snmp-server enable traps through snmp-server enable traps ospf cisco-specific retransmit

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.

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.
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.

Command	Description
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.

snmp-server enable traps (MPLS)

To enable a label switch router (LSR) to send Simple Network Management Protocol (SNMP) notifications or informs to an SNMP host, use the **snmp-server enable traps**command in global configuration mode. To disable notifications or informs, use the **no**form of this command.

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

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

Syntax Description

notification-type	

(Optional) Specifies the particular type of SNMP notification(s) to be enabled on the LSR. If a notification type is not specified, all SNMP notifications applicable to the LSR are enabled and sent to the SNMP host. Any one or all of the following keywords can be specified in any combination as the *notification-type* (family name) in the **snmp-server enable traps**command:

- **bgp** --Sends Border Gateway Protocol (BGP) state change notifications.
- **config** --Sends configuration notifications.
- **entity** --Sends entity MIB modification notifications.
- envmon--Sends Cisco enterprise-specific environmental monitor notifications whenever certain environmental thresholds are exceeded. *Notification-option* arguments (below) can be specified in combination with thiskeyword.
- **frame-relay** --Sends Frame Relay notifications.
- **hsrp** --Sends Hot Standby Routing Protocol (HSRP) notifications.
- isdn--Sends ISDN notifications. *Notification-option* arguments (see examples below) can be specified in combination with thiskeyword.
- repeater--Sends Ethernet repeater (hub) notifications. *Notification-option* arguments (see examples below) can be specified in combination with thiskeyword.
- **rsvp** --Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr** --Sends Service Assurance Agent/Response Time Reporter (RTR) notifications.
- **snmp** [**authentication**]--Sends RFC 1157 SNMP notifications. Using the **authentication** keyword produces the same effect as not using it. Both the **snmp-server enable traps snmp** and the **snmp-server enable traps snmp authentication**forms of this command globally enable the following SNMP notifications (or, if you are using the **no** form of the command, disables such notifications): **authenticationFailure**, **linkUp**, **linkDown**, and **warmstart**.

	• **syslog** --Sends system error message (syslog) notifications. You can specify the level of messages to be sent using the **logging history level** command.
notification-type (continued)	• **mpls ldp** --Sends notifications about status changes in LDP sessions. Note that this keyword is specified as *mpls ldp* . This syntax, which the CLI interprets as a two-word construct, has been implemented in this manner to maintain consistency with other MPLS commands. *Notification-option* arguments (below) can be specified in combination with thiskeyword. • **mpls traffic-eng** --Sends notifications about status changes in MPLS label distribution tunnels. This keyword is specified as *mpls traffic-eng* . This syntax, which the CLI interprets as a two-word construct, has been implemented in this manner to maintain consistency with other MPLS commands. *Notification-option* arguments (below) can be specified in combination with thiskeyword.

notification-option	

(Optional) Defines the particular options associated with the specified *notification-type* that are to be enabled on the LSR.

- **envmon** [**voltage** | **shutdown** | **supply** | **fan** | **temperature**]

When you specify the **envmon** keyword, you can enable any one or all of the following environmental notifications in any combination: **voltage**, **shutdown**, **supply**, **fan**, or **temperature**. If you do not specify an argument with the **envmon** keyword, all types of system environmental notifications are enabled on the LSR.

- **isdn** [**call-information** | **isdn u-interface**]

When you specify the **isdn** keyword , you can use either the **call-information** argument (to enable an SNMP ISDN call information option for the ISDN MIB subsystem) or the **isdn u-interface** argument (to enable an SNMP ISDN U interface option for the ISDN U Interfaces MIB subsystem), or both. If you do not specify an argument with the **isdn** keyword, both types of isdn notifications are enabled on the LSR.

- **repeater** [**health** | **reset**]

When you specify the **repeater** keyword, you can use either the **health** argument or the **reset** argument, or both (to enable the IETF Repeater Hub MIB [RFC 1516] notification). If you do not specify an argument with the **repeater** keyword, both types of notifications are enabled on the LSR.

- **mpls ldp** [**session-up** | **session-down** | **pv-limit** | **threshold**]

When you specify the **mpls ldp** keyword, you can use any one or all of the following arguments in any combination to indicate status changes in LDP sessions: **session-up**, session-down, pv-limit, or threshold. If you do not specify an argument with the **mpls ldp** keyword, all four types of LDP session notifications are enabled on the LSR.

- **mpls traffic-eng** [**up** | **down** | **reroute**]

When you specify the **mpls traffic-eng** keyword, you can use any one or all of the following arguments in any combination to enable the sending of notifications regarding status changes in MPLS label distribution

	tunnels: **up**, **down**, or **reroute**. If you do not specify an argument with the **mpls traffic-eng** keyword, all three types of tunnel notifications are enabled on the LSR.

Command Default

If you issue this command on an LSR without specifying any *notification-type* keywords, the default behavior of the LSR is to enable all notification types controlled by the command (some notification types cannot be controlled by means of this command).

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	The **snmp-server enable traps snmp authentication** form of this command was introduced to replace the **snmp-server trap-authentication** command.
12.0(17)ST	The **mpls traffic-eng**keyword was added to define a class or family of specific SNMP notifications for use with the *notification-type*and *notification-option*parameters of the **snmp-server enable traps**command.
12.0(21)ST	The **mpls ldp** keyword was added to define a class or family of specific SNMP notifications for use with the *notification-type*and *notification-option*parameters of the **snmp-server enable traps**command.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
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

To configure an LSR to send SNMP LDP notifications, you must issue at least one **snmp-server enable traps**command on the router.

To configure an LSR to send either notifications (traps) or informs to a designated network management station (NMS), you must issue the **snmp-server host**command on that device, usingthe keyword (**traps** or **informs**) that suits your purposes.

If you issue the **snmp-server enable traps**command without keywords, all SNMP notification types are enabled on the LSR. If you issue this command with specific keywords, only the notification types associated with those particular keywords are enabled on the LSR.

The **snmp-server enable traps**command is used in conjunction with the **snmp-server host**command. You use the latter command to specify the NMS host (or hosts) targeted as the recipient(s) of the SNMP notifications generated by SNMP-enabled LSRs in the network. To enable an LSR to send such notifications, you must issue at least one **snmp-server host** command on the LSR.

Examples

In the following example, the router is enabled to send all notifications to the host specified as myhost.cisco.com. The community string is defined as public.

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

In the following example, the router is enabled to send Frame Relay and environmental monitor notifications to the host specified as myhost.cisco.com. The community string is defined as public:

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

In the following example, notifications are not sent to any host. BGP notifications are enabled for all hosts, but the only notifications enabled to be sent to a host are ISDN notifications (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host host1 public isdn
```

In the following example, the router is enabled to send all inform requests to the host specified as myhost.cisco.com. The community string is defined as public.

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

In the following example, HSRP MIB notifications are sent to the host specified as myhost.cisco.com. The community string is defined as public.

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

Related Commands

Command	Description
snmp-server host	Specifies the intended recipient of an SNMP notification (that is, the designated NMS workstation in the network).

snmp-server enable traps aaa_server

To enable authentication, authorization, and accounting (AAA) server state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps aaa_server**command in global configuration mode. To disable AAA server state-change SNMP notifications, use the **no**form of this command.

snmp-server enable traps aaa_server

no snmp-server enable traps aaa_server

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
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.
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) AAA Server state change (casServerStateChange) notifications. ServerStateChange notifications, when enabled, will be sent when the server moves from an “up” to “dead” state or when a server moves from a “dead” to “up” state.

The Cisco AAA Server State is defined by the casState object in the Cisco AAA Server MIB. The possible values are as follows:

- up(1)--Server is responding to requests.
- dead(2)--Server failed to respond to requests.

A server is marked "dead" if it does not respond after maximum retransmissions. A server is marked "up" again either after a waiting period or if some response is received from it. The initial value of casState is "up(1)" at system startup. This will only transition to "dead(2)" if an attempt to communicate fails.

For a complete description of this notification and additional MIB functions, see the CISCO-AAA-SERVER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps aaa_sever**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 AAA server up/down informs to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
aaa session-mib disconnect	Allows a remote network management system to perform Set operations and disconnect users on the configured device using SNMP.
show caller	Displays caller information for async, dialer, and serial interfaces.
show radius statistics	Displays AAA server MIB statistics for AAA functions.
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 atm pvc

To enable the sending of ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps atm pvc**command in global configuration mode. To disable ATM PVC-specific SNMP notifications, use the **no**form of this command.

snmp-server enable traps atm pvc [**interval** *seconds*] [**fail-interval** *seconds*]

no snmp-server enable traps atm pvc [**interval** *seconds*] [**fail-interval** *seconds*]

Syntax Description

interval *seconds*	(Optional) Specifies a minimum period between successive traps. Generation of PVC traps is dampened by the notification interval to prevent trap storms. No traps are sent until the interval lapses. The *seconds* argument is an integer in the range from 1 to 3600. The default is 30.
fail-interval *seconds*	(Optional) Specifies a minimum period for storing the failed time stamp. The *seconds* argument is an integer in the range from 0 to 3600. The default is 0.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced for the platforms that support ATM PVC Management.
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.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Software Release 2.3 and implemented on the Cisco ASR 1000 series routers.

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. ATM notifications are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file, available from the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/

ATM PVC failure notifications are sent when a PVC on an ATM interface fails or leaves the UP operational state. Only one trap is generated per hardware interface, within the specified interval defined by the **interval** keyword (stored as the atmIntfPvcNotificationInterval in the MIB). If other PVCs on the same interface go DOWN during this interval, traps are generated and held until the fail interval has elapsed. When the interval has elapsed, the traps are sent if the PVCs are still DOWN.

No notifications are generated when a PVC returns to the UP state after having been in the DOWN state. If you need to detect the recovery of PVCs, you must use the SNMP management application to regularly poll your router.

The **snmp-server enable traps atm pvc**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.

Examples

The following example shows the enabling of ATM PVC traps on a router, so that if PVC 0/1 goes down, host 172.16.61.90 will receive the notifications:

```
!For ATM PVC Trap Support to work on your router, you must first have SNMP support and
!an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro

Router(config)# snmp-server host 172.16.61.90 public

Router(config)# ip routing

Router(config)# router igrp 109

Router(config-router)# network 172.16.0.0

!
!Enable ATM PVC Trap Support and OAM management:
Router(config)# snmp-server enable traps atm pvc interval 40 fail-interval 10

Router(config)# interface atm 1/0.1

Router(config-if)# pvc 0/1

Router(config-if-atm-vc)# oam-pvc manage
```

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.
snmp-server enable traps	Enables all available SNMP notifications on your system.
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 atm pvc extension

To enable the sending of extended ATM permanent virtual circuit (PVC) SNMP notifications and SNMP notifications for ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC), ATM OAM F5 alarm indication signals/remote defect indications (AIS/RDI), and loopback failures, use the **snmp-server enable traps atm pvc extension**command in global configuration mode. To disable these SNMP notifications, use the **no**form of this command.

snmp-server enable traps atm pvc extension {**up**| **down**| **oam failure** [**aisrdi**| **endCC**| **loopback**| **segmentCC**]}

no snmp-server enable traps atm pvc extension {**up**| **down**| **oam failure** [**aisrdi**| **endCC**| **loopback**| **segmentCC**]}

Syntax Description

up	Enables ATM PVC up traps. These notifications are generated when a PVC changes from the DOWN to the UP state.
down	Enables ATM PVC failure traps. These notifications are generated when a PVC changes from the UP to the DOWN state.
oam failure	Enables ATM PVC OAM failure traps. These notifications are generated when any type of OAM failure occurs on the PVC.
aisrdi	(Optional) Enables AIS/RDI OAM failure traps. These notifications are generated when AIS/RDI OAM failure occurs on the PVC.
endCC	(Optional) Enables end-to-end OAM CC failure traps. These notifications are generated when end-to-end CC failures occur on the PVC.
loopback	(Optional) Enables OAM failure loopback traps. These notifications are generated when OAM loopback failure occurs on the PVC.
segmentCC	(Optional) Enables segment OAM CC failure traps. These notifications are generated when segment CC failures occur on the PVC.

Command Default

SNMP notifications are disabled. The interval between successive traps is 30 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced for those platforms that support ATM PVC management.
12.2(13)T	This command was modified to configure SNMP notification support for ATM OAM F5 CC and ATM OAM F5 AIS/RDI failures.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Software Release 2.3 and implemented on the Cisco ASR 1000 series routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

For PVCs that are not part of a range, extended ATM PVC traps include virtual path identifier/virtual channel identifier (VPI/ VCI) information, the number of state transitions a PVC goes through in an interval, and the timestamp for the start and end of the transitions. For PVCs that are part of a range, extended ATM PVC traps include the first and last VPI/VCI of the range and the timestamp for the first failure and the last failure within the same range.

Extended ATM PVC and ATM OAM F5 CC traps cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before extended ATM PVC traps can be configured.

The extended ATM PVC failure trap (which is enabled by the **snmp-server enable traps atm pvc extension down** command) is the same trap as the legacy ATM PVC failure trap (which is enabled by the **snmp-server enable traps atm pvc** command), but with the following differences:

- The extended ATM PVC failure trap contains information in the form of VPI/VCI ranges.
- The extended ATM PVC failure trap contains timestamps for when PVCs go down.
- The legacy ATM PVC failure trap contains only one VPI/VCI per trap.

Note You must configure the **snmp-server enable traps atm pvc extension mibversion 2**command before you can enable the ATM OAM F5 AIS/RDI failure traps, the end-to-end ATM OAM F5 CC failure traps, the OAM failure loopback traps, and the segment ATM OAM F5 CC failure traps. This command enables the MIB that supports these traps.

OAM management must be enabled on the PVC before you can use ATM PVC traps. To generate F5 loopback failure traps, enable OAM management using the **oam-pvc manage** command. To generate segment F5 CC failure traps, enable segment OAM CC management by using the **oam-pvc manage cc segment** command. To generate end-to-end F5 CC failure traps, enable end-to-end OAM CC management by using the **oam-pvc manage cc end** command. To generate OAM F5 AIS/RDI failure traps, enable any of the three types of OAM management listed above.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The interval between successive traps is 30 seconds.

The extended ATM PVC notifications for MIB version 1 are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file.The extended ATM PVC notifications for MIB version 2 are defined in the CISCO-ATM-PVCTRAP-EXTN-MIB.my file. Both of these MIB files are available from the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/ .

ATM PVC traps are generated at the end of the notification interval. It is possible to generate all three types of ATM PVC traps (the ATM PVC failure trap, ATM PVC up trap, and ATM PVC OAM failure trap) at the end of the same notification interval; however, only one type of trap will be generated for each PVC.

The **snmp-server enable traps atm pvc extension**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.

When the ATM OAM F5 loopback, AIS/RDI, or CC failure trap is enabled, the PVC remains in the UP state when an OAM loopback, AIS/RDI, or CC failure is detected, so that the flow of data will still be possible. If one of these traps is not enabled, the PVC will be placed in the DOWN state when an OAM loopback, AIS/RDI, or CC failure is detected.

Examples

Examples

The following example shows all three of the extended ATM PVC traps enabled on a router. If PVC 0/1 leaves the UP state, leaves the DOWN state, or has an OAM loopback failure, host 172.16.61.90 will receive the SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension down
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

Examples

The following example shows output for extended ATM PVC failure trap for PVCs 1/100, 1/102, and 1/103. Note that only one trap is generated for all the PVCs associated with the same interface or subinterface (in contrast to the legacy ATM PVC failure trap, which generates a separate trap for each PVC). The VPI/VCI information and timing information are located in the objects associated with the trap.

```
00:23:56:SNMP:Queuing packet to 10.1.1.1
00:23:56:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 143636
snmpTrapOID.0 = atmIntfPvcFailuresTrap
ifEntry.1.19 = 19
atmIntfPvcFailures.2 = 7
atmIntfCurrentlyFailingPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 140643
atmPVclRangeStatusChangeEnd.19.1.2 = 140698
atmPVclStatusTransition.19.1.100 = 1
```

```
atmPVclStatusChangeStart.19.1.100 = 140636
atmPVclStatusChangeEnd.19.1.100 = 140636
00:23:56:SNMP:Packet sent via UDP to 10.1.1.1
```

Examples

The following example shows output for the extended ATM PVC up trap for PVCs 1/100, 1/102, and 1/103:

```
00:31:29:SNMP:Queuing packet to 10.1.1.1
00:31:29:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 188990
snmpTrapOID.0 = atmIntfPvcUpTrap
ifEntry.1.19 = 19
atmIntfCurrentlyDownToUpPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 186005
atmPVclRangeStatusChangeEnd.19.1.2 = 186053
atmPVclStatusTransition.19.1.100 = 1
atmPVclStatusChangeStart.19.1.100 = 185990
atmPVclStatusChangeEnd.19.1.100 = 185990
00:31:30:SNMP:Packet sent via UDP to 10.1.1.1
```

Examples

In the following example, the ATM OAM CC notifications and an extended ATM PVC notification are enabled. If connectivity failures are detected on PVC 0/1, host 172.16.61.90 will receive the SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension mibversion 2
Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi
Router(config)# snmp-server enable traps atm pvc extension oam failure endcc
Router(config)# snmp-server enable traps atm pvc extension oam failure segmentcc
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# interface atm 0
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage cc end
```

Related Commands

Command	Description
oam-pvc manage	Enables end-to-end F5 OAM loopback cell generation and OAM management.
oam-pvc manage cc	Configures ATM OAM F5 CC management.
show atm pvc	Displays all ATM PVCs and traffic information.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of legacy ATM PVC failure traps.

Command	Description
snmp-server enable traps atm pvc extension mibversion	Specifies the MIB that supports extended ATM PVC SNMP notifications or the MIB that supports SNMP notifications for ATM OAM F5 CC, F5 AIS/RDI, and F5 loopback failures.
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 atm pvc extension mibversion

To specify the MIB that supports extended ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications or the MIB that supports SNMP notifications for ATM Operation, Administration, and Maintenance (OAM) F5 continuity check (CC) management, ATM OAM F5 AIS/RDI management, and F5 loopback failure management, use the **snmp-server enable traps atm pvc extension mibversion**command in global configuration mode. To remove the MIB specification, use the **no**form of this command.

snmp-server enable traps atm pvc extension mibversion {**1**| **2**}

no snmp-server enable traps atm pvc extension mibversion {**1**| **2**}

Syntax Description

1	Specifies the MIB that supports the extended ATM permanent virtual circuit (PVC) SNMP notifications. This is the default.
2	Specifies the MIB that supports ATM OAM F5 CC and ATM OAM F5 AIS/RDI SNMP notifications, in addition to the notifications supported by MIB version 1.

Command Default

SNMP notifications **are disabled.**

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

MIB version 1 specifies the MIB that supports legacy extended ATM PVC traps and is defined in the file CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN.my. MIB version 1 is implemented by default. Use the **snmp-server enable traps atm pvc extension mibversion 1**command or the **no snmp-server enable traps atm pvc** extens**ion mibversion 2**command to reenable this MIB if it was previously disabled with the **snmp-server enable traps atm pvc extension mibversion 2**command.

Use the **snmp-server enable traps atm pvc** extens**ion mibversion 2**command to specify the MIB that supports ATM OAM F5 CC and ATM OAM AID/RDI failure notifications. This MIB is defined in the file CISCO-ATM-PVCTRAP-EXTN-MIB.my.

To enable the SNMP notifications that support ATM OAM F5 continuity checking, use the **snmp-server enable traps atm pvc** extens**ion**command in global configuration mode. These SNMP notifications are defined in the file CISCO-ATM-PVCTRAP-EXTN-MIB.my, available from the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/

OAM management and support for OAM F5 continuity checking must be enabled on the PVC by using the oam-pvc manage cc command before you can use the ATM OAM continuity check SNMP notifications.

Examples

In the following example, the MIB that supports the SNMP notifications for ATM OAM continuity checking is implemented, and the ATM OAM continuity checking notifications are enabled. Support for end-to-end OAM F5 continuity checking is enabled on PVC 0/1:

```
Router(config)# snmp-server enable traps atm pvc extension mibversion 2
Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi
Router(config)# snmp-server enable traps atm pvc extension oam failure endcc
Router(config)# snmp-server enable traps atm pvc extension oam failure segmentcc
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# interface atm 0
Router(config-if)# pvc 0/40
Router(config-if-atm-vc)# oam-pvc manage cc end
```

Related Commands

Command	Description
debug atm oam cc	Displays ATM OAM F5 CC management activity.
oam-pvc manage cc	Configures ATM OAM F5 CC management.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of legacy ATM PVC DOWN traps.
snmp-server enable traps atm pvc extension	Enables the sending of extended ATM PVC SNMP notifications and SNMP notifications for ATM OAM F5 CC, ATM OAM F5 AIS/RDI, and loopback failures.

snmp-server enable traps atm subif

To enable Simple Network Management Protocol (SNMP) traps (notifications) for ATM subinterfaces, use the **snmp-server enable traps atm subif** command in global configuration mode. To disable ATM subinterface-specific SNMP traps, use the **no** form of this command.

snmp-server enable traps atm subif [**count max-traps**] [**interval** *seconds*]

no snmp-server enable traps atm subif [**count max-traps**] [**interval** *seconds*]

Syntax Description

count	(Optional) Specifies the maximum number of traps that will be sent in the specified interval.
max-traps	(Optional) Number of traps. The range is from 1 to 1000. The default is 10.
interval	(Optional) Specifies the minimum period between successive traps.
seconds	(Optional) Interval, in seconds. The range is from 0 to 3600. The default is 10.

Command Default

ATM subinterface SNMP traps are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE6	This command was modified. To enable the sending of ATM subinterface SNMP notifications, after this command is configured in global configuration mode, the **snmp trap link-status** command must be configured on each ATM subinterface.
15.1(3)S3	This command was integrated in Cisco IOS Release 15.1(3)S3.

Usage Guidelines

The **snmp-server trap link ietf** command must be configured in order to use the **snmp-server enable traps atm subif** command. The **snmp-server trap link ietf** command is used to configure a router to use the RFC 2233 IETF standards-based implementation of linkUp/linkDown traps. The default Cisco object definitions do not generate linkUp/linkDown traps correctly for subinterfaces.

In order to enable SNMP notifications for ATM subinterfaces, after the **snmp-server enable traps atm subif** command has been configured in global configuration mode, the **snmp trap link-status** command must be configured on each ATM subinterface for which you want to enable SNMP notifications.

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

ATM subinterface traps are sent to the network management system (NMS) when a subinterface enters or leaves the down state.

To prevent trap storms, the **count** and **interval** keywords can be configured to limit the number of traps and the frequency at which they are sent. Configuring an interval of 0 seconds causes all ATM subinterface traps to be sent.

You can disable ATM subinterface traps by using the **no snmp-server enable traps atm subif** command. When traps are disabled, you can use the SNMP management application to poll your router for subinterface status information.

The **snmp-server enable traps atm subif** 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.

By default (when the **snmp-server enable traps atm subif** command is not configured), the ifLinkUpDownTrapEnable object returns disabled(2), and no traps are generated for the subinterfaces.

When the **snmp-server enable traps atm subif** command is configured, the ifLinkUpDownTrapEnable object is set to enabled(1) for all the ATM AAL5 layers of the subinterfaces. To verify that the traps are generated (with the **debug snmp packets** command enabled), enter the **shutdown** or **no shutdown** commands to display the traps.

Configuring the **snmp trap link-status** command on a subinterface generates the traps and sets the ifLinkUpDownTrapEnable object to enabled(1). If the **snmp trap link-status** command is not configured on the subinterface, the ifLinkUpDownTrapEnable object is set to disabled(2) for that subinterface, and the **shutdown** or **no shutdown** commands no longer generate traps for that subinterface.

Examples

The following example shows how to enable ATM subinterface traps on a device. If an ATM subinterface on this device changes state, host 172.16.61.90 will receive the notifications.

```
! For ATM subinterface trap to work on your router, you must first have SNMP support and
! an IP routing protocol configured on your router.
Device(config)# snmp-server community public ro

Device(config)# snmp-server host 172.16.61.90 public
Device(config)# snmp-server trap link ietf
Device(config)# snmp-server enable traps snmp
Device(config)# ip routing

Device(config)# router igrp 109

Device(config-router)# network 172.16.0.0

! Enable ATM subinterface trap support.
Device(config)# snmp-server enable traps atm subif count 5 interval 60
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP traps on your system.
snmp-server enable traps atm pvc	Enables the sending of ATM PVC SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap link ietf	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp trap link-status	Enables SNMP link trap generation.

snmp-server enable traps bfd

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

snmp-server enable traps bfd [session-down] [session-up]

no snmp-server enable traps bfd [session-down] [session-up]

Syntax Description

session-down	(Optional) Enables or disables BFD session down notifications (bfdSessDown).
session-up	(Optional) Enables or disables BFD session up notifications (bfdSessUp).

Command Default

The sending of SNMP notifications is disabled. If you do not specify an optional keyword, all types of BFD notifications are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

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

If the **session-down** keyword is used with the **snmp-server enable traps bfd** command, a session-down message is generated when a BFD session between the router and its adjacent peer is terminated.

If the **session-up** keyword is used with the **snmp-server enable traps bfd** command, a message is generated when the router establishes a BFD session.

Examples

In the following example, BFD-specific informs are enabled and will be sent to the host myhost.cisco.com through use of community string defined as public:

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

Related Commands

Command	Description
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 recipient (host) of the notifications.

snmp-server enable traps bgp

To enable Border Gateway Protocol (BGP) support for Simple Network Management Protocol (SNMP) operations on a router, use the **snmp-server enable traps bgp** command in global configuration mode. To disable BGP support for SNMP operations, use the **no** form of this command.

snmp-server enable traps bgp [cbgp2] [**state-changes [all] [backward-trans] [limited]**| **threshold prefix**]

no snmp-server enable traps bgp [cbgp2][**state-changes [all] [backward-trans] [limited]**| **threshold prefix**]

Syntax Description

cbgp2	(Optional) Enables generation of the CISCO-BGP-MIBv8.1 traps.
state-changes	(Optional) Enables traps for finite state machine (FSM) state changes.
all	(Optional) Enables Cisco specific traps for all FSM state changes
backward-trans	(Optional) Enables Cisco specific traps for backward transition events.
limited	(Optional) Enables traps for standard backward transition and established events.
threshold prefix	(Optional) Enables Cisco-specific trap for prefix threshold events.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.
12.0(26)S	This command was modified. The **state-changes**, **all**, **backward-trans**, **limited**, and **threshold prefix** keywords were added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Release	Modification
12.2(27)SBC	This command was implemented on the Cisco 7304.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the following platforms: Cisco 7301, Cisco 7200 series, and Cisco 10000 series.
15.2(3)T	This command was modified. The **cbgp2** keyword was added.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests and this command enables both notification types. If this command is entered with no keywords specified, support for all configurable options is enabled.

Use this command to enable or disable BGP server state change notifications for the BGP4-MIB (enterprise 1.3.6.1.2.1.15.7). The notifications types are:

- bgpEstablished
- bgpBackwardsTransition

For a complete description of BGP notifications and additional MIB functions, see the BGP4-MIB.my file, available through the Cisco FTP site at ftp://ftp.cisco.com/pub/mibs/v2/.

Note You may notice incorrect BGP trap object ID (OID) output when using the SNMP version 1 BGP4-MIB that is available for download at ftp://ftp.cisco.com/pub/mibs/v1/BGP4-MIB-V1SMI.my. When a router sends out BGP traps (notifications) about state changes on an SNMP version 1 monitored BGP peer, the enterprise OID is incorrectly displayed as .1.3.6.1.2.1.15 (bgp) instead of .1.3.6.1.2.1.15.7 (bgpTraps). This problem occurs because the BGP4-MIB does not follow RFC 1908 rules for version 1 and version 2 trap compliance. The problem is not due to an error in Cisco IOS software. This MIB is controlled by IANA under the guidance of the IETF, and work is currently in progress by the IETF to replace this MIB with a new version that represents the current state of the BGP protocol. In the meantime, we recommend that you use the SNMP version 2 BGP4-MIB or the CISCO-BGP4-MIB to avoid an incorrect trap OID.

The **snmp-server enable traps bgp** command also can be enabled to control BGP server state change notifications for the CISCO-BGP4-MIB. This MIB contains support the following SNMP operations:

- Notification for all BGP FSM transition changes.
- Notifications to query for total number of routes received by a BGP peer.
- Notifications for the maximum prefix-limit threshold on a BGP peer.
- GET operations for VPNv4 unicast routes.

For a complete description of BGP notifications and additional MIB functions, see the CISCO-BGP4-MIB.my file, available through the Cisco FTP site at ftp://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps bgp** 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.

You may enable or disable the **snmp-server enable traps bgp** command and the **snmp-server enable traps bgp cbgp2** command independently of each other. If both commands are enabled, both traps are generated. If only one of the two commands is enabled, only that version of traps is generated.

Examples

The following example shows how to enable the router to send BGP state change informs to the host at the address myhost.cisco.com using the community string defined as public:

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

The following example shows how to enable generation of the CISCO-BGP-MIBv8.1 traps:

```
Router(config)# snmp-server enable traps bgp cbgp2
```

Related Commands

Command	Description
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 bulkstat

To enable the sending of Simple Network Management Protocol (SNMP) bulk statistics collection and transfer SNMP notifications, use the **snmp-server enable traps bulkstat**command in global configuration mode. To disable bulk statistics SNMP notifications, use the **no**form of this command.

snmp-server enable traps bulkstat [collection] [transfer]

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

Syntax Description

collection	(Optional) Controls bulk statistics collection notifications, which are sent when data collection cannot be carried out successfully. (Defined as cdcVFileCollectionError in the CISCO-DATA-COLLECTION-MIB.)
transfer	(Optional) Controls bulk statistics transfer notifications, which are sent when a transfer attempt is successful or when a transfer attempt fails. (Defined as cdcFileXferComplete in the CISCO-DATA-COLLECTION-MIB. The varbind cdcFilXferStatus object in the trap indicates if the transfer is successful or not.)

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. The **snmp-server enable traps bulkstat**command enables both traps and inform requests for the specified notification types. Use this command with the **snmp-server host** [**bulkstat**] command.

The optional **collection** keyword controls bulk statistics collection notifications that are sent when data collection cannot be carried out successfully. One possible reason for this condition is insufficient memory on the device.

If the optional keywords are not used, all bulk statistics notification types are enabled (or disabled, if the **no** form of the command is used).

Examples

In the following example, bulk statistics collection and transfer notifications are configured to be sent to the host myhost.cisco.com using the community string public:

```
Device> enable
Device(config)# snmp-server enable traps bulkstat
Device(config)# snmp-server host myhost.cisco.com traps version 2c public bulkstat
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.
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 c6kxbar

To enable CISCO-CAT6K-CROSSBAR-MIB Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps c6kxbar**command in global configuration mode. To disable cc6kxbar notifications, use the **no** form of this command.

snmp-server enable traps c6kxbar [**flowctrl-bus**| **intbus-crccvrd**| **intbus-crcexcd**| **swbus**| **tm-channel**| **tm-swbus**]

no snmp-server enable traps c6kxbar [**flowctrl-bus**| **intbus-crcexcd**| **intbus-crccvrd**| **swbus**| **tm-channel**| **tm-swbus**]

Syntax Description

flowctrl-bus	(Optional) Enables SNMP cc6kxbarFlowCtrlBusThrExcdNotif notifications.
intbus-crcvrd	(Optional) Enables SNMP cc6kxbarIntBusCRCErrRcvrdNotif notifications.
intbus-crcexcd	(Optional) Enables SNMP cc6kxbarIntBusCRCErrExcdNotif notifications.
swbus	(Optional) Enables SNMP cc6kxbarSwBusStatusChangeNotif notifications.
tm-channel	(Optional) Enables cc6kxbarTMChUtilAboveNotif and cc6kxbarTMChUtilBelowNotif notifications.
tm-swbus	(Optional) Enables cc6kxbarTMSwBusUtilAboveNotif and cc6kxbarTMSwBusUtilBelowNotif notifications.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(18)SXF	Added **intbus-crcexce** and **intbus-crcrcvrd** keywords.
12.2(33)SXH	Added **flowctrl-bus** keyword for Supervisor Engine 32 only.

Release	Modification
12.2(33)SXI4	Added **tm-channel** for Supervisor Engine 720 only and **tm-swbus** keywords.

Usage Guidelines

The **flowctrl-bus** keyword is supported on the Supervisor Engine 32 only.

The **tm-channel** keyword is not supported on the Supervisor Engine 32.

Examples

This example shows how to enable SNMP cc6kxbarFlowCtrlBusThrExcdNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar flowctrl-bus
Router(config)#
```

This example shows how to enable SNMP cc6kxbarIntBusCRCErrExcdNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar intbus-crcexcd
Router(config)#
```

This example shows how to enable SNMP cc6kxbarIntBusCRCErrRcvrdNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar intbus-crcvrd
Router(config)#
```

This example shows how to enable SNMP cc6kxbarSwBusStatusChangeNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar swbus
Router(config)#
```

This example shows how to enable SNMP cc6kxbarTMChUtilAboveNotif and cc6kxbarTMChUtilBelowNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar tm-channel
Router(config)#
```

This example shows how to enable SNMP cc6kxbarTMSwBusUtilAboveNotif and cc6kxbarTMSwBusUtilBelowNotif notifications:

```
Router(config)# snmp-server enable traps c6kxbar tm-swbus
Router(config)#
```

Related Commands

Command	Description
test snmp trap c6kxbar	Tests the SNMP c6kxbar notification traps.

snmp-server enable traps calltracker

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

snmp-server enable traps calltracker

no snmp-server enable traps calltracker

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS580 access servers.
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) Call Tracker CallSetup and CallTerminate notifications. CallSetup notifications are generated at the start of each call, when an entry is created in the active table (cctActiveTable), and CallTerminate notifications are generated at the end of each call, when an entry is created in the history table (cctHistoryTable).

For a complete description of these notifications and additional MIB functions, refer to the CISCO-CALL-TRACKER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps calltracker**command is used in conjunction with the **snmp-server host**global configurationcommand. 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 call-start and call-stop informs to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
calltracker call-record	Enables call record SYSLOG generation for the purpose of debugging, monitoring, or externally saving detailed call record information.
calltracker enable	Enables the Call Tracker feature on an access server.
isdn snmp busyout b-channel	Enables PRI B channels to be busied out via SNMP.
show call calltracker	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.
show modem calltracker	Displays all of the information stored within the Call Tracker Active or History Database for the latest call assigned to specified modem.
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 cnpd

To enable Cisco Network-Based Application Recognition (NBAR) Protocol Discovery (CNPD) MIB notifications, use the **snmp-server enable traps cnpd** command in global configuration mode. To disable CNPD MIB notifications, use the **no** form of this command.

snmp-server enable traps cnpd

no snmp-server enable traps cnpd

Syntax Description

This command has no arguments or keywords.

Command Default

CNPD MIB notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

CNPD notifications are used with the CNPD MIB to provide information related to protocol discovery. The **snmp-server enable traps cnpd** command enables these notifications. It also enables SNMP notifications as either traps or inform requests.

The **snmp-server enable traps cnpd** command is used in conjunction with the **snmp-server host** command, which specifies the host or hosts that will receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command. The default action is to send notifications to the default port, but you can specify a port by configuring the **udp-port** option of the **snmp-server host**command.

Examples

The following example shows how to enable CNPD notifications:

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

Related Commands

Command	Description
snmp-server host	Specifies the recipient of SNMP notifications.

snmp-server enable traps cpu

To enable a device to send CPU thresholding violation notifications, use the **snmp-server enable traps cpu**command in global configuration mode. To stop a device from sending CPU thresholding notifications, use the **no**form of this command.

snmp-server enable traps cpu threshold

no snmp-server enable traps cpu

Syntax Description

threshold	Enables notifications of CPU threshold violations.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests and controls CPU thresholding notifications, as defined in the Process MIB (CISCO-PROCESS-MIB).

This command enables the following notifications:

- cpmCPURisingThreshold--Indicates that CPU usage has risen and remains above the configured CPU threshold settings.
- cpmCPUFallingThreshold--Indicates that CPU usage has fallen and remains below the configured CPU threshold settings.

For a complete description of these notification types, and for information about the other MIB functions, see the CISCO-PROCESS-MIB.my file available from Cisco.com at http://www.cisco.com/go/mibs .

The **snmp-server enable traps cpu**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 CPU threshold related informs to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps dhcp

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

snmp-server enable traps dhcp [duplicate] [interface] [pool] [subnet] [time]

no snmp-server enable traps dhcp [duplicate] [interface] [pool] [subnet] [time]

Syntax Description

duplicate	(Optional) Sends notification about duplicate IP addresses.
interface	(Optional) Sends notification that a per interface lease limit is exceeded.
pool	(Optional) Sends notification when address utilization for an address pool has risen above or fallen below a configurable threshold.
subnet	(Optional) Sends notification when address utilization for a subnet has risen above or fallen below a configurable threshold.
time	(Optional) Sends notification that the DHCP server has started or stopped.

Command Default

DHCP trap notifications are not sent.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

If you do not specify any of the optional keywords, all DHCP trap notifications are enabled.

Examples

The following example shows how to send SNMP trap notifications to the SNMP manager when the secondary subnet utilization falls below or exceeds the configured threshold:

```
Router(config)# ip dhcp pool pool2
```

```
Router(dhcp-config)# utilization mark high 80 log
Router(dhcp-config)# utilization mark low 70 log
Router(dhcp-config)# network 192.0.2.0 255.255.255.0
Router(dhcp-config)# network 192.0.4.0 255.255.255.252 secondary
Router(config-dhcp-subnet-secondary)# override utilization high 40
Router(config-dhcp-subnet-secondary)# override utilization low 30
!
Router(config)# snmp-server enable traps dhcp subnet
```

In the following example, all DHCP trap notifications will be sent to the SNMP manager in response to DHCP server events:

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

snmp-server enable traps dhcp-snooping bindings

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

snmp-server enable traps dhcp-snooping bindings

no snmp-server enable traps dhcp-snooping bindings

Syntax Description

This command has no keywords or arguments.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXI4	This command was introduced on the Supervisor Engine 720.

Usage Guidelines

This command controls (enables or disables) SNMP notifications for DHCP-snooping binding activity.

Examples

This example shows how to enable DHCP-snooping bindings SNMP notifications:

```
Router(config)# snmp-server enable traps dhcp-snooping bindings
Router(config)#
```

snmp-server enable traps director

Note Effective with Cisco IOS Release 12.4(24)T, the **snmp-server enable traps director**command is not available in Cisco IOS software.

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

snmp-server enable traps director [**server-up**| **server-down**]

no snmp-server enable traps director [**server-up**| **server-down**]

Syntax Description

server-up	(Optional) Enables the DistributedDirector notification that the server has changed to the “up” state.
server-down	(Optional) Enables the DistributedDirector notification that the server has changed to the “down” state.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	This command was removed.

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) DistributedDirector status notifications for systems. If none of the optional keywords is specified, all available environmental notifications are enabled.

Examples

In the following example, both ciscoDistDirEventServerUp and ciscoDistDirEventServerDown notifications are enabled:

```
Router(config)# snmp-server enable traps director
Router# show running-config
ip host myhost 172.20.2.10 172.20.2.20 172.20.2.30
.
.
.
ip director host myhost
ip dns primary myhost soa myhost myhost@com
ip director host myhost priority boomerang 1
no ip director drp synchronized
snmp-server enable traps director server-up server-down
```

Related Commands

Command	Description
snmp-server enable traps	Enables the router to send SNMP traps.
snmp-server host	Specifies the recipient of an SNMP notification.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
snmp trap link-status	Enables SNMP trap notifications to be generated when a specific port is brought up or down.

snmp-server enable traps dlsw

To enable the sending of Data Link Switch (DLSw) circuit and peer connection Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps dlsw** command in global configuration mode. To disable DLSw notifications, use the **no** form of this command.

snmp-server enable traps dlsw [**circuit**| **tconn**]

no snmp-server enable traps dlsw [**circuit**| **tconn**]

Syntax Description

circuit	(Optional) Enables DLSw circuit traps: • (5) ciscoDlswTrapCircuitUp • (6) ciscoDlswTrapCircuitDown
tconn	(Optional) Enables DLSw peer transport connection traps: • (1) ciscoDlswTrapTConnPartnerReject • (2) ciscoDlswTrapTConnProtViolation • (3) ciscoDlswTrapTConnUp • (4) ciscoDlswTrapTConnDown

Command Default

SNMP notifications are disabled.

If the optional keywords are not used, all DLSw notification types are enabled (or disabled, if the **no** form of the command is used).

Command Modes

Global configuration

Command History

Release	Modification
12.1	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. Use this command in conjunction with the **snmp-server host** command.

This command controls (enables or disables) SNMP notifications for Data Link Switch (DLSw) circuit and connection activity. DLSw objects are defined in the Cisco DLSw MIB module (CISCO-DLSW-MIB.my) and the DLSw+ (Cisco Specific Features) MIB module (CISCO-DLSW-EXT-MIB.my), available through Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

In the following example the device is configured to send DLSw circuit state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps dlsw circuit
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 eigrp

To enable support for Enhanced Interior Gateway Routing Protocol (EIGRP) notifications on a Cisco router, use the snmp-server enable traps eigrp command in global configuration mode. To disable EIGRP notification support, use the **no** form of this command.

snmp-server enable traps eigrp

no snmp-server enable traps eigrp

Syntax Description

This command has no keywords or arguments.

Command Default

EIGRP notification support is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

The snmp-server enable traps eigrp command is used to enable notifications (traps) for stuck-in-active (SIA) and neighbor authentication failure events. Support for trap events is not activated until a trap destination is configured with the snmp-server host command and until a community string is defined with the snmp-server community command.

Examples

In the following example, an SNMP server host is specified, a community string is configured, and support for EIGRP notifications is enabled:

```
Router(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp
Router(config)# snmp-server community EIGRP1NET1A
Router(config)# snmp-server enable traps eigrp
```

Related Commands

Command	Description
snmp-server community	Configures a community access string to permit SNMP access to the local router by the remote SNMP software client.
snmp-server host	Specifies the destination host or address for SNMP notifications.

snmp-server enable traps envmon

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

snmp-server enable traps envmon [shutdown] [voltage] [temperature] [fan] [supply]

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

Syntax Description

shutdown	(Optional) Controls shutdown notifications.
voltage	(Optional) Controls voltage notifications.
temperature	(Optional) Controls temperature notifications.
fan	(Optional) Controls fan failure notifications.
supply	(Optional) Controls redundant power supply (RPS) failure notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
11.3(6)AA	This command is supported on the Cisco AS5300 access server.
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.
15.0(1)SE	This command was modified. The following notifications were added: ciscoEnvMonVoltStatusChangeNotif, ciscoEnvMonTempStatusChangeNotif, ciscoEnvMonFanStatusChangeNotif, and ciscoEnvMonSuppStatusChangeNotif.

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 Environmental Monitor (EnvMon) status notifications for supported systems. The Cisco enterprise EnvMon notifications that are listed in the table below are triggered when an environmental threshold is exceeded. If none of the optional keywords are specified, all available environmental notifications are enabled.

Keyword Enabled	EnvMon Notification Sent	Trigger
shutdown	ciscoEnvMonShutdownNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.1)	The environmental monitor detects a testpoint that is reaching a critical state and is about to initiate a shutdown.
voltage	ciscoEnvMonVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.2)	The voltage measured at a given testpoint is outside the normal range for the testpoint (that is, the voltage is at the warning, critical, or shutdown stage). For access servers, this notification is defined as caemVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.2).
temperature	ciscoEnvMonTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.3)	The temperature measured at a given testpoint is outside the normal range for the testpoint (that is, the temperature is at the warning, critical, or shutdown stage). For access servers, this notification is defined as caemTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.1).
fan	ciscoEnvMonFanNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.4)	A fan in a fan array fails.
supply	ciscoEnvMonRedundantSupplyNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.2.5)	A redundant power supply fails.

The Cisco enterprise EnvMon notifications that are listed in the table below are triggered when there is a change in the state of a device being monitored. If none of the optional keywords are specified, all available environmental notifications are enabled.

Keyword Enabled	EnvMon Notification Sent	Trigger
voltage	ciscoEnvMonVoltStatusChangeNotif (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.0.6)	There is a change in the state of a device being monitored by ciscoEnvMonVoltageState.
temperature	ciscoEnvMonTempStatusChangeNotif (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.0.7)	There is a change in the state of a device being monitored by ciscoEnvMonTemperatureState.
fan	ciscoEnvMonFanStatusChangeNotif (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.0.8)	There is a change in the state of a device being monitored by ciscoEnvMonFanState.
supply	ciscoEnvMonSuppStatusChangeNotif (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.0.9)	There is a change in the state of a device being monitored by ciscoEnvMonSupplyState.

For a complete description of these notifications and additional MIB functions, see the CISCO-ENVMON-MIB.my and CISCO-ACCESS-ENVMON-MIB.my files available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

You can view the status of EnvMon by using the **show environment** command.

The **snmp-server enable traps envmon** command is used in combination 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 a Cisco 12000 Gigabit Switch Router (GSR) to send environmental failure informs to the host at the address myhost.cisco.com by using the community string defined as public:

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

Related Commands

Command	Description
show environment	Displays environmental conditions on the system.
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 errdisable

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

snmp-server enable traps errdisable [**notification-rate** *rate*]

no snmp-server enable traps [**notification-rate** *rate*]

Syntax Description

notification-rate *rate*	(Optional) Sets the number of notifications per minute.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXI4	This command was introduced on the Supervisor Engine 720 and Supervisor Engine 32.

Examples

This example shows how to enable the SNMP errdisable notifications:

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

This example shows how to set the SNMP errdisable notification rate to 500 per minute:

```
Router(config)# snmp-server enable traps errdisable notification-rate 500
Router(config)#
```

Related Commands

Command	Description
test snmp trap errdisable ifevent	Tests the cErrDisableInterfaceEventRev1 trap.

snmp-server enable traps firewall

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

snmp-server enable traps firewall serverstatus

no snmp-server enable traps firewall serverstatus

Syntax Description

serverstatus	Displays the status of configured servers.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

SNMP notifications are sent as traps by the agent. Currently, only one URL filtering trap is generated.

For a complete description of the notification types and additional MIB functions, refer to the CISCO-UNIFIED-FIREWALL-MIB.my and CISCO-FIREWALL-TC.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps firewall** 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, the router is configured to send firewall MIB inform notifications to the host nms.cisco.com using the community string named “public”:

```
snmp-server enable traps firewall serverstatus
snmp-server host nms.cisco.com informs public firewall
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps flash

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

snmp-server enable traps flash [insertion] [removal]

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

Syntax Description

insertion	(Optional) Controls Flash card insertion notifications.
removal	(Optional) Controls Flash card removal notifications.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(23)S	This command was integrated in Cisco IOS Release 12.0 S.
12.1(13)E4	This command was implemented on the Cisco Catalyst 6000 Series.

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 Flash card insertion and removal notifications, as defined by the ciscoFlashDeviceInsertedNotif and ciscoFlashDeviceRemovedNotif objects in the Cisco Flash MIB.

When the **insertion** keyword is used, a ciscoFlashDeviceInsertedNotif (OID 1.3.6.1.4.1.9.9.10.1.3.0.5) is sent whenever a removable Flash device is inserted.

When the **removal** keyword is used, a ciscoFlashDeviceRemovedNotif (OID 1.3.6.1.4.1.9.9.10.1.3.0.6) notification is sent whenever a removable Flash device is removed.

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

The **snmp-server enable traps flash**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 Flash card insertion and removal informs to the host at the address myhost.cisco.com using the community string defined as public:

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

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 flowmon

To enable flow monitoring SNMP trap notifications, use the **snmp-server enable traps flowmon** command in global configuration mode. To disable flow monitoring trap notifications, use the **no** form of this command.

snmp-server enable traps flowmon

no snmp-server enable traps flowmon

Syntax Description

This command has no arguments or keywords.

Command Default

Flow monitoring trap notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or informs. This command enables trap notification requests only.

By default all notifications (traps) are disabled. You must explicitly enable any notifications that you need in your system. The **snmp-server enable traps flowmon** 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.

Note For a complete description of the MIB tables for flow monitoring, see the appropriate CISCO_MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs .

Examples

The following example shows how to enable flow monitoring traps:

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

Related Commands

Command	Description
snmp -server community	Enables SNMP and sets the community string and access privileges.
snmp -server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps frame-relay

To enable Frame Relay Data Link Connection Identifier (DLCI) and subinterface Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay** command in global configuration mode. To disable Frame Relay DLCI and subinterface SNMP notifications, use the **no** form of this command.

snmp-server enable traps frame-relay

no snmp-server enable traps frame-relay

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command was modified to enable Frame Relay subinterface traps in addition to DLCI traps.
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) DLCI Frame Relay notifications, as defined in the RFC1315-MIB (enterprise 1.3.6.1.2.1.10.32).

This trap indicates that the indicated virtual circuit (VC) or subinterface has changed state, meaning that the VC or subinterface has either been created or invalidated, or has toggled between the active and inactive states.

To enable only Frame Relay subinterface traps, use the **snmp-server enable traps frame-relay subif** command.

Note For large scale configurations (systems containing hundreds of Frame Relay point-to-point subinterfaces), note that having Frame Relay notifications enabled could potentially have a negative impact on network performance when there are line status changes.

For a complete description of this notification and additional MIB functions, see the RFC1315-MIB.my file and the CISCO-FRAME-RELAY-MIB.my file, available in the "v1" and "v2" directories, respectively, at the Cisco.com MIB web site at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

The **snmp-server enable traps frame-relay**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, the router is configured to send Frame Relay DLCI and subinterface state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps frame-relay
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 frame-relay multilink bundle-mismatch

To enable multilink Frame Relay Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay multilink bundle-mismatch**command in global configuration mode. To disable these notifications, use the **no** form of this command.

snmp-server enable traps frame-relay multilink bundle-mismatch

no snmp-server enable traps frame-relay multilink bundle-mismatch

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the multilink Frame Relay MIB to manage devices that are configured with multilink Frame Relay.

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

Although the bundle-mismatch trap is one of five traps defined in RFC 3020, Cisco IOS supports only the bundle-mismatch trap.

For a complete description of MIB functions, see the CISCO-FRAME-RELAY-MIB.my file, which is available in the “SNMP v2 MIBs” directory found at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Examples

In the following example, multilink Frame Relay is configured on the host router with one bundle, and the peer router is configured with zero bundle links.

On the host router:

```
Router(config)# interface MFR1
Router(config)# ip address 209.165.200.225 255.255.255.224
```

```
Router(config)# frame-relay multilink bid UUT_BUNDLE_ONE
Router(config)# frame-relay interface-dlci 100
!
Router(config)# snmp-server community public RW
Router(config)# snmp-server enable traps frame-relay multilink bundle-mismatch
Router(config)# snmp-server host 10.0.47.4 public
```

On the peer router:

```
Router(config)# interface MFR1
Router(config)# ip address 209.165.200.226 255.255.255.224
Router(config)# frame-relay multilink bid PEER_BUNDLE_ONE
Router(config)# frame-relay interface-dlci 100
Router(config)# frame-relay intf-type dce
Router(config)# snmp-server enable traps frame-relay multilink bundle-mismatch
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 from which an SNMP trap should originate.

snmp-server enable traps frame-relay subif

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

snmp-server enable traps frame-relay subif [[**interval** *seconds*] **count** *number-of-traps*]

no snmp-server enable traps frame-relay subif [[**interval** *seconds*] **count** *number-of-traps*]

Syntax Description

interval	(Optional) Specifies a minimum period between successive traps,
seconds	(Optional) Integer in the range from 0 to 3600. The default is 10.
count	(Optional) Specifies a maximum number of traps that will be sent in the specified interval.
number-of-traps	(Optional) Integer in the range from 1 to 1000. The default is 10.

Command Default

Frame Relay subinterface SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

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

Frame Relay subinterface traps are sent to the network management system (NMS) when a subinterface enters or leaves the down state.

To prevent trap storms, the **count** and **interval** keywords can be configured to limit the number of traps and the frequency at which they are sent. Configuring an interval of 0 seconds causes all Frame Relay subinterface traps to be sent.

Note The **snmp-server enable traps frame-relay** command enables both Frame Relay data-link connection identifier (DLCI) and subinterface traps. The **snmp-server enable traps frame-relay subif**command enables only Frame Relay subinterface traps.

You can disable Frame Relay subinterface traps by using the **no snmp-server enable traps frame-relay subif**command. When traps are disabled, you can use the SNMP management application to poll your router for subinterface status information.

The **snmp-server enable traps frame-relay subif**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.

The **snmp-server trap link ietf** command must be configured in order to use the **snmp-server enable traps frame-relay subif**command. The **snmp-server trap link ietf** command is used to configure your router to use the RFC 2233 IETF standards-based implementation of linkUp/linkDown traps. The default Cisco object definitions do not generate linkUp/linkDown traps correctly for subinterfaces.

Examples

The following example shows how to enable Frame Relay subinterface traps on a router. If a Frame Relay subinterface on this router changes state, host 172.16.61.90 will receive the notifications:

```
! For Frame Relay subinterface traps to work on your router, you must first have SNMP !
support and an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro

Router(config)# snmp-server host 172.16.61.90 public
Router(config)# snmp-server trap link ietf
Router(config)# snmp-server enable traps snmp
Router(config)# ip routing

Router(config)# router igrp 109

Router(config-router)# network 172.16.0.0

!Enable Frame Relay subinterface trap support:
Router(config)# snmp-server enable traps frame-relay subif interval 60 count 5
```

Related Commands

Command	Description
snmp-server enable traps frame-relay	Enables Frame Relay DLCI link status SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap link ietf	Enables linkUp/linkDown SNMP traps that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server enable traps if-monitor

To globally enable if-monitor traps, use the **snmp-server enable traps if-monitor** command in global configuration mode. To disable if-monitor traps, use the **no** form of this command.

snmp-server enable traps if-monitor

no snmp-server enable traps if-monitor

Syntax Description

This command has no arguments or keywords.

Command Default

Traps are not generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **snmp-server enable traps if-monitor** command enables the if-monitor threshold traps for link monitoring. To enable traps for a particular interface, you must enable them globally using the **snmp-server enable traps if-monitor** command and then explicitly on that interface using the **snmp trap if-monitor** command.

A high threshold limit is the highest value for a parameter on a specific link. If that value is reached or exceeded in the configured major monitoring interval, a trap is sent and a message is logged. The link is brought down if the restart mechanism is enabled.

A low threshold limit is the lowest value for a parameter on a specified link. If that value is reached or exceeded in the major monitoring interval, a trap is sent and a message is logged.

Examples

The following example shows how to enable if-monitor traps on all interfaces:

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

Related Commands

Command	Description
snmp trap if-monitor	Enables if-monitor traps for a particular interface.

snmp-server enable traps ip local pool

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

snmp-server enable traps ip local pool

no snmp-server enable traps ip local pool

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled; no notifications are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example shows how to enable the sending of local IP SNMP notifications:

```
Router(config)# snmp-server enable traps ip local pool
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps isdn

To enable the sending of Integrated Services Digital Network (ISDN)-specific Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isdn**command in global configuration mode. To disable ISDN-specific SNMP notifications, use the **no**form of this command.

snmp-server enable traps isdn [call-information] [chan-not-avail] [ietf] [isdnu-interface] [layer2]

no snmp-server enable traps isdn [call-information] [chan-not-avail] [ietf] [isdnu-interface] [layer2]

Syntax Description

call-information	(Optional) Controls SNMP ISDN call information notifications, as defined in the CISCO-ISDN-MIB (enterprise 1.3.6.1.4.1.9.9.26.2). Notification types are: • demandNbrCallInformation (1) This notification is sent to the manager whenever a successful call clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type. • demandNbrCallDetails (2) This notification is sent to the manager whenever a call connects, or clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type.
chan-not-avail	(Optional) Controls SNMP ISDN channel-not-available notifications. ISDN PRI channel-not-available traps are generated when a requested DS-0 channel is not available, or when there is no modem available to take the incoming call. These notifications are available only for ISDN PRI interfaces.
ietf	(Optional) Controls the SNMP ISDN IETF traps.
isdnu-interface	(Optional) Controls SNMP ISDN U interface notifications.

layer2	(Optional) Controls SNMP ISDN Layer 2 transition notifications.

Command Default

SNMP notifications are disabled by default.

If you enter this command with none of the optional keywords, all available notifications are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
11.3	This command was modified. The **call-information** and **isdnu-interface** keywords were added for the Cisco 1600 series router.
12.0	This command was modified. Support for the **call-information** and **isdnu-interface** keywords was introduced for most voice platforms.
12.1(5)T	This command was modified. Support for the **chan-not-available** keyword was added for the Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers only.

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. ISDN notifications are defined in the CISCO-ISDN-MIB.my and CISCO-ISDNU-IF-MIB.my files, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Availability of notifications will depend on your platform. To see what notifications are available, use the **snmp-server enable traps isdn ?** command.

If you do not enter an **snmp-server enable traps isdn**command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps isdn**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.

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. To send SNMP notifications, you must configure at least one **snmp-server host**command.

Examples

The following example shows how to determine what notification types are available on a Cisco AS5300 and then shows how to enable channel-not-available and Layer 2 informs:

```
NAS(config)# snmp-server enable traps isdn ?
  call-information  Enable SNMP isdn call information traps
  chan-not-avail    Enable SNMP isdn channel not avail traps
  ietf              Enable SNMP isdn ietf traps
  layer2            Enable SNMP isdn layer2 transition traps
```

```
  <cr>
NAS(config)# snmp-server enable traps isdn chan-not-avail layer2
NAS(config)# snmp-server host myhost.cisco.com informs version 2c public isdn
```

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-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps l2tun pseudowire status

To enable the sending of Simple Network Management Protocol (SNMP) notifications when a pseudowire changes state, use the **snmp-server enable traps l2tun pseudowire status**command in global configuration mode. To disable SNMP notifications of pseudowire state changes, use the **no** form of this command.

snmp-server enable traps l2tun pseudowire status

no snmp-server enable traps l2tun pseudowire statuszo

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
12.0(31)S	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

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) notification of pseudowire state changes. For a complete description of these notification types, and for information about the other MIB functions, see the VPDN MIB, available through the Cisco Technical Assistance Center (TAC) SNMP Object Navigator tool at http://www.cisco.com/go/mibs.

The **snmp-server enable traps l2tun pseudowire status**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.

Use the **snmp-server enable traps** command without any additional syntax to disable all SNMP notification types supported on your system.

Examples

The following example enables the router to send pseudowire state change informs to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps l2tun pseudowire status
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps	Enables all SNMP notifications (traps or informs) available on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
xconnect logging pseudowire status	Enables syslog reporting of pseudowire status events.

snmp-server enable traps l2tun session

To enable Simple Network Management Protocol (SNMP) notifications (traps or inform requests) for Layer 2 Tunnel Protocol Version 3 (L2TPv3) sessions, use the **snmp-server enable traps l2tun session**command in global configuration mode. To disable SNMP notifications, use the **no**form of this command.

snmp-server enable traps l2tun session

no snmp-server enable traps l2tun session

Syntax Description

This command has no arguments or keywords.

Command Default

No SNMP notifications for L2TPv3 sessions are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

In this command **l2tun** indicates “layer 2 tunneling.” Layer 2 tunneling session notifications are defined by the cvpdnNotifSession object { ciscoVpdnMgmtMIBNotifs 3 } in the Cisco VPDN Management MIB (CISCO-VPDN-MGMT-MIB.my). MIB files are available from Cisco.com at http://www.cisco.com/go/mibs .

SNMP notifications can be sent as traps or inform requests and this command enables both types of notifications for L2TP sessions. To specify whether the notifications should be sent as traps or informs, and to specify which host or hosts receive SNMP notifications, use the **snmp-server host** [**traps** | **informs**] command.

Use the **snmp-server enable traps** command without any additional syntax to disable all SNMP notification types supported on your system.

Examples

The following example shows how to enable a router to send L2TP session traps to the host specified by the name myhost.example.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps l2tun session
Router(config)# snmp-server host myhost.example.com public l2tun-session
```

Related Commands

Command	Description
snmp-server enable traps	Enables all SNMP notifications available on your system.
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 recipient (host) of the notifications.

snmp-server enable traps memory

To enable a device to send Simple Network Management Protocol (SNMP) notifications when memory pool buffer usage reaches a new peak, use the **snmp-server enable traps memory** command in global configuration mode. To stop notifications from being generated, use the **no** form of this command.

snmp-server enable traps memory [bufferpeak]

no snmp-server enable traps memory [bufferpeak]

Syntax Description

bufferpeak	(Optional) Specifies memory buffer peak notifications.

Command Default

SNMP notifications in the MEMPOOL-MIB are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.

This command enables or disables memory buffer peak (cempMemBufferNotify) notifications.When they are enabled, these notifications are sent when the value of the maximum number of buffer objects changes.

In current releases of Cisco IOS software, this command has the same behavior whether you use or omit the **bufferpeak** keyword.

The cempMemBufferNotify notification type is defined as {cempMIBNotifications 1} in the CISCO-ENHANCED-MEMPOOL-MIB. For a complete description of this notification and additional MIB functions, see the CISCO-ENHANCED-MEMPOOL-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs/ .

Examples

In the following example all available memory related SNMP notifications are enabled and configured to be sent as informs to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps memory
Router(config)# snmp-server host myhost.cisco.com informs version 3 public memory
```

Related Commands

Command	Description
show buffers	Displays memory buffer pool related information.
show memory	Displays memory pool related information.
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 recipient (host) of the notifications.

snmp-serverenabletrapsospfcisco-specificerrorsconfig-error

To e nable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) nonvirtual interface mismatch errors, use the **snmp-server enable traps ospf cisco-specific errors config-error**command in global configuration mode. To disable OSPF nonvirtual interface mismatch error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific errors config-error

no snmp-server enable traps ospf cisco-specific errors config-error

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF nonvirtual interface mismatch errors 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.
12.2(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

To enable the cospfShamLinkConfigError trap, you must first enter the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. The **snmp-server enable traps ospf cisco-specific errors config-error** command enables the cospfConfigError trap, so that both traps can be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links.

If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.

Examples

The following example enables the router to send nonvirtual interface mismatch error 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 errors config-error
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
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 ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific errors shamlink

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

snmp-server enable traps ospf cisco-specific errors shamlink [**authentication [bad-packet]** [**[config]**| **config [bad-packet]**]]

no snmp-server enable traps ospf cisco-specific errors shamlink [**authentication [bad-packet]** [**[config]**| **config [bad-packet]**]]

Syntax Description

authentication	(Optional) Enables SNMP notifications only for authentication failures on OSPF sham-link interfaces.
bad-packet	(Optional) Enables SNMP notifications only for packet parsing failures on OSPF sham-link interfaces.
config	(Optional) Enables SNMP notifications only for configuration mismatch errors on OSPF sham-link interfaces.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF sham-link errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
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

To enable the cospfShamLinkConfigError trap, you must first enter the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. The **snmp-server enable traps ospf cisco-specific errors config-error** command enables the cospfConfigError trap, so that both traps can

be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links.

If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.

Examples

The following example enables the router to send OSPF sham-link error 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 errors config-error
Router(config)# snmp-server enable traps ospf cisco-specific errors 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 retransmit	Enables SNMP notifications for OSPF retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific retransmit

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

snmp-server enable traps ospf cisco-specific retransmit [**packets** [**shamlink**| **virt-packets**]| **shamlink** [**packets**| **virt-packets**]| **virt-packets [shamlink]**]

no snmp-server enable traps ospf cisco-specific retransmit [**packets** [**shamlink**| **virt-packets**]| **shamlink** [**packets**| **virt-packets**]| **virt-packets [shamlink]**]

Syntax Description

packets	(Optional) Enables SNMP notifications only for packet retransmissions on nonvirtual interfaces.
shamlink	(Optional) Enables SNMP notifications only for sham-link retransmission notifications.
virt-packets	(Optional) Enables SNMP notifications only for packet retransmissions on virtual interfaces.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF retransmission errors 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** keyword and related options were added.
12.3(14)T	Support was added for the **shamlink** keyword and related options.
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.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example enables the router to send OSPF sham-link retransmission notifications:

```
Router(config)# snmp-server enable traps ospf cisco-specific retransmit shamlink
```

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 state-change	Enables SNMP notifications for OSPF transition state changes.