SNMPv2c

Last Updated: January 29, 2013

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 at the end of this module.

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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**]}] [**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. **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**]}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** *access-list*] **Example:** `Device(config)# snmp-server group group1 v2c 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.

	Command or Action	Purpose

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*] **Example:** `Device(config)# snmp-server user user1 group1 v2c auth md5 password123`	Adds a new user to an SNMPv2c 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: 00000009020000000C025808
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, page 6

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for SNMV2c

Feature Name	Releases	Feature Information
SNMV2c	Cisco IOS XE Release 3.2SE	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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.