAuthFailVlanNotif notification. • **no-auth-fail-vlan** --Enables the SNMP cpaeNoAuthFailVlanNotif notification. • **guest-vlan** --Enables the SNMP cpaeGuestVlanNotif notification. • **no-guest-vlan** --Enables the SNMP cpaeNoGuestVlanNotif notification.
	• **ds0-busyout** --Sends notification when the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This notification is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2), and the notification type is (1) cpmDS0BusyoutNotification. • **ds1-loopback** --Sends notification when the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as (2) cpmDS1LoopbackNotification. • **dsp** --Enables SNMP digital signal processing (DSP) traps. This notification type is defined in the CISCO-DSP-MGMT-MIB. • **dsp oper-state** --Sends a DSP notification made up of both a DSP ID that indicates which DSP is affected and an operational state that indicates whether the DSP has failed or recovered.
	• **l2tc** --Enable the SNMP Layer 2 tunnel configuration traps. This notification type is defined in CISCO-L2-TUNNEL-CONFIG-MIB.[1]

	• **entity** --Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as (1) entConfigChange.

	• **entity-diag** *type* -- Enables the SNMP CISCO-ENTITY-DIAG-MIB traps. The valid *type*values are as follows: 1
	  • **boot-up-fail**--(Optional) Enables the SNMP ceDiagBootUpFailedNotif traps. 1
	  • **hm-test-recover**--(Optional) Enables the SNMP ceDiagHMTestRecoverNotif traps. 1
	  • **hm-thresh-reached**--(Optional) Enables the SNMP ceDiagHMThresholdReachedNotif traps. 1
	  • **scheduled-fail**--(Optional) Enables the SNMP ceDiagScheduledJobFailedNotif traps. 1

	• **flowmon** --Controls flow monitoring notifications.
	• **hsrp** --Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is (1) cHsrpStateChange.
	• **ipmulticast** --Controls IP multicast notifications.

	• **license** --Enables licensing notifications as traps or informs. The notifications are grouped into categories that can be individually controlled by combining the keywords with the **license** keyword, or as a group by using the **license** keyword by itself. • **deploy**--Controls notifications generated as a result of install, clear, or revoke license events. • **error**--Controls notifications generated as a result of a problem with the license or with the usage of the license. • **imagelevel**--Controls notifications related to the image level of the license. • **usage**--Controls usage notifications related to the license.
	• **modem-health** --Controls modem-health notifications.
	• **module-auto-shutdown** [**status**]--Enables the SNMP CISCO-MODULE-AUTO-SHUTDOWN-MIB traps. The optional **status** keyword enables the SNMP Module Auto Shutdown status change traps. 1
	• **rsvp** --Controls Resource Reservation Protocol (RSVP) flow change notifications.
	• **sys-threshold** --(Optional) Enables the SNMP cltcTunnelSysDropThresholdExceeded notification. This notification type is an enhancement to the CISCO-L2-TUNNEL-CONFIG-MIB. 1
	• **tty** --Controls TCP connection notifications.

	• **xgcp** --Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-V1SMI.my, and the notification is enterprise 1.3.6.1.3.90.2 (1) xgcpUpDownNotification. **Note** For additional notification types, see the Related Commands table.
vrrp	(Optional) Specifies the Virtual Router Redundancy Protocol (VRRP).

[1] Supported on the Catalyst 6500 series switches.

Command Default No notifications controlled by this command are sent.

Command Modes Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(2)T	The **rsvp** notification type was added in Cisco IOS Release 12.0(2)T.
12.0(3)T	The **hsrp** notification type was added in Cisco IOS Release 12.0(3)T.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.3(11)T	The **vrrp**notification type was added in Cisco IOS Release 12.3(11)T.
12.4(4)T	Support for the **alarms**notification type and *severity* argument was added in Cisco IOS Release 12.4(4)T. Support for the **dsp** and **dsp oper-state**notification types was added in Cisco IOS Release 12.4(4)T.
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.

Release	Modification
12.4(11)T	The **dot1x** notification type was added in Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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.
12.4(20)T	The **license**notification type keyword was added.
12.2(33)SXH	The **l2tc** keyword was added and supported on the Catalyst 6500 series switch.
12.2(33)SXI	The following keywords were added and supported on the Catalyst 6500 series switch: • **auth-fail-vlan** • **entity-diag** • **guest-vlan** • **module-auto-shutdown** • **no-auth-fail-vlan** • **no-guest-vlan** • **sys-threshold**
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)S	This command was modified. The **flowmon** notification type was added in Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1.0SG	This command was modified. Licensing SNMP traps are enabled by default on Catalyst 4500 series switches.
Cisco IOS XE Release 3.2SE	This command was implemented in Cisco IOS XE Release 3.2SE.
Cisco IOS XE Release 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines

For additional notification types, see the Related Commands table for this command.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps** | **informs**] command.

To configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps**command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple

types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

Most notification types are disabled by default but some cannot be controlled with the **snmp-server enable traps** command.

The **snmp-server enable traps**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 notifications, you must configure at least one **snmp-server host** command.

Catalyst 6500 Series Switches

The following MIBs were enhanced or supported in Cisco IOS Release 12.2(33)SXI and later releases on the Catalyst 6500 series switch:

- CISCO-L2-TUNNEL-CONFIG-MIB-LLDP--Enhancement. The CISCO-L2-TUNNEL-CONFIG-MIB provides SNMP access to the Layer 2 tunneling-related configurations.
- CISCO-PAE-MIB--Enhancement for critical condition and includes traps when the port goes into the Guest Vlan or AuthFail VLAN.
- CISCO-MODULE-AUTO-SHUTDOWN-MIB--Supported. The CISCO-MODULE-AUTO-SHUTDOWN-MIB provides SNMP access to the Catalyst 6500 series switch Module Automatic Shutdown component.
- CISCO-AUTH-FRAMEWORK-MIB--Supported. The CISCO-AUTH-FRAMEWORK-MIB provides SNMP access to the Authentication Manager component.
- CISCO-ENTITY-DIAG-MIB--The CISCO-ENTITY-DIAG-MIB provides SNMP traps for generic online diagnostics (GOLD) notification enhancements.

Examples

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

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

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

The following example shows how to configure an alarm severity threshold of 3:

```
Router# snmp-server enable traps alarms 3
```

The following example shows how to enable the generation of a DSP operational state notification from from the command-line interface (CLI):

```
Router(config)# snmp-server enable traps dsp oper-state
```

The following example shows how to enable the generation of a DSP operational state notification from a network management device:

```
setany -v2c 1.4.198.75 test cdspEnableOperStateNotification.0 -i 1
cdspEnableOperStateNotification.0=true(1)
```

The following example shows how to send no traps to any host. The Border Gateway Protocol (BGP) traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps (which are not enabled in this example).

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

Router(config)# snmp-server host user1 public isdn
```

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

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

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

The following example shows how to send HSRP MIB traps to the host myhost.cisco.com using the community string public:

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

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

The following example shows that VRRP will be used as the protocol to enable the traps:

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

The following example shows how to send IEEE 802.1X MIB traps to the host “myhost.example.com” using the community string defined as public:

```
Router(config)# snmp-server enable traps dot1x
Router(config)# snmp-server host myhost.example.com traps public
```

Related Commands

Command	Description
snmp-server enable traps atm pvc	Enables ATM PVC SNMP notifications.
snmp-server enable traps atm pvc extension	Enables extended ATM PVC SNMP notifications.
snmp-server enable traps bgp	Enables BGP server state change SNMP notifications.
snmp-server enable traps calltracker	Enables Call Tracker callSetup and callTerminate SNMP notifications.
snmp-server enable traps envmon	Enables environmental monitor SNMP notifications.
snmp-server enable traps frame-relay	Enables Frame Relay DLCI link status change SNMP notifications.
snmp-server enable traps ipsec	Enables IPsec SNMP notifications.
snmp-server enable traps isakmp	Enables IPsec ISAKMP SNMP notifications.
snmp-server enable traps isdn	Enables ISDN SNMP notifications.
snmp-server enable traps memory	Enables memory pool and buffer pool SNMP notifications.
snmp-server enable traps mpls ldp	Enables MPLS LDP SNMP notifications.
snmp-server enable traps mpls traffic-eng	Enables MPLS TE tunnel state-change SNMP notifications.

Command	Description
snmp-server enable traps mpls vpn	Enables MPLS VPN specific SNMP notifications.
snmp-server enable traps repeater	Enables RFC 1516 hub notifications.
snmp-server enable traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server enable traps syslog	Enables the sending of system logging messages via SNMP.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the destination host (recipient) for the notifications.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and the corresponding IP address) from which an SNMP trap should originate.
snmp trap illegal-address	Issues an SNMP trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router.
vrrp shutdown	Disables a VRRP group.