SNMPv3

Feature Summary

Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:

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

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. Table 1 identifies what the combinations of security models and levels mean:

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	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	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 the following about SNMPv3 objects:

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- An access policy is what SNMP objects can be accessed for reading, writing, and creating.
- A group determines the list of notifications its users can receive.
- A group also defines the security model and security level for its users.

Benefits

- Data can be collected securely from SNMP devices without fear of the data being tampered with or corrupted.
- Confidential information, for example, SNMP Set command packets that change a router's configuration, can be encrypted to prevent its contents from being exposed on the network.

List of Terms

authentication—The process of ensuring message integrity and protection against message replays. It includes both data integrity and data origin authentication.

authoritative SNMP engine—One of the SNMP copies involved in network communication designated to be the allowed SNMP engine to protect against message replay, delay, and redirection. The security keys used for authenticating and encrypting SNMPv3 packets are generated as a function of the authoritative SNMP engine's engine ID and user passwords. When an SNMP message expects a response (for example, get exact, get next, set request), the *receiver* of these messages is authoritative. When an SNMP message does not expect a response, the *sender* is authoritative.

community string—A text string used to authenticate messages between a management station and an SNMP v1/v2c engine.

data integrity—A condition or state of data in which a message packet has not been altered or destroyed in an unauthorized manner.

data origin authentication—The ability to verify the identity of a user on whose behalf the message is supposedly sent. This ability protects users against both message capture and replay by a different SNMP engine, and against packets received or sent to a particular user that use an incorrect password or security level.

encryption—A method of hiding data from an unauthorized user by scrambling the contents of an SNMP packet.

group—A set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define what SNMP objects can be read, written to, or created. In addition, the group defines what notifications a user is allowed to receive.

notification host—An SNMP entity to which notifications (traps and informs) are to be sent.

notify view—A view name (not to exceed 64 characters) for each group that defines the list of notifications that can be sent to each user in the group.

privacy—An encrypted state of the contents of an SNMP packet where they are prevented from being disclosed on a network. Encryption is performed with an algorithm called CBC-DES (DES-56).

read view—A view name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are accessible for reading by users belonging to the group.

security level—A type of security algorithm performed on each SNMP packet. The three levels are: noauth, auth, and priv. noauth authenticates a packet by a string match of the user name. auth authenticates a packet by using either the HMAC MD5 or SHA algorithms. priv authenticates a packet by using either the HMAC MD5 or SHA algorithms and encrypts the packet using the CBC-DES (DES-56) algorithm.

security model—The security strategy used by the SNMP agent. Currently, Cisco IOS supports three security models: SNMPv1, SNMPv2c, and SNMPv3.

Simple Network Management Protocol (SNMP)—A network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Simple Network Management Protocol Version 2c (SNMPv2c)—The second version of SNMP, it supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

SNMP engine—A copy of SNMP that can either reside on the local or remote device.

SNMP group—A collection of SNMP users that belong to a common SNMP list that defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of these attributes defined by the group.

SNMP user—A person for which an SNMP management operation is performed. For informs, the user is the person on a remote SNMP engine who receives the informs.

SNMP view—A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.

write view—A view name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.

Platforms

This feature is supported on the following routers and access servers:

- Cisco 700 series
- Cisco 1000 series
- Cisco 1600 series
- Cisco 2500 series
- Cisco 2500 series access servers
- Cisco 3600 series
- Cisco 3800 series
- Cisco 4000 series
- Cisco 4500 series
- Cisco AS5100 access server

- Cisco AS5200 universal access server
- Cisco AS5300 access server
- Cisco 7000 series
- Cisco 7200 series
- Cisco 7500 series

Supported MIBs and RFCs

This feature supports the following RFCs:

- RFC 1901, Introduction to Community-Based SNMPv2. SNMPv2 Working Group.
- RFC 1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group.
- RFC 1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group.
- RFC 1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group.
- RFC 1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group.
- RFC 1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2).
- RFC 1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group.
- RFC 1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework. SNMPv2 Working Group.
- RFC 2104, Keyed Hashing for Message Authentication
- RFC 2271, An Architecture for Describing SNMP Management Frameworks.
- RFC 2272, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).
- RFC 2273, SNMPv3 Applications.
- RFC 2274, User-Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).
- RFC 2275, View-Based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).

No new MIBs are supported by this feature.

Configuration Tasks

This section describes the following Cisco IOS SNMPv3 server configuration tasks:

- Configure SNMP-Server EngineID
- Configure SNMP-Server Group Names
- Configure SNMP-Server Hosts
- Configure SNMP-Server Users

Configure SNMP-Server EngineID

To configure a name for either the local or remote SNMP engine on the router, use the following command in global configuration mode:

Command	Purpose
snmp-server engineID [**local** *engineid-string*] | [**remote** *ip-address* **udp-port** *port-number* *engineid-string*]	Configures names for both the local and remote SNMP engine (or copy of SNMP) on the router.

Configure SNMP-Server Group Names

To configure a new SNMP group, or a table that maps SNMP users to SNMP views, use the following command in global configuration mode:

Command	Purpose
snmp-server group [*groupname* {**v1** | **v2c** | **v3**{**auth** | **noauth** | **priv**}}] [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	Configures a new SNMP group, or a table that maps SNMP users to SNMP views.

Configure SNMP-Server Hosts

To configure the recipient of an SNMP trap operation, use the following command in global configuration mode:

Command	Purpose
snmp-server host [*host* [**traps** | **informs**]] [**version** {**1** | **2c** | **3** [{**auth** | **noauth** | **priv**}]] *community-string* [**udp-port** *port*] [*notification-type*]	Configures the recipient of an SNMP trap operation.

Configure SNMP-Server Users

To configure a new user to an SNMP group, use the following command in global configuration mode:

Command	Purpose
snmp-server user *username* [*groupname* **remote** *ip-address* [**udp-port** *port*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv password*]] [**access** *access-list*]	Configures a new user to an SNMP group.

Monitor and Maintain the Cisco SNMPv3 Server

To display information about SNMP commands, use one of the following commands in EXEC mode:

Command	Purpose
show snmp engineID [**local** | **remote**]	Displays information on the local SNMP engine and all remote engines that have been configured on the device.
show snmp groups	Displays information on each SNMP group on the network.
show snmp user	Displays information on each SNMP username in the SNMP users table.

Command Reference

This section documents the following new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

- **show snmp engineID**
- **show snmp group**
- **show snmp user**
- **snmp-server engineID**
- **snmp-server group**
- **snmp-server host**
- **snmp-server user**

show snmp engineID

To display the identification of the local SNMP engine and all remote engines that have been configured on the router, use the **show snmp engineID** EXEC command.

show snmp engineID

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

Examples

The following example specifies 00000009020000000C025808 as the local engineID and 123456789ABCDEF000000000 as the remote engine ID, 171.69.37.61 as the IP address of the remote engine, or copy of SNMP, and `162` as the port from which the remote device is connected to the local device:

```
router# show snmp engineID

Local SNMP engineID: 00000009020000000C025808
Remomte Engine ID          IP-addr          Port
123456789ABCDEF000000000   171.69.37.61     162
```

Table 1 describes the fields shown in the example.

Table 2 show snmp engineID Field Descriptions

Field	Definition
Local SNMP engine ID	A string that identifies the copy of SNMP on the local device.
Remote Engine ID	A string that identifies the copy of SNMP on the remote device.
IP-addr	The IP address of the remote device.
Port	The port number on the local device to which the remote device is connected.

Related Commands

snmp-server engineID

show snmp group

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

show snmp group

Syntax Description

This command has no keywords or arguments.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

Examples

The following example specifies the group name as public, the security model as v1, the read view name as v1default, the notify view name as *tv.FFFFFFFF, and the storage type as volatile:

```
router# show snmp group

groupname: public        security model:v1
readview:v1default
writeview:  no writeview specified
notifyview: *tv.FFFFFFFF
storage-type: volatile
```

Table 2 describes the fields shown in the example.

Table 3 show snmp group Field Descriptions

Field	Definition
groupname	The name of the SNMP group, or collection of users who have a common access policy.
security model	The security model used by the group, either v1, v2c, or v3.
readview	A string identifying the read view of the group.
writeview	A string identifying the write view of the group.
notifyview	A string identifying the notify view of the group.
storage-type	Indicates whether the settings have been set in volatile or temporary memory on the device, or in non-volatile or persistent memory where settings will remain after the device has been turned off and on again.

Related Commands

snmp-server group

show snmp user

To display information on each SNMP username in the group username table, use the **show snmp groups** EXEC command.

show snmp user

Syntax Description

This command has no keywords or arguments.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

Examples

The following example specifies the username as authuser, the engine ID string as 00000009020000000C025808, and the storage-type as nonvolatile:

```
router# show snmp user

User name: authuser
Engine ID: 00000009020000000C025808
storage-type: nonvolatile
```

Table 3 describes fields shown in the example.

Table 4 show snmp user Field Descriptions

Field	Definition
User name	A string identifying the name of the SNMP user.
Engine ID	A string identifying the name of the copy of SNMP on the device.
storage-type	Indicates whether the settings have been set in volatile or temporary memory on the device, or in non-volatile or persistent memory where settings will remain after the device has been turned off and on again.

Related Commands

snmp-server user

snmp-server engineID

To configure a name for either the local or remote SNMP engine on the router, use the **snmp-server engineID** global configuration command. Use the **no** form of this command to remove a specified SNMP group.

snmp-server engineID [**local** *engineid-string*] | [**remote** *ip-address* **udp-port** *port* *engineid-string*]
no snmp-server engineID

Syntax Description

local	(Optional) Specifies the local copy of SNMP on the router.
engineid-string	(Optional) The name of a copy of SNMP.
remote	(Optional) Specifies the remote copy of SNMP on the router.
ip-address	(Optional) The IP address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a UDP port of the host to use.
port	(Optional) The socket number on the remote device that contains the remote copy of SNMP. The default is 161.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

Note that you need not specify the entire 24-character engine ID if it contains trailing zeros. Specify only the portion of the Engine ID up until the point where only zeros remain in the value. To configure an engine ID of 123400000000000000000000, you can specify the value 1234, for example, **snmp-server engineID** local 1234.

Changing the value of snmpEngineID has important side-effects. A user's password (entered on the command line) is converted to an MD5 or SHA security digest. This digest is based on both the password and the local engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of engineID changes, the security digests of SNMPv3 users will be invalid, and the users will have to be reconfigured.

Similar restrictions require the reconfiguration of community strings when the engine ID changes. A remote engine ID is required when an SNMPv3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. Please refer to the examples in the Configuring Informs section in the **snmp-server host** command reference page.

Related Commands

show snmp engineID
snmp-server host

snmp-server group

To configure a new SNMP group, or a table that maps SNMP users to SNMP views, use the **snmp-server group** global configuration command. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group [*groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}] [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]
no snmp-server group

Syntax Description

groupname	The name of the group.
v1	(Optional) The least secure of the possible security models.
v2c	(Optional) The second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	(Optional) The most secure of the possible security models.
auth	(Optional) Specifies authentication of a packet without encrypting it.
noauth	(Optional) Specifies no authentication of a packet.
priv	(Optional) Specifies authentication of a packet and then scrambles it.
read	(Optional) The option that allows you to specify a read view.
readview	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables you only to view the contents of the agent.
write	(Optional) The option that allows you to specify a write view.
writeview	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables you to enter data and configure the contents of the agent.
notify	(Optional) The option that allows you to specify a notify view
notifyview	(Optional) A string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.
access	(Optional) The option that enables you to specify an access list.
access-list	(Optional) A string (not to exceed 64 characters) that is the name of the access list.

Default

Table 4 describes default values for the different views.

Table 5 snmp server group Default Descriptions

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

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.(3)T.

When a community string is configured internally, two groups with the name “public” are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

Configuring Notify Views

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

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

The *notifyview* option is available for two reasons:

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

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

Step	Command	Purpose
1	**snmp-server user**	Configure an SNMP user.
2	**snmp-server group**	Configure an SNMP group, without adding a notify view.
3	**snmp-server host**	Autogenerate the notify view by specifying the recipient of a trap operation.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using eight characters for security. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized MD5 digest.

The following example shows how to enter a plain-text password for the string arizona2 for user John in group Johngroup, type the following command line:

```
snmp-server user John Johngroup v3 auth md5 arizona2.
```

When you enter a **show running-config** command, you will not see a line for this user. To see if this user has been added to the configuration, type the **show snmp user** command.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hex values. Also, the digest should be exactly 16 octets long.

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

```
snmp-server user John Johngroup v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

Related Commands

show snmp group

snmp-server host

To configure the recipient of an SNMP trap operation, use the **snmp-server host** global configuration command. To remove the specified host, use the **no** form of this command.

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

Syntax Description

host — The address of the recipient for which the traps are targeted.

traps — (Optional) Specifies the type of notification being sent should be a trap.

informs — (Optional) Specifies the type of notification being sent should be an inform.

version — (Optional) Specifies the security model to use.

1 — (Optional) The least secure of the possible security models.

2c — (Optional) The second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.

3 — (Optional) The most secure of the possible security models.

auth — (Optional) Specifies authentication of a packet without encrypting it.

noauth — (Optional) Specifies no authentication of a packet.

priv — (Optional) Specifies authentication of a packet and then scrambles it.

community-string — A string that is used as the name of the community; acts as a password by controlling access to the SNMP community. This string can be set using the **snmp-server host** command, but it is recommended that you set the string using the **snmp-server community** command before using the **snmp-server host** command.

udp-port — (Optional) Specifies a UDP port of the host to use.

port — (Optional) A UDP port number that the host uses. The default is 162.

notification-type (Optional) Type of trap to be sent to the host. If no type is specified, all traps are sent.

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

- **bgp**—Sends Border Gateway Protocol (BGP) state change traps.
- **config**—Sends configuration traps.
- **dspu**—Sends downstream physical unit (DSPU) traps.
- **entity**—Sends Entity MIB modification traps.
- **envmon**—Sends Cisco enterprise-specific environmental monitor traps when an environmental threshold is exceeded.
- **frame-relay**—Sends Frame Relay traps.
- **hsrp**—Sends Hot Stanby Routing Protocol (HSRP) notifications.
- **isdn**—Sends Integrated Services Digital Network (ISDN) traps.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) traps.
- **rptr**—Sends standard repeater (hub) traps.
- **rsrb**—Sends remote source-route bridging (RSRB) traps.
- **rtr**—Sends response time reporter (RTR) traps.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) traps.
- **sdllc**—Sends SDLC Logical Link Control traps.
- **snmp**—Sends Simple Network Management Protocol (SNMP) traps defined in RFC 1157.
- **stun**—Sends serial tunnel (STUN) traps.
- **syslog**—Sends error message traps (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.
- **tty**—Sends Cisco enterprise-specific traps when a Transmission Control Protocol (TCP) connection closes.
- **x25**—Sends X.25 event traps.

Default

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to this host.

If no **version** keyword is present, the default is version 1. If no **traps** or **informs** keyword is present, traps are enabled.

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

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

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. This command was expanded in Cisco IOS Release 12.0(3)T to include **hsrp** recognition and **version 3** selection. This command was also modified in Release 12.0(3)T to automatically write the **snmp-server community** command to the configuration if it was not used to specify the *community-string*.

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

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

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

In order 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.

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

A notification type option's availability depends on the router type and Cisco IOS software features supported on the router. For example, the envmon notification type is available only if the environmental monitor is part of the system.

Configuring Informs

To be able to send an inform, you need to perform the following steps:

Step	Task
1	Configure a remote engine ID.
2	Configure a remote user.
3	Configure a group on a remote device.

Step	Task
4	Enable traps on the remote device.
5	Enable the SNMP manager.

The following example shows how to send configuration informs:

```
snmp engineid remote 16.20.11.14 00000063000100a1ac151003
snmp enable traps config
snmp manager
```

The following example shows how to configure a remote user to receive traps at the v3 security model and the noAuthNoPriv security level:

```
snmp-server group remotegroup v3 noauth
snmp-server user remoteuser remotegroup remote 16.20.11.14 v3
snmp-server host 16.20.11.14 informs version 3 noauth remoteuser config
```

The following example shows how configure a remote user in a group called remotegroup to receive traps at the v3 security model and the authNoPriv security level.

```
snmp group remotegroup v3 auth
snmp-server user remoteAuthUser remoteAuthGroup remote 16.20.11.14 v3 auth md5
password1
```

The following example shows how to configure a user in a group called remotegroup using the v3 security model and the priv security level.

```
snmp-server group remotegroup v3 priv
snmp-server user remote PrivUser remotePrivGroup remote 16.20.11.14 v3 auth md5
password1 priv des56 password2
```

Examples

If you want to configure a unique snmp community string for traps, but you want to prevent snmp polling access with this string, the configuration should include an access-list. In the following example, the community string is named "comaccess" and the access list is numbered 10:

```
snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

The following example sends the SNMP traps defined in RFC 1157 to the host specified by the name myhost.cisco.com. The community string is defined as comaccess.

```
snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

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

```
snmp-server enable traps
snmp-server host 172.30.2.160 public snmp envmon
```

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

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

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

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

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

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version 2c public
```

If you configure a host for a noAuthNoPriv user or community security model string, note the following:

- If a user or community string does not exist, a user is created automatically.
- If a user has been automatically created or if the user already exists, but has no group associated with it, a new group is automatically created. The name of the group will be the same as the username specified in the **snmp-server host** command.
- A view allowing access to the selected traps is automatically generated.

Related Commands

snmp-server host
snmp-server informs
snmp-server trap-source
snmp-server trap-timeout

snmp-server user

To configure a new user to an SNMP group, use the **snmp-server user** global configuration command. To remove a user from an SNMP group, use the **no** form of the command .

snmp-server user *username* [*groupname* **remote** *ip-address* [**udp-port** *port*] {**v1** | **v2c** | **v3**
[**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv password*]] [**access** *access-list*]
no snmp-server user

Syntax Description

username The name of the user on the host that connects to the agent.

groupname (Optional) The name of the group to which the user is associated.

remote (Optional) Specifies the remote copy of SNMP on the router.

ip-address (Optional) The IP address of the device that contains the remote copy of SNMP.

udp-port (Optional) Specifies a UDP port of the host to use.

port (Optional) A UDP port number that the host uses. The default is 162.

v1 (Optional) The least secure of the possible security models.

v2c (Optional) The second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.

v3 (Optional) The most secure of the possible security models.

encrypted (Optional) Specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).

auth (Optional) Initiates an authentication level setting session.

md5 (Optional) The HMAC-MD5-96 authentication level.

sha (Optional) The HMAC-SHA-96 authentication level.

auth-password (Optional) A string (not to exceed 64 characters) that enables the agent to receive packets from the host.

priv (Optional) The option that initiates a privacy authentication level setting session.

des56 (Optional) The CBC-DES privacy authentication algorithm.

priv password (Optional) A string (not to exceed 64 characters) that enables the host to encrypt the contents of the message it sends to the agent.

access (Optional) The option that enables you to specify an access list.

access-list (Optional) A string (not to exceed 64 characters) that is the name of the access list.

Default

Table 5 describes default values for the **encrypted** option, passwords and access lists:

Table 6 snmp server user Default Descriptions

Default	Definition
encrypted	Not present by default. It is used to specify that the **auth** and **priv** passwords are **MD5** digests and not text passwords.
passwords	Assumed to be text strings.
access lists	Access from all IP access lists is permitted.
remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the remote option.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(3)T.

Configuring a Remote User

To configure a remote user, 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, using the command **snmp-server engineID** with the **remote** option. The remote agent's SNMP engine ID is needed when computing the authentication/privacy digests from the 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 informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

Related Commands

show snmp user

What to Do Next

For more information, see sections on IP configuration in the *Network Protocols Configuration Guide, Part 1* and the *Configuration Fundamentals Configuration Guide*.