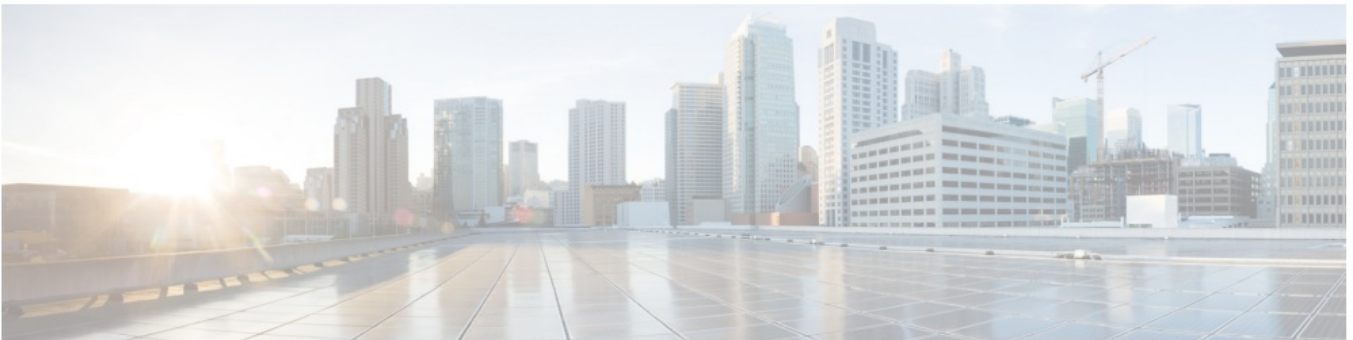




CISCO ASR 9000 Series Aggregation Services Routers User Guide

[Home](#) » [Cisco](#) » CISCO ASR 9000 Series Aggregation Services Routers User Guide 



Contents

- [1 Configuring Simple Network Management Protocol](#)
- [2 Prerequisites for Implementing SNMP](#)
- [3 SNMP Notifications](#)
- [4 SNMP Versions](#)
- [5 SNMPv3 Benefits](#)
- [6 SNMPv3 Costs](#)
- [7 IP Precedence and DSCP Support for SNMP](#)
- [8 Session Types](#)
- [9 How to Implement SNMP on Cisco IOS XR Software](#)
- [10 Defining the Maximum SNMP Agent Packet Size](#)
- [11 Configuration Examples for Implementing SNMP](#)
- [12 Additional References](#)
- [13 Documents / Resources](#)
 - [13.1 References](#)

Configuring Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

This module describes the new and revised tasks you need to implement SNMP on your Cisco IOS XR network. For detailed conceptual information about SNMP on the Cisco IOS XR software and complete descriptions of the SNMP commands listed in this module, see *Related Documents*, on page 29. For information on specific MIBs, refer to *Cisco ASR 9000 Series Aggregation Services Routers MIB Specifications Guide*. To locate documentation for other commands that might appear in the course of performing a configuration task, search online in *Cisco ASR 9000 Series Aggregation Services Router Commands Master List*.

Table 1: Feature History for Implementing SNMP on Cisco IOS XR Software

Release	Modification
Release 3.7.2	This feature was introduced.
Release 3.9.0	Support was added for 3DES and AES encryption. The ability to preserve ENTITY-MIB and CISCO-CLASS-BASED-QOS-MIB data was added.
Release 4.2.0	Support was added for SNMP over IPv6.

This module contains the following topics:

- Prerequisites for Implementing SNMP, on page 2
- Restrictions for SNMP Use on Cisco IOS XR Software, on page 2
- Information About Implementing SNMP, on page 2
- Session MIB support on subscriber sessions , on page 9
- How to Implement SNMP on Cisco IOS XR Software, on page 11
- Configuration Examples for Implementing SNMP, on page 21
- SNMP Context Mapping Configuration, on page 27
- Additional References, on page 29

Prerequisites for Implementing SNMP

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Restrictions for SNMP Use on Cisco IOS XR Software

SNMP outputs are only 32-bits wide and therefore cannot display any information greater than 2 is equal to 4.29 Gigabits. Note that a 10 Gigabit interface is greater than this and so if you are trying to display speed information regarding the interface, you might see concatenated results.

The recommended maximum number of object identifiers (OIDs) that can be accommodated in a single SNMP request is 75. A request with more than 75 OIDs can result in SNMP requests being dropped with SNMP polling timeout.

Information About Implementing SNMP

To implement SNMP, you need to understand the concepts described in this section.

SNMP Functional Overview

The SNMP framework consists of three parts:

- SNMP manager
- SNMP agent
- Management Information Base (MIB)

SNMP Manager

The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP.

The most common managing system is called a network management system (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on such a device.

A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks 2000 line of products).

SNMP Agent

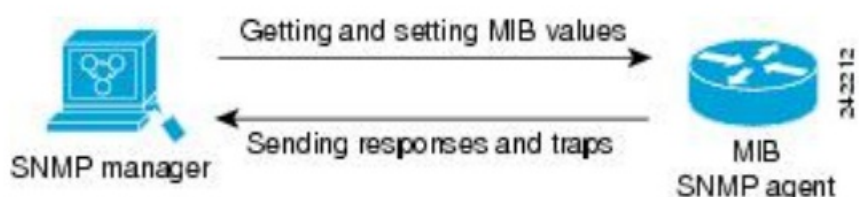
The SNMP agent is the software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. The agent and MIB reside on the router. To enable the SNMP agent, you must define the relationship between the manager and the agent.

MIB

The Management Information Base (MIB) is a virtual information storage area for network management information, which consists of collections of managed objects. Within the MIB there are collections of related objects, defined in MIB modules. MIB modules are written in the SNMP MIB module language, as defined in STD 58, RFC 2578, RFC 2579, and RFC 2580. Note that individual MIB modules are also referred to as MIBs; for example, the Interfaces Group MIB (IF-MIB) is a MIB module within the MIB on your system. The SNMP agent contains MIB variables whose values the SNMP manager can request or change through Get or Set operations. A manager can get a value from an agent or store a value into that agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to manager requests to get or set data.

This figure illustrates the communications relationship between the SNMP manager and agent. A manager can send the agent requests to get and set MIB values. The agent can respond to these requests. Independent of this interaction, the agent can send unsolicited notifications (traps) to the manager to notify the manager of network conditions.

Figure 1: Communication Between an SNMP Agent and Manager



IP-MIB Support

RFC4293 IP-MIB was specifically designed to provide IPv4 and IPv6 statistics individually. The `ipIfStatsTable` defined in RFC 4293, lists the interface specific statistics. IPv6 statistics support in `ipIfStatsTable` was added earlier but, IOS- XR implementation of IP-MIB did not support IPv4 statistics as per RFC4293 in earlier releases. From Release 6.3.2 onwards, IOS-XR implementation of IP-MIB supports IPv4 statistics as per RFC4293.

This will enable you to collect the IPV4 and IPV6 statistics separately for each interface. The `ipIfStatsTable` is indexed by two sub-ids address type (IPv4 or IPv6) and the interface `ifindex[1]`. The implementation of IP-MIB support for IPv4 and IPv6 is separated from Release 6.3.2 for better readability and maintainability.

The list of OIDs added to the `ipIfStatsTable` for IPv4 statistics are:

- `ipIfStatsInReceives`


- ipIfStatsHCInReceives
- ipIfStatsInOctets
- ipIfStatsHCInOctets
- ipIfStatsOutTransmits
- ipIfStatsHCOOutTransmits
- ipIfStatsOutOctets
- ipIfStatsHCOOutOctets
- ipIfStatsDiscontinuityTime

For more information on the list of new OIDs added for IPv4 statistics, see SNMP OID Navigator.

Related Topics

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. On Cisco IOS XR software, unsolicited (asynchronous) notifications can be generated only as traps. Traps are messages alerting the SNMP manager to a condition on the network. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

 **Note** Inform requests (inform operations) are supported in Cisco IOS XR software from release 4.1 onwards. For more information see,

http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-3/sysman/command/reference/b-sysman-cr53xasr/b-sysman-cr53xasr_chapter_010010.html#wp2863682680

Traps are less reliable than informs because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, traps are often preferred because informs consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, and an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and resources.

Figure 2: Trap Received by the SNMP Manager

In this illustration, the agent router sends a trap to the SNMP manager. Although the manager receives the trap, it does not send any acknowledgment to the agent. The agent has no way of knowing that the trap reached its destination.

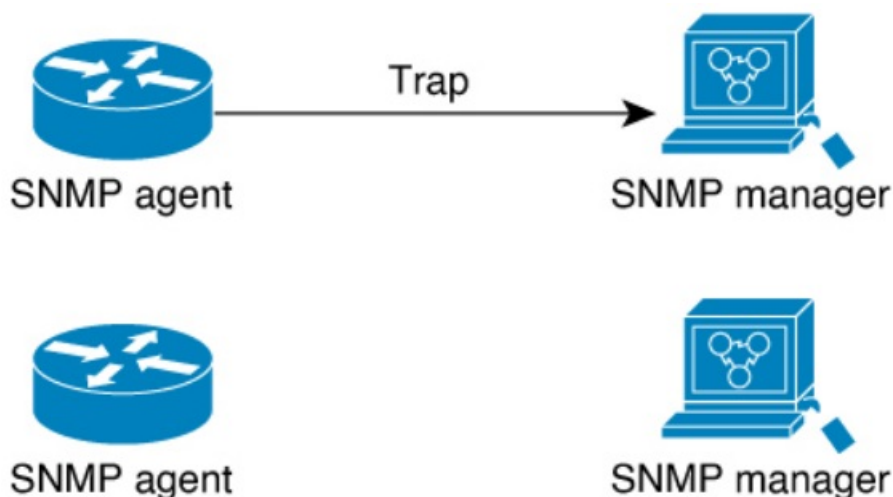
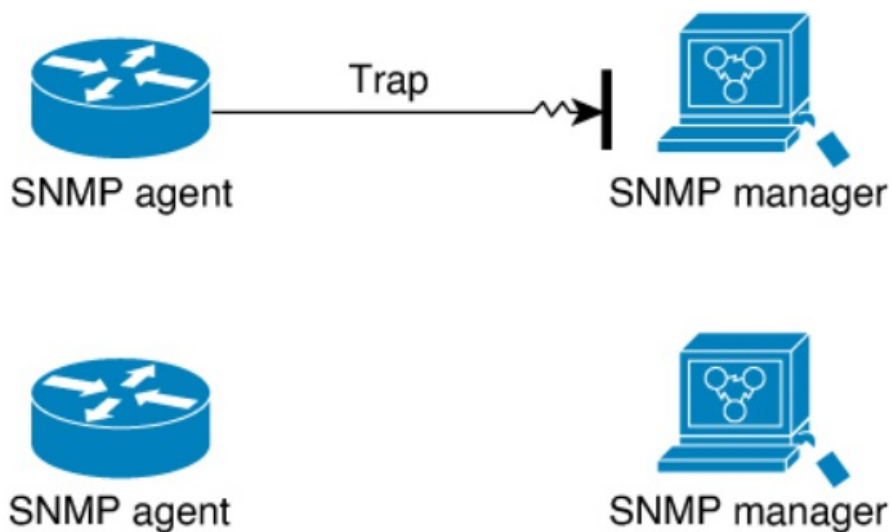


Figure 3: Trap Not Received by the SNMP Manager

In this illustration, the agent sends a trap to the manager, but the trap does not reach the manager. Because the agent has no way of knowing that the trap did not reach its destination, the trap is not sent again. The manager never receives the trap.



SNMP Versions

Cisco IOS XR software supports the following versions of SNMP:

- Simple Network Management Protocol Version 1 (SNMPv1)
- Simple Network Management Protocol Version 2c (SNMPv2c)
- Simple Network Management Protocol Version 3 (SNMPv3)

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is defined by an IP address access control list and password.

SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2c improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported: no such object exceptions, no such instance exceptions, and end of MIB view exceptions.

SNMPv3 is a security model. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when an SNMP packet is handled. See Table 3: SNMP Security Models and Levels, on page 6 for a list of security levels available in SNMPv3. The SNMPv3 feature supports RFCs 3411 to 3418.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; for this reason, you can configure the Cisco IOS-XR software to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SNMPv3.

Comparison of SNMPv1, v2c, and v3

SNMP v1, v2c, and v3 all support the following operations:

- get-request—Retrieves a value from a specific variable.
- get-next-request—Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable

name. The SNMP manager searches sequentially to find the needed variable from within the MIB.

- get-response—Operation that replies to a get-request, get-next-request, and set-request sent by an NMS.
- set-request—Operation that stores a value in a specific variable.
- trap—Unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

The below table identifies other key SNMP features supported by the SNMP v1, v2c, and v3.

Table 2: SNMPv1, v2c, and v3 Feature Support

Feature	SNMP v1	SNMP v2c	SNMP v3
Get-Bulk Operation	No	Yes	Yes
Inform Operation	No	Yes (No on the Cisco IOS XR software)	Yes (No on the Cisco LOS XR software)
64 Bit Counter	No	Yes	Yes
Textual. Conventions	No	Yes	Yes
Authentication	No	No	Yes
Privacy (Encryption)	No	No	Yes
Authorization and Access Controls (Views)	No	No	Yes

Security Models and Levels for SNMPv1, v2, v3

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption.
- authNoPriv—Security level that provides authentication but does not provide encryption.
- authPriv—Security level that provides both authentication and encryption.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed. The below table identifies what the combinations of security models and levels mean.

Table 3: SNMP Security Models and Levels

Mod e)	Level	Authentication	Encryptio n	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	\u	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the HMAC1-MD52 algorithm or the HMAC-SHA1.
v3	authrm	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES4 56-bit encryption in addition to authentication based on the CBC5 DES (DES-56) standard.
v3	authPI i \	HMAC-MD5 or HMAC-SHA	3DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides 168-bit 3DESII level of encryption.
v3	flith Priv	HMAC-MD5 or HMAC-SHA	AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides 128-bit AES1 level of encryption.

1. Hash-Based Message Authentication Code
2. Message Digest 5
3. Secure Hash Algorithm
4. Data Encryption Standard
5. Cipher Block Chaining
6. Triple Data Encryption Standard
7. Advanced Encryption Standard

Use of 3DES and AES encryption standards requires that the security package (k9sec) be installed. For information on installing software packages, see *Upgrading and Managing Cisco IOS XR Software*.

SNMPv3 Benefits

SNMPv3 provides secure access to devices by providing authentication, encryption and access control. These added security benefits secure SNMP against the following security threats:

- **Masquerade**—The threat that an SNMP user may assume the identity of another SNMP user to perform management operations for which that SNMP user does not have authorization.
- **Message stream modification**—The threat that messages may be maliciously reordered, delayed, or replayed (to an extent that is greater than can occur through the natural operation of a subnetwork service) to cause SNMP to perform unauthorized management operations.
- **Disclosure**—The threat that exchanges between SNMP engines could be eavesdropped. Protecting against this threat may be required as a matter of local policy.

In addition, SNMPv3 provides access control over protocol operations on SNMP managed objects.

SNMPv3 Costs

SNMPv3 authentication and encryption contribute to a slight increase in the response time when SNMP operations on MIB objects are performed. This cost is far outweighed by the security advantages provided by SNMPv3.

This table shows the order of response time (from least to greatest) for the various security model and security level combinations.

Table 4: Order of Response Times from Least to Greatest

Security Model	Security Level
SNMPv2c	noAuthNoPriv
SNMPv3	noAuthNoPriv
SNMPv3	authNoPriv
SNMPv3	authPriv

User-Based Security Model

SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur nonmaliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages.

USM uses two authentication protocols:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

USM uses Cipher Block Chaining (CBC)-DES (DES-56) as the privacy protocol for message encryption.

View-Based Access Control Model

The View-Based Access Control Model (VACM) enables SNMP users to control access to SNMP managed objects by supplying read, write, or notify access to SNMP objects. It prevents access to objects restricted by views. These access policies can be set when user groups are configured with the `snmp-server group` command.

MIB Views

For security reasons, it is often valuable to be able to restrict the access rights of some groups to only a subset of the management information within the management domain. To provide this capability, access to a management object is controlled through MIB views, which contain the set of managed object types (and, optionally, the specific instances of object types) that can be viewed.

IP Precedence and DSCP Support for SNMP

SNMP IP Precedence and differentiated services code point (DSCP) support delivers QoS specifically for SNMP traffic. You can change the priority setting so that SNMP traffic generated in a router is assigned a specific QoS class. The IP Precedence or IP DSCP code point value is used to determine how packets are handled in weighted random early detection (WRED).

After the IP Precedence or DSCP is set for the SNMP traffic generated in a router, different QoS classes cannot

be assigned to different types of SNMP traffic in that router.


The IP Precedence value is the first three bits in the type of service (ToS) byte of an IP header. The IP DSCP code point value is the first six bits of the differentiate services (DiffServ Field) byte. You can configure up to eight different IP Precedence markings or 64 different IP DSCP markings.

Session MIB support on subscriber sessions

SNMP monitoring requires information about subscribers of all types. The CISCO-SUBSCRIBER-SESSION-MIB is defined to model per-subscriber data as well as aggregate subscriber (PPPoE) data. It is required to support notifications (traps) for aggregate session counts crossing configured thresholds. Generic MIB Data Collector Manager (DCM) support for CISCO-SUBSCRIBER-SESSION-MIB, helps faster data collection and also better handling of parallel data.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. On Cisco IOS XR software, unsolicited (asynchronous) notifications can be generated only as traps. Traps are messages alerting the SNMP manager to a condition on the network. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

 Note Inform requests (inform operations) are supported in Cisco IOS XR software from release 4.1 onwards. For more information see,

http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-3/sysman/command/reference/b-sysman-cr53xasr/b-sysman-cr53xasr_chapter_010010.html#wp2863682680

Traps are less reliable than informs because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, traps are often preferred because informs consume more resources in the router and in the network.

Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, and an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and resources.

Figure 4: Trap Received by the SNMP Manager

In this illustration, the agent router sends a trap to the SNMP manager. Although the manager receives the trap, it does not send any acknowledgment to the agent. The agent has no way of knowing that the trap reached its destination.

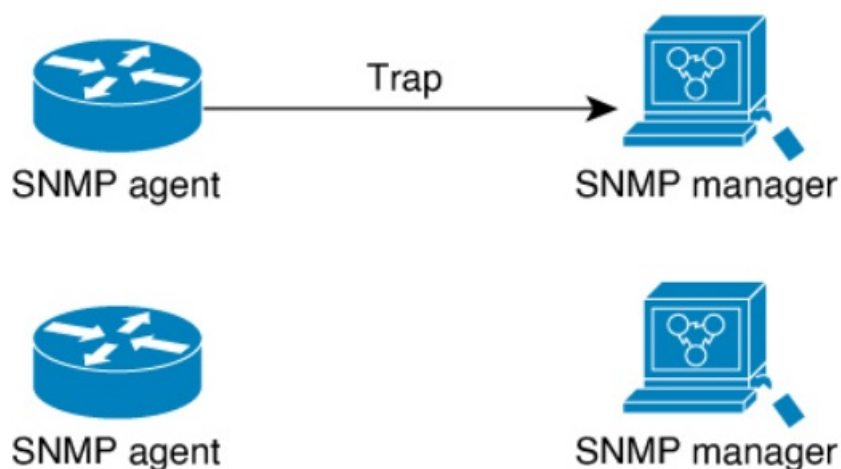
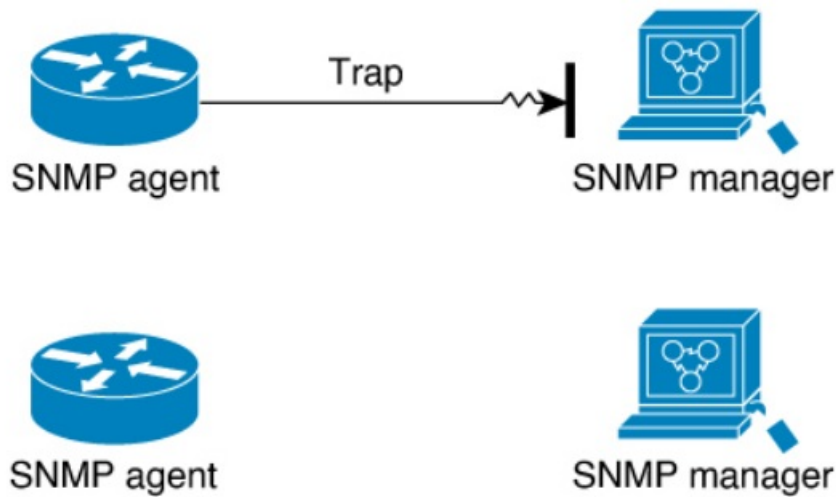


Figure 5: Trap Not Received by the SNMP Manager

In this illustration, the agent sends a trap to the manager, but the trap does not reach the manager. Because the agent has no way of knowing that the trap did not reach its destination, the trap is not sent again. The manager never receives the trap.



Session Types

The supported session types are:

- PPPoE
- IP SUB PKT
- IP SUB DHCP


How to Implement SNMP on Cisco IOS XR Software

This section describes how to implement SNMP.

The `snmp-server` commands enable SNMP on Management Ethernet interfaces by default. For information on how to enable SNMP server support on other inband interfaces, see the Implementing Management Plane Protection on Cisco IOS XR Software module in System Security Configuration Guide for Cisco ASR 9000 Series Routers.

Configuring SNMPv3

This task explains how to configure SNMPv3 for network management and monitoring.

 **Note** No specific command enables SNMPv3; the first `snmp-server` global configuration command (`config`), that you issue enables SNMPv3. Therefore, the sequence in which you issue the `snmp-server` commands for this task does not matter.

SUMMARY STEPS

1. `configure`
2. `snmp-server view view-name oid-tree {included | excluded}`
3. `snmp-server group name {v1 | v2c | v3 [auth | noauth | priv]} [read view] [write view] [notify view] [access-list-name]`
4. `snmp-server user username groupname {v1 | v2c | v3 [auth {md5 | sha} {clear | encrypted} auth-password [priv-des56 {clear | encrypted} priv-password]]} [access-list-name]`
5. Use the `commit` or `end` command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RSP0/CPU0:router# configure	Enters global configuration mode.
Step 2	snmp-server view view-name oid-tree {i ncluded excluded} Example: RP/0/RSP0/CPU0:router(config)# snmp-server view view_name 1.3.6.1.2.1.1.5 included	Creates or modifies a view record.
Step 3	snmp-server group name {v1 v2c v3 { auth noauth priv}} [read view] [write vie w] [notify view] [access-list-name]	Configures a new SNMP group or a table that maps S NMP users to SNMP views.
Step 4	snmp-server user username groupname {v1 v2c v3 [auth {md5 sha} {clear e ncrypted} auth-password [priv des56 {clear encry pted} priv-password]]} [access-list-name] Exa mple: RP/0/RSP0/CPU0:router(config)# snmp-server user noauthuser group_name v3	Configures a new user to an SNMP group. Note Only one remote host can be assigned to the same us ername for SNMP version 3. If you configure the same username with different remote hosts, only the last us ername and remote host combination will be accepted and will be seen in the show running configuration. In t he case of multiple SNMP managers, multiple unique usernames are required. Note When you execute an SNMP bulk request using the sn mpbulkget command to an unavailable MIB, it provides a next available MIB.
Step 5	Use the commit or end command.	commit —Saves the configuration changes and remains within the configuration session. end —Prompts user to take one of these actions: • Yes — Saves configuration changes and exits the Oc nfiguration session. • No —Exits the configuration session without committi ng the configuration changes. • Cancel —Remains in the configuration session, witho ut committing the configuration changes.

Configuring SNMP Trap Notifications

This task explains how to configure the router to send SNMP trap notifications.



Note

You can omit Step 3, on page 11 if you have already completed the steps documented under the Configuring SNMPv3, on page 11 task.

SUMMARY STEPS

1. configure
2. snmp-server group name {v1 | v2c | v3 {auth | noauth | priv}} [read view] [write view] [notify view] [access-list-name]
3. snmp-server user username groupname {v1 | v2c | v3 [auth {md5 | sha} {clear | encrypted} auth-password [priv

des56 {clear | encrypted} priv-password]]] [access-list-name]

4. snmp-server host address [traps] [version {1 | 2c | 3 [auth | noauth | priv]]] community-string [udp-port port] [notification-type]
5. snmp-server traps [notification-type]
6. Use the commit or end command.
7. (Optional) show snmp host

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RSP0/CPU0:router# configure	Enters global configuration mode.
Step 2	snmp-server group name {v1 v2c v3 { auth noauth priv}} [read view] [write view] [notify view] [access-list-name] Example: RP/0/RSP0/CPU0:router(config)# snmp-server group group_name v3 noauth read view_name 1 write view_name2	Configures a new SNMP group or a table that maps S NMP users to SNMP views.
Step 3	snmp-server user username groupname {v1 v2c v3 [auth {md5 sha} {clear e ncrypted} auth-password [priv des56 {clear encry pted} priv-password]]] [access-list-name] Exa mple: RP/0/RSP0/CPU0:router(config)# snmp-server user noauthuser group_name v3	Configures a new user to an SNMP group. Note Only one remote host can be assigned to the ame user name for SNMP version 3. If you configure the same u sername with different remote hosts, only the last username and remote host combination will be accepted and will be seen in the show running configu ration. In the case of multiple SNMP managers, multipl e unique usernames are required. Note When you execute an SNMP bulk request using the sn mpbulkget command to an unavailable MIB, it provides a next available MIB.
Step 4	snmp-server host address [traps] [versio n {1 2c 3 [auth noauth priv]]] community-string [udp-port port] [notification-type] Example:	Specifies SNMP trap notifications, the version of SNM P to use, the security level of the notifications, and the recipient (host) of the notifications.
Step 5	snmp-server traps [notification-type] Exa mple: RP/0/RP0/CPU0:router(config)# snmp-s erver traps bgp	Enables the sending of trap notifications and specifies the type of trap notifications to be sent. • If a trap is not specified with the notification-type argu ment, all supported trap notifications are enabled on th e router. To display which trap notifications are availabl e on your router, enter the snmp-server traps ? comma nd.

Step 6	Use the commit or end command.	commit —Saves the configuration changes and remains within the configuration session. end —Prompts user to take one of these actions: <ul style="list-style-type: none"> • Yes — Saves configuration changes and exits the configuration session. • No —Exits the configuration session without committing the configuration changes. • Cancel —Remains in the configuration session, without committing the configuration changes.
Step 7	(Optional) show snmp host Example: RP/0/RSP0/CPU0:router# show snmp host	Displays information about the configured SNMP notification recipient (host), port number, and security model.

Setting the Contact, Location, and Serial Number of the SNMP Agent

This task explains how to set the system contact string, system location string, and system serial number of the SNMP agent.

Note

The sequence in which you issue the snmp-server commands for this task does not matter.

SUMMARY STEPS

1. configure
2. (Optional) snmp-server contact system-contact-string
3. (Optional) snmp-server location system-location
4. (Optional) snmp-server chassis-id serial-number
5. Use the commit or end command.

Defining the Maximum SNMP Agent Packet Size

This task shows how to configure the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.



Note

The sequence in which you issue the snmp-server commands for this task does not matter.

SUMMARY STEPS

1. configure
2. (Optional) snmp-server packet-size byte-count
3. Use the commit or end command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/O/RSPO/CPUO:router# configure	Enters global configuration mode.
Step 2	(Optional) snmp-server packet-size byte-count Example: RP/O/RSPO/CPUO:router(config)# snmp-server packet-size 1024	Sets the maximum packet size.
Step 3	Use the commit or end command.	commit —Saves the configuration changes and remains within the configuration session. end —Prompts user to take one of these actions: •Yes — Saves configuration changes and exits the configuration session. •No —Exits the configuration session without committing the configuration changes. •Cancel —Remains in the configuration session, without committing the configuration changes.

Changing Notification Operation Values

After SNMP notifications have been enabled, you can specify a value other than the default for the source interface, message queue length, or retransmission interval.

This task explains how to specify a source interface for trap notifications, the message queue length for each host, and the retransmission interval.

Note

The sequence in which you issue the snmp-server commands for this task does not matter.

SUMMARY STEPS

1. configure
2. (Optional) snmp-server trap-source type interface-path-id
3. (Optional) snmp-server queue-length length
4. (Optional) snmp-server trap-timeout seconds
5. Use the commit or end command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/O/RSPO/CPUO:routerf configure	Enters global configuration mode.
Step 2	(Optional) snmp-server trap-source type interface-path-id Example: RP/O/RSPO/CPUO:router(config)if snmp-server trap-source POS 0/0/1/0	Specifies a source interface for trap notifications.
Step 3	(Optional) snmp-server queue-length length Example: AP/O/RSPO/CPUO:router(config)* snmp-server queue-length 20	Establishes the message queue length for each notification.
Step 4	(Optional) snmp-server trap-timeout seconds Example: RP/O/RSPO/CPUO:router(config)0 snmp-server trap-timeout 20	Defines how often to resend notifications on the retransmission queue.
Step 5	Use the commit or end command.	commit —Saves the configuration changes and remains within the configuration session. end —Prompts user to take one of these actions: •Yes – Saves configuration changes and exits the configuration session. •No —Exits the configuration session without committing the configuration changes. •Cancel —Remains in the configuration session, without committing the configuration changes.

Setting IP Precedence and DSCP Values

This task describes how to configure IP Precedence or IP DSCP for SNMP traffic.

Before you begin

SNMP must be configured.

SUMMARY STEPS

1. configure
2. Use one of the following commands:
 - snmp-server ipv4 precedence value
 - snmp-server ipv4 dscp value
3. Use the commit or end command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/O/RSPO/CPUO:routerf configure	Enters global configuration mode.
Step 2	(Optional) snmp-server trap-source type interface-path-id Example: RP/O/RSPO/CPUO:router(config)if snmp-server trap-source POS 0/0/1/0	Specifies a source interface for trap notifications.
Step 3	(Optional) snmp-server queue-length length Example: AP/O/RSPO/CPUO:router(config)* snmp-server queue-length 20	Establishes the message queue length for each notification.
Step 4	(Optional) snmp-server trap-timeout seconds Example: RP/O/RSPO/CPUO:router(config)0 snmp-server trap-timeout 20	Defines how often to resend notifications on the retransmission queue.
Step 5	Use the commit or end command.	commit —Saves the configuration changes and remains within the configuration session. end —Prompts user to take one of these actions: •Yes – Saves configuration changes and exits the configuration session. •No —Exits the configuration session without committing the configuration changes. •Cancel —Remains in the configuration session, without committing the configuration changes.

Configuring MIB Data to be Persistent

Many SNMP MIB definitions define arbitrary 32-bit indices for their object tables. MIB implementations often do a mapping from the MIB indices to some internal data structure that is keyed by some other set of data. In these MIB tables the data contained in the table are often other identifiers of the element being modelled. For example, in the ENTITY-MIB, entries in the entPhysicalTable are indexed by the 31-bit value, entPhysicalIndex, but the entities could also be identified by the entPhysicalName or a combination of the other objects in the table.

Because of the size of some MIB tables, significant processing is required to discover all the mappings from the 32-bit MIB indices to the other data which the network management station identifies the entry. For this reason, it may be necessary for some MIB indices to be persistent across process restarts, switchovers, or device reloads. The ENTITY-MIB entPhysicalTable and CISCO-CLASS-BASED-QOS-MIB are two such MIBs that often require index values to be persistent.

Also, because of query response times and CPU utilization during CISCO-CLASS-BASED-QOS-MIB statistics queries, it is desirable to cache service policy statistics.

SUMMARY STEPS

1. (Optional) snmp-server entityindex persist
2. (Optional) snmp-server mibs cbqosmib persist
3. (Optional) snmp-server cbqosmib cache refresh time time
4. (Optional) snmp-server cbqosmib cache service-policy count count
5. snmp-server ifindex persist

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) snmp-server entityindex persist Example: RP/O/RSPO/CPUO:router(config)# snmp-server entityindex persist	Enables the persistent storage of ENTITY-MIB data.
Step 2	(Optional) snmp-server mibs cbqosmib persist Example: RP/O/RSPO/CPUO:router(config)# snmp-server mibs cbqosmib persist	Enables persistent storage of the CISCO-CLASS-BASED-QoS-MIB data.
Step 3	(Optional) snmp-server cbqosmib cache refresh time time Example: HP/O/RSPO/CPUO:router(config)# snmp-server 'albs cbqosmib cache refresh time 45	Enables QoS MIB caching with a specified cache refresh time.
Step 4	(Optional) snmp-server cbqosmib cache service-policy count count Example: PP/O/RSPO/CPUO:router(config)# snmp-server mibs cbqosmib cache service-policy count 50	Enables QoS MIB caching with a limited number of service policies to cache.
Step 5	snmp-server ifindex persist Example: .-P/O/RSPO/CPUO:router(config)# snmp-server ifindex persist	Enables ifindex persistence globally on all Simple Network Management Protocol (SNMP) interfaces.

Configuring LinkUp and LinkDown Traps for a Subset of Interfaces

By specifying a regular expression to represent the interfaces for which you are interested in setting traps, you can enable or disable linkUp and linkDown traps for a large number of interfaces simultaneously.

Before you begin

SNMP must be configured.

SUMMARY STEPS

1. configure
2. snmp-server interface subset subset-number regular-expression expression
3. notification linkupdown disable
4. Use the commit or end command.
5. (Optional) show snmp interface notification subset subset-number
6. (Optional) show snmp interface notification regular-expression expression
7. (Optional) show snmp interface notification type interface-path-id

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RSPO/CPUO:router# configure	Enters global configuration mode.
Step 2	snmp-server interface subset subset-number regular-expression expression Example: RP/0/RSPO/CPUO:router(config)* snmp-server interface subset 10 regular-expression “^Gigla-zA-Z)+[0-9/]+\.” R P/0/RSPO/CPUO:router(config-snmp-if-subset)11	Enters snmp-server interface mode for the interface s identified by the regular expression. The subset-number argument identifies the set of interfaces, and also assigns a priority to the subset in the event that an interface is included in more than one subset. Lower numbers have higher priority and their configuration takes precedent over interface subsets with higher numbers. The expression argument must be entered surrounded by double quotes. Refer to the Understanding Regular Expressions, Special Characters, and Patterns module in Cisco AS R 9000 Series Aggregation Services Router Getting Started Guide for more information regarding regular expressions.
Step 3	notification linkupdown disable Example: RP/0/RSPO/CPUO:router(config-snmp-if-subset)1 notification linkupdown disable	Disables linkUp and linkDown traps for all interfaces being configured. To enable previously disabled interfaces, use the no form of this command.

Configuration Examples for Implementing SNMP

Configuring SNMPv3: Examples

Setting an Engine ID

This example shows how to set the identification of the local SNMP engine: snmp-server engineID local 00:00:00:09:00:00:00:a1:61:6c:20:61



Note

Verifying the Identification of the Local SNMP Engines

This example shows how to verify the identification of the local SNMP engine: config show snmp engineid
SNMP engineID 00000009000000a1ffffff

Creating a View

There are two ways to create a view:

- You can include the object identifier (OID) of an ASN.1 subtree of a MIB family from a view by using the included keyword of the snmp-server view command.
- You can exclude the OID subtree of the ASN.1 subtree of a MIB family from a view by using the excluded keyword of the snmp-server view command.

This example shows how to create a view that includes the sysName (1.3.6.1.2.1.1.5) object: configsnmp-server view SNMP_VIEW1 1.3.6.1.2.1.1.5 included

This example shows how to create a view that includes all the OIDs of a system group: config snmp-server view SNMP_VIEW1 1.3.6.1.2.1.1 included

This example shows how to create a view that includes all the OIDs under the system group except the sysName object (1.3.6.1.2.1.1.5), which has been excluded: config

snmp-server view SNMP_VIEW1 1.3.6.1.2.1.1 included

snmp-server view SNMP_VIEW1 1.3.6.1.2.1.1.5 excluded

Verifying Configured Views

This example shows how to display information about the configured views: RP/0/RSP0/CPU0:router# show snmp view v1default 1.3.6.1 – included nonVolatile active

SNMP_VIEW1 1.3.6.1.2.1.1 – included nonVolatile active SNMP_VIEW1 1.3.6.1.2.1.1.5 – excluded nonVolatile active

Creating Groups

If you do not explicitly specify a notify, read, or write view, the Cisco IOS XR software uses the v1 default (1.3.6.1). This example shows how to create a group that utilizes the default view: RP/0/RSP0/CPU0:router(config)# snmp-server group group-name v3 auth The following configuration example shows how to create a group that has read access to all the OIDs in the system except the sysUpTime object (1.3.6.1.2.1.1.3), which has been excluded from the view applied to the group, but write access only to the sysName object (1.3.6.1.2.1.1.5): !

```
snmp-server view view_name1 1.3.6.1.2.1.1 included
snmp-server view view_name1 1.3.6.1.2.1.1.3 excluded
snmp-server view view_name2 1.3.6.1.2.1.1.5 included
snmp-server group group_name1 v3 auth read view_name1 write view_name2
```

Verifying Groups

This example shows how to verify the attributes of configured groups:

RP/0/RSP0/CPU0:router# show snmp group

```
groupname: group_name1
readview : view_name1
notifyview: v1default
row status: nonVolatile
|security model:usm
writeview: view_name2
```

Given the following SNMPv3 view and SNMPv3 group configuration:

```
!snmp-server view view_name 1.3.6.1.2.1.1 included
snmp-server group group_name v3 noauth read view_name write view-name
```

!This example shows how to create a noAuthNoPriv user with read and write view access to a system group:
config snmp-server user noauthuser group_name v3



Note

The user must belong to a noauth group before a noAuthNoPriv user can be created.

Only one remote host can be assigned to the same username for SNMP version 3. If you configure the same username with different remote hosts, only the last username and remote host combination will be accepted and will be seen in the show running configuration. In the case of multiple SNMP managers, multiple unique usernames are required.

This example shows the same username case which only the last configuration will be accepted: snmp-server user username nerverctrgrp remote 10.69.236.146 udp-port 162 v3 auth sha <password> priv aes 128 <password> snmp-server user username nerverctrgrp remote 10.214.127.2 udp-port 162 v3 auth sha <password> priv aes 128 <password>

```
snmp-server user username nerverctrgrp remote 10.69.236.147 udp-port 162 v3 auth sha <password> priv aes 128 <password>
RP/0/RSP0/CPU0:router# show run snmp-server user snmp-server user username nerverctrgrp remote 10.69.236.147 udp-port 162 v3 auth sha encrypted <password> priv aes 128 encrypted <password>
```

This example shows all 3 hosts for username1, username2, and username3 will be accepted.

```
:snmp-server user username1 nerverctrgrp remote 10.69.236.146 udp-port 162 v3 auth sha <password> priv aes 128 <password>
snmp-server user username2 nerverctrgrp remote 10.214.127.2 udp-port 162 v3 auth sha <password> priv aes 128 <password>
snmp-server user username3 nerverctrgrp remote 10.69.236.147 udp-port 162 v3 auth sha <password> priv aes 128 <password>
RP/0/RSP0/CPU0:router# show run snmp-server user snmp-server user batmanusr1 nerverctrgrp remote 10.69.236.146 udp-port 162 v3 auth sha encrypted <password> priv aes 128 encrypted <password>
snmp-server user batmanusr2 nerverctrgrp remote 10.214.127.2
```

```
udp-port 162 v3 auth sha encrypted <password> priv aes 128 encrypted <password> snmp-server user
batmanusr3 nerverctrgrp remote 10.69.236.147 udp-port 162 v3 auth sha encrypted <password> priv aes 128
encrypted <password> This example shows how to verify the attributes that apply to the SNMP user:
RP/0/RSP0/CPU0:router# show snmp user User name: noauthuser
Engine ID: localSnmpID
storage-type: nonvolatile active
Given the following SNMPv3 view and SNMPv3 group configuration:
snmp-server view SNMP_VIEW1 1.3.6.1.2.1.1 included
snmp-server group SNMP_GROUP1 v3 auth notify SNMP_VIEW1 read SNMP_VIEW1 write SNMP_VIEW1
```

This example shows how to create a user with authentication (including encryption), read, and write view access to a system group: config

```
snmp-server user userv3authpriv SNMP_GROUP1 v3 auth md5 password123 priv aes 128 password123
```

Given the following SNMPv3 view and SNMPv3 group configuration:

```
! snmp-server view view_name 1.3.6.1.2.1.1 included
```

```
snmp group group_name v3 priv read view_name write view_name
```

! This example shows how to create authNoPriv user with read and write view access to a system group:

```
RP/0/RSP0/CPU0:router(config)# snmp-server user authuser group_name v3 auth md5 clear auth_passwd
```

Note

Because the group is configured at a security level of Auth, the user must be configured as “auth” at a minimum to access this group (“priv” users could also access this group). The authNoPriv user configured in this group, authuser, must supply an authentication password to access the view. In the example, auth_passwd is set as the authentication password string. Note that clear keyword is specified before the auth_passwd password string. The clear keyword indicates that the password string being supplied is unencrypted.

This example shows how to verify the attributes that apply to SNMP user:

```
RP/0/RSP0/CPU0:router# show snmp user
```

```
User name: authuser
```

```
Engine ID: localSnmpID
```

```
storage-type: nonvolatile active
```

Given the following SNMPv3 view and SNMPv3 group configuration:

```
!snmp view view_name 1.3.6.1.2.1.1 included
```

```
snmp group group_name v3 priv read view_name write view_name
```

!This example shows how to create an authPriv user with read and write view access to a system

```
group: config snmp-server user privuser group_name v3 auth md5 clear auth_passwd priv des56 clear
priv_passwd
```

Note

Because the group has a security level of Priv, the user must be configured as a “priv” user to access this group. In this example, the user, privuser, must supply both an authentication password and privacy password to access the OIDs in the view.

This example shows how to verify the attributes that apply to the SNMP user:

```
RP/0/RSP0/CPU0:router# show snmp user
```

```
User name: privuser
```

```
Engine ID: localSnmpID
```

```
storage-type: nonvolatile active
```

Configuring Trap Notifications: Example

The following example configures an SNMP agent to send out different types of traps. The configuration includes a v2c user, a noAuthNoPriv user, anauthNoPriv user, and an AuthPriv user.

Note

The default User Datagram Protocol (UDP) port is 161. If you do not specify a UDP port with the udp-port keyword and port argument, then the configured SNMP trap notifications are sent to port 161.

```
! snmp-server host 10.50.32.170 version 2c public udp-port 2345
```

```

snmp-server host 10.50.32.170 version 3 auth userV3auth udp-port 2345
snmp-server host 10.50.32.170 version 3 priv userV3priv udp-port 2345
snmp-server host 10.50.32.170 version 3 noauth userV3noauth udp-port 2345
snmp-server user userv2c groupv2c v2c
snmp-server user userV3auth groupV3auth v3 auth md5 encrypted 140F0A13
snmp-server user userV3priv groupV3priv v3 auth md5 encrypted 021E1C43 priv des56 encrypted 1110001C
snmp-server user userV3noauth groupV3noauth v3 LROwner
snmp-server view view_name 1.3 included
snmp-server community public RW
snmp-server group groupv2c v2c read view_name
snmp-server group groupV3auth v3 auth read view_name
snmp-server group groupV3priv v3 priv read view_name
snmp-server group groupV3noauth v3 noauth read view_name
! This example shows how to verify the configuration SNMP trap notification recipients host, the recipients of
SNMP trap notifications. The output displays the following information:

```

- IP address of the configured notification host
- UDP port where SNMP notification messages are sent
- Type of trap configured
- Security level of the configured user
- Security model configured 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

```

Setting an IP Precedence Value for SNMP Traffic: Example

The following example shows how to set the SNMP IP Precedence value to 7: configure snmp-server ipv4 precedence 7 exit Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: y

Setting an IP DSCP Value for SNMP Traffic: Example

The following example shows how to set the IP DSCP value of SNMP traffic to 45: configure snmp-server ipv4 dscp 45 exit
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: y

SNMP Context Mapping Configuration

Configuration of VRF Aware SNMP Context for Polling BGP Data

VRF awareness is usually done using existing, non-VRF aware MIB definitions. This means that MIB definition doesn't mention anything about VRFs. However they could be used within VRF context.

The VRF-awareness is done using SNMP contexts, where a SNMP context maps to a specific VRF.

Before you begin

- Ensure that MIB implementation is VRF-aware.
- Ensure that the implementation of all get requests support VRF context.

The following example configures VRF aware SNMP context to allow polling BGP data using BGP4-MIB.

```

snmp-server vrf <vrf_1> context <context_1>
snmp-server community <vrf_1> RW
snmp-server context <context_1>
snmp-server community-map <vrf_1> context <context_1>
snmp-server host <IP> traps version 2c <vrf_1>

```

Verification

The following configuration extracts BGP data from a peer VRF using context.

```
snmp-server vrf V1
context V1_bgp
! snmp-server community V1 RW
snmp-server context V1_bgp
snmp-server community-map V1 context V1_bgp
router bgp 65000 nsr
address-family ipv4 unicast
! address-family vpnv4 unicast
! neighbor 192.0.2.254 remote-as 65001 address-family ipv4 unicast
route-policy ALL in
route-policy ALL out
! vrf V1
rd 111:111
address-family ipv4 unicast
! neighbor 192.0.2.255
remote-as 65003
address-family ipv4 unicast
!
!
!
!
end
```

Configuration of OSPF processes Using SNMP Context

The following example configures data polling from two OSPF processes.

```
snmp-server community com1 RW
snmp-server community com2 RW
snmp-server context ctx1
snmp-server context ctx2
snmp-server community-map com1 context ctx1
snmp-server community-map com2 context ctx2
router ospf one
snmp context ctx1
area 0
interface GigabitEthernet0/2/0/0
!
!
!
router ospf two
snmp context ctx2
area 0
interface GigabitEthernet0/2/0/1
!
!
!
```

Configuration of OSPF Neighbour in VRF

The following example configures OSPF neighbours in VRF using SNMP context.

```
snmp-server vrf VRF_A
context ctx1
!
snmp-server community com1 RW
snmp-server context ctx1
snmp-server community-map com1 context ctx1
router ospf core
vrf VRF_A
snmp context ctx1
!
```

!
end

Additional References

The following sections provide references related to Implementing SNMP on Cisco IOS XR software.

Related Documents

Related Topic	Document Title
Cisco 105 XR SNMP commands	SNMP Server Commands on the Cisco ASR 9000 Series Router module of System Management Command Reference for Cisco ASR 9000 Series Routers
MIB information	Cisco ASR 9000 Series Aggregation Services Routers MIB Specifications Guide
Cisco 105 XR commands	Cisco ASR 9000 Series Aggregation Services Router Commands Master List
Getting started with Cisco 105 XR software	Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide
Information about user groups and task IDs	Configuring AAA Services on the Cisco ASR 9000 Series Router module of System Security Configuration Guide for Cisco ASR 9000 Series Routers
Cisco 105 XR Quality of Service	Modular QoS Configuration Guide for Cisco ASR 9000 Series Routers

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

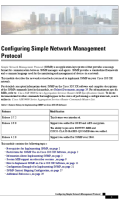
RFCs

RFCs	Title
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC 3417	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Documents / Resources

	<p>CISCO ASR 9000 Series Aggregation Services Routers [pdf] User Guide ASR 9000 Series Aggregation Services Routers, ASR 9000 Series, Aggregation Services Routers, Services Routers, Routers</p>
-------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

References

- [Cisco](#)
- [Cisco](#)
- [Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference, Release 5.3.x - Simple Network Management Protocol \(SNMP\) Server Commands \[Cisco IOS XR Software \(End-of-Sale\)\] - Cisco](#)
- [Support - Cisco Support and Downloads – Documentation, Tools, Cases - Cisco](#)
- [User Manual](#)

