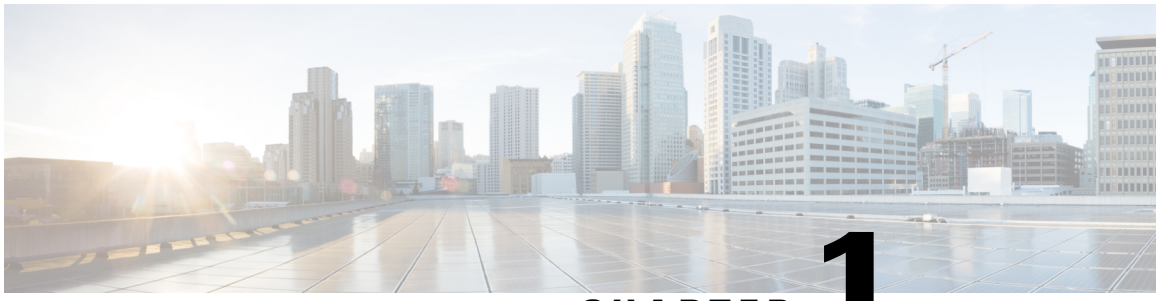
SNMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

First Published: November 19, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

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 that is used for monitoring and managing devices in a network.

This module discusses how to enable an SNMP agent on a Cisco device and how to control the sending of SNMP notifications from the agent. For information about using SNMP management systems, see the appropriate documentation for your network management system (NMS) application.

For a complete description of the device monitoring commands mentioned in this document, see the Cisco Network Management Command Reference. To locate documentation of other commands that appear in this document, use the Cisco IOS Master Command List or search online.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for SNMP

Not all Cisco platforms are supported on the features described in this module. Use Cisco Feature Navigator to find information about platform support and Cisco software image support.

Information About Configuring SNMP Support

Components of SNMP

The 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 monitoring and managing devices in a network.

The SNMP framework has the following components, which are described in the following sections:

SNMP Operations

SNMP applications perform the following operations to retrieve data, modify SNMP object variables, and send notifications:

SNMP Get

The Simple Network Management Protocol (SNMP) GET operation is performed by an Network Management Server (NMS) to retrieve SNMP object variables. There are three types of GET operations:

- GET—Retrieves the exact object instance from the SNMP agent.
- GETNEXT—Retrieves the next object variable, which is a lexicographical successor to the specified variable.
- GETBULK—Retrieves a large amount of object variable data, without the need for repeated GETNEXT operations.

SNMP SET

The Simple Network Management Protocol (SNMP) SET operation is performed by a Network Management Server (NMS) to modify the value of an object variable.

SNMP Notifications

A key feature of SNMP is its capability to generate unsolicited notifications from an SNMP agent.

Traps and Informs

Unsolicited (asynchronous) notifications can be generated as traps or inform requests (informs). Traps are messages alerting the SNMP manager to a condition on the network. Informs are traps that include a request for confirmation of receipt from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighboring device, or other significant events.

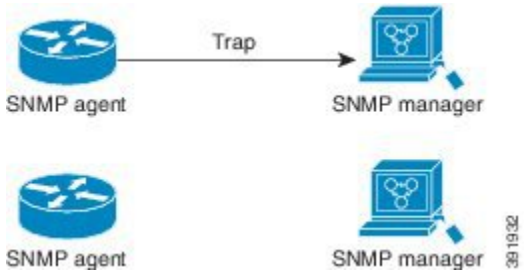
Traps are less reliable than informs because the receiver does not send an acknowledgment when it receives a trap. The sender does not know if the trap was received. An SNMP manager that receives an inform, acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives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

Traps are often preferred even though they are less reliable because informs consume more resources in the device and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform must be held in memory until a response is received or the request times out. Also, traps are sent only once, whereas an inform may be resent several times. The retries increase traffic and contribute to higher overhead on the network. Use of traps and informs requires a trade-off between reliability and resources. If it is important that the SNMP manager receives every notification, use informs, but if traffic volume or memory usage are concerns and receipt of every notification is not required, use traps.

The following figures illustrate the differences between traps and informs.

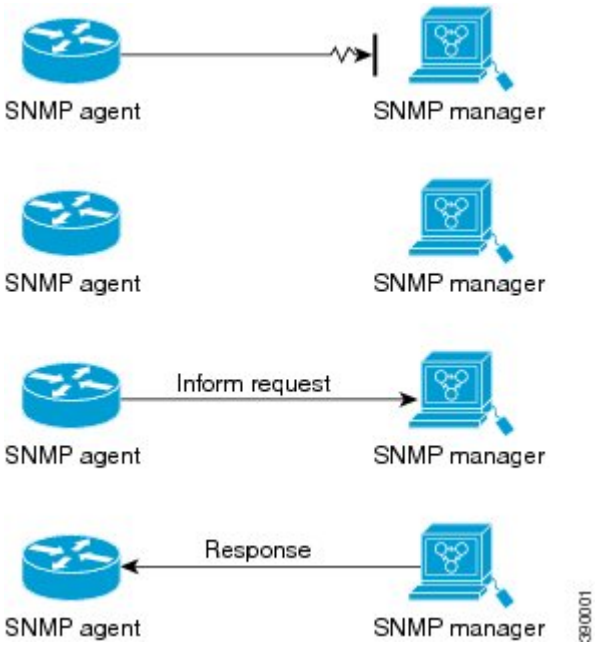
The figure below shows that an agent successfully sends a trap to an SNMP manager. Although the manager receives the trap, it does not send an acknowledgment. The agent has no way of knowing that the trap reached its destination.

Figure 1: Trap Successfully Sent to SNMP Manager



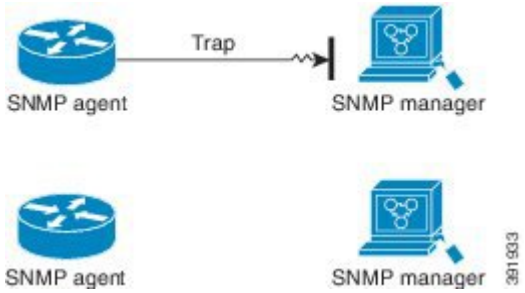
In the figure below, the agent successfully sends an inform to the manager. When the manager receives the inform, a response is sent to the agent and the agent knows that the inform reached its destination. Notice that in this example, the traffic generated is twice as much as in the interaction shown in the table above.

Figure 2: Inform Request Successfully Sent to SNMP Manager



The figure below shows an agent sending a trap to a manager that the manager does not receive. The agent has no way of knowing that the trap did not reach its destination. The manager never receives the trap because traps are not resent.

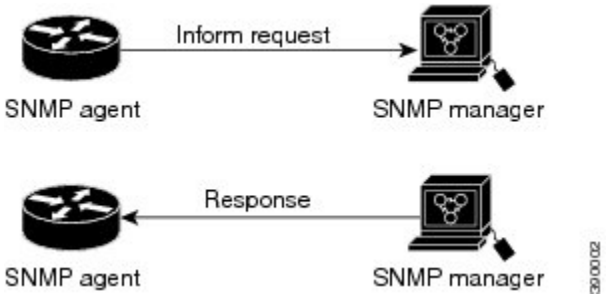
Figure 3: Trap Unsuccessfully Sent to SNMP Manager



The figure below shows an agent sending an inform to a manager that does not reach the manager. Because the manager did not receive the inform, it does not send a response. After a period of time, the agent resends the inform. The manager receives the inform from the second transmission and replies. In this example, more

traffic is generated than in the scenario shown in the table above but the notification reaches the SNMP manager.

Figure 4: Inform Unsuccessfully Sent to SNMP Manager



Versions of SNMP

The Cisco IOS software supports the following versions of SNMP:

- SNMPv1—Simple Network Management Protocol: a full Internet standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.
- SNMPv2c—The community string-based Administrative Framework for SNMPv2. SNMPv2c (the "c" is for "community") is an experimental Internet protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic) and uses the community-based security model of SNMPv1.
- SNMPv3—Version 3 of SNMP. SNMPv3 is an interoperable standards-based protocol defined in RFCs 3413 to 3415. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network.

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensuring that a packet has not been tampered with in transit.
- Authentication—Determining that the message is from a valid source.
- Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of SNMP managers able to access the agent MIB is defined by a community string.

SNMPv2c support includes a bulk retrieval mechanism and 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 types of errors; these conditions are reported through a single error code in SNMPv1. The following three types of exceptions are also reported: no such object, no such instance, and end of MIB view.

SNMPv3 is a security model in which an authentication strategy 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 determines which security mechanism is employed when handling an SNMP packet.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The table below lists the combinations of security models and levels and their meanings.

Table 1: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	Data Encryption Standard (DES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

Note SNMPv2p (SNMPv2 Classic) is not supported in Cisco IOS Release 11.2 and later releases. SNMPv2c replaces the Party-based Administrative and Security Framework of SNMPv2p with a Community-based Administrative Framework. SNMPv2c retained the bulk retrieval and error handling capabilities of SNMPv2p.

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

SNMPv3 supports RFCs 1901 to 1908, 2104, 2206, 2213, 2214, and 2271 to 2275. For additional information about SNMPv3, see RFC 2570, *Introduction to Version 3 of the Internet-standard Network Management Framework* (this is not a standards document).

How to Configure SNMP Support

There is no specific command to enable SNMP. The first **snmp-server** command that you enter enables supported versions of SNMP. All other configurations are optional.

Configuring System Information

You can set the system contact, location, and serial number of the SNMP agent so that these descriptions can be accessed through the configuration file. Although the configuration steps described in this section are optional, configuring the basic information is recommended because it may be useful when troubleshooting your configuration. In addition, the first **snmp-server** command that you issue enables SNMP on the device.

Perform this task as needed.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server contact** *text*
4. **snmp-server location** *text*
5. **snmp-server chassis-id** *number*
6. end
7. **show snmp contact**
8. **show snmp location**
9. **show snmp chassis**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**snmp-server contact** *text* **Example:** `Device(config)# snmp-server contact NameOne`	Sets the system contact string.
Step 4	**snmp-server location** *text* **Example:** `Device(config)# snmp-server location LocationOne`	Sets the system location string.
Step 5	**snmp-server chassis-id** *number* **Example:** `Device(config)# snmp-server chassis-id 015A619T`	Sets the system serial number.
Step 6	end **Example:** `Device(config)# end`	Exits global configuration mode.
Step 7	**show snmp contact** **Example:** `Device# show snmp contact`	(Optional) Displays the contact strings configured for the system.
Step 8	**show snmp location** **Example:** `Device# show snmp location`	(Optional) Displays the location string configured for the system.
Step 9	**show snmp chassis** **Example:** `Device# show snmp chassis`	(Optional) Displays the system serial number.

Enabling the SNMP Agent Shutdown Mechanism

Using SNMP packets, a network management tool can send messages to users on virtual terminals and on the console. This facility operates in a similar fashion to the **send** EXEC command; however, the SNMP request that causes the message to be issued to the users also specifies the action to be taken after the message is delivered. One possible action is a shutdown request. After a system is shut down, typically it is reloaded.

Because the ability to cause a reload from the network is a powerful feature, it is protected by the **snmp-server system-shutdown** global configuration command. If you do not issue this command, the shutdown mechanism is not enabled.

Perform this task to enable the SNMP agent shutdown mechanism.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server system-shutdown**
4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server system-shutdown** **Example:** `Device(config)# snmp-server system-shutdown`	Enables system shutdown using the SNMP message reload feature.
Step 4	end **Example:** `Device(config)# end`	Exits global configuration mode.

Defining the Maximum SNMP Agent Packet Size

You can define the maximum packet size permitted when the SNMP agent is receiving a request or generating a reply.

Perform this task to set the maximum permitted packet size.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server packetsize** *byte-count*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server packetsize** *byte-count* **Example:** `Device(config)# snmp-server packetsize 512`	Establishes the maximum packet size.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Limiting the Number of TFTP Servers Used via SNMP

You can limit the number of TFTP servers used for saving and loading configuration files via SNMP by using an access list. Limiting the use of TFTP servers in this way conserves system resources and centralizes the operation for manageability.

Perform this task to limit the number of TFTP servers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server tftp-server-list** *number*
4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server tftp-server-list** *number* **Example:** `Device(config)# snmp-server tftp-server-list 12`	Limits the number of TFTP servers used for configuration file copies via SNMP to the servers in an access list.
Step 4	end **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

An alternative to using the ifAlias value for the identification of interfaces across reboots is to use the cciDescr object in the Cisco Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB.my). This MIB object can be used only for circuit-based interfaces such as ATM or Frame Relay interfaces. Cisco IOS feature FTS-731 introduced the Circuit Interface Identification Persistence for the Simple Network Management Protocol (SNMP), which maintains the user-defined name of the circuit (defined in the cciDescr object) across reboots and allows consistent identification of circuit-based interfaces.

Configuring SNMP Versions 1 and 2

When you configure SNMP versions 1 and 2, you can optionally create or modify views for community strings to limit which MIB objects an SNMP manager can access.

Perform the following tasks when configuring SNMP version 1 or version 2.

Creating or Modifying an SNMP View Record

You can assign views to community strings to limit which MIB objects an SNMP manager can access. You can use a predefined view or create your own view. If you are using a predefined view or no view at all, skip this task.

Perform this task to create or modify an SNMP view record.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server view** *view-name oid-tree* {**included** | **excluded**}
4. **no snmp-server view** *view-name oid-tree* {**included** | **excluded**}
5. **end**
6. show snmp view

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server view** *view-name oid-tree* {**included** | **excluded**} **Example:** `Device(config)# snmp-server view mib2 mib-2 included`	Creates a view record. • In this example, the mib2 view that includes all objects in the MIB-II subtree is created. **Note** You can use this command multiple times to create the same view record. If a view record for the same OID value is created multiple times, the latest entry of the object identifier takes precedence.

	Command or Action	Purpose
Step 4	**no snmp-server view** *view-name oid-tree* {**included** | **excluded**} **Example:** `Device(config)# no snmp-server view mib2 mib-2 included`	Removes a server view.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode.
Step 6	show snmp view **Example:** `Device# show snmp view`	(Optional) Displays a view of the MIBs associated with SNMP.

Creating or Modifying Access Control for an SNMP Community

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to regulate access to the agent on the device. Optionally, you can specify one or more of the following characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.
- A MIB view, which defines the subset of all MIB objects accessible to the given community.
- Read and write or read-only permission for the MIB objects accessible to the community.

Perform this task to create or modify a community string.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*]
4. **no snmp-server community** *string*
5. **end**
6. **show snmp community**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*] **Example:** `Device(config)# snmp-server community comaccess ro 4`	Defines the community access string. • You can configure one or more community strings.
Step 4	**no snmp-server community** *string* **Example:** `Device(config)# no snmp-server community comaccess`	Removes the community string from the configuration.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode.
Step 6	**show snmp community** **Example:** `Device# show snmp community`	(Optional) Displays the community access strings configured for the system.

Configuring a Recipient of an SNMP Trap Operation

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

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

then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

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

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

A *notification-type* option's availability depends on the device type and Cisco IOS software features supported on the device. For example, the Cisco IOS software does not support the envmon notification type. To see what notification types are available on your system, use the command help (?) at the end of the **snmp-server host** command.

Perform this task to configure the recipient of an SNMP trap operation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-id* [**traps** | **informs**][**version** {**1**| **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port-number*] [*notification-type*]
4. **end**
5. **show snmp host**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** *host-id* [**traps**	**informs**][**version** {**1**| **2c**	**3** [**auth**	**noauth**	**priv**]}] *community-string* [**udp-port** *port-number*] [*notification-type*] **Example:** `Device(config)# snmp-server host 172.16.1.27 version 2c public`	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode.
Step 5	**show snmp host** **Example:** `Device# show snmp host`	(Optional) Displays the SNMP notifications sent as traps, the version of SNMP, and the host IP address of the notifications.

Disabling the SNMP Agent

Perform this task to disable any version of an SNMP agent.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no snmp-server**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no snmp-server** **Example:** `Device(config)# no snmp-server`	Disables SNMP agent operation.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Configuration Examples for SNMP Support

Example: Configuring SNMPv1 Support

The following example shows how to enable SNMPv1. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string named public. This configuration does not cause the router to send traps.

```
Device(config)# snmp-server community public
```

The following example shows how to permit SNMP access to all objects with read-only permission using the community string named public. The router also will send BGP traps to the hosts 172.16.1.111 and 172.16.1.33 using SNMPv1. The community string named public is sent with the traps.

```
Device(config)# snmp-server community public
Device(config)# snmp-server enable traps bgp
Device(config)# snmp-server host 172.16.1.111 version 1 public
Device(config)# snmp-server host 172.16.1.33 public
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host 172.30.2.160 public snmp envmon
```

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

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host example.com public
```

The following example shows a configuration in which no traps are sent to a host. The BGP traps are enabled for all hosts, but only the OSPF traps are enabled to be sent to a host.

```
Device(config)# snmp-server enable traps bgp
Device(config)# snmp-server host host1 public ospf
```

The following example shows how to enable a router to send all informs to the host example.com using the community string named public:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host example.com informs version 2c public
```

The following example shows how to enable the SNMP manager and set the session timeout to a value greater than the default:

```
Device(config)# snmp-server manager
Device(config)# snmp-server manager session-timeout 1000
```

The following example shows how to enable the SNMP manager to access all objects with read-only permissions. The user is specified as *abcd* and the authentication password is *abcdpasswd*. To obtain the automatically generated default local engine ID, use the **show snmp engineID** command.

```
Device(config)# snmp-server view readview internet included
Device(config)# snmp-server view readview iso included
Device(config)# snmp-server group group1 v3 noauth read readview
Device(config)# snmp-server user abcd group1 v3 auth md5 abcdpasswd
```

Example: Show SNMP View

The following example shows the SNMP view for the system OID tree:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server view test system included
Device(config)# end
Device# show snmp view

test system - included nonvolatile active
cac_view pimMIB - included read-only active
cac_view msdpMIB - included read-only active
cac_view interfaces - included read-only active
cac_view ip - included read-only active
cac_view ospf - included read-only active
.
.
.
v1default iso - included permanent active
v1default internet - included permanent active
v1default snmpUsmMIB - excluded permanent active
v1default snmpVacmMIB - excluded permanent active
v1default snmpCommunityMIB - excluded permanent active
v1default ciscoIpTapMIB - excluded permanent active
v1default ciscoMgmt.395 - excluded permanent active
v1default ciscoTap2MIB - excluded permanent active
.
.
.
```

Example Configuring SNMP Community Access Strings

The following example shows the community access strings configured to enable access to the SNMP manager:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server community public ro
Device(config)# snmp-server community private rw
Device(config)# end
Device# show snmp community

Community name: private
```

```
Community Index: private
Community SecurityName: private
storage-type: nonvolatile active
Community name: public
Community Index: public
Community SecurityName: public
storage-type: nonvolatile active
```

Example Configuring Host Information

The following example shows the host information configured for SNMP notifications:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server host 10.2.28.1 inform version 2c public
Device(config)# end
Device# show snmp host

Notification host: 10.2.28.1 udp-port: 162   type: inform
user: public    security model: v2c
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
SNMP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS SNMP Command Reference
Cisco implementation of RFC 1724, RIP Version 2 MIB Extensions	RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions feature module
DSP Operational State Notifications for notifications to be generated when a digital signaling processor (DSP) is used	DSP Operational State Notifications feature module

Standards and RFCs

Standard/RFC	Title
CBC-DES (DES-56) standard	*Symmetric Encryption Protocol*
STD: 58	*Structure of Management Information Version 2 (SMIv2)*
RFC 1067	*A Simple Network Management Protocol*

Standard/RFC	Title
RFC 1091	*Telnet terminal-type option*
RFC 1098	*Simple Network Management Protocol (SNMP)*
RFC 1157	*Simple Network Management Protocol (SNMP)*
RFC 1213	*Management Information Base for Network Management of TCP/IP-based internets:MIB-II*
RFC 1215	*Convention for defining traps for use with the SNMP*
RFC 1901	*Introduction to Community-based SNMPv2*
RFC 1905	*Common Management Information Services and Protocol over TCP/IP (CMOT)*
RFC 1906	*Telnet X Display Location Option*
RFC 1908	*Simple Network Management Protocol (SNMP)*
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*
RFC 2206	*RSVP Management Information Base using SMIv2*
RFC 2213	*Integrated Services Management Information Base using SMIv2*
RFC 2214	*Integrated Services Management Information Base Guaranteed Service Extensions using SMIv2*
RFC 2271	*An Architecture for Describing SNMP Management Frameworks*
RFC 2570	*Introduction to Version 3 of the Internet-standard Network Management Framework*
RFC 2578	*Structure of Management Information Version 2 (SMIv2)*
RFC 2579	*Textual Conventions for SMIv2*
RFC 2580	*Conformance Statements for SMIv2*
RFC 2981	*Event MIB*
RFC 2982	*Distributed Management Expression MIB*
RFC 3413	*SNMPv3 Applications*
RFC 3415	*View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

Standard/RFC	Title
RFC 3418	*Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

MIBs

MIB	MIBs Link
• Circuit Interface Identification MIB • Cisco SNMPv2 • Ethernet-like Interfaces MIB • Event MIB • Expression MIB Support for Delta, Wildcarding, and Aggregation • Interfaces Group MIB (IF-MIB) • Interfaces Group MIB Enhancements • MIB Enhancements for Universal Gateways and Access Servers • MSDP MIB • NTP MIB • Response Time Monitor MIB • Virtual Switch MIB	To locate and download MIBs for selected platforms, releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

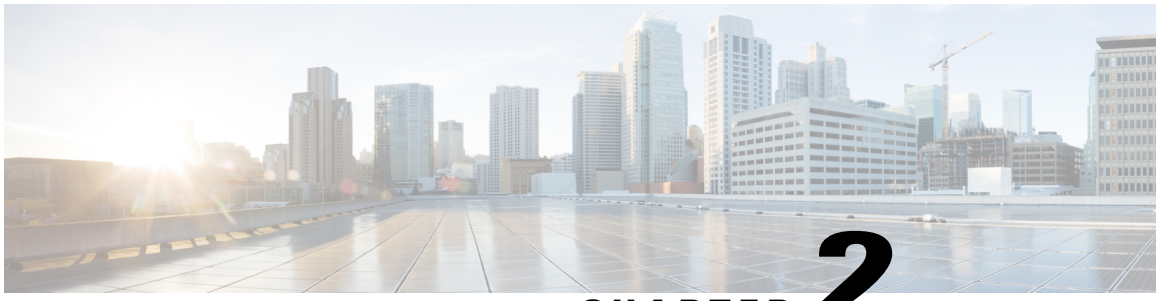
Feature Information for Simple Network Management Protocol

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 2: Feature Information for Simple Network Management Protocol

Feature Name	Releases	Feature Information
SNMP (Simple Network Management Protocol)	Cisco IOS XE Release 3.3SE	The Simple Network Management Protocol (SNMP) feature provides an application-layer protocol that facilitates the exchange of management information between network devices. SNMP is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.



CHAPTER 2

SNMP Inform Request

The Simple Network Management Protocol (SNMP) Inform Requests feature allows devices to send inform requests to SNMP managers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About SNMP Inform Requests

SNMP Inform Request

The SNMP Inform Request feature supports sending inform requests. SNMP asynchronous notifications are usually sent as SNMP traps.

Traps are less reliable than informs because an acknowledgment is not sent from the receiving end when a trap is received; however, an SNMP manager that receives an inform acknowledges the message with an SNMP response PDU. If the sender does not receive a response for an inform, the inform can be sent again.

How to Configure SNMP Inform Requests

Configuring Devices to Send Traps

Perform the following task to configure the device to send traps to a host in global configuration mode:

SUMMARY STEPS

1. enable
2. **configure terminal**
3. **snmp-server host** *host*[**version {1|2c}**]*community-string*[**udp-port** *port*][*notification-type*]
4. **snmp-server enable traps**[*notification-type*] [*notification-option*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** *host*[**version {1|2c}**]*community-string*[**udp-port** *port*][*notification-type*] **Example:** `Device(config)# snmp-server host 10.10.10.10 version 1 public udp-port 2012`	Specifies the recipient of the trap message.
Step 4	**snmp-server enable traps**[*notification-type*] [*notification-option*] **Example:** `Device(config)# snmp-server enable traps alarms 3`	Globally enables the trap production mechanism for the specified traps. **Note** Some traps are not controlled by the **snmp-serverenabletraps** command. These traps are either enabled by default or controlled through other commands. For example, by default, SNMP link traps are sent when an interface goes up or down. For interfaces expected to go up and down during normal usage, such as ISDN interfaces, the output generated by

	Command or Action	Purpose
		these traps may not be useful. Use the **nosnmptrapslink-status** interface configuration command to disable these traps. In order for a host to receive a trap, an **snmp-serverhost** command must be configured for that host, and the trap must be enabled globally through the **snmp-serverenabletraps** command, through a different command, such as **snmptrapslink-status**, or by default.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Changing Inform Operation Values

Perform the following optional task in global configuration mode to change inform operation values:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server informs** [**retries** *retries*] [**timeout** *seconds*] [**pending** *pending*]
4. **snmp-server trap-source** *interface*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server informs** [**retries** *retries*] [**timeout** *seconds*] [**pending** *pending*]	Configures inform-specific operation values. • This example sets the maximum number of times to resend an inform, the number of seconds to wait for an

	Command or Action	Purpose
	Example: `Device(config)# snmp-server informs retries 10 timeout 30 pending 100`	acknowledgment before resending, and the maximum number of informs waiting for acknowledgments at any one time.
Step 4	**snmp-server trap-source** *interface* **Example:** `Device(config)# snmp-server trap-source Gigabitethernet 1/2/1`	This example sets the IP address for the Fast Ethernet interface in slot2, port 1 as the source for all SNMP notifications.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Configuration Examples for SNMP Inform Request

Example: Configuring SNMP Inform Request

The following configuration example shows how to configure the SNMP Inform Request feature for SNMPv1 or SNMPv2:

The following example sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host 172.30.2.160 public snmp envmon
```

The following example enables the device to send all traps to the host myhost.example.com using the community string public:

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

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

```
Device(config)# snmp-server enable traps bgp
Device(config)# snmp-server host bob public isdn
```

The following example enables the device to send all inform requests to the host myhost.example.com using the community string public:

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
SNMP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS SNMP Command Reference
Cisco implementation of RFC 1724, RIP Version 2 MIB Extensions	RIPv2 Monitoring with SNMP Using the RFC 1724 MIB Extensions feature module
DSP Operational State Notifications for notifications to be generated when a digital signaling processor (DSP) is used	DSP Operational State Notifications feature module

Standards and RFCs

Standard/RFC	Title
CBC-DES (DES-56) standard	*Symmetric Encryption Protocol*
STD: 58	*Structure of Management Information Version 2 (SMIv2)*
RFC 1067	*A Simple Network Management Protocol*
RFC 1091	*Telnet terminal-type option*
RFC 1098	*Simple Network Management Protocol (SNMP)*
RFC 1157	*Simple Network Management Protocol (SNMP)*
RFC 1213	*Management Information Base for Network Management of TCP/IP-based internets:MIB-II*
RFC 1215	*Convention for defining traps for use with the SNMP*
RFC 1901	*Introduction to Community-based SNMPv2*
RFC 1905	*Common Management Information Services and Protocol over TCP/IP (CMOT)*
RFC 1906	*Telnet X Display Location Option*
RFC 1908	*Simple Network Management Protocol (SNMP)*

Standard/RFC	Title
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*
RFC 2206	*RSVP Management Information Base using SMIv2*
RFC 2213	*Integrated Services Management Information Base using SMIv2*
RFC 2214	*Integrated Services Management Information Base Guaranteed Service Extensions using SMIv2*
RFC 2271	*An Architecture for Describing SNMP Management Frameworks*
RFC 2570	*Introduction to Version 3 of the Internet-standard Network Management Framework*
RFC 2578	*Structure of Management Information Version 2 (SMIv2)*
RFC 2579	*Textual Conventions for SMIv2*
RFC 2580	*Conformance Statements for SMIv2*
RFC 2981	*Event MIB*
RFC 2982	*Distributed Management Expression MIB*
RFC 3413	*SNMPv3 Applications*
RFC 3415	*View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*
RFC 3418	*Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

MIBs

MIB	MIBs Link
• Circuit Interface Identification MIB • Cisco SNMPv2 • Ethernet-like Interfaces MIB • Event MIB • Expression MIB Support for Delta, Wildcarding, and Aggregation • Interfaces Group MIB (IF-MIB) • Interfaces Group MIB Enhancements • MIB Enhancements for Universal Gateways and Access Servers • MSDP MIB • NTP MIB • Response Time Monitor MIB • Virtual Switch MIB	To locate and download MIBs for selected platforms, releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

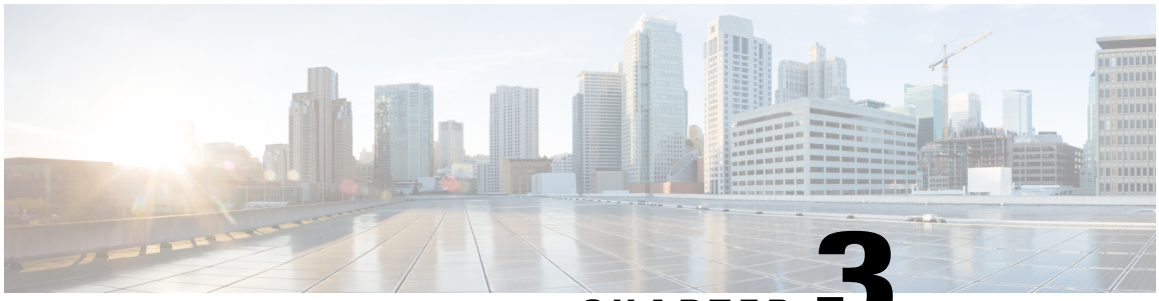
Feature Information for SNMP Inform Request

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 3: Feature Information for SNMP Inform Request

Feature Name	Releases	Feature Information
SNMP Inform Request	Cisco IOS XE Release 3.3SE	The SNMP Inform Request feature supports sending inform requests. SNMP asynchronous notifications are usually sent as SNMP traps. Traps are less reliable than informs because an acknowledgment is not sent from the receiving end when a trap is received; however, an SNMP manager that receives an inform acknowledges the message with an SNMP response PDU. If the sender does not receive a response for an inform, the inform can be sent again. In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.



CHAPTER 3

SNMPv2c

Community-based Simple Network Management Protocol Version 2 (SNMPv2c) is an experimental Internet protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is the community string-based administrative framework for SNMPv2. Community string is a type of password, which is transmitted in cleartext. SNMPv2c is an update of the protocol operations and data types of party-based Simple Network Management Protocol Version 2 (SNMPv2p) and uses the community-based security model of SNMPv1.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About SNMPv2c

Security Features in SNMPv2c

Community-based Simple Network Management Protocol Version 2 (SNMPv2c) uses a community-based form of security. The community of SNMP managers that are able to access the agent MIB is defined by an IP address access control list (ACL) and password.

The improved error handling support provided by SNMPv2c includes expanded error codes that distinguish different types of errors; all types of errors are reported through a single error code in SNMPv1. The following three types of exceptions are also reported: no such object, no such instance, and end of MIB view. The following are the details of SNMv2c security model:

- Level of security: noAuthNoPriv
- Authentication method: Community String
- Availability of encryption: No

Depending on your release, the party-based SNMP Version 2 (SNMPv2p), which is another variant of SNMPv2, is not supported. SNMPv2c replaces the party-based administrative and security framework of SNMPv2p with a community-based administrative framework. SNMPv2c retains the bulk retrieval and error handling capabilities of SNMPv2p.

How to Configure SNMPv2c

Configuring the SNMP Server for SNMPv2c

To configure a Simple Network Management Protocol (SNMP) server user, specify an SNMP group or a table that maps SNMP users to SNMP views. Then, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID by using the **snmp-server engineID** command for the remote agent. The SNMP engine ID of the remote agent is required to compute the authentication or privacy digests for the SNMP password. If the remote engine ID is not configured first, the configuration command will fail.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For SNMP notifications such as inform requests, the authoritative SNMP agent is the remote agent. You must configure the SNMP engine ID of the remote agent in the SNMP database before you can send proxy requests or inform requests to it.

Note An SNMP user cannot be removed if the engine ID is changed after configuring the SNMP user. To remove the user, you must first reconfigure all the SNMP configurations.

Note Default values do not exist for authentication or privacy algorithms when you configure the SNMP commands. Also, no default passwords exist. The minimum length for a password is one character, although we recommend that you use at least eight characters for security. If you forget a password, you cannot recover it and must reconfigure the user. You can specify either a plain text password or a localized Message Digest 5 (MD5) digest.

Perform this task to specify an SNMP server group name and to add a new user to an SNMP group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server group** [*group-name* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}] [**access** *access-list* | *access-list-name* | **ipv6-list**]
4. **snmp-server engineID** {**local** *engine-id* | **remote** *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engine-id-string*}
5. **snmp-server user** *user-name group-name* [**remote** *ip-address* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server group** [*group-name* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}] [**access** *access-list* | *access-list-name* | **ipv6-list**] **Example:** `Device(config)# snmp-server group g1 v3 auth access lmnop`	Configures the SNMP server group to enable authentication for members of a specified named access list. • In this example, the SNMP server group group1 is configured to enable user authentication for members of the named access list lmnop.
Step 4	**snmp-server engineID** {**local** *engine-id* | **remote** *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engine-id-string*}	Configures the SNMP engine ID. • In this example, the SNMP engine ID is configured for a remote user.

	Command or Action	Purpose
	Example: `Device(config)# snmp-server engineID remote 172.16.15.4 udp-port 120 1a2833c0129a`	
Step 5	**snmp-server user** *user-name group-name* [**remote** *ip-address* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*] **Example:** `Device(config)# snmp-server user user1 group1 v3 auth md5 password123`	Adds a new user to an SNMP v3 group and configures a plain text password for the user. **Note** For the *auth-password* argument, the minimum length is one character; the recommended length is at least eight characters, and the password should include both letters and numbers. **Note** If you have the localized MD5 or Secure Hash Algorithm (SHA) digest, you can specify the digest 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. Also, the digest should be exactly 16 octets in length.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Verifying SNMPv2c

Perform this task to verify the SNMPv2c configuration. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show snmp group**
3. **show snmp user** [*username*]
4. **show snmp engineID**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

Example:
```
Device> enable
```

Step 2 **show snmp group**

Displays information about each SNMP group in the network.

Example:

```
Device# show snmp group

groupname: V1                                 security model:v1
readview : v1default                          writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active
groupname: ILMI                               security model:v1
readview : *ilmi                              writeview: *ilmi
notifyview: <no notifyview specified>
row status: active
groupname: ILMI                               security model:v2c
readview : *ilmi                              writeview: *ilmi
notifyview: <no notifyview specified>
row status: active
groupname: group1                             security model:v1
readview : v1default                          writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active
```

Step 3 **show snmp user** [*username*]

Displays information about configured characteristics of an SNMP user.

Example:

```
Device# show snmp user user1

User name: user1
Engine ID: 000000090200000000C025808
storage-type: nonvolatile       active access-list: 10
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: group1
```

Step 4 **show snmp engineID**

Displays information about the SNMP engine ID that is configured for an SNMP user.

Example:

```
Device# show snmp engineID

Local SNMP engineID: 1A2836C0129A
Remote Engine ID          IP-addr    Port
1A2833C0129A            remote  10.2.28.1 120
```

Configuration Examples for SNMPv2c

Example: Configuring the SNMP Server for SNMPv2c

The following example shows how to configure SNMPv2c. The configuration permits any SNMP manager to access all objects with read-only permissions by using the community string named “public”. This configuration does not cause the device to send traps.

```
Device(config)# snmp-server community public
```

The following example shows how to configure a remote user to receive traps at the “noAuthNoPriv” security level when the SNMPv2c security model is enabled:

```
Device(config)# snmp-server group group1 v2c noauth
Device(config)# snmp-server user remoteuser1 group1 remote 10.12.8.4
Device(config)# snmp-server host 10.12.8.4 informs version 2c noauth remoteuser config
```

The following example shows how to configure a remote user to receive traps at the “authNoPriv” security level when the SNMPv2c security model is enabled:

```
Device(config)# snmp-server group group2 v2c auth
Device(config)# snmp-server user AuthUser group2 remote 10.12.8.4 v2c auth md5 password1
```

The following example shows how to configure a remote user to receive traps at the “priv” security level when the SNMPv2c security model is enabled:

```
Device(config)# snmp-server group group3 v2c priv
Device(config)# snmp-server user PrivateUser group3 remote 10.12.8.4 v2c auth md5 password1
 priv access des56
```

Additional References for SNMPv2c

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
SNMP commands	Cisco IOS SNMP Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 1901	*Community-based SNMPv2*
RFC 1905	*Simple Network Management Protocol (SNMPv2)*
RFC 1907	*Management Information Base for SNMPv2*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

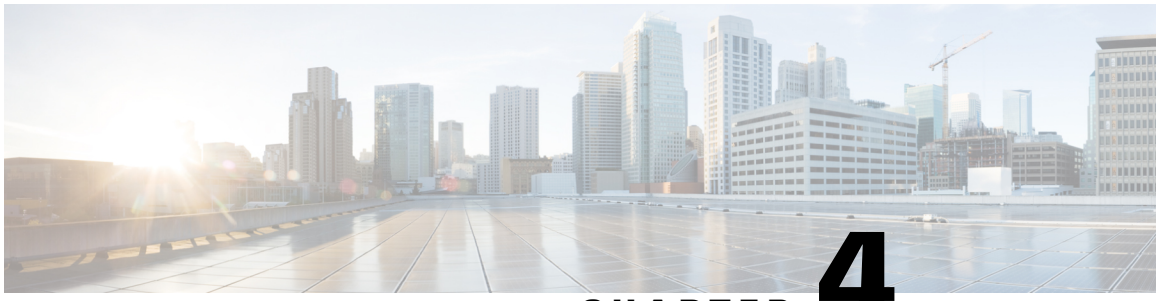
Feature Information for SNMPv2c

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 4: Feature Information for SNMV2c

Feature Name	Releases	Feature Information
SNMV2c	Cisco IOS XE Release 3.3SE	SNMPv2c feature represents the community string-based administrative framework for SNMPv2. SNMPv2c support includes a bulk retrieval mechanism and detailed error message reporting to management stations. In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.



CHAPTER 4

SNMP Version 3

The SNMP Version 3 feature provides secure access to devices by authenticating and encrypting data packets over the network. Simple Network Management Protocol version 3 (SNMPv3) is an interoperable, standards-based protocol that is defined in RFCs 3413 to 3415. This module discusses the security features provided in SNMPv3 and describes how to configure the security mechanism to handle SNMP packets.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About SNMP Version 3

Security Features in SNMP Version 3

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with during transit.

- Authentication—Determines that the message is from a valid source.
- Encryption—Scrambles the content of a packet to prevent it from being learned by an unauthorized source.

SNMPv3 is a security model in which an authentication strategy is set up for a user and the group in which the user resides. Security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used when handling an SNMP packet.

The table below describes the combinations of SNMPv3 security models and levels.

Table 5: SNMP Version 3 Security Levels

Level	Authentication	Encryption	What Happens
noAuthNoPriv	Username	No	Uses a username match for authentication.
authNoPriv	Message Digest Algorithm 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the Hashed Message Authentication Code (HMAC)-MD5 or HMAC-SHA algorithms.
authPriv	MD5 or SHA	Data Encryption Standard (DES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. In addition to authentication, provides DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES (DES-56) standard.

SNMPv3 supports RFCs 1901 to 1908, 2104, 2206, 2213, 2214, and 2271 to 2275. For more information about SNMPv3, see *RFC 2570, Introduction to Version 3 of the Internet-standard Network Management Framework* (this document is not a standard).

Cisco-Specific Error Messages for SNMP Version 3

Simple Network Management Protocol Version 3 (SNMPv3) provides different levels of security. If an authentication or an authorization request fails, a descriptive error message appears to indicate what went wrong. These error messages comply with *RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

You can use the **snmp-server usm cisco** command to disable the descriptive messages, thus preventing malicious users from misusing the information shown in the error messages. The table below describes the Cisco-specific error messages shown when the **snmp-server usm cisco** command is used, and the table compares these messages with the corresponding RFC 3414-compliant error messages.

Table 6: Cisco-Specific Error Messages for SNMPv3

Configured Security Level	Security Level of Incoming SNMP Message	RFC 3414-Compliant Error Indication	Cisco-Specific Error Messages
noAuthNoPriv	noAuthNoPriv	No error	No error
	authNoPriv	unsupportedSecurityLevel	unknownUserName
	authPriv	unsupportedSecurityLevel	unknownUserName
authNoPriv	noAuthNoPriv	AUTHORIZATION_ERROR	unknownUserName
	authNoPriv with correct authentication password	No error	No error
	authNoPriv with incorrect authentication password	wrongDigests	unknownUserName
	authPriv	unsupportedSecurityLevel	unknownUserName
authPriv	noAuthNoPriv	AUTHORIZATION_ERROR	unknownUserName
	authNoPriv with correct authentication password	AUTHORIZATION_ERROR	unknownUserName
	authNoPriv with incorrect authentication password	AUTHORIZATION_ERROR	unknownUserName
	authPriv with correct authentication password and correct privacy password	No error	No error
	authPriv with correct authentication password and incorrect privacy password	No response	No response
	authPriv with incorrect authentication password and correct privacy password	wrongDigests	unknownUserName
	authPriv with incorrect authentication password and incorrect privacy password	wrongDigests	unknownUserName

Note If an SNMP user belonging to an SNMP group is not configured with the password or if the group security level is not the same as the user security level, the error shown is “AUTHORIZATION_ERROR”. The Cisco-specific error message for this scenario is “unknownUserName”.

How to Configure SNMP Version 3

To configure the Simple Network Management Protocol Version 3 (SNMPv3) security mechanism and to use it to handle SNMP packets, you must configure SNMP groups and users with passwords.

Configuring the SNMP Server

To configure an SNMP server user, specify an SNMP group or a table that maps SNMP users to SNMP views. Then, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID by using the **snmp-server engineID** command for the remote agent. The SNMP engine ID of the remote agent is required to compute the authentication or privacy digests for the SNMP password. If the remote engine ID is not configured first, the configuration command will fail.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For SNMP notifications such as inform requests, the authoritative SNMP agent is the remote agent. You must configure the SNMP engine ID of the remote agent in the SNMP database before you can send proxy requests or inform requests to it.

Note The SNMP user cannot be removed if the engine ID is changed after configuring the SNMP user. To remove the user, you must first reconfigure all the SNMP configurations.

Note Default values do not exist for authentication or privacy algorithms when you configure the SNMP commands. Also, no default passwords exist. The minimum length for a password is one character, although it is recommended to use at least eight characters for security. If you forget a password, you cannot recover it and must reconfigure the user. You can specify either a plain text password or a localized MD5 digest.

Perform this task to specify an SNMP server group name and to add a new user to an SNMP group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server group** [*group-name* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** *access-list*]
4. **snmp-server engineID** {**local** *engine-id* | **remote** *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engine-id-string*}
5. **snmp-server user** *user-name group-name* [**remote** *ip-address* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server group** [*group-name* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** *access-list*] **Example:** `Device(config)# snmp-server group group1 v3 auth access lmnop`	Configures the SNMP server group to enable authentication for members of a specified named access list. • In this example, the SNMP server group group1 is configured to enable user authentication for members of the named access list lmnop.
Step 4	**snmp-server engineID** {**local** *engine-id* | **remote** *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engine-id-string*} **Example:** `Device(config)# snmp-server engineID remote 172.16.15.4 udp-port 120 1a2833c0129a`	Configures the SNMP engine ID. • In this example, the SNMP engine ID is configured for a remote user.
Step 5	**snmp-server user** *user-name group-name* [**remote** *ip-address* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]	Adds a new user to an SNMPv3 group and configures a plain text password for the user. **Note** For the *auth-password* argument, the minimum length is one character; the recommended length is at least eight characters, and the password should include both letters and numbers.

	Command or Action	Purpose
	Example: `Device(config)# snmp-server user user1 group1 v3 auth md5 password123`	**Note** If you have the localized MD5 or SHA digest, you can specify the digest 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. Also, the digest should be exactly 16 octets in length.
Step 6	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Verifying SNMP Version 3

Perform this task to verify the Simple Network Management Protocol Version 3 (SNMPv3) configuration. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show snmp group**
3. **show snmp user** [*username*]
4. **show snmp engineID**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**show snmp group**
	Example:
	`Device# show snmp group`
	`groupname: V1 security model:v1`
	`readview : v1default writeview: <no writeview specified>`
	`notifyview: <no notifyview specified>`
	`row status: active`
	`groupname: ILMI security model:v1`
	`readview : *ilmi writeview: *ilmi`
	`notifyview: <no notifyview specified>`
	`row status: active`
		Displays information about each SNMP group in the network.
		Displays information about each SNMP group in the network.

	Command or Action	Purpose
	groupname: ILMI security model:v2c readview : *ilmi writeview: *ilmi notifyview: <no notifyview specified> row status: active groupname: group1 security model:v1 readview : v1default writeview: <no writeview specified> notifyview: <no notifyview specified> row status: active	

Step 3	**show snmp user** [*username*]
	
	Example:
	`Device# show snmp user user1`
	
	`User name: user1`
	`Engine ID: 000000090200000000C025808`
	`storage-type: nonvolatile active access-list: 10`
	`Rowstatus: active`
	`Authentication Protocol: MD5`
	`Privacy protocol: DES`
	`Group name: group1`
		Displays information about configured characteristics of an SNMP user.

Step 4	**show snmp engineID**
	
	Example:
	`Device# show snmp engineID`
	
	`Local SNMP engineID: 1A2836C0129A`
	`Remote Engine ID IP-addr Port`
	`1A2833C0129A remote 10.2.28.1 120`
		Displays information about the SNMP engine ID that is configured for an SNMP user.

Configuration Examples for SNMP Version 3

Example: Configuring SNMP Version 3

The following example shows how to enable Simple Network Management Protocol Version 3 (SNMPv3). The configuration permits any SNMP manager to access all objects with read-only permissions using the community string named “public”. This configuration does not cause the device to send traps.

```
Device(config)# snmp-server community public
```

The following example shows how to configure a remote user to receive traps at the “noAuthNoPriv” security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server group group1 v3 noauth
Device(config)# snmp-server user remoteuser1 group1 remote 10.12.8.4
Device(config)# snmp-server host 10.12.8.4 informs version 3 noauth remoteuser config
```

The following example shows how to configure a remote user to receive traps at the “authNoPriv” security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server group group2 v3 auth
Device(config)# snmp-server user AuthUser group2 remote 10.12.8.4 v3 auth md5 password1
```

The following example shows how to configure a remote user to receive traps at the “priv” security level when the SNMPv3 security model is enabled:

```
Device(config)# snmp-server group group3 v3 priv
Device(config)# snmp-server user PrivateUser group3 remote 10.12.8.4 v3 auth md5 password1
 priv access des56
```

Additional References for SNMP Version 3

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
SNMP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS SNMP Support Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*
RFC 2570	*Introduction to Version 3 of the Internet-standard Network Management Framework*
RFC 2576	*Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*
RFC 3413	*SNMPv3 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)*

MIBs

MIB	MIBs Link
SNMP-COMMUNITY-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

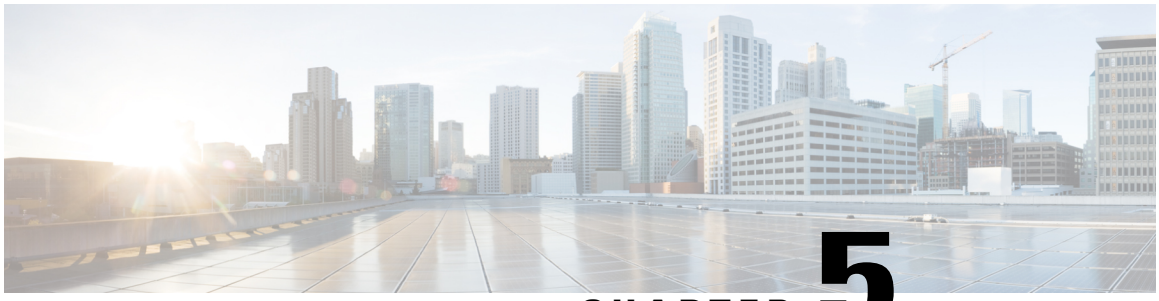
Feature Information for SNMP Version 3

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 7: Feature Information for SNMP Version 3

Feature Name	Releases	Feature Information
SNMP Version 3	Cisco IOS XE Release 3.3SE	The SNMP Version 3 feature is used to provide secure access to devices by authenticating and encrypting data packets over the network. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco Catalyst 3850 Series Switches.



CHAPTER 5

AES and 3-DES Encryption Support for SNMP Version 3

The AES and 3-DES Encryption Support for SNMP Version 3feature enhances the encryption capabilities of SNMP version 3. This support for Simple Network Management Protocol (SNMP) version 3 User-Based Security Model (USM) is complaint with RFC 3414, which defines DES as the only required method of message encryption for SNMP version 3 authPriv mode.

The AES and 3-DES Encryption Support for SNMP Version 3 feature adds Advanced Encryption Standard (AES) 128-bit encryption in compliance with RFC 3826. RFC 3826 extensions have been included in the SNMP-USM-AES-MIB. In addition, Cisco-specific extensions to support Triple-Data Encryption Algorithm (3-DES) and AES 192-bit and 256-bit encryption have been added to the CISCO-SNMP-USM-MIB. Additional information can be found in the Internet-Draft titled *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in "Outside" CBC Mode,* which can be found at the following URL: http://www.snmp.com/eso/draft-reeder-snmpv3-usm-3desede-00.txt.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for AES and 3-DES Encryption Support for SNMP Version 3

- The network management station (NMS) must support SNMP version 3 to use this feature of the SNMP agent.
- This feature is available in Cisco IOS XE software images where encryption algorithms are supported.

Information About AES and 3-DES Encryption Support for SNMP Version 3

SNMP Architecture

The architecture for describing Internet Management Frameworks contained in RFC 3411 describes the SNMP engine as composed of the following components:

- Dispatcher
- Message Processing Subsystem
- Security Subsystem
- Access Control Subsystem

Applications make use of the services of these subsystems. It is important to understand the SNMP architecture and the terminology of the architecture to understand where the Security Model fits into the architecture and interacts with the other subsystems within the architecture. The information is contained in RFC 3411 and your are encouraged to review this RFC to obtain an understanding of the SNMP architecture and subsystem interactions.

Encryption Key Support

In the AES and 3-DES Encryption Support for SNMP Version 3 feature the Cipher Block Chaining/Data Encryption Standard (CBC-DES) is the privacy protocol. Originally only DES was supported (as per RFC 3414). This feature adds support for AES-128 (as per RFC 3826) and AES-192, AES-256 and 3-DES (as per CISCO-SNMP-USM-OIDS-MIB).

- AES encryption uses the Cipher Feedback (CFB) mode with encryption key sizes of 128, 192, or 256 bits.
- 3DES encryption uses the 168-bit key size for encryption.

The AES Cipher Algorithm in the SNMP User-based Security Model draft describes the use of AES with 128-bit key size. However, the other options are also implemented with the extension to use the USM. There is currently no standard for generating localized keys for 192- or 256-bit size keys for AES or for 168-bit size key for 3-DES. There is no authentication protocol available with longer keys.

Management Information Base Support

The AES and 3-DES Encryption Support for SNMP Version 3AES and 3-DES Encryption Support for SNMP Version 3 feature supports the selection of privacy protocols through the CLI and the Management Information Base (MIB). A new standard MIB, SNMP-USM-AES-MIB, provides support for the 128-bit key in AES. The extended options of AES with 192- or 256-bit keys and 3-DES are supported as extensions to the SNMP-USM-MIB, in the Cisco-specific MIB, CISCO-SNMP-USM-OIDS-MIB.

How to Configure AES and 3-DES Encryption Support for SNMP Version 3

Adding a New User to an SNMP Group

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**priv** {**des** | **3des** | **aes {128 | 192 |256}**} *privpassword*] [**access** [**ipv6** *nacl*] {*acl-number* | *acl-name*}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**priv** {**des** | **3des** | **aes {128 | 192 |256}**} *privpassword*] [**access** [**ipv6** *nacl*] {*acl-number* | *acl-name*}]	Adds an SNMP user, specifies a group to which the user belongs, specifies the authorization algorithm to be used (MD5 or SHA), specifies the privacy algorithm to be used (DES, 3-DES, AES, AES-192, or AES-256), and specifies the password to be associated with this privacy protocol.

	Command or Action	Purpose
	Example: `Device(config)# snmp-server user new-user new-group v3 auth md5 secureone priv aes 128 privatetwo access 2`	

Verifying SNMP User Configuration

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

Note The **show snmp user** command displays all the users configured on the router. However, unlike other SNMP configurations, the **snmp-server user** command will not appear on the "show running" output.

SUMMARY STEPS

1. **enable**
2. **show snmp user** [*username*

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode. Enter your password when prompted.

Step 2 **show snmp user** [*username*
The following example specifies the username as abcd, the engine ID string as 00000090200000000C025808, and the storage type as nonvolatile:

Example:

```
Device# show snmp user
 abcd
User name: abcd
Engine ID: 00000090200000000C025808
storage-type: nonvolatile       active access-list: 10
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: 3DES
Group name: VacmGroupName
Group name: VacmGroupName
```

Additional References

Related Documents

Related Topic	Document Title
Cisco software commands	Cisco IOS Master Command List, All Releases
Cisco Network Management commands	*Cisco IOS Network Management Command Reference*
SNMP configuration	" Configuring SNMP Support " chapter in the *Cisco Network Management Configuration Guide*
SNMP Support for VPNs	SNMP Notification Support for VPNs

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• CISCO-PING-MIB • IP-FORWARD-MIB • SNMP-VACM-MIB, *The View-based Access Control Model (ACM) MIB for SNMP*	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1441	*Introduction to version 2 of the Internet-standard Network Management Framework*
RFC 1442	*Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1443	*Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)*

RFC	Title
RFC 1444	*Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1445	*Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1446	*Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1447	*Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1448	*Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1449	*Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1450	*Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 2571	*An Architecture for Describing SNMP Management Frameworks*
RFC 2576	*Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

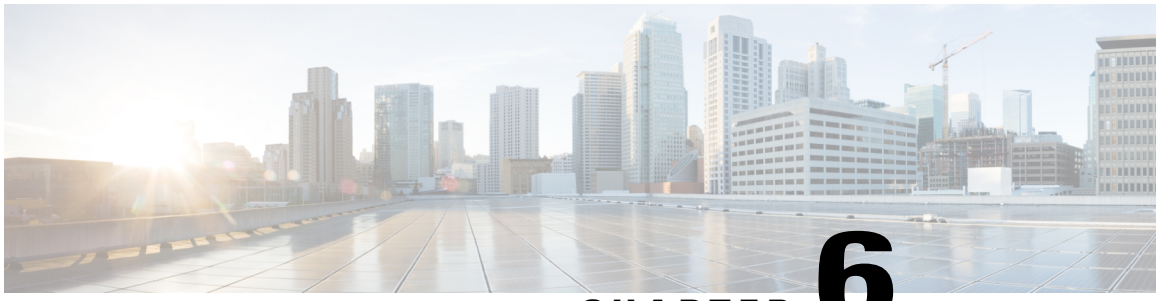
Feature Information for AES and 3-DES Encryption Support for SNMP Version 3

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 8: Feature Information for AES and 3-DES Encryption Support for SNMP Version 3

Feature Name	Releases	Feature Information
AES and 3-DES Encryption Support for SNMP Version 3	Cisco IOS XE Release 3.3SE	The AES and 3-DES Encryption Support for SNMP Version 3 feature enhances the encryption capabilities of SNMP version 3. This support for SNMP version 3 USM is complaint with RFC 3414, which defines DES as the only required method of message encryption for SNMP version 3 authPriv mode. The AES and 3-DES Encryption Support for SNMP Version 3 feature adds AES 128-bit encryption in compliance with RFC 3826. In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.



CHAPTER 6

Cisco Enhanced Image MIB

The Cisco Enhanced Image MIB provides information about images running on the system. It has been extended to be useful for modular operating systems.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Cisco Enhanced Image MIB

Cisco Enhanced Image MIB Overview

The CISCO-ENHANCED-IMAGE-MIB is used to obtain information about images running on various entities or nodes on Cisco IOS devices, such as routers and switches. The MIB provides support to query package information on the Cisco IOS XE system for installed images. The MIB supports the following three tables: ceImageInstallableTable, ceImageLocationTable, and ceImageTable.

The three image tables provide information about currently running images on the system. A modular operating system image consists of a base image and all the installables loaded on the base image. The ceImageInstallableTable provides a list of all installables installed on base images, the ceImageLocationTable

provides a list of all locations where these images are running and also the status of the images at these locations, and the ceImageTable provides the base images.

Image Table

The Cisco Enhanced Image MIB, ceImageTable, shows details about the currently running image on the active device. In a stack or a High Availability (HA) scenario, this table includes details about all the members in the stack. The table below describes the image table objects and the values populated for each object.

Image Table Object	Description
ceImageDescription	Description of the running OS image.
ceImageFamily	Name of the family of the running OS image. The image family indicates the platform for which the image is built. Examples of image families are C3640, C7200, and so on.
ceImageFeature	Feature set supported on the running image.
ceImageMedia	Media on which the image represented by this entry is running.
ceImageName	Name of the running OS image on the device.
ceImageVersion	Version of the running OS image.

Location Table

The Cisco Enhanced Image MIB location table, ceImageLocationTable, consists of a list of all locations where the images are running along with the status of images at these locations. The location table is applicable to modular operating systems. The term *location* in ceImageLocationTable describes the location on the file system where the installed software is placed. The table below describes the location table objects and the values populated for each object.

Location Table Object	Description
ceImageLocation	Location where the operating system is currently loaded on the system.
ceImageLocationRunningStatus	Status of the image currently running on the system. This object has a value *True*, if the image from this location is currently running on the system.

Installable Table

The Cisco Enhanced Image MIB installable table, csImageInstallableTable, specifies a list of software installables installed on the system. This table is applicable to operating systems that support installables. A

modular operating system can consist of a base image and installables. Every image has a table of installables. Entries are added in this table when an installable is installed on the image. Entries are deleted from this table when installables are removed or rolled back from the image. The table below describes the installable table objects and the values populated for each object.

Installable Table Object	Description
ceImageInstallableDate	Date on which package was installed
ceImageInstallableMajorVerNumber	Major version number of the software installable. Version is represented as *major.minor.maintenance*. For example, the major number for version 12.3(18.1)S is 12.
ceImageInstallableMinorVerNumber	Minor version number of the software installable. For example, the minor number for the version 12.3(18.1)S is 3.
ceImageInstallableName	Name of the package.
ceImageInstallableRevisionVerNum	Maintenance version string of the software installable. This string represents incremental change in the image over the minor release number. For example, the revision number for the version 12.3(18.1)S is (18.1)S.
ceImageInstallableRowStatus	Status of the conceptual row. The Simple Network Management Protocol (SNMP) Get operation is the only supported option for this table; so this entry always has a default value of 1.
ceImageInstallableStatus	Status of the software installable.
ceImageInstallableType	Type of the software package.

Sample Output from Cisco Enhanced Image MIB Query

The output obtained from the MIB query is as follows:

```
/opt/cisco-net-snmp/bin/snmpwalk -v2c -c public 172.16.0.1 1.3.6.1.4.1.9.9.249

SNMPv2-SMI::enterprises.9.9.249.1.1.1.1.2.1 = STRING: "CAT3K_CAA-UNIVERSALK9-M"
SNMPv2-SMI::enterprises.9.9.249.1.1.1.1.3.1 = STRING: "CAT3K_CAA"
SNMPv2-SMI::enterprises.9.9.249.1.1.1.1.4.1 = STRING:
"IP|SLA|IPv6|IS-IS|FIREWALL|PLUS|QoS|HA|NAT|MPLS|
VPN|LEGACY PROTOCOLS|3DES|SSH|APPN|IPSEC"
SNMPv2-SMI::enterprises.9.9.249.1.1.1.1.5.1 = STRING: "0.DEV-0"
SNMPv2-SMI::enterprises.9.9.249.1.1.1.1.6.1 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.1.1.1.7.1 = STRING: "Cisco IOS Software, IOS-XE Software,

Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-MClosePair(')'), ExperimentalVersion
0.DEV-0
SNMPv2-SMI::enterprises.9.9.249.1.2.1.1.2.1.1 = STRING:
"tftp://172.30.255.0/shapeng/cat3k.bin"
SNMPv2-SMI::enterprises.9.9.249.1.2.1.1.3.1.1 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.2.1.1.1 = INTEGER: 4
```

```
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.2.1.1.2 = INTEGER: 4
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.2.1.1.3 = INTEGER: 4
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.2.1.1.4 = INTEGER: 4
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.2.1.1.5 = INTEGER: 4
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.2.1.1.6 = INTEGER: 4
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.3.1.1.1 = STRING: "Drivers"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.3.1.1.2 = STRING: "WCM"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.3.1.1.3 = STRING: "IOS"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.3.1.1.4 = STRING: "Platform"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.3.1.1.5 = STRING: "Infra"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.3.1.1.6 = STRING: "Base"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.4.1.1.1 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.4.1.1.2 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.4.1.1.3 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.4.1.1.4 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.4.1.1.5 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.4.1.1.6 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.5.1.1.1 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.5.1.1.2 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.5.1.1.3 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.5.1.1.4 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.5.1.1.5 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.5.1.1.6 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.6.1.1.1 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.6.1.1.2 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.6.1.1.3 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.6.1.1.4 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.6.1.1.5 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.6.1.1.6 = Gauge32: 0
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.7.1.1.1 = STRING: "DEV-0"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.7.1.1.2 = STRING: "DEV-0"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.7.1.1.3 = STRING: "0"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.7.1.1.4 = STRING: "DEV-0"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.7.1.1.5 = STRING: "DEV-0"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.7.1.1.6 = STRING: "DEV-0"
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.8.1.1.1 = Hex-STRING: B2 07 01 01 00 0008 00
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.8.1.1.2 = Hex-STRING: B2 07 01 01 00 0008 00
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.8.1.1.3 = Hex-STRING: B2 07 01 01 00 0008 00
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.8.1.1.4 = Hex-STRING: B2 07 01 01 00 0008 00
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.8.1.1.5 = Hex-STRING: B2 07 01 01 00 0008 00
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.8.1.1.6 = Hex-STRING: B2 07 01 01 00 0008 00
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.9.1.1.1 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.9.1.1.2 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.9.1.1.3 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.9.1.1.4 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.9.1.1.5 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.249.1.2.2.1.9.1.1.6 = INTEGER: 1
```

The output shown above is similar to that obtained from running the **show version** and **show version running** commands from the CLI.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
SNMP commands	Cisco IOS SNMP Support Command Reference
SNMP configuration tasks	*Network Management Configuration Guide*

MIBs

MIB	MIBs Link
CISCO-ENHANCED-IMAGE-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco Enhanced Image MIB

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 9: Feature Information for Cisco Enhanced Image MIB

Feature Name	Releases	Feature Information
Cisco Enhanced Image MIB	Cisco IOS XE Release 3.3SE	The CISCO-ENHANCED-IMAGE-MIB provides information about events running on the system and has been extended to be useful for modular operating systems. In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.