Cisco SNMP Configuration and Verfication Process

Enable SNMP Community Strings

This procedure is the same for both routers and Cisco IOS® software-based XL Catalyst Switches.

1. Telnet to the router:

```
prompt# telnet 172.16.99.20
```

2. Enter the enable password at the prompt in order to enter the enable mode:

```
Router>enable
Password:
Router#
```

3. Go into the configuration mode:

```
Router#configure terminal
Enter configuration commands, one
per line.  End
with CNTL/Z.
Router(config)#
```

4. Use this command in order to enable the read-only (RO) community string:

```
Router(config)#snmp-server community
public RO
```

where "public" is the read-only community string.

5. Use this command in order to enable the read-write (RW) community string:

```
Router(config)#snmp-server community
private RW
```

where "private" is the read-write community string.

6. Exit out of the configuration mode and return to the main prompt:

```
Router(config)#exit
Router#
```

7. Write the modified configuration to nonvolatile RAM (NVRAM) to save the settings:

```
Router#write memory
Building configuration...
[OK]
Router#
```

Configuring a Specific IP Address for an SNMP Operation

Testing

1. From the Linux Server running NMIS try to ping the device to verify connectivity
2. Then verify SNMP communication by doing an snmpwalk of the device:

```
snmpwalk -v 2c -c NMISread
<cisco_device_name_or_ip> 1.3.6.1.2.1.1
```

This command should output something like this:

```
NMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software,
1841 Software (C1841-ADVENTERPRISEK9-M), Version
12.4(25f), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Tue 16-Aug-11 06:21 by prod_rel_team
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::
enterprises.9.1.620
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks:
(96372878) 11 days, 3:42:08.78
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING:
cisco_device_name_or_ip
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:
00.00
```

If you do not enter a snmp-server host command, no notifications are sent. To configure the device to send SNMP notifications, you must enter at least one snmp-server host command. If you enter the command without keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate snmp-server host c ommand 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 type of notification, 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 replaces 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 sn mp-server host command for that host must be enabled.

SUMMARY STEPS

1. enable
2. configure terminal
3. snmp-server host host-id [traps | informs] [version {1 | 2c | 3 [au th | noauth | priv]}] community-string [udp-port port-number] [n otification-type]
4. exit
5. show snmp host

DETAILED STEPS

	Command or Action	Purpose
Ste p 1	enable Example: `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Ste p 2	configure terminal Example: `Device# configure terminal`	Enters global configuration mode.
Ste p 3	snmp-server host host-id [traps	informs] [version { 1	2c	3 [auth	noauth	priv]}] community-string [udp-port port-number] [n otification-type] Example: `Device(config)# snmp-server host 172.16.1.27 informs version 2c public alarms`	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.
Ste p 4	exit Example: `Device(config)# exit`	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.

Examples

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 informs
version 2c public
Device(config)# exit
Device# show snmp host

Notification host: 10.2.28.1 udp-port: 162   type:
inform
user: public    security model: v2c
traps: 00001000.00000000.00000000
```

Configuring SNMP Version 3

When you configure SNMPv3 and you want to use the SNMPv3 security mechanism for handling SNMP packets, you must establish SNMP groups and users with passwords.

Perform the following tasks to configure SNMPv3.

- Specifying SNMP-Server Group Names
- Configuring SNMP Server Users

Specifying SNMP-Server Group Names

SNMPv3 is a security model. A security model is an authentication strategy that is set up for a user and the group in which the user resides.

No default values exist for authentication or privacy algorithms when you configure the snmp-server group command. Also, no default passwords exist. For information about specifying a MD5 password, see the documentation for the snmp-server user command.

Perform this task to specify a new SNMP group or a table that maps SNMP users to SNMP views.

SUMMARY STEPS

1. enable
2. configure terminal
3. snmp-server group [groupname {v1 | v2c | v3 [auth | noauth | priv]}] [read readview] [write writeview] [notify notifyview] [access access-list]
4. exit
5. show snmp group

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 [groupname {v1 | v2c | v3 [auth | noauth | priv]}] [read readview] [write writeview] [notify notifyview] [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	exit Example: `Device(config)# exit`	Exits global configuration mode.
Step 5	show snmp group Example: `Device# show snmp group`	Displays information about each SNMP group on the network.