

show license call-home

To display the stock keeping unit (SKU) list and features available in a product authorization key (PAK), use the **show license call-home** command in privileged EXEC mode.

Cisco 860, 880, and 890 Series Routers, and Cisco 1900, 2900, and 3900 Series Integrated Services Router Platforms

```
show license call-home pak pak-id
```

Cisco uBR10012 Universal Broadband Router

```
show license [call-home pak pak-id]
```

Cisco Catalyst 3560-E and Cisco Catalyst 3750-E Switch Platforms

```
show license call-home pak pak-id
```

Syntax Description

pak	Shows the product authorization key.
<i>pak-id</i>	The product authorization key sent through e-mail or through regular mail by manufacturing to authorize software upgrades.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC on the Cisco uBR10012 universal broadband router.

Usage Guidelines

The Cisco License Call Home feature allows a Cisco router to communicate with the Cisco licensing infrastructure through the Internet and retrieve licensing information. This command requires that the router be connected to the Internet.

This command requires the following:

- The router or switch must have an Internet connection and use HTTPS to connect to the Cisco licensing infrastructure. To set up a secure HTTP connection, see the HTTP 1.1 Web Server and Client module in the *Network Management Configuration Guide*: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_http_web.html.
- Only certain platforms support the Cisco License Call Home feature, and those devices must be running a Cisco IOS crypto K9 image.
- You must obtain the device certificate from the Cisco licensing infrastructure.
- You need a Cisco.com user login account.

Issuing the **show license call-home** command causes these actions to occur:

- The Cisco licensing infrastructure returns parsed XML content to the command line. The parsed content contains information about SKUs and feature names. The content might also contain warning messages.
- The SKU information and any warning messages are displayed as formatted output on the router command line.

Cisco uBR10012 Universal Broadband Router

In the Cisco uBR10012 universal broadband router, the **call-home** keyword is optional in the **show license** command syntax.

Examples

The following example shows the PAKs and SKUs associated with a software license:

```
Router# show license call-home pak 3XPXR9E7D30

CCO User name : User1
CCO password  : *****

Pak Number      : 3XPXR9E7D30
Pak Fulfillment type: SINGLE

  1. SKU Name      : Gatekeeper
     SKU Type      : Product
     Description    : Gatekeeper
     Ordered Qty    : 1
     Available Qty  : 1
     Feature List   :
       Feature name:      gatekeeper Count: Uncounted
     Platform Supported : 5400
                          5350
                          2800
                          3800
```

[Table 5](#) describes the significant fields shown in the display.

Table 5 *show license call-home Field Descriptions*

Field	Description
Pak Number	Product authorization key number, which is provided to you when you order and purchase the right to use a feature set for a particular platform. The PAK serves as a receipt and is used as part of the process to obtain a license.
SKU Name	Stock keeping unit name, which maps to one or more Cisco software features.
Description	Description provided for the SKU.
Ordered Qty	Quantity ordered.
Feature List	List of features.
Platform Supported	List of Cisco device platforms supported.

Related Commands

Command	Description
license call-home install	Installs a license by using the Cisco License Call Home feature.

Command	Description
license call-home resend	Restores a lost license by using the Cisco License Call Home feature.
license call-home revoke	Rehosts (revokes and transfers) a license by using the Cisco License Call Home feature.

show license statistics

To display license statistics information, use the **show license statistics** command in privileged EXEC mode.

Cisco 860, 880, and 890 Series Routers, and Cisco 1900, 2900, and 3900 Series Integrated Services Router Platforms

```
show license statistics
```

Cisco Catalyst 3560-E Switch Platforms

```
show license statistics
```

Cisco Catalyst 3750-E Switch and Switch Stack Platforms

```
show license statistics [switch switch-num]
```

Cisco Catalyst 3750-E Switch Mixed Stack Platforms

```
show license statistics switch switch-num
```

Cisco uBR10012 Universal Broadband Routers

```
show license [statistics subslot slot/subslot]
```

Cisco uBR7225VXR and Cisco uBR7246VXR Universal Broadband Routers

```
show license [statistics slot slot]
```

Syntax	Description
switch <i>switch-num</i>	Specifies a switch in a switch stack or in a mixed switch stack. The range is 1 to 9.
subslot	(Cisco uBR10012 universal broadband routers only) Shows the slot and subslot information of a line card.
slot	Shows the slot information of a line card.
<i>slot</i>	Slot where the line card resides: <ul style="list-style-type: none"> • Cisco uBR7246VXR router—The range is 3 to 6. • Cisco uBR7225VXR router—The range is 1 to 2. • Cisco uBR10012 router—The range is 5 to 8.
<i>subslot</i>	(Cisco uBR10012 universal broadband routers only) The value is either 0 or 1.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC on Cisco uBR10012 universal broadband routers.
12.2(33)SCD	This command was modified. The slot slot keyword and argument were added for the Cisco uBR7225VXR and Cisco uBR7246VXR routers.

Usage Guidelines**Cisco uBR10012 Universal Broadband Routers**

The command displays statistics information of the line card in the specified *slot/subslot*. The keyword **subslot** and *slot/subslot* arguments were added for Cisco uBR10012 universal broadband routers.

Examples

The following is sample output from the **show license statistics** command:

```
Router# show license statistics

      Administrative statistics
Install success count:   4
Install failure count:  1
Install duplicate count: 12
Comment add count:      2
Comment delete count:   0
Clear count:            10
Save count:              1
Save cred count:        6

      Client statistics
Request success count 0
Request failure count 0
Release count         0
Global Notify count   21

      SWIFT url status
Swift value changed by user
Current Value : https://cisco.com/SWIFT/Licensing
Default Value : https://cisco.com/SWIFT/Licensing
```

Cisco uBR10012 Universal Broadband Routers: Example

The following is sample output from the **show license statistics subslot 8/1** command executed on the Cisco uBR10012 router:

```
Router# show license statistics subslot 8/1

Administrative statistics
  Install success count:  0
  Install failure count:  0
  Install duplicate count: 0
  Comment add count:      0
  Comment delete count:   0
  Clear count:            0
  Save count:              0
  Save cred count:        0

      Client statistics
```

```

Request success count: 1
Request failure count: 1
Release count: 0
Global Notify count: 1

```

Table 6 describes the significant fields shown in the display.

Table 6 *show license statistics Field Descriptions*

Field	Description
Administrative statistics	<ul style="list-style-type: none"> • Install success count—Number of successful installations • Install failure count—Number of failed installation attempts • Install duplicate count—Number of duplicate installations • Comment add count—Number of added comments • Comment delete count—Number of deleted comments • Clear count—Number of License Clear events • Save count—Number of License Save events • Save cred count—Number of License Save Credentials
Client statistics	<ul style="list-style-type: none"> • Request success count—Number of successful license requests • Request failure count—Number of failed license requests • Release count—Number of released licenses • Global Notify count—Number of global notifications
SWIFT url status	<ul style="list-style-type: none"> • Current Value—Current SWIFT URL • Default Value—Default SWIFT URL

Cisco uBR7225VXR and Cisco uBR7246VXR Universal Broadband Routers: Example

The following is sample output from the **show license statistics slot 5** command executed on the Cisco uBR7246VXR router:

```

Router# show license statistics slot 5

      Administrative statistics
Install success count: 0
Install failure count: 0
Install duplicate count: 0
Comment add count: 0
Comment delete count: 0
Clear count: 0
Save count: 0
Save cred count: 0

      Client statistics
Request success count: 2
Request failure count: 0
Release count: 0

```

```
Global Notify count:      0
```

Table 7 describes the significant fields shown in the display.

Table 7 *show license statistics Field Descriptions*

Field	Description
Administrative statistics	<ul style="list-style-type: none"> • Install success count—Number of successful installations • Install failure count—Number of failed installation attempts • Install duplicate count—Number of duplicate installations • Comment add count—Number of added comments • Comment delete count—Number of deleted comments • Clear count—Number of License Clear events • Save count—Number of License Save events • Save cred count—Number of License Save Credentials
Client statistics	<ul style="list-style-type: none"> • Request success count—Number of successful license requests • Request failure count—Number of failed license requests • Release count—Number of released licenses • Global Notify count—Number of global notifications

Related Commands

Command	Description
debug license	Enables controlled debugging options in the Cisco software licensing module.
show license status	Displays license information to troubleshoot licensing issues.

show subsys

To display the subsystem information, use the **show subsys** command in privileged EXEC mode.

```
show subsys [class class | name name]
```

Syntax Description		
class <i>class</i>	(Optional) Displays the subsystems of the specified class. Valid classes are driver , ehsa , ifs , kernel , library , license , management , microcode , pre-ehsa , pre-driver , protocol , registry , and sysinit .	
name <i>name</i>	(Optional) Displays the specified subsystem. Use the asterisk (*) as a wildcard at the end of the name to list all subsystems, starting with the specified characters.	

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	11.1	This command was introduced.
	12.3	This command was modified. The ehsa , ifs , microcode , pre-driver , and sysinit classes were added.
	12.3T	This command was modified. The pre-ehsa class was added.
	12.2(33)SRA	This command was modified. The driver , ehsa , kernel , library , management , pre-driver , pre-ehsa , protocol , and registry classes were added.
	12.2(35)SE2	This command was modified. The driver , ehsa , kernel , library , license , management , pre-driver , pre-ehsa , protocol , and registry classes were added.

Usage Guidelines Use the **show subsys** command to confirm that all required features are in the running image.

Examples The following is sample output from the **show subsys** command:

```
Router# show subsys

Name           Class      Version
static_map    Kernel    1.000.001
arp           Kernel    1.000.001
ether         Kernel    1.000.001
compress     Kernel    1.000.001
alignment     Kernel    1.000.002
monvar        Kernel    1.000.001
slot          Kernel    1.000.001
oir           Kernel    1.000.001
atm           Kernel    1.000.001
ip_addrpool_sys Library    1.000.001
chat          Library    1.000.001
dialer        Library    1.000.001
```

```

flash_services      Library      1.000.001
ip_localpool_sys    Library      1.000.001
nvram_common        Driver       1.000.001
ASP                 Driver       1.000.001
sonict              Driver       1.000.001
oc3suni             Driver       1.000.001
oc12suni            Driver       1.000.001
ds3suni             Driver       1.000.001

```

The following is sample output from the **show subsys** command that includes the **license** class:

```
Router# show subsys name license
```

```

Name                Class      Version
license_mgmt_local  Management 1.000.001
license_admin_local Management 1.000.001
license_debug_core  Management 1.000.001
license_test_ui     Management 1.000.001
test_license_parser Management 1.000.001
license_ui          Management 1.000.001
license_parser      Management 1.000.001
license_registry    Registry   1.000.001
license_client      License    1.000.001

```

[Table 8](#) describes the fields shown in the display.

Table 8 *show subsys Field Descriptions*

Field	Description
Name	Name of the subsystem.
Class	Class of the subsystem. Possible classes include Driver, Ehsa, Ifs, Kernel, Library, License, Management, Microcode, Pre-Ehsa, Pre-driver, Protocol, Registry, and Sysinit.
Version	Version of the subsystem.

show subsys license

To display the subsystem running for a feature set, use the **show subsys license** command in either user EXEC or privileged EXEC mode.

show subsys license *subsystem*

Syntax Description	<i>subsystem</i>	Name of the subsystem for a specified license.
--------------------	------------------	--

Command Default Subsystem information is not displayed.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	12.2(35)SE2	This command was introduced.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines Use this command to display license information and to help with troubleshooting issues related to Cisco IOS software licenses.

Examples The following is sample output that shows the subsystem running the IP base feature set:

```
Router# show subsys license ipbase
```

```
License level: ipbase
```

Name	Class	Version
obfl_env_app	Kernel	1.000.001
exception	Kernel	1.000.001
xml_proxy_client	Kernel	1.000.000
proto_counter	Kernel	1.000.001
sched_ui	Kernel	1.000.001
policy_manager	Kernel	1.000.001
fib_table_trace	Kernel	1.000.001
ifmibapi_access	Kernel	1.000.000
xml_engine	Kernel	1.000.000
fddi_mtu	Kernel	1.000.001
fib_trace	Kernel	1.000.001
.		
.		
qos_set	Protocol	1.000.001
rip	Protocol	1.000.001
ipdiag	Protocol	1.000.001
aaa_peruser	Protocol	1.000.001
identity_cli	Management	1.000.001

show subsys license

```

notification_log_mib           Management  1.000.000
pagpmib                        Management  1.000.000
ifmib                          Management  1.000.000
rtty_chain                     Management  1.000.001
cdpmib                         Management  1.000.000
vlmem                          Management  1.000.000
.
.
.
psecure_registry              Registry   1.000.001
ip_ios_registry                Registry   1.000.001
sys_name_registry              Registry   1.000.001
INIT                           SystemInit 2.000.001
parser                         EHSA      1.000.001
tmphys_ifs                     EHSA      1.000.001
hulc_fib_rf_ehsa               EHSA      1.000.001
regexp_ui                       EHSA      1.000.001
system_ifs                     EHSA      1.000.001
chunk_ui                       EHSA      1.000.001
rbcp                            EHSA      1.000.000
gdb_ui                         EHSA      1.000.001
ifs_image_elf                  EHSA      1.000.001
nvram_common                   EHSA      1.000.001
ifs_image_ascii                EHSA      1.000.001
clock_ui                       EHSA      1.000.001
nv_ifs                         EHSA      1.000.001
sff8472                        Pre-Driver 1.000.001
aggmgr                         Pre-Driver 1.000.000
ifindex_pers                   Pre-Driver 1.000.001
sff8472_fixed                  Pre-Driver 1.000.000
fib_rp_predriver               Pre-Driver 1.000.001
system_capability              Pre-Driver 1.000.001
fib_lc_predriver               Pre-Driver 1.000.001
fib_ios_chain                  Pre-Driver 1.000.001
transceiver                    Pre-Driver 1.000.002
fib_ios_predriver              Pre-Driver 1.000.001
license_client                  License    1.000.001
hulc_flash                     License    1.000.001
ios_licensing_image_application License    1.000.001
ifs                            License    1.000.001
sdb                            License    1.000.001
boot_upgrade                   License    1.000.001
hulc_universal_only            License    1.000.001

```

Table 8 describes the fields shown in the display.

Table 9 show subsys license Field Descriptions

Field	Description
License level	Feature set for which the license is issued; for example, Advanced IP services, IP services, or IP base.
Name	Name of the subsystem.
Class	Class of the subsystem. Possible classes include Driver, Kernel, Library, License, Management, Protocol, Registry.
Version	Version of the subsystem.

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 <i>severity</i> 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.
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.

Release	Modification
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: <ul style="list-style-type: none"> • 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.
	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 host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

```
snmp-server host {hostname | ip-address} [vrf vrf-name] [informs | traps] [version {1 | 2c | 3}
[auth | noauth | priv]] community-string [udp-port port] [notification-type]
```

```
no snmp-server host {hostname | ip-address} [vrf vrf-name] [informs | traps] [version {1 | 2c | 3}
[auth | noauth | priv]] community-string [udp-port port] [notification-type]
```

Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches

```
snmp-server host ip-address {community-string | {informs | traps} {community-string |
version {1 | 2c | 3 {auth | noauth}}}} community-string | version {1 | 2c | 3 {auth | noauth}}
community-string | vrf vrf-name {informs | traps} {community-string | version {1 | 2c | 3 {auth
| noauth}} community-string}} [notification-type]
```

```
no snmp-server host ip-address {community-string | {informs | traps} {community-string |
version {1 | 2c | 3 {auth | noauth}} community-string | version {1 | 2c | 3 {auth | noauth}}
community-string | vrf vrf-name {informs | traps} {community-string | version {1 | 2c | 3 {auth
| noauth}} community-string}} [notification-type]
```

Command Syntax on Cisco 7600 Series Router

```
snmp-server host ip-address {community-string | {informs | traps} {community-string |
version {1 | 2c | 3 {auth | noauth | priv}} community-string | version {1 | 2c | 3 {auth | noauth
| priv}} community-string | vrf vrf-name {informs | traps} {community-string | version {1 | 2c
| 3 {auth | noauth | priv}} community-string}} [notification-type]
```

```
no snmp-server host ip-address {community-string | {informs | traps} {community-string |
version {1 | 2c | 3 {auth | noauth | priv}} community-string | version {1 | 2c | 3 {auth | noauth
| priv}} community-string | vrf vrf-name {informs | traps} {community-string | version {1 | 2c
| 3 {auth | noauth | priv}} community-string}} [notification-type]
```

Syntax Description

<i>hostname</i>	Name of the host. The SNMP notification host is typically a network management station (NMS) or SNMP manager. This host is the recipient of the SNMP traps or informs.
<i>ip-address</i>	IPv4 address or IPv6 address of the SNMP notification host.
vrf	(Optional) Specifies that a Virtual Private Network (VPN) routing and forwarding (VRF) instance should be used to send SNMP notifications. <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the vrf keyword is required.
<i>vrf-name</i>	(Optional) VPN VRF instance used to send SNMP notifications. <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the <i>vrf-name</i> argument is required.
informs	(Optional) Specifies that notifications should be sent as informs. <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the informs keyword is required.

traps	(Optional) Specifies that notifications should be sent as traps. This is the default. <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the traps keyword is required.
version	(Optional) Specifies the version of the SNMP that is used to send the traps or informs. The default is 1. <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the version keyword is required and the priv keyword is not supported. <p>If you use the version keyword, one of the following keywords must be specified:</p> <ul style="list-style-type: none"> 1—SNMPv1. 2c—SNMPv2C. 3—SNMPv3. The most secure model because it allows packet encryption with the priv keyword. The default is noauth. <p>One of the following three optional security level keywords can follow the 3 keyword:</p> <ul style="list-style-type: none"> auth—Enables message digest algorithm 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. noauth—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. priv—Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
<i>community-string</i>	Password-like community string sent with the notification operation. <p>Note You can set this string using the snmp-server host command by itself, but Cisco recommends that you define the string using the snmp-server community command prior to using the snmp-server host command.</p> <p>Note The “at” sign (@) is used for delimiting the context information.</p>
udp-port	(Optional) Specifies that SNMP traps or informs are to be sent to an NMS host. <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the udp-port keyword is not supported.
<i>port</i>	(Optional) User Datagram Protocol (UDP) port number of the NMS host. The default is 162. <ul style="list-style-type: none"> In Cisco IOS Release 12.2(54)SE, the <i>port</i> argument is not supported.
<i>notification-type</i>	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. See the “Notification-Type Keywords” section on page 89 for more information about the keywords available.

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
Cisco IOS Release 12 Mainline/T Train	
12.0(3)T	<ul style="list-style-type: none"> The version 3 [auth noauth priv] syntax was added as part of the SNMPv3 Support feature. The hsrp notification-type keyword was added. The voice notification-type keyword was added.
12.1(3)T	The calltracker notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	<ul style="list-style-type: none"> The vrf <i>vrf-name</i> keyword and argument combination was added. The ipmobile notification-type keyword was added. Support for the vsimaster notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.
12.2(4)T	<ul style="list-style-type: none"> The pim notification-type keyword was added. The ipsec notification-type keyword was added.
12.2(8)T	<ul style="list-style-type: none"> The mpls-traffic-eng notification-type keyword was added. The director notification-type keyword was added.
12.2(13)T	<ul style="list-style-type: none"> The srp notification-type keyword was added. The mpls-ldp notification-type keyword was added.
12.3(2)T	<ul style="list-style-type: none"> The flash notification-type keyword was added. The l2tun-session notification-type keyword was added.
12.3(4)T	<ul style="list-style-type: none"> The cpu notification-type keyword was added. The memory notification-type keyword was added. The ospf notification-type keyword was added.
12.3(8)T	The iplocalpool notification-type keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	The vrrp keyword was added.
12.3(14)T	<ul style="list-style-type: none"> Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the <i>hostname</i> argument. The igrp notification-type keyword was added.
12.4(20)T	The license notification-type keyword was added.
15.0(1)M	<ul style="list-style-type: none"> The nhrp notification-type keyword was added. The automatic insertion of the snmp-server community command into the configuration, along with the community string specified in the snmp-server host command, is changed. The snmp-server community command has to be manually configured.
Cisco IOS Release 12.0S	
12.0(17)ST	The mpls-traffic-eng notification-type keyword was added.
12.0(21)ST	The mpls-ldp notification-type keyword was added.

Release	Modification
12.0(22)S	<ul style="list-style-type: none"> All features in Cisco IOS Release 12.0ST were integrated into Cisco IOS Release 12.0(22)S. The mpls-vpn notification-type keyword was added.
12.0(23)S	The l2tun-session notification-type keyword was added.
12.0(26)S	The memory notification-type keyword was added.
12.0(27)S	<ul style="list-style-type: none"> Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the <i>hostname</i> argument. The vrf vrf-name keyword and argument combination was added to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.
12.0(31)S	The l2tun-pseudowire-status notification-type keyword was added.
Release 12.2S	
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(25)S	<ul style="list-style-type: none"> The cpu notification-type keyword was added. The memory notification-type keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The cef notification-type keyword was added.
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.
12.2(33)SXI5	<ul style="list-style-type: none"> The dhcp-snooping notification-type keyword was added. The errdisable notification-type keyword was added.
12.2(54)SE	This command was modified. See the “Command Syntax on Cisco ME 3400, ME 3400E, and Catalyst 3750 Metro Switches” section on page 84 for the command syntax for these switches.
Cisco IOS Release 15S	
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. The flowmon notification-type keyword was added.
Cisco IOS XE	
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

If you enter this command with no optional keywords, the default is to send all notification-type traps to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

**Note**

If a community string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** will be the same as that specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enable** command. Some notification types are always enabled, and others are enabled by a different command. For example, the **linkUpDown** notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

The availability of a notification-type options depends on the router type and the Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command **help ?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific Virtual Routing and Forwarding (VRF) VPN. The VRF defines a VPN membership of a user so data is stored using the VPN.

In the case of the NMS sending the query having a correct SNMP community but that does not have a read or a write view, the SNMP agent returns the following error values:

- For a get or a getnext query, returns **GEN_ERROR** for SNMPv1 and **AUTHORIZATION_ERROR** for SNMPv2C.
- For a set query, returns **NO_ACCESS_ERROR**.

Notification-Type Keywords

The notification type can be one or more of the following keywords:



Note The available notification types differ based on the platform and Cisco IOS release. For a complete list of available notification types, use the question mark (?) online help function.

- **aaa server**—Sends SNMP authentication, authorization, and accounting (AAA) traps.
- **adslline**—Sends Asymmetric Digital Subscriber Line (ADSL) LINE-MIB traps.
- **atm**—Sends ATM notifications.
- **authenticate-fail**—Sends SNMP 802.11 Authentication Fail Trap.
- **auth-framework**—Sends SNMP CISCO-AUTH-FRAMEWORK-MIB notifications.
- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
- **bridge**—Sends SNMP STP Bridge MIB notifications.
- **bstun**—Sends Block Serial Tunneling (bstun) event notifications.
- **bulkstat**—Sends Data-Collection-MIB notifications.
- **c6kxbar**—Sends SNMP crossbar notifications.
- **callhome**—Sends Call Home MIB notifications.
- **calltracker**—Sends Call Tracker call-start/call-end notifications.
- **casa**—Sends Cisco Appliances Services Architecture (CASA) event notifications.
- **ccme**—Sends SNMP ccme traps.
- **cef**—Sends notifications related to Cisco Express Forwarding.
- **chassis**—Sends SNMP chassis notifications.
- **cnpd**—Sends Network-Based application Recognition (NBAR) Protocol Discovery traps.
- **config**—Sends configuration change notifications.
- **config-copy**—Sends SNMP config-copy notifications.
- **config-ctid**—Sends SNMP config-ctid notifications.
- **cpu**—Sends CPU-related notifications.
- **csg**—Sends SNMP Content Services Gateway (CSG) notifications.
- **deauthenticate**—Sends an SNMP 802.11 Deauthentication Trap.
- **dhcp-snooping**—Sends Dynamic Host Configuration Protocol (DHCP) snooping MIB notifications.
- **director**—Sends notifications related to DistributedDirector.
- **disassociate**—Sends SNMP 802.11 Disassociation Trap.
- **dls**—Sends data-link switching (DLSW) notifications.
- **dnis**—Sends SNMP Dialed Number Identification Service (DNIS) traps.
- **dot1x**—Sends 802.1X notifications.
- **dot11-mibs**—Sends dot11 traps.
- **dot11-qos**—Sends SNMP 802.11 QoS Change Trap.
- **ds0-busyout** —Sends ds0-busyout traps.

- **ds1**—Sends SNMP digital signaling 1 (DS1) notifications.
- **ds1-loopback**—Sends ds1-loopback traps.
- **dspu**—Sends downstream physical unit (DSPU) notifications.
- **eigrp**—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.
- **energywise**—Sends SNMP energywise notifications.
- **entity**—Sends Entity MIB modification notifications.
- **entity-diag**—Sends SNMP entity diagnostic MIB notifications.
- **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
- **errdisable**—Sends error disable notifications.
- **ethernet-cfm**—Sends SNMP Ethernet Connectivity Fault Management (CFM) notifications.
- **event-manager**—Sends SNMP Embedded Event Manager notifications.
- **firewall**—Sends SNMP Firewall traps.
- **flash**—Sends flash media insertion and removal notifications.
- **flexlinks**—Sends FLEX links notifications.
- **flowmon**—Sends flow monitoring notifications.
- **frame-relay**—Sends Frame Relay notifications.
- **fru-ctrl**—Sends entity field-replaceable unit (FRU) control notifications.
- **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
- **icsudsu**—Sends SNMP ICSUDSU traps.
- **iplocalpool**—Sends IP local pool notifications.
- **ipmulticast**—Sends IP multicast notifications.
- **ipmobile**—Sends Mobile IP notifications.
- **ipsec**—Sends IP Security (IPsec) notifications.
- **isakmp**—Sends SNMP ISAKMP notifications.
- **isdn**—Sends ISDN notifications.
- **l2tc**—Sends SNMP L2 tunnel configuration notifications.
- **l2tun-pseudowire-status**—Sends pseudowire state change notifications.
- **l2tun-session**—Sends Layer 2 tunneling session notifications.
- **license**—Sends licensing notifications as traps or informs.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
- **mac-notification**—Sends SNMP MAC notifications.
- **memory**—Sends memory pool and memory buffer pool notifications.
- **module**—Sends SNMP module notifications.
- **module-auto-shutdown**—Sends SNMP module autosutdown MIB notifications.
- **mpls-fast-reroute**—Sends SNMP Multiprotocol Label Switching (MPLS) traffic engineering fast reroute notifications.

- **mpls-ldp**—Sends MPLS Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.
- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **msdp**—Sends SNMP Multicast Source Discovery Protocol (MSDP) notifications.
- **mvpn**—Sends multicast VPN notifications.
- **nhrp**—Sends Next Hop Resolution Protocol (NHRP) notifications.
- **ospf**—Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) notifications.
- **port-security**—Sends SNMP port-security notifications.
- **power-ethernet**—Sends SNMP power Ethernet notifications.
- **pw-vc**—Sends SNMP pseudowire virtual circuit (VC) notifications.
- **repeater**—Sends standard repeater (hub) notifications.
- **resource-policy**—Sends CISCO-ERM-MIB notifications.
- **rf**—Sends SNMP RF MIB notifications.
- **rogue-ap**—Sends an SNMP 802.11 Rogue AP Trap.
- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Response Time Reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **slb**—Sends SNMP server load balancer (SLB) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.



Note To enable RFC 2233-compliant link up/down notifications, you should use the **snmp server link trap** command.

- **sonet**—Sends SNMP SONET notifications.
- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **stpx**—Sends SNMP STPX MIB notifications.
- **srst**—Sends SNMP SRST traps.
- **stun**—Sends serial tunnel (STUN) notifications.
- **switch-over**—Sends an SNMP 802.11 Standby Switch-over Trap.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Use the **logging history level** command to specify the level of messages to be sent.
- **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.

- **udp-port**—Sends the notification host's UDP port number.
- **vlan-mac-limit**—Sends SNMP L2 control VLAN MAC limit notifications.
- **vlancreate**—Sends SNMP VLAN created notifications.
- **vlandelete**—Sends SNMP VLAN deleted notifications.
- **voice**—Sends SNMP voice traps.
- **vrrp**—Sends Virtual Router Redundancy Protocol (VRRP) notifications.
- **vsimaster**—Sends Virtual Switch Interface (VSI) Master notifications.
- **vswitch**—Sends SNMP virtual switch notifications.
- **vtp**—Sends SNMP VLAN Trunking Protocol (VTP) notifications.
- **wlan-wep**—Sends an SNMP 802.11 WLAN WEP trap.
- **x25**—Sends X.25 event notifications.
- **xgcp**—Sends XGCP protocol traps.

SNMP-Related Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no embedded spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an embedded space and a hyphen).

This syntax difference is necessary to ensure that the command-line interface (CLI) interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. Table 10 maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 10 *SNMP-server enable traps Commands and Corresponding Notification Keywords*

snmp-server enable traps Command	snmp-server host Command Keyword
snmp-server enable traps l2tun session	l2tun-session
snmp-server enable traps mpls ldp	mpls-ldp
snmp-server enable traps mpls traffic-eng¹	mpls-traffic-eng
snmp-server enable traps mpls vpn	mpls-vpn

1. See the *Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 192.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

**Note**

The “at” sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using *community@VLAN-ID* (for example, public@100), where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a specified host named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

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

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 192.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 192.30.2.160 public snmp envmon
```

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

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

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host. The community string is defined as public.

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

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string 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 informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

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

The following example shows how to send all SNMP notifications to example.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host example.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

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

The following example shows how to send all Cisco Express Forwarding informs to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps cef
Router(config)# snmp-server host 192.40.3.130 informs version 2c public cef
```

The following example shows how to enable all NHRP traps, and how to send all NHRP traps to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 192.40.3.130 traps version 2c public nhrp
```

Related Commands

Command	Description
show snmp host	Displays recipient details configured for SNMP notifications.
snmp-server enable peer-trap poor qov	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server enable traps nhrp	Enables SNMP notifications (traps) for NHRP.
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP trap that are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.

