SNMP Server Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software commands used to configure and monitor the Simple Network Management Protocol (SNMP) for network monitoring and management.

For detailed information about SNMP concepts, configuration tasks, and examples, see the *Implementing SNMP on Cisco IOS XR Software* configuration module in *Cisco IOS XR System Management Configuration Guide*.

Note The **snmp-server** commands enable SNMP on Management Ethernet interfaces by default. For information about how to enable SNMP server support on other inband interfaces, refer to the *Implementing Management Plane Protection on Cisco IOS XR Software* module in *Cisco IOS XR System Security Configuration Guide*.

clear snmp counters

To clear the Simple Network Management Protocol (SNMP) packet statistics shown by the **show snmp** command, use the **clear snmp counters** command in EXEC mode.

clear snmp counters

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.6.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **clear snmp counters** command provides the ability to clear all SNMP counters used in the **show snmp** command without restarting any processes.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to clear the SNMP counters:

```
RP/0/RP0/CPU0:Router# clear snmp counters
```

Related Commands

Command	Description
show snmp	Displays the status of SNMP communications.

index persistence

To enable index persistency on an Simple Network Management Protocol (SNMP) interface, use the **index persistence** command in SNMP interface configuration mode. To restore the default conditions with respect to this command, use the **no** form of this command.

index persistence

no index persistence

Syntax Description

This command has no arguments or keywords.

Defaults

Index persistency is disabled.

Command Modes

SNMP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Issue the **index persistence** command to enable ifIndex persistence for individual entries (corresponding to individual interfaces) in the ifIndex table of the IF-MIB. IfIndex persistence retains the mapping between the ifName object values and the ifIndex object values (generated from the IF-MIB) across reboots, allowing for consistent identification of specific interfaces using SNMP.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to assign ifIndex persistence on Packet-over-SONET/SDH (POS) interface 0/0/1/0:

```
RP/0/RP0/CPU0:Router(config)# snmp-server interface pos 0/0/1/0
RP/0/RP0/CPU0:Router(config-snmp-if)# index persistence
```

Related Commands

Command	Description
show snmp interface	Displays the ifIndex value for an SNMP interface.
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server ifindex persist	Enables ifIndex persistence globally for all SNMP interfaces.
snmp-server interface	Enables an interface to send SNMP trap notifications and enter SNMP interface configuration mode.

notification linkupdown disable

To disable linkUp and linkDown trap notifications on a Simple Network Management Protocol (SNMP) interface, use the **notification linkupdown disable** command in SNMP interface configuration mode. To enable linkUp and linkDown trap notifications, use the **no** form of this command.

notification linkupdown disable

no notification linkupdown disable

Syntax Description

This command has no arguments or keywords.

Defaults

LinkUp and linkDown trap notifications are enabled.

Command Modes

SNMP interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The **enable** keyword was removed.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

By default, linkUp and linkDown notifications are enabled on physical interfaces. Issue the **notification linkupdown disable** command to disable linkUp and linkDown notifications on an interface.

Use the **no** form of this command to enable linkUp and linkDown notifications on an interface, if linkUp and linkDown notifications have been disabled.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to disable linkUp and linkDown trap notifications on Packet-over-SONET/SDH (POS) interface 0/0/1/0:

```
RP/0/RP0/CPU0:Router(config)# snmp-server interface pos 0/0/1/0
RP/0/RP0/CPU0:Router(config-snmp-if)# notification linkupdown disable
```

Related Commands

Command	Description
show snmp interface	Displays the ifIndex value for an SNMP interface.
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server ifindex persist	Enables ifIndex persistence globally for all SNMP interfaces.
snmp-server interface	Enables an interface to send SNMP trap notifications and enter SNMP interface configuration mode.

show snmp

To display the status of Simple Network Management Protocol (SNMP) communications, use the **show snmp** command in EXEC mode.

show snmp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show snmp** command to show counter information for SNMP operations. It also displays the chassis ID string defined with the **snmp-server chassis-id** command.

Task ID

Task ID	Operations
snmp	read

Examples

The following is sample output from the **show snmp** command:

```
RP/0/RP0/CPU0:Router# show snmp

Chassis: 01506199
37 SNMP packets input
    0 Bad SNMP version errors
    4 Unknown community name
    0 Illegal operation for community name supplied
```

```
    0 Encoding errors
    24 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    28 Get-next PDUs
    0 Set-request PDUs
78 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    24 Response PDUs
    13 Trap PDUs
SNMP logging: enabled
    Logging to 172.25.58.33.162, 0/10, 13 sent, 0 dropped.
```

Table 86 describes the significant fields shown in the display.

Table 86 show snmp Field Descriptions

Field	Description
Chassis	Chassis ID string.
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of get requests received
Get-next PDUs	Number of get-next requests received.
Set-request PDUs	Number of set requests received.
SNMP packets output	Total number of SNMP packets sent by the device.
Too big errors	Number of SNMP packets that were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified a MIB object that does not exist.
Bad values errors	Number of SNMP set requests that specified an invalid value for a MIB object.
General errors	Number of SNMP set requests that failed due to some other error. (It is not a noSuchName error, badValue error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.

Table 86 show snmp Field Descriptions (continued)

Field	Description
SNMP logging	Enabled or disabled logging.
sent	Number of traps sent.
dropped	Number of traps dropped. Traps are dropped when the trap queue for a destination exceeds the maximum length of the queue, as set by the **snmp-server queue-length** command.

Related Commands

Command	Description
show snmp mib	Displays a list of the MIB objects registered on the system.
snmp-server chassis-id	Provides a message line identifying the SNMP server serial number.
snmp-server queue-length	Establishes the message queue length for each trap host.

show snmp engineid

To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the **show snmp engineid** command in EXEC mode.

show snmp engineid

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show snmp engineid** command to display the identification of the SNMP engine and all remote engines that have been configured on the router.

An SNMP engine is a copy of SNMP that can reside on a local device.

Task ID

Task ID	Operations
snmp	read

Examples

The following is sample output from the **show snmp engineid** command:

```
RP/0/RP0/CPU0:Router# show snmp engineid

Local SNMP engineID: 00000009020000000C025808
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.

show snmp group

To display the names of groups on the router, security model, status of the different views, and storage type of each group, use the **show snmp group** command in EXEC mode.

show snmp group

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
snmp	read

Examples

The following is sample output from the **show snmp group** command:

```
RP/0/RP0/CPU0:Router# show snmp group

groupname: public security model:snmpv1
readview : v1default writeview: -
notifyview: v1default
row status: nonVolatile

groupname: public security model:snmpv2c
readview : v1default writeview: -
```

```
notifyview: v1default
row status: nonVolatile
```

Table 87 describes the significant fields shown in the display.

Table 87 show snmp group Field Descriptions

Field	Definition
groupname:	Name of the Simple Network Management Protocol (SNMP) group, or collection of users that have a common access policy.
readview:	String identifying the read view of the group.
security model:	Security model used by the group, either v1, v2c, or v3.
writeview:	String identifying the write view of the group.
notifyview:	String identifying the notify view of the group.
row status:	Settings that are set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings remain after the device is turned off and on again.

Related Commands

Command	Description
snmp-server group	Configures an SNMP user group.

show snmp host

To display the configured Simple Network Management Protocol (SNMP) notification recipient host, User Datagram Protocol (UDP) port number, user, and security model, use the **show snmp host** command in EXEC mode.

show snmp host

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
snmp	read

Examples

The following is sample output from the **show snmp host** command:

```
RP/0/RP1/CPU0:Router(config)# show snmp host

Notification host: 10.50.32.170 udp-port: 2345 type: trap
user: userV3auth security model: v3 auth

Notification host: 10.50.32.170 udp-port: 2345 type: trap
user: userV3noauth security model: v3 noauth
```

```
Notification host: 10.50.32.170 udp-port: 2345 type: trap
user: userV3priv security model: v3 priv

Notification host: 10.50.32.170 udp-port: 2345 type: trap
user: userv2c security model: v2c
```

Table 88 describes the significant fields shown in the display.

Table 88 show snmp host Field Descriptions

Field	Definition
Notification host:	Name or IP address of target host.
udp-port:	UDP port number to which notifications are sent.
type:	Type of notification configured.
user:	Security level of the user.
security model:	Version of SNMP used to send the trap, either v1, v2c, or v3.

Related Commands

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

show snmp interface

To display the interface index identification numbers (ifIndex values) for all the interfaces or a specified interface, use the **show snmp interface** command in EXEC mode.

show snmp interface [*type interface-id* **ifindex**]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-id	(Optional) Identifies a physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
ifindex	(Optional) Displays the ifIndex value for the specifies interface.

Defaults

Enter the **show snmp interface** command without keywords or arguments to display the ifIndex value for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
snmp	read

Examples

The following example displays the ifIndex value for a specific interface:

```
RP/0/RP0/CPU0:Router# show snmp interface pos 0/1/0/1 ifindex
```

```
ifName : POS0/1/0/1            ifIndex : 12
```

The following example displays the ifIndex value for all interfaces:

```
RP/0/RP0/CPU0:Router# show snmp interface

ifName : Loopback0             ifIndex : 1
ifName : POS0/1/0/1            ifIndex : 12
ifName : POS0/1/4/2            ifIndex : 14
ifName : POS0/1/4/3            ifIndex : 15
ifName : POS0/6/0/1            ifIndex : 2
ifName : POS0/6/4/4            ifIndex : 18
ifName : POS0/6/4/5            ifIndex : 19
ifName : POS0/6/4/6            ifIndex : 20
ifName : Bundle-POS24          ifIndex : 4
ifName : Bundle-Ether28        ifIndex : 5
ifName : Bundle-Ether28.1      ifIndex : 7
ifName : Bundle-Ether28.2      ifIndex : 8
ifName : Bundle-Ether28.3      ifIndex : 9
ifName : MgmtEth0/RP0/CPU0/0   ifIndex : 6
ifName : MgmtEth0/RP1/CPU0/0   ifIndex : 10
ifName : GigabitEthernet0/1/5/0  ifIndex : 11
ifName : GigabitEthernet0/1/5/1  ifIndex : 13
ifName : GigabitEthernet0/1/5/2  ifIndex : 3
ifName : GigabitEthernet0/6/5/1  ifIndex : 16
ifName : GigabitEthernet0/6/5/2  ifIndex : 17
ifName : GigabitEthernet0/6/5/7  ifIndex : 21
```

Table 89 describes the significant fields shown in the display.

Table 89 show snmp interface Field Descriptions

Field	Definition
ifName:	Interface name.
ifIndex:	ifIndex value.

Related Commands

Command	Description
snmp-server ifindex persist	Enables ifIndex persistence globally on all SNMP interfaces,.
snmp-server interface	Enables an interface to send SNMP trap notifications and enter SNMP interface configuration mode.

show snmp mib

To display a list of MIB module object identifiers (OIDs) registered on the system, use the **show snmp mib** command in EXEC mode.

show snmp mib [*object-name* | **detailed** | **dll**]

Syntax Description

object-name	(Optional) Specific MIB object identifier or object name.
detailed	(Optional) Displays a list of all MIBs and corresponding dynamically loadable library (DLL) names on the system.
dll	(Optional) Displays a list of all MIB DLL filenames and the OID supported by each DLL filename on the system.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	Support was added for the *object-name* argument.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show snmp mib** command to display a list of the MIB module instance identifiers registered on the system.

Although the **show snmp mib** command can be used to display a list of MIB OIDs registered on the system, the use of a Network Management System (NMS) application is the recommended alternative for gathering this information.

The **show snmp mib** command is intended only for network managers who are familiar with Abstract Syntax Notation One (ASN.1) syntax, and the Structure of Management Information (SMI) of Open Systems Interconnection (OSI) Reference Model.

SNMP management information is viewed as a collection of managed objects, residing in a virtual information store, termed the MIB. Collections of related objects are defined in MIB modules. These modules are written using a subset of ASN.1, termed the SMI.

The definitions for the OIDs displayed by this command can be found in the relevant RFCs and MIB modules. For example, RFC 1907 defines the system.x, sysOREntry.x, snmp.x, and snmpTrap.x OIDs, and this information is supplemented by the extensions defined in the CISCO-SYSTEM-MIB.

Use the **detailed** keyword to display a list of the MIB module instance identifiers registered on the system. The output displays additional details, such as DLL and configuration information.

Use the **dll** keyword to display a list of the MIB modules loaded into the agent. This command can be used to find the supported MIBs.

Note This command produces a high volume of output if SNMP is enabled on the system. To exit from a --More-- prompt, press Crtl-Z.

Task ID

Task ID	Operations
snmp	read

Examples

The following is sample output from the **show snmp mib** command:

```
RP/0/RP0/CPU0:Router# show snmp mib

  1.3.6.1.2.1.47.1.1.1.1.2
  1.3.6.1.2.1.47.1.1.1.1.3
  1.3.6.1.2.1.47.1.1.1.1.4
  1.3.6.1.2.1.47.1.1.1.1.5
  1.3.6.1.2.1.47.1.1.1.1.6
  1.3.6.1.2.1.47.1.1.1.1.7
  1.3.6.1.2.1.47.1.1.1.1.8
  1.3.6.1.2.1.47.1.1.1.1.9
  1.3.6.1.2.1.47.1.1.1.1.10
  1.3.6.1.2.1.47.1.1.1.1.11
  1.3.6.1.2.1.47.1.1.1.1.12
  1.3.6.1.2.1.47.1.1.1.1.13
  1.3.6.1.2.1.47.1.1.1.1.14
  1.3.6.1.2.1.47.1.1.1.1.15
  1.3.6.1.2.1.47.1.1.1.1.16
  1.3.6.1.2.1.47.1.2.1.1.2
  1.3.6.1.2.1.47.1.2.1.1.3
  1.3.6.1.2.1.47.1.2.1.1.4
  1.3.6.1.2.1.47.1.2.1.1.5
  1.3.6.1.2.1.47.1.2.1.1.6
  1.3.6.1.2.1.47.1.2.1.1.7
  1.3.6.1.2.1.47.1.2.1.1.8
  1.3.6.1.2.1.47.1.3.1.1.1
 --More-
```

The following is sample output from the **show snmp mib detailed** command:

```
RP/0/RP0/CPU0:Router# show snmp mib detailed

Entitymib:dll=/pkg/lib/mib/libEntitymib.dll, config=Entity.mib, loaded
1.3.6.1.2.1.47.1.1.1.1.2
1.3.6.1.2.1.47.1.1.1.1.3
1.3.6.1.2.1.47.1.1.1.1.4
```

```
1.3.6.1.2.1.47.1.1.1.1.5
1.3.6.1.2.1.47.1.1.1.1.6
1.3.6.1.2.1.47.1.1.1.1.7
1.3.6.1.2.1.47.1.1.1.1.8
1.3.6.1.2.1.47.1.1.1.1.9
1.3.6.1.2.1.47.1.1.1.1.10
1.3.6.1.2.1.47.1.1.1.1.11
1.3.6.1.2.1.47.1.1.1.1.12
1.3.6.1.2.1.47.1.1.1.1.13
1.3.6.1.2.1.47.1.1.1.1.14
1.3.6.1.2.1.47.1.1.1.1.15
1.3.6.1.2.1.47.1.1.1.1.16
1.3.6.1.2.1.47.1.2.1.1.2
1.3.6.1.2.1.47.1.2.1.1.3
1.3.6.1.2.1.47.1.2.1.1.4
1.3.6.1.2.1.47.1.2.1.1.5
1.3.6.1.2.1.47.1.2.1.1.6
1.3.6.1.2.1.47.1.2.1.1.7
1.3.6.1.2.1.47.1.2.1.1.8
--More--
```

The following is sample output from the **show snmp mib dll** command:

```
RP/0/RP0/CPU0:Router# show snmp mib dll

Entitymib:dll=/pkg/lib/mib/libEntitymib.dll, config=Entity.mib, loaded
bgp4mib:dll=/pkg/lib/mib/libbgp4mib.dll, config=bgp4.mib, loaded
cdpmib:dll=/pkg/lib/mib/libcdpmib.dll, config=cdp.mib, loaded
ciscoprocessmib:dll=/pkg/lib/mib/libciscoprocessmib.dll, config=ciscoprocess.mi
b, loaded
ciscosyslogmib:dll=/pkg/lib/mib/libciscosyslogmib.dll, config=ciscosyslog.mib,
loaded
ciscosystemmib:dll=/pkg/lib/mib/libciscosystemmib.dll, config=ciscosystem.mib,
loaded
confcopymib:dll=/pkg/lib/mib/libconfcopymib.dll, config=confcopy.mib, loaded
configmanmib:dll=/pkg/lib/mib/libconfigmanmib.dll, config=configman.mib, loaded
dot3admib:dll=/pkg/lib/mib/libdot3admib.dll, config=dot3ad.mib, loaded
fabhfrmib:dll=/pkg/lib/mib/libfabhfrmib.dll, config=fabhfr.mib, loaded
fabmcastapplmib:dll=/pkg/lib/mib/libfabmcastapplmib.dll, config=fabmcastappl.mi
b, loaded
fabmcastmib:dll=/pkg/lib/mib/libfabmcastmib.dll, config=fabmcast.mib, loaded
flashmib:dll=/pkg/lib/mib/libflashmib.dll, config=flash.mib, loaded
hsrpmib:dll=/pkg/lib/mib/libhsrpmib.dll, config=hsrp.mib, loaded
icmpmib:dll=/pkg/lib/mib/libicmpmib.dll, config=icmp.mib, loaded
ifmib:dll=/pkg/lib/mib/libifmib.dll, config=if.mib, loaded
ipmib:dll=/pkg/lib/mib/libipmib.dll, config=ip.mib, loaded
mempoolmib:dll=/pkg/lib/mib/libmempoolmib.dll, config=mempool.mib, loaded
mplsldpmib:dll=/pkg/lib/mib/libmplsldpmib.dll, config=mplsldp.mib, loaded
.
.
.
```

Related Commands

Command	Description
show snmp	Displays the status of SNMP communications.

show snmp users

To display information about the configured characteristics of Simple Network Management Protocol (SNMP) users, use the **show snmp users** command in EXEC mode.

show snmp users

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

An SNMP user must be part of an SNMP group, as configured using the **snmp-server user** command.

Use the **show snmp users** command to display information about all configured users.

When configuring SNMP, you may see the logging message "Configuring snmpv3 USM user." USM stands for the User-Based Security Model (USM) for SNMP Version 3 (SNMPv3). For further information about USM, see RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

Task ID

Task ID	Operations
snmp	read

Examples

The following is sample output from the **show snmp users** command:

```
RP/0/RP0/CPU0:Router# show snmp users
```

```
User name:user1
Engine ID:localSnmpID
storage-type:nonvolatile active
```

Table 90 describes the significant fields shown in the display.

Table 90 show snmp users Field Descriptions

Field	Definition
User name:	String identifying the name of the SNMP user.
Engine ID:	String identifying the name of the copy of SNMP on the device.
storage-type:	Settings that are set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings remain after the device is turned off and on again.

Related Commands

Command	Description
snmp-server group	Configures an SNMP user group.
snmp-server user	Configures a new user to an SNMP group.

show snmp view

To display the configured views and the associated MIB view family name, storage type, and status, use the **show snmp view** command in EXEC mode.

show snmp view

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
snmp	read

Examples

The following is sample output from the **show snmp view** command:

```
RP/0/RP0/CPU0:Router# show snmp view

view1 1.3 - included nonVolatile active
v1default 1.3.6.1 - included nonVolatile active
```

Related Commands

Command	Description
snmp-server group	Configures an SNMP user group.
snmp-server user	Configures a new user to an SNMP group.

snmp-server chassis-id

To provide a message line identifying the Simple Network Management Protocol (SNMP) server serial number, use the **snmp-server chassis-id** command in global configuration mode. To restore the default value, if any, use the **no** form of this command.

snmp-server chassis-id *serial-number*

no snmp-server chassis-id

Syntax Description

serial-number	Unique identification string to identify the chassis serial number.

Defaults

On hardware platforms, where the serial number can be device read, the default is the serial number. For example, some Cisco devices have default chassis ID values of their serial numbers.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server chassis-id** command to provide a message line identifying the SNMP server serial number.

The chassis ID message can be displayed with the **show snmp** command.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to specify the chassis serial number 1234456:

```
RP/0/RP0/CPU0:Router(config)# snmp-server chassis-id 1234456
```

Related Commands

Command	Description
show snmp	Displays the status of SNMP communications.

snmp-server community

To configure the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

snmp-server community [**clear** | **encrypted**] *community-string* [**view** *view-name*] [**RO** | **RW**] [**SDROwner** | **SystemOwner**] [*access-list-name*]

no snmp-server community *community-string*

Syntax Description

clear	(Optional) Specifies that the entered *community-string* is clear text and should be encrypted when displayed by the **show running** command.
encrypted	(Optional) Specifies that the entered *community-string* is encrypted text and should be displayed as such by the **show running** command.
string	Community string that acts like a password and permits access to the SNMP protocol. If the **clear** keyword was used, *string* is assumed to be clear text. If the **encrypted** keyword was used, *string* is assumed to be encrypted. If neither was used, *string* is assumed to be clear text.
view *view-name*	(Optional) Specifies the name of a previously defined view. The view defines the objects available to the community.
RO	(Optional) Specifies read-only access. Authorized management stations are able only to retrieve MIB objects.
RW	(Optional) Specifies read-write access. Authorized management stations are able both to retrieve and to modify MIB objects.
SDROwner	(Optional) Limits access to the owner service domain router (SDR).
SystemOwner	(Optional) Provides system-wide access including access to all non-owner SDRs.
access-list-name	(Optional) Name of an access list of IP addresses allowed to use the community string to gain access to the SNMP agent.

Defaults

By default, an SNMP community string permits read-only access to all MIB objects.
By default, a community string is assigned to the SDR owner.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	The optional keywords **LROwner** and **SystemOwner** were added.
Release 3.4.0	No modification.

Release	Modification
Release 3.5.0	No modification.
Release 3.6.0	**LROwner** was changed to **SDROwner**. The **clear** and **encrypted** keywords were added.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server community** command to configure the community access string to permit access to SNMP.

To remove the specified community string, use the **no** form of this command.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

When the command **snmp-server community** is entered with the **SDROwner** keyword, SNMP access is granted only to the MIB object instances in the owner SDR.

When the command **snmp-server community** is entered with the **SystemOwner** keyword, SNMP access is granted to all SDRs in the system.

Note In a non-owner SDR, a community name provides access only to the object instances that belong to that SDR, regardless of the access privilege assigned to the community name. Access to the owner SDR and system-wide access privileges are available only from the owner SDR.

Note Secure domain routers (SDRs) were previously known as logical routers (LRs). The name was changed as of Cisco IOS XR Release 3.3.0.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to assign the string comaccess to SNMP, allowing read-only access, and to specify that IP access list 4 can use the community string:

```
RP/0/RP0/CPU0:Router(config)# snmp-server community comaccess ro 4
```

The following example shows how to assign the string mgr to SNMP, allowing read-write access to the objects in the restricted view:

```
RP/0/RP0/CPU0:Router(config)# snmp-server community mgr view restricted rw
```

The following example shows how to remove the community comaccess:

```
RP/0/RP0/CPU0:Router(config)# no snmp-server community comaccess
```

Related Commands

Command	Description
snmp-server view	Creates or updates a view entry.

snmp-server community-map

To associate a Simple Network Management Protocol (SNMP) community with an SNMP context, security name, or a target-list use the **snmp-server community-map** command in global configuration mode. To change an SNMP community mapping to its default mapping, use the **no** form of this command.

snmp-server community-map [**clear** | **encrypted**] *community-string* [**context** *context-name*] [**security-name** *security-name*] [**target-list** *target*]

no snmp-server community-map [**clear** | **encrypted**] *community-string*

Syntax Description

clear	(Optional) Specifies that the *community-string* argument is clear text.
encrypted	(Optional) Specifies that the *community-string* argument is encrypted text.
community-name	Name of the community.
context *context-name*	Name of the SNMP context to which this community name is to be mapped.
security-name *security-name*	Security name for this community. By default, the *community-name* is the security name.
target-list *target*	Name of the target list for this community.

Defaults

The value of the *community-string* argument is also the security name.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server community-map** command to map an SNMPv1 or SNMPv2c community name to one or more of the following:

- **context name**: Maps a community name to a specific SNMP context name. This allows MIB instances in an SNMP context to be accessed through SNMPv1 or SNMPv2c using this community name.

- **security name**: By default, the community name is used to authenticate SNMPv1 and SNMPv2c. Configure a security name for a community name to override the default and authenticate SNMP with the security name.
- **target**: Target list identifies a list of valid hosts from which SNMP access can be made using a specific security name. When such mapping is done for a particular community name, SNMP access is allowed only from hosts included in the target list.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example maps the community name “sample 2” to the SNMP context name “sample1:”

```
RP/0/RP0/CPU0:Router(config)# snmp-server community-map sample2 context sample1
```

Related Commands

Command	Description
snmp-server context	Creates an SNMP context.
snmp-server target list	Creates an SNMP target list.

snmp-server contact

To set the Simple Network Management Protocol (SNMP) system contact, use the **snmp-server contact** command in global configuration mode. To remove the system contact information, use the **no** form of this command.

snmp-server contact *system-contact-string*

no snmp-server contact

Syntax Description

system-contact-string	String that describes the system contact information. The maximum string length is 255 alphanumeric characters.

Defaults

No system contact is set.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server contact** command to set the system contact string. Use the **no** form of this command to remove the system contact information.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to specify a system contact string:

```
RP/0/RP0/CPU0:Router(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Related Commands

Command	Description
snmp-server location	Sets the system location string.

snmp-server context

To create a Simple Network Management Protocol (SNMP) context, use the **snmp-server context** command in global configuration mode. To remove an SNMP context, use the **no** form of this command.

snmp-server context *context-name*

no snmp-server context *context-name*

Syntax Description

context-name	Name of the SNMP context.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This command creates an SNMP context. By default all the SNMP MIB instances are in a default context. Create an SNMP context and map it to a particular feature to enable similar instances of the same object to co-exist in different SNMP contexts.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example creates a new SNMP context named “sample1:”

```
RP/0/RP0/CPU0:Router(config)# snmp-server context sample1
```

Related Commands

Command	Description
snmp-server community-map	Associates an SNMP community with an SNMP context, security name, or a target list.
snmp-server vrf	Configures the VRF properties of SNMP.

snmp-server engineid

To specify Simple Network Management Protocol (SNMP) engine ID on the local device, use the **snmp-server engineid local** command in global configuration mode. To return the engine ID to the default, use the **no** form of this command.

snmp-server engineid local *engine-id*

no snmp-server engineid local *engine-id*

Syntax Description

engine-id	Character string that identifies the engine ID. Consists of up to 24 characters in hexadecimal format. Each hexidecimal number is separated by a colon (**:**).

Defaults

An SNMP engine ID is generated automatically.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to configure the SNMP engine ID on the local device:

```
RP/0/RP0/CPU0:Router(config)# snmp-server engineID local
00:00:00:09:00:00:00:a1:61:6c:20:61
```

Related Commands

Command	Description
show snmp engineid	Displays information about the local SNMP engine.

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *view*] [**write** *view*] [**notify** *view*] [**context** *context-name*] [*access-list-name*]

no snmp-server group *name*

Syntax Description

name	Name of the group.
v1	Specifies a group that uses the SNMPv1 security model. The SNMP v1 security model is the least secure of the possible security models.
v2c	Specifies a group that uses the SNMPv2c security model. The SNMPv2c security model is the second least secure of the possible security models.
v3	Specifies a group that uses the SNMPv3 security model. The SNMP v3 security is the most secure of the possible security models.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read *view*	(Optional) Specifies a read view string (not to exceed 64 characters) that is the name of the view that allows only the contents of the agent to be viewed.
write *view*	(Optional) Specifies a write view string (not to exceed 64 characters) that is the name of the view used to enter data and configure the contents of the agent.
notify *view*	(Optional) Specifies a notify view string (not to exceed 64 characters) that is the name of the view used to specify a notify or trap.
context *context-name*	(Optional) Specifies the SNMP context to associate with this SNMP group and associated views.
access-list-name	(Optional) Access list string (not to exceed 64 characters) that is the name of the access list.

Defaults

See Table 91 in the “Usage Guidelines” section.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The **access** keyword was removed.

Release	Modification
Release 3.3.0	Support was added for the **context** *context-name* keyword and argument.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Table 91 describes the default values for the different views.

Table 91 snmp-server group Default Descriptions

Default	Definition
read *view*	Assumed to be every object belonging to the Internet (1.3.6.1) object identifier (OID) space, unless the user uses the **read** option to override this state.
write *view*	Nothing is defined for the write view (that is, the null OID). You must configure write access.
notify *view*	Nothing is defined for the notify view (that is, the null OID). If a view is specified, any notifications in that view that are generated are sent to all users associated with the group (provided an SNMP server host configuration exists for the user).

Configuring Notify Views

Do not specify a notify view when configuring an SNMP group for the following reasons:

- The **snmp-server host** command autogenerates a notify view for the user, and then adds it to the group associated with that user.
- Modifying the notify view of the group affects all users associated with that group.

The **notify** *view* option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
- The **snmp-server host** command may have been configured before the **snmp-server group** command. In this case, reconfigure the **snmp-server host** command or specify the appropriate notify view.

Instead of specifying the notify view for a group as part of the **snmp-server group** command, use the following commands in global configuration mode:

- **snmp-server user**: Configures an SNMP user.
- **snmp-server group**: Configures an SNMP group, without adding a notify view.
- **snmp-server host**: Autogenerates the notify view by specifying the recipient of a trap operation.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when this command is configured. In addition, no default passwords exist. The minimum length for a password is one character, although we recommend using eight characters for security. A plain-text password or localized Message Digest 5 (MD5) password can be specified. Forgotten passwords cannot be recovered, and the user must be reconfigured.

SNMP Contexts

SNMP contexts provide Virtual Private Network (VPN) users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to configure an SNMP version 3 group named group1 that requires the authentication of packets with encryption:

```
RP/0/RP0/CPU0:Router(config)# snmp-server group group1 v3 priv
```

Related Commands

Command	Description
show snmp	Displays the status of SNMP communications.
show snmp group	Displays information about each SNMP group on the network.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server view	Creates or updates a view entry.

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, use the **no** form of this command.

snmp-server host *address* [**clear** | **encrypted**] [**traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [**udp-port** *port*] [*notification-type*]

no snmp-server host *address* [**clear** | **encrypted**] [**traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [**udp-port** *port*] [*notification-type*]

Syntax Description

address	Name or IP address of the host (the targeted recipient).
clear	(Optional) Specifies that the *community-string* argument is clear text.
encrypted	(Optional) Specifies that the *community-string* argument is encrypted text.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
version {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}	(Optional) Specifies the version of the SNMP used to send the traps. The default is SNMPv1. Version 3 is the most secure model, because it allows packet encryption with the **priv** keyword. When the **version** keyword is used, one of the following keywords must be specified: • **1**—Specifies SNMPv1. • **2c**—Specifies SNMPv2C. • **3**—Specifies SNMPv3. If you specify the SNMPv3 **3** optional keyword, you must specify the security level using one of the following required keywords: – **auth**—Enables Message Digest 5 (MD5) algorithm 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"). If you do specify a security level, the default is **noauth**.
community-string	Password-like community string sent with the notification operation. We recommend defining this string using the **snmp-server community** command prior to using the **snmp-server host** command.

udp-port *port*	(Optional) Specifies the User Datagram Protocol (UDP) port of the host to use. Range is from 1 to 65535. The default UDP port is 161.
notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. The notification type can be one or more of the following keywords: • **bgp**—Enables SNMP Border Gateway Protocol Version 4 (BGPv4) traps. • **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. • **copy-complete**—Enables CISCO-CONFIG-COPY-MIB ccCopyCompletion traps. • **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. • **fabric**—Enables SNMP fabric traps. • **fru-ctrl**—Enables SNMP entity field-replaceable unit (FRU) control traps. • **mpls**—Enables SNMP Multiprotocol Label Switching (MPLS) traps. • **sensor**—Enables SNMP entity sensor traps. • **snmp**—Enables SNMP traps. • **syslog**—Controls error message notifications (Cisco-syslog-MIB). Specify the level of messages to be sent with the **logging history** command.

Defaults

This command is disabled by default. No notifications are sent.
The default UDP port is 161.
When this command is entered without keywords, the default is to send all trap types to the host.
If no version keyword is entered, the default is version 1.
If version 3 is specified, but the security level is not specified, the default security level is noauth.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

SNMP notifications can be sent as traps. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. Traps are discarded as soon as they are sent. Traps are also sent only once.

When the **snmp-server host** command is not entered, no notifications are sent. To configure the device to send SNMP notifications, configure at least one **snmp-server host** command. When the command is entered without keywords, all trap types are enabled for the host.

To enable multiple hosts, 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), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if an **snmp-server host** command with the **traps** keyword is entered for a host and then another **snmp-server host** command with the **traps** keyword is entered for the same host, the second command replaces the first.

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

However, some notification types cannot be controlled with the **snmp-server traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The availability of a notification-type depends on the device type and Cisco software features supported on the device.

To display which notification types are available on the system, use the question mark (**?**) online help function at the end of the **snmp-server host** command.

The **no snmp-server host** *command used with no keywords disables traps.*

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

Task ID

Task ID	Operations
snmp	read, write

Examples

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

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP traps to address 172.30.2.160:

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps snmp
RP/0/RP0/CPU0:Router(config)# snmp-server host 172.30.2.160 public snmp
```

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

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com public
```

The following example shows how to prevent traps from being sent to any host. The BGP traps are enabled for all hosts, but only the configuration traps are enabled to be sent to a host.

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps bgp
RP/0/RP0/CPU0:Router(config)# snmp-server host hostabc public config
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps bgp	Enables BGP state-change SNMP notifications.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server ifindex persist

To enable ifIndex persistence globally on all Simple Network Management Protocol (SNMP) interfaces, use the **snmp-server ifindex persist** command in global configuration mode. To disable global interface persistence, use the **no** form of this command.

snmp-server ifindex persist

no snmp-server ifindex persist

Syntax Description

This command has no arguments or keywords.

Defaults

Global interface persistence is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server ifindex persist** command to enable ifIndex persistence on all interfaces that have entries in the ifIndex table of the IF-MIB. When enabled, this command retains the mapping between the ifName object values and the ifIndex object values (generated from the IF-MIB) persistent during reloads, allowing for consistent identification of specific interfaces using SNMP. Applications such as device inventory, billing, and fault detection depend on this feature.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable ifIndex persistence globally:

```
RP/0/RP0/CPU0:Router(config)# snmp-server ifindex persist
```

Related Commands

Command	Description
index persistence	Enables ifIndex persistence for an SNMP interface.
notification linkupdown disable	Disables linkUp and linkDown notifications for an SNMP interface.
show snmp interface	Displays the ifIndex value for an SNMP interface.

snmp-server ifmib ifalias long

To enable the ifAlias IF-MIB object to accept an interface alias name that exceeds the 64-byte default, use the **snmp-server ifmib ifalias long** command. Use the **no** form of this command to revert to the default length.

snmp-server ifmib ifalias long

no snmp-server ifmib ifalias long

Syntax Description

This command has no arguments or keywords.

Defaults

Global interface persistence is disabled.
The alias name is 64 bytes in length.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server ifmib ifalias long** command to enable the IF-MIB object ifAlias to accept an interface alias name that is greater than 64 bytes in length. The default length for the alias name is 64 bytes.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable the IF-MIB object ifAlias:

```
RP/0/RP0/CPU0:Router(config)# snmp-server ifmib ifalias long
```

```
RP/0/RP0/CPU0:Router(config)# exit
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes
RP/0/RP0/CPU0:Router#
```

snmp-server ifmib stats cache

To enable retrieval of cached statistics instead of real-time statistics, use the **snmp-server ifmib stats cache** command. To revert to the default, use the **no** form of this command.

snmp-server ifmib stats cache

no snmp-server ifmib stats cache

Syntax Description

This command has no arguments or keywords.

Defaults

Cached statistics are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	This command was not supported.
Release 3.5.0	This command was supported on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Cisco IOS XR statistics infrastructure maintains a cache of statistics for all interfaces. This cache is updated every 30 seconds. Use the **snmp-server ifmib stats cache** command to enable the IF-MIB to retrieve these cached statistics rather than real-time statistics. Accessing cached statistics is less CPU-intensive than accessing real-time statistics.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable the IF-MIB caches statistics:

```
RP/0/RP0/CPU0:Router(config)# snmp-server ifmib stats cache
RP/0/RP0/CPU0:Router(config)# exit
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes
RP/0/RP0/CPU0:Router#
```

snmp-server interface

To enable an interface to send Simple Network Management Protocol (SNMP) trap notifications and enter SNMP interface configuration mode, use the **snmp-server interface** command in global configuration mode. To disable the sending of SNMP trap notifications on an interface, use the **no** form of this command.

snmp-server interface *interface-type interface-id*

no snmp-server interface *interface-type interface-id*

Syntax Description

interface-type	Interface type. For more information, use the question mark (**?**) online help function.
interface-id	Either a physical or virtual interface identifier as follows: • Physical interface identifier. Naming notation is *rack*/*slot*/*module*/*port* and a slash between values is required as part of the notation. – *rack*: Chassis number of the rack. – *slot*: Physical slot number of the modular services card or line card. – *module*: Module number. A physical layer interface module (PLIM) is always 0. – *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. • Virtual interface identifier. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (**?**) online help function.

Defaults

Ethernet interfaces are enabled to send SNMP trap notifications. SNMP trap notifications are disabled on all other physical and logical interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The **ifindex**, **clear**, **persist**, **enable**, and **trap link-status** keywords were removed.

Release	Modification
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **snmp-server interface** command enters SNMP interface configuration mode for you to configure the available SNMP options.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to assign ifIndex persistence on Packet-over-SONET/SDH (POS) interface 0/0/1/0:

```
RP/0/RP0/CPU0:Router(config)# snmp-server interface pos 0/0/1/0
RP/0/RP0/CPU0:Router(config-snmp-if)#
```

Related Commands

Command	Description
show snmp interface	Displays the ifIndex value for an SNMP interface.
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server ifindex persist	Enables ifIndex persistence globally for all SNMP interfaces.

snmp-server ipv4 dscp

To mark packets with a specific differentiated services code point (DSCP) value, use the **snmp-server ipv4 dscp** command in global configuration mode. To remove matching criteria, use the **no** form of this command.

snmp-server ipv4 dscp *value*

no snmp-server ipv4 dscp [*value*]

Syntax Description

value	Value of the DSCP. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **default**, **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, or **cs7**.

Defaults

The IP DSCP default value for SNMP traffic is 0.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server ipv4 dscp** command to specify an IP DSCP value to give SNMP traffic higher or lower priority in your network.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to configure the DSCP value to af32:

```
RP/0/RP0/CPU0:router(config)# snmp-server ipv4 dscp af32
```

snmp-server ipv4 precedence

To mark packets with a specific precedence level to use for packet matching, use the **snmp-server ipv4 precedence** command in global configuration mode. To restore the system to its default interval values, use the **no** form of this command.

snmp-server ipv4 precedence *value*

no snmp-server ipv4 precedence [*value*]

Syntax Description

value	Value of the precedence. The precedence value can be a number from 0 to 7, or it can be one of the following keywords: • **critical**—Set packets with critical precedence (5) • **flash**— Set packets with flash precedence (3) • **flash-override**—Set packets with flash override precedence (4) • **immediate**—Set packets with immediate precedence (2) • **internet**—Set packets with internetwork control precedence (6) • **network**—Set packets with network control precedence (7) • **priority**—Set packets with priority precedence (1) • **routine**—Set packets with routine precedence (0)

Defaults

The IP Precedence default value for SNMP traffic is 0.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.6.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server ipv4 precedence** command to specify an IP Precedence value to give SNMP traffic higher or lower priority in your network.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to set the precedence to 2:

```
RP/0/RP0/CPU0:router(config)# snmp-server ipv4 precedence 2
```

snmp-server location

To specify the system location for Simple Network Management Protocol (SNMP), use the **snmp-server location** command in global configuration mode. To remove the location string, use the **no** form of this command.

snmp-server location *system-location*

no snmp-server location

Syntax Description

system-location	String indicating the physical location of this device. The maximum string length is 255 alphanumeric characters.

Defaults

No system location string is set.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to specify a system location string:

```
RP/0/RP0/CPU0:Router(config)# snmp-server location Building 3/Room 214
```

Related Commands

Command	Description
snmp-server contact	Sets the system contact string.

snmp-server notification-log-mib

To configure the NOTIFICATION-LOG-MIB, use the **snmp-server notification-log-mib** command in global configuration mode. To remove the specified configuration, use the **no** form of this command.

snmp-server notification-log-mib {**globalAgeOut** *time* | **globalSize** *size* | **default** | **disable** | **size** *size*}

no snmp-server notification-log-mib {**globalAgeOut** | **globalSize** | **default** | **disable** | **size**}

Syntax Description

globalAgeOut *time*	Specifies how much time, in minutes, a notification remains in the log. Values for *minutes* can range from 0 to 4294967295.
globalSize *size*	Specifies the maximum number of notifications that can be logged in all logs.
default	Specifies to create a default log.
disable	Specifies to disable logging to the default log.
size *size*	Specifies the maximum number of notifications that the default log can hold.

Defaults

globalAgeOut *time*: 15
globalSize *size*: 500
size *size*: 500

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Logging of NOTIFICATION-LOG-MIB notifications begins when the default log is created. Named logs are not supported, therefore only the default log can be created.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example creates a default log for notifications:

```
RP/0/RP0/CPU0:Router(config)# snmp-server notification-log-mib default
```

The following example removes the default log:

```
RP/0/RP0/CPU0:Router(config)# no snmp-server notification-log-mib default
```

The following example configures the size of all logs to be 1500:

```
RP/0/RP0/CPU0:Router(config)# snmp-server notification-log-mib globalSize 1500
```

Related Commands

Command	Description
snmp-server community-map	Associates an SNMP community with an SNMP context, security name, or target list.

snmp-server packetsize

To establish control over the largest Simple Network Management Protocol (SNMP) packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp-server packetsize *size*

no snmp-server packetsize

Syntax Description

size	Packet size in bytes. Range is from 484 to 65500.

Defaults

size: 1500

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server packetsize** command to establish control over the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.

Task ID

Task ID	Operations
snmp	read, write

Examples

```
The following example shows how to set the maximum size of SNMP packets to 1024 bytes:

RP/0/RP0/CPU0:Router(config)# snmp-server packetsize 1024
```

snmp-server queue-length

To establish the message queue length for each trap host for Simple Network Management Protocol (SNMP), use the **snmp-server queue-length** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp-server queue-length *length*

no snmp-server queue-length

Syntax Description

length	Integer that specifies the number of trap events that can be held before the queue must be emptied. Range is from 1 to 1000.

Defaults

length: 10

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server queue-length** command to define the length of the message queue for each trap host. After a trap message is successfully sent, the Cisco IOS XR software continues to empty the queue at a throttled rate to prevent trap flooding.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to set the SNMP notification queue to 20 events:

```
RP/0/RP0/CPU0:Router(config)# snmp-server queue-length 20
```

snmp-server target list

To create an Simple Network Management Protocol (SNMP) target list, use the **snmp-server target list** command in global configuration mode. To remove a target list, use the **no** form of this command.

snmp-server target list *target-list* {**vrf** *vrf-name* | **host** *hostname*}

no snmp-server target list *target-list*

Syntax Description

target-list	Name of the target list.
vrf *vrf-name*	Specifies the name of the VRF hosts included in the target list.
host *hostname*	Assigns a hostname to the target list. The *hostname* variable is a name or IPv4 address.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use this command to create an SNMP target list and assign hosts to the list. When a target list is mapped to a community name using the **snmp-server community-map** command, SNMP access is restricted to the hosts in the target list (for that community name).

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example, a new target list “sample3” is created, and assigned to the vrf server “server2”:

```
RP/0/RP0/CPU0:Router(config)# snmp-server target list sample3 vrf server2
```

Related Commands

Command	Description
snmp-server community-map	Associates an SNMP community with an SNMP context, security name, or a target list.

snmp-server throttle-time

To specify the throttle time for handling incoming Simple Network Management Protocol (SNMP) messages, use the **snmp-server throttle-time** command in global configuration mode. To restore the throttle time to its default value, use the **no** form of this command.

snmp-server throttle-time *time*

no snmp-server throttle-time

Syntax Description

time	Throttle time for the incoming queue in msec. Values can be from 50 to 1000 msec.

Defaults

time: 0

Command Modes

Global configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
snmp	read, write

Examples

In the following example, the throttle time is set to 500 msec:

```
RP/0/RP0/CPU0:Router(config)# snmp-server throttle-time 500
```

Related Commands

Command	Description
snmp-server community-map	Associates an SNMP community with an SNMP context, security name, or target list.

snmp-server trap link ietf

To enable the varbind used for linkUp and linkDown SNMP traps to utilize the RFC 2863 standard varbind, use the **snmp-server trap link ietf** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp-server trap link ietf

no snmp-server trap link ietf

Syntax Description

This command has no arguments or keywords.

Defaults

The default varbind used is cisco.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

For more information about linkUP and linkDown notifications, see RFC 2863, *The Interface Group MIB*, and RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable the RFC 2863 standard varbind:

```
RP/0/RP0/CPU0:Router(config)# snmp-server trap link ietf
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps bgp	Enables BGP state-change SNMP notifications.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server traps

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

snmp-server traps [*notification-type*]

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

Syntax Description

notification-type (Optional) Type of notification (trap) to enable or disable. If no type is specified, all notifications available on the device are enabled or disabled.

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

- **bgp**—Enables BGP4-MIB and CISCO-BGP4-MIB traps.
- **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.
- **copy-complete**—Enables CISCO-CONFIG-COPY-MIB ccCopyCompletion traps.
- **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.
- **fabric bundle**—Enables SNMP fabric bundle traps.
- **fabric plane**—Enables SNMP fabric plane state-change traps.
- **flash insertion**—Enable ciscoFlashDeviceInsertedNotif.
- **flash removal**—Enable ciscoFlashDeviceRemovedNotif.
- **fru-ctrl**—Enables SNMP entity field replaceable unit (FRU) control traps.
- **hsrp**—Enables SNMP HSRP traps.
- **ipsec tunnel start**—Enables SNMP IPSec tunnel start traps.
- **ipsec tunnel stop**—Enables SNMP IPSec tunnel stop traps.
- **isakmp**—Enables ISAKMP traps.
- **l2vpn all**—Enables all Layer 2 VPN traps.
- **l2vpn vc-down**—Enables Layer 2 VPN VC down traps.
- **l2vpn vc-up**—Enables Layer 2 VPN VC up traps.
- **mpls frr all**—Enables all MPLS fast reroute MIB traps.
- **mpls frr protected**—Enables MPLS fast reroute tunnel protected traps.
- **mpls ldp**—Enables SNMP Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) traps.
- **mpls traffic-eng**—Enables SNMP MPLS traffic engineering traps.
- **msdp peer-state-change**—Enables SNMP MSDP Peer state change trap.
- **ntp**—Enables SNMP Cisco NTP traps.

- **pim**—Enables SNMP PIM traps.
- **rf**—Enables RF-MIB traps.
- **sbc-dbl**—Enables SNMP SBC dynamic blacklist traps.
- **sbc-mgm**—Enables SNMP SBC Media Gateway Manager (MGM) traps.
- **sensor**—Enables SNMP entity sensor traps.
- **snmp**—Enables SNMP traps.
- **sonet**—Enables SONET traps.
- **syslog**—Controls error message notifications (Cisco-syslog-MIB). Specify the level of messages to be sent with the **logging history** command.
- **vpls**—Enables virtual private LAN service (VPLS) traps.

Note To display the trap notifications supported on a platform, use the online help (**?**) function.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The **enable** keyword was removed from the command name.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	The **flash**, **ipsec**, **l2vpn**, and **mpls** traps were introduced.
Release 3.6.0	The RF-MIB trap was introduced.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server traps** command to enable trap requests for the specified notification types. To configure the router to send SNMP notifications, specify at least one **snmp-server traps** command. When the command is entered with no keyword, all notification types are enabled. When a notification type keyword is specified, only the notification type related to that keyword is enabled. To enable multiple types of notifications, issue a separate **snmp-server traps** command for each notification type.

More information about individual MIBs can be found in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

Some SNMP trap notifications require additional Task IDs as indicated in the following table:

Notification Type	Task ID	Operations
bgp	bgp	read, write
copy-complete	config-services	read, write
ipsec	crypto	read, write
isakmp	crypto	read, write
l2vpn	l2vpn	read, write
mpls frr	mpls-ldp	read, write
	mpls-te	read, write
mpls l3vpn	ipv4	read, write
	mpls-ldp	read, write
	mpls-te	read, write
mpls ldp	mpls-ldp	read, write
	mpls-te	read, write
mpls traffic-eng	mpls-ldp	read, write
	mpls-te	read, write
ospf	ospf	read, write
syslog	sysmgr	read, write
vpls	l2vpn	read, write

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:

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps bgp	Enables BGP server state-change SNMP notifications.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server traps bgp

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

snmp-server traps bgp

no snmp-server traps bgp

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The **enable** keyword was removed from the command name.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

SNMP notifications can be sent as traps.

Use the **snmp-server traps bgp** command to enable or disable BGP server state-change notifications, as defined in the BGP4-MIB (enterprise 1.3.6.1.2.1.15.7). The notifications types are:

- bgpEstablished
- bgpBackwardTransition

The BGP notifications are defined in the BGP-4 MIB as follows:

```
bgpTraps                OBJECT IDENTIFIER ::= { bgp 7 }

bgpEstablished NOTIFICATION-TYPE
    OBJECTS { bgpPeerLastError,
    bgpPeerState      }
```

```
    STATUS  current
    DESCRIPTION
    "The BGP Established event is generated when the BGP FSM enters the ESTABLISHED
    state."
    ::= { bgpTraps 1 }

bgpBackwardTransition NOTIFICATION-TYPE
    OBJECTS { bgpPeerLastError,
        bgpPeerState      }
    STATUS  current
    DESCRIPTION
    "The BGPBackwardTransition Event is generated when the BGP FSM moves from a higher
    numbered state to a lower numbered state."
    ::= {bgpTraps 2}
```

For a complete description of these notifications and additional MIB functions, see the BGP4-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps bgp** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write
bgp	read, write

Examples

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

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps bgp
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server traps mpls l3vpn

To enable the sending of MPLS Layer 3 VPN Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps mpls l3vpn** command in global configuration mode. To disable MPLS Layer 3 VPN SNMP notifications, use the **no** form of this command.

snmp-server traps mpls l3vpn {**all** | **max-threshold-cleared** | **max-threshold-exceeded** | **max-threshold-reissue-notif-time** | **mid-threshold-exceeded** | **vrf-down** | **vrf-up**}

no snmp-server traps mpls l3vpn

Syntax Description

all	Enables all MPLS Layer 3 VPN traps.
max-threshold-cleared	Enables maximum threshold cleared traps.
max-threshold-exceeded	Enables maximum threshold exceeded traps.
max-threshold-reissue-notif-time *seconds*	Specifies the time interval, in seconds, for reissuing a maximum threshold notification.
mid-threshold-exceeded	Enables mid-threshold exceeded traps.
vrf-down	Enables VRF down traps.
vrf-up	Enables VRF up traps.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable the device to send MPLS Layer 3 VPN traps:

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps mpls l3vpn all
```

Related Commands

Command	Description
snmp-server traps	Enables SNMP trap notifications.

snmp-server traps ospf errors

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

snmp-server traps ospf errors {**authentication-failure** | **bad-packet** | **config-error** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error**}

no snmp-server traps ospf errors {**authentication-failure** | **bad-packet** | **config-error** | **virt-authentication-failure** | **virt-bad-packet** | **virt-config-error**}

Syntax Description

authentication-failure	Enables SNMP traps for authentication failure errors on physical interfaces.
bad-packet	Enables SNMP traps for bad packet errors on physical interfaces.
config-error	Enables SNMP traps for configuration errors on physical interfaces.
virt-authentication-failure	Enables SNMP traps for authentication failure errors on virtual interfaces.
virt-bad-packet	Enables SNMP traps for bad packet errors on virtual interfaces.
virt-config-error	Enables SNMP traps for configuration errors on virtual interfaces.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.1	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

SNMP notifications can be sent as traps.

For a complete description of OSPF error notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf errors** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

Examples

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

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps ospf errors
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server traps ospf lsa

To enable Open Shortest Path First (OSPF) link-state advertisement Simple Network Management Protocol (SNMP) notifications, use the **snmp-server traps ospf lsa** command in global configuration mode. To disable OSPF link state SNMP notifications, use the **no** form of this command.

snmp-server traps ospf lsa {**lsa-maxage** | **lsa-originate**}

no snmp-server traps ospf lsa {**lsa-maxage** | **lsa-originate**}

Syntax Description

lsa-maxage	Enables SNMP traps for link-state advertisement maxage.
lsa-originate	Enables SNMP traps for new link-state advertisement origination.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.1	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

SNMP notifications can be sent as traps.

For a complete description of OSPF link-state advertisement notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf lsa** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable the router to send OSPF link-state advertisement notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps ospf lsa lsa-maxage
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server traps ospf retransmit

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

snmp-server traps ospf retransmit {**packets** | **virt-packets**}

no snmp-server traps ospf retransmit {**packets** | **virt-packets**}

Syntax Description

packets	Enables SNMP traps for packet retransmissions on physical interfaces.
virt-packets	Enables SNMP traps for packet retransmissions on virtual interfaces.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.1	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

SNMP notifications can be sent as traps.

For a complete description of OSPF retransmission notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf retransmit** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

Examples

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

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps ospf retransmit packets
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server traps ospf state-change neighbor-state-change

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

snmp-server traps ospf state-change neighbor-state-change

no snmp-server traps ospf state-change neighbor-state-change

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.1	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

SNMP notifications can be sent as traps.

Use the **snmp-server traps ospf state-change neighbor-state-change** command to enable or disable OSPF server state-change notifications, as defined in the MIB. One notification types is:

- ospfNbrStateChange

For example, the OSPF ospfNbrStateChange notification is defined in the OSPF MIB as follows:

```
!     ospfNbrStateChange NOTIFICATION-TYPE
!         OBJECTS {
!                     ospfRouterId, -- The originator of the trap
!                     ospfNbrIpAddr,
!                     ospfNbrAddressLessIndex,
!                     ospfNbrRtrId,
!                     ospfNbrState  -- The new state
!                   }
!         STATUS             current
```

For a complete description of these notifications and additional MIB functions, see the OSPF-TRAP-MIB in the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

The **snmp-server traps ospf state-change neighbor-state-change** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

Examples

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

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps ospf state-change neighbor-state-change
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server traps pim interface-state-change

To enable Protocol Independent Multicast (PIM) interface status notification, use the **snmp-server traps pim interface-state-change** command in global configuration mode. To disable this command so no notification is sent, use the **no** form of this command.

snmp-server traps pim interface-state-change

no snmp-server traps pim interface-state-change

Syntax Description

This command has no arguments or keywords.

Defaults

Simple Network Management Protocol (SNMP) notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Use the **snmp-server traps pim interface-state-change** command to send notifications when a PIM interface changes status from up to down. When the status is up, the notification signifies the restoration of a PIM interface. When the status is down, the notification signifies the loss of a PIM interface.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to use the **snmp-server traps pim interface-state-change** command:

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps pim interface-state-change
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps pim invalid-message-received	Enables notifications for monitoring invalid PIM protocol operations.
snmp-server traps pim neighbor-change	Enables PIM neighbor status down notifications.
snmp-server traps pim rp-mapping-change	Enables notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notification for Cisco-syslog-MIB error messages.

snmp-server traps pim invalid-message-received

To enable notifications for monitoring invalid Protocol Independent Multicast (PIM) protocol operations, such as invalid register received and invalid join or prune received, use the **snmp-server traps pim invalid-message-received** command in global configuration mode. To disable this command so that no notification is sent, use the **no** form of this command.

snmp-server traps pim invalid-message-received

no snmp-server traps pim invalid-message-received

Syntax Description

This command has no arguments or keywords.

Defaults

Simple Network Management Protocol (SNMP) notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

A router can receive a join or prune message in which the RP specified in the packet is not the RP for the multicast group. Or a router can receive a register message from a multicast group in which it is not the RP.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to use the **snmp-server traps pim invalid-message-received** command:

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps pim invalid-message-received
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps pim interface-state-change	Enables PIM interface status notification.
snmp-server traps pim neighbor-change	Enables PIM neighbor status down notifications.
snmp-server traps pim rp-mapping-change	Enables notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notification for Cisco-syslog-MIB error messages.

snmp-server traps pim neighbor-change

To enable Protocol Independent Multicast (PIM) neighbor status down notifications, use the **snmp-server traps pim neighbor-change** command in global configuration mode. To disable PIM neighbor down notifications, use the **no** form of this command.

snmp-server traps pim neighbor-change

no snmp-server traps pim neighbor-change

Syntax Description

This command has no arguments or keywords.

Defaults

PIM Simple Network Management Protocol (SNMP) notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server traps pim neighbor-change** command to send notifications when a PIM neighbor changes status from up to down on an interface. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

Examples

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

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps pim neighbor-change
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps pim interface-state-change	Enables PIM interface status notification.
snmp-server traps pim invalid-message-received	Enables notifications for monitoring invalid PIM protocol operations.
snmp-server traps pim rp-mapping-change	Enables notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server traps pim rp-mapping-change

To enable notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages, use the **snmp-server traps pim rp-mapping-change** command in global configuration mode. To disable this command so no notification is sent, use the **no** form of this command.

snmp-server traps pim rp-mapping-change

no snmp-server traps pim rp-mapping-change

Syntax Description

This command has no arguments or keywords.

Defaults

PIM SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files that can be accessed from the SNMP Object Navigator, available through cisco.com at http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to use the **snmp-server traps pim rp-mapping-change** command:

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps pim rp-mapping-change
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps pim interface-state-change	Enables PIM interface status notification.
snmp-server traps pim invalid-message-received	Enables notifications for monitoring invalid PIM protocol operations.
snmp-server traps pim neighbor-change	Enables PIM neighbor status down notifications.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notification for Cisco-syslog-MIB error messages.

snmp-server traps snmp

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

snmp-server traps snmp [**authentication**]

no snmp-server traps snmp [**authentication**]

Syntax Description

authentication	(Optional) Controls the sending of SNMP authentication failure notifications.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The **enable** keyword was removed from the command name.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **snmp-server traps snmp** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

An authentication Failure(4) trap signifies that the sending device is the addressee of a protocol message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs for packets with an incorrect community string. For SNMPv3, authentication failure occurs for packets with an incorrect Secure Hash Algorithm (SHA) or Message Digest 5 (MD5) authentication key or for a packet that is outside the window of the authoritative SNMP engine.

Task ID

Task ID	Operations
snmp	read, write

Examples

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

```
RP/0/0/1:Router (config)# snmp-server traps snmp authentication
RP/0/0/1:Router (config)# snmp-server host myhost.cisco.com public snmp
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps bgp	Enables BGP server state-change SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server traps syslog

To enable Simple Network Management Protocol (SNMP) notifications of Cisco-syslog-MIB error messages, use the **snmp-server traps syslog** command in global configuration mode. To disable these types of notifications, use the **no** form of this command.

snmp-server traps syslog

no snmp-server traps syslog

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The **enable** keyword was removed from the command name.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **snmp-server traps syslog** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enable Cisco-syslog-MIB error message notifications to the host at the address myhost.cisco.com, using the community string defined as public:

```
RP/0/RP0/CPU0:Router(config)# snmp-server traps syslog
RP/0/RP0/CPU0:Router(config)# snmp-server host myhost.cisco.com version 2c public
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps bgp	Enables BGP server state-change SNMP notifications.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.

snmp-server trap-source

To specify the interface (and hence the corresponding IP address) from which a Simple Network Management Protocol (SNMP) trap should originate, use the **snmp-server trap-source** command in global configuration mode. To remove the source designation, use the **no** form of this command.

snmp-server trap-source *interface-type interface-id*

no snmp-server trap-source

Syntax Description

interface-type	Interface type. For more information, use the question mark (**?**) online help function.
interface-id	Either a physical or virtual interface identifier as follows: • Physical interface identifier. Naming notation is *rack*/*slot*/*module*/*port* and a slash between values is required as part of the notation. – *rack*: Chassis number of the rack. – *slot*: Physical slot number of the modular services card or line card. – *module*: Module number. A physical layer interface module (PLIM) is always 0. – *port*: Physical port number of the interface. **Note** In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. • Virtual interface identifier. Number range varies depending on interface type. **Note** For more information about the syntax for the router, use the question mark (**?**) online help function.

Defaults

No interface is specified.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.

Release	Modification
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When an SNMP trap is sent from a Cisco SNMP device, it has a notification address of the interface it happened to exit at that time. Use the **snmp-server trap-source** command to monitor notifications from a particular interface.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to specify that the IP address for Packet-over-SONET/SDH (POS) interface 0/0/1/0 is the source for all SNMP notifications:

```
RP/0/RP0/CPU0:Router(config)# snmp-server trap-source POS 0/0/1/0
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps bgp	Enables BGP state-change SNMP notifications.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server trap-timeout

To define how often to try resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** command in global configuration mode. To restore the default value, use the **no** form of this command.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout *seconds*

Syntax Description

seconds	Integer that sets the interval (in seconds) for resending the messages. Value can be from 1 to 1000.

Defaults

seconds: 30

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Before the Cisco IOS XR software tries to send a trap, it looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. Use the **snmp-server trap-timeout** command to determine the number of seconds between retransmission attempts.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to set an interval of 20 seconds to try resending trap messages on the retransmission queue:

```
RP/0/RP0/CPU0:Router(config)# snmp-server trap-timeout 20
```

Related Commands

Command	Description
snmp-server engineid	Specifies the identification number of the local SNMP engine.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server traps bgp	Enables BGP state-change SNMP notifications.
snmp-server traps snmp	Enables RFC 1157 SNMP notifications.
snmp-server traps syslog	Enables SNMP notifications for Cisco-syslog-MIB error messages.

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command in global configuration mode. To remove a user from an SNMP group, use the **no** form of this command.

snmp-server user *username groupname* {**v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} {**clear** | **encrypted**} *auth-password* [**priv des56** {**clear** | **encrypted**} *priv-password*]]} [**SDROwner** | **SystemOwner**] [*access-list-name*]

no snmp-server user *username groupname*

Syntax Description

username	Name of the user on the host that connects to the agent.
groupname	Name of the group to which the user belongs.
v1	Specifies that the SNMPv1 security model should be used.
v2c	Specifies that the SNMPv2c security model should be used.
v3	Specifies that the SNMPv3 security model should be used.
auth {**md5** | **sha**} {**clear** | **encrypted**} *auth-password*	(Optional) Specifies which authentication level should be used. If you specify the **auth** keyword, you must specify the an authentication level with one of the following keywords: • **md5**—Specifies the HMAC-MD5-96 authentication level. • **sha**—Specifies the HMAC-SHA-96 authentication level. After you specify the authentication level, you must specify an authorization password. Before setting the authorization password, you must specify one of the following required keywords: • **clear**—Specifies that an unencrypted password follows. • **encrypted**—Specifies that an encrypted password follows. After specifying the type of password, specify the authentication password for the *auth-password* argument: • *auth-password*—String (not to exceed 64 characters) that enables the agent to receive packets from the host.
priv des56 {**clear** | **encrypted**} *priv-password*	(Optional) Specifies the 56-bit Data Encryption Standard (DES) level of encryption for the user. After you specify encryption parameters for the user, you must specify a privacy password. Before setting the privacy password, you must specify one of the following required keywords: • **clear**—Specifies that an unencrypted password follows. • **encrypted**—Specifies that an encrypted password follows. After specifying the type of privacy password that follows, specify the privacy password for the *priv-password* argument: • *priv-password*—Unencrypted, clear-text privacy password.
SDROwner	(Optional) Limits access to the agents for the owner secure domain router (SDR) only.

SystemOwner	(Optional) Provides system-wide access to the agents for all SDRs.
access-list-name	(Optional) Specifies an access list to be associated with this SNMP user. The *list* argument represents a value from 1 to 99, that is, the identifier of the standard IP access list.

Defaults

By default, access is limited to agents on the owner SDR only.

See also Table 92 in the "Usage Guidelines" section.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The **access** keyword was removed. The **0** and **7** keywords were replaced by the **clear** and **encrypted** keywords, respectively.
Release 3.3.0	Optional keywords **LROwner** and **SystemOwner** were added
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	**LROwner** was changed to **SDROwner**.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Table 92 describes default behaviors for passwords and access lists.

Table 92 snmp-server user Default Descriptions

Characteristic	Default
passwords	Text strings are assumed.
access lists	Access from all IP access lists is permitted.

SDR and System-wide Access

When the command **snmp-server user** is entered with the **SDROwner** keyword, SNMP access is granted only to the MIB object instances in the owner SDR.

When the command **snmp-server user** is entered with the **SystemOwner** keyword, SNMP access is granted to all SDRs in the system. Only one user can be configured with **SystemOwner** privileges.

Note In a non-owner SDR, user access is provided only to the object instances in that SDR, regardless of the access privilege assigned. Access to the owner SDR and system-wide access privileges are available only from the owner SDR.

Note Secure domain routers (SDRs) were previously known as logical routers (LRs). The name was changed as of Cisco IOS XR Release 3.3.0.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to enter a plain-text password for the string *abcd* for user2 in group2:

```
RP/0/RP0/CPU0:Router(config)# snmp-server user user2 group2 v3 auth md5 clear abcd
```

To learn if this user has been added to the configuration, issue the **show snmp user** command.

If the localized Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) digest is known, specify that string instead of the plain-text password. The digest should be formatted as AA:BB:CC:DD where AA, BB, CC, and DD are hexadecimal values. The digest should also be exactly 16 octets long.

The following example shows how to specify the command with a digest name of 00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:

```
RP/0/RP0/CPU0:Router(config)# snmp-server user user2 group2 v3 auth md5 encrypted
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

Related Commands

Command	Description
snmp-server group	Configures an SNMP user group.

snmp-server view

To create or update a Simple Network Management Protocol (SNMP) view entry, use the **snmp-server view** command in global configuration mode. To remove the specified server view entry, use the **no** form of this command.

snmp-server view *view-name oid-tree* {**excluded** | **included**}

no snmp-server view *view-name oid-tree* {**excluded** | **included**}

Syntax Description

view-name	Label for the view record being updated or created. The name is used to reference the record.
oid-tree	Object identifier (OID) of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as *system*. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
excluded	Excludes the MIB family from the view.
included	Includes the MIB family in the view.

Defaults

No view entry exists.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Other SNMP commands require a view as a keyword. Use the **snmp-server view** command to create a view to be used as keywords for other commands that create records including a view.

Instead of defining a view explicitly, you can rely on the following predefined views, which are supported by the SNMP agent:

- all—Predefined view indicating that a user can see all objects.
- CfgProt—Predefined view indicating that a user can see all objects except the SNMPv3 configuration tables.
- vacmViewTreeFamilyEntry—Predefined view indicating that a user can see the default configuration of vacmViewTreeFamilyEntry.

The predefined views supported on the Cisco IOS XR software, however, do not match the predefined views specified in RFC 3415.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example creates a view that includes all objects in the MIB-II subtree:

```
RP/0/RP0/CPU0:Router(config)# snmp-server view mib2 1.3.6.1.2.1 included
```

The following example shows how to create a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:

```
RP/0/RP0/CPU0:Router(config)# snmp-server view view1 1.3.6.1.2.1.1 included
RP/0/RP0/CPU0:Router(config)# snmp-server view view1 1.3.6.1.4.1.9 included
```

The following example shows how to create a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
RP/0/RP0/CPU0:Router(config)# snmp-server view view1 1.3.6.1.2.1.1 included
RP/0/RP0/CPU0:Router(config)# snmp-server view view1 1.3.6.1.2.1.1.7 excluded
RP/0/RP0/CPU0:Router(config)# snmp-server view view1 1.3.6.1.2.1.2.2.1.*.1 included
```

Related Commands

Command	Description
show snmp view	Displays information about the configured views.
snmp-server group	Configures an SNMP user group.

snmp-server vrf

To configure the VPN routing and forwarding (VRF) properties of Simple Network Management Protocol (SNMP), use the **snmp-server vrf** command in global configuration mode. To remove the configuration, use the **no** form of this command.

snmp-server vrf *vrf-name* [**host** *address* [**clear** | **encrypted**] [**traps**] [**version** {**1** | **2c** | **3** *security-level*}] *community-string* [**udp-port** *port*]] [**context** *context-name*]

no snmp-server vrf *vrf-name*

Syntax Description

vrf-name	Name of the VRF.
host *address*	(Optional) Specifies the name or IP address of the host (the targeted recipient).
clear	(Optional) Specifies that the *community-string* argument is clear text.
encrypted	(Optional) Specifies that the *community-string* argument is encrypted text.
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
version {**1** | **2c** | **3**}	(Optional) Specifies the version of the SNMP used to send the traps. The default is SNMPv1. When the **version** keyword is used, one of the following keywords must be specified: • **1**—SNMPv1 • **2c**—SNMPv2C • **3**—SNMPv3
security-level	(Optional) Security level for SNMPv3. Options are: • **auth**—authNoPriv • **noauth**—noAuthNoPriv • **priv**—authPriv
string	Specifies the community string for SNMPv1 and SNMPv2, or the SNMPv3 user.
udp-port *port*	(Optional) Specifies the UDP port to which notifications should be sent.
context *context-name*	(Optional) Name of the context that must be mapped to VRF identified by value of the *vrf-name* argument.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.3.0	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use this command to enter SNMP VRF configuration submode and configure an SNMP notification recipient on a VRF. You can also map a VRF to an SNMP context.

SNMP notification recipient that is reachable by way of a VRF can be configured. Notification is forwarded to the recipient represented by its address using the routing table instance identified by the VRF name.

Use the **clear** keyword to specify that the clear text community string you enter is displayed encrypted in the **show running** command output. To enter an encrypted string, use the **encrypted** keyword. To enter a clear text community string that is not encrypted by the system, use neither of these keywords.

An SNMP context identified by the value of the *context-name* argument can be mapped to a VRF in this submode. This context must be created using **snmp-server context** command.

Task ID

Task ID	Operations
snmp	read, write

Examples

The following example shows how to configure a host IP address for a VRF name:

```
RP/0/RP0/CPU0:Router(config)# snmp-server vrf vrfa
RP/0/RP0/CPU0:Router(config-snmp-vrf)# host 12.21.0.1 traps version 2c public udp-port
2525
```

Related Commands

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