CHAPTER 2

Configuring Network Devices for Management

Revised: December 15, 2009, OL-18339-03

After a short overview, this chapter describes how to configure the various devices in the Cisco PGW 2200 Softswitch node. This task is typically done by the system administrator.

Note Take precautions to avoid more than one user simultaneously accessing and modifying the same network device or any of its components. Establish access schedules for all your users.

Overview of Configuration

In Cisco Media Gateway Controller (MGC) Node Manager (MNM), device configuration means setting up devices that are in the Cisco PGW 2200 Softswitch node to forward alarms (Simple Network Management Protocol [SNMP traps] from the point of view of the device) to Cisco MNM. For Cisco MNM to be able to receive and manage alarms, the devices must be configured to send them. Configuration involves editing the SNMP configuration file on the device to specify the following:

- The Cisco MNM management server's IP address as the SNMP trap destination
- Depending on the device, the severity level of traps to be forwarded, the configuration of SNMP community strings, and the SNMP trap source

Note

- The other task in setting up the management of your network is deploying the network devices and adding them to the Cisco MNM network model. Deployment tells Cisco MNM how to communicate with the managed devices; configuration tells the devices how to communicate with Cisco MNM. Deployment is typically performed by users, and the configuration is typically performed by the system administrator. See Chapter 5, "Deploying Your Network in Cisco MNM" for details of deployment.
- For information on configuring trap forwarding from Cisco MNM to northbound management systems, see Chapter 6, "Managing Faults with Cisco MNM," "Forwarding Traps to Other Systems" section on page 6-24.
- Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, ITP-L will replace SLT in publications and the product.

The Cisco PGW 2200 Softswitch host, Cisco Billing and Measurements Server (BAMS), Cisco ITP-L, Cisco H.323 Signaling Interface (HSI) server, and the Cisco LAN Switch are configured by opening a Telnet session with the device and entering the prescribed SNMP configuration settings. You can initiate the Telnet session at the UNIX command prompt, or, if the device has been deployed in Cisco MNM, you can use Cisco MNM to initiate the Telnet session.

If you deploy firewalls between Cisco MNM and other network elements, configure the firewalls to open the following ports,

- 22 for SSH
- 23 for Telnet
- 161and 162 for SNMP

Information Needed for Configuration

Have the following information available:

- For the Cisco PGW 2200 Softswitch, the Cisco BAMS, and the Cisco HSI server, the superuser password.
- For the Cisco ITP-L and the Cisco LAN switch, the login and enable passwords for the device.
- The IP address of the Cisco MNM server (standalone server or management server in a distributed configuration), to be used as the SNMP trap destination. If multiple IP addresses and host names are configured on your server, choose the IP address that is in the same LAN as the devices.
- For the Cisco ITP-L and Cisco LAN Switch, the IP address of the device (this is the same address that is entered when the device is deployed in Cisco MNM).

Configuring the Cisco PGW 2200 Softswitch

For the procedure of configuring the Cisco PGW 2200 Softswitch for network management, see the section, “Configuring SNMP Support Resources”, of the *Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide* at the following link

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9.8/Installation/Guide/Install98.html

Configuring the Cisco ITP-L

Use the following procedure to configure the Cisco ITP-L for network management:

Step 1 Access the Cisco ITP-L in either of the following ways:

- Enter the command:

  telnet *Cisco-ITP-L-IP-address*

- If the device has been deployed in Cisco MNM, in the Map Viewer, right-click the device and choose **Tools > Connection Service**.

  A Telnet window opens and the `password` prompt displays.

Step 2 Enter the login password for the Cisco ITP-L.

The `itp-l` prompt displays.

Step 3 Enter the command **enable**.

The `password` prompt displays.

Step 4 Enter the enable password for the Cisco ITP-L.

The `itp-l` prompt displays.

Step 5 Enter the command **configure terminal**.

The `itp-l (config)` prompt displays.

Community strings can be found at snmpCommunityEntry. The following are default community entries:

```
snmpCommunityEntry  admin mgcusr mgcusr localSnmpID - - nonVolatile
snmpCommunityEntry  readonly public public localSnmpID - - nonVolatile
snmpCommunityEntry  user private private localSnmpID - - nonvolatile
```

Note Do not change the default values or attempt to add more entries.

Step 6 Configure SNMP community strings. For example, to set the read-only community string to public and the read-write community string to private, enter the commands

```
snmp-server community public RO
snmp-server community private RW
```

Step 7 Configure traps to be sent to Cisco MNM.

a. To configure the Cisco ITP-L to send all types of traps, enter the command

```
snmp-server enable traps
```

b. To configure the Cisco ITP-L to send traps for all syslog messages with a severity of warnings or worse, enter the command (you can set this severity to the level you want)

```
logging history warnings
```

c. To configure the IP address of Cisco MNM to which traps are sent, enter the command (in this example the IP address of the Cisco MNM is 10.1.1.1)

```
snmp-server host 10.1.1.1 public
```

By default, this trap will send out SNMP v1 traps. To send SNMP v2c traps, use the following command:

```
snmp-server host 10.1.1.1 version 2c public
```

Step 8 Set the SNMP trap source, which specifies the Cisco ITP-L interface from which traps are sent. The SNMP trap source should be the interface with the IP address that the Cisco MNM is configured to use for SNMP communications.

For example, suppose that the IP address 10.2.2.2 is assigned to interface Ethernet 0/0 on the Cisco ITP-L. If Cisco MNM is configured to communicate with the Cisco ITP-L using IP address 10.2.2.2 (the address given when the device is deployed in Cisco MNM), then the trap interface on the Cisco ITP-L should be Ethernet 0/0. In this example, you would enter the command

```
snmp-server trap-source Ethernet0/0
```

Step 9 Set the maximum SNMP packet size to 2KB by entering the command

```
snmp-server packetsize 2048
```

Step 10 To exit the configuration mode, press **Ctrl-Z**, and then enter the **write** command to write the configuration to Flash memory.

Configuring the Cisco LAN Switch Catalyst 2900XL

Use the following procedure to configure the Cisco Catalyst 2900XL LAN switch for network management:

Step 1 Access the Cisco LAN Switch in either of the following ways:

- Enter the command

  telnet *Cisco-LAN-switch-IP-address*

- If the device has been deployed in Cisco MNM, in the Map Viewer, right-click the device and choose **Tools > Connection Service**.

  A Telnet window opens and the `password` prompt.

Step 2 Enter the login password for the LAN switch.

The `2900xl` prompt displays.

Step 3 Enter the command **enable**.

The `password` prompt displays.

Step 4 Enter the enable password for the LAN switch.

The `2900xl` prompt displays.

Step 5 Enter the command and press Enter:

```
configure terminal
```

The `2900xl(config)` prompt displays.

Step 6 Configure SNMP community strings. For example, to set the read-only community string to public and the read-write community string to private, enter the commands

```
snmp-server community public RO
snmp-server community private RW
```

Step 7 Configure traps to be sent to Cisco MNM.

a. To configure the LAN switch to send all types of traps, enter the command

```
snmp-server enable traps
```

b. To configure the IP address of the Cisco MNM to which traps are sent, enter the command (in this example the IP address of the Cisco MNM is 10.1.1.1)

```
snmp-server host 10.1.1.1 public
```

c. By default, this trap will send out SNMP v1 traps. To send SNMP v2c traps, use the following command:

```
snmp-server host 10.1.1.1 version 2c public
```

Step 8 Set the SNMP trap source, which specifies the LAN switch interface from which traps are sent. The SNMP trap source should be the interface with the IP address that the Cisco MNM is configured to use for SNMP communications.

For example, let's assume that the IP address 10.2.2.2 is assigned to interface VLAN1 on the LAN switch. If Cisco MNM is configured to communicate with the LAN switch using IP address 10.2.2.2 (the address given when the device is deployed in Cisco MNM), the trap interface on the LAN switch should be VLAN1. In this example, you would enter the command

```
snmp-server trap-source VLAN1
```

Step 9 Set the maximum SNMP packet size to 2KB by entering the command

```
snmp-server packetsize 2048
```

Step 10 To exit the configuration mode, press **Ctrl-Z**, and then enter the **write** command to write the configuration to Flash memory.

Configuring the Cisco Catalyst 5500 or 6509 LAN Switch

Use the following procedure to configure the Cisco Catalyst 5500 or 6509 LAN switch for network management:

Step 1 Access the Cisco LAN Switch in either of the following ways:

- Enter the command:

  telnet *Cisco-LAN-switch-IP-address*
- If the device has been deployed in Cisco MNM, in the Map Viewer, right-click the device and choose **Tools > Connection Service**.

  A Telnet window opens and the `password` prompt displays.

Step 2 Enter the login password for the LAN switch.

The *cat* prompt displays.

Step 3 Enter the command **enable**.

The *password* prompt displays.

Step 4 Enter the enable password for the LAN switch.

The *cat*`(enable)` prompt displays.

Step 5 Configure SNMP community strings. For example, to set the read-only community string to public and the read-write community string to private, enter the commands

```
set snmp-community read-only public
set snmp-community read-write private
```

Community strings can be found at snmpCommunityEntry. The following are default community entries:

```
snmpCommunityEntry  admin mgcusr mgcusr localSnmpID - - nonVolatile
snmpCommunityEntry  readonly public public localSnmpID - - nonVolatile
snmpCommunityEntry  user private private localSnmpID - - nonvolatile
```

Do not change the default values or attempt to add more entries.

Step 6 Configure traps to be sent to Cisco MNM.

a. To configure the LAN switch to send all types of traps, enter the command

```
set snmp trap enable
```

b. To configure the IP address of the Cisco MNM to which traps are sent, enter the command (in this example the IP address of the Cisco MNM is 10.1.1.1):

```
set snmp trap 10.1.1.1 public
```

Note Currently, Catalyst 5500 and 6500 LAN switches only send snmp v1 traps, not snmp v2c or v3.

Step 7 To exit enable mode, enter **exit**.

Configuring a Cisco BAMS

Use the following procedure to configure a BAMS for network management:

Step 1 Access the BAMS in either of the following ways:

- Enter the command:

  telnet *Cisco-<BAMS server>-IP-address*

- If the device has been deployed in Cisco MNM, in the Map Viewer, right-click the device and choose **Tools > Connection Service**.

  A Telnet window opens.

Step 2 Use the following command to become the root user:

```
su - root
```

Step 3 Use the following command to change the directory:

```
cd /etc/srconf/agt
```

Step 4 Use a text editor to edit the snmpd.cnf file.

Step 5 Search for the keyword sysName and change the system name to the host name of the BAMS. The entry should be

sysName *<BAMS-server-hostname>*

Step 6 Enter the following lines after the existing snmpNotifyEntry lines:

```
snmpNotifyEntry 31 Console trap nonVolatile
snmpNotifyEntry 32 TrapSink trap nonVolatile
```

Note The second field on each line (31 and 32 in the example) must be a value that is unique in the snmpNotifyEntry section.

Step 7 Enter the following lines after the existing snmpTargetAddrEntry lines:

```
snmpTargetAddrEntry 33 snmpUDPDomain 127.0.0.1:0 100 3 Console
\ v1ExampleParams nonVolatile 255.255.255.255:0 2048
```

```
snmpTargetAddrEntry 34 snmpUDPDomain 127.0.0.1:0 100 3 Console
\ v2cExampleParams nonVolatile 255.255.255.255:0 2048
```

- To send SNMP v1 traps, add the following lines:

```
snmpTargetAddrEntry 35 snmpUDPDomain 10.1.1.1:0 100 3 TrapSink
\ v1ExampleParams nonVolatile 255.255.255.255:0 2048
```

- To send SNMP v2c traps, add the following lines:

```
snmpTargetAddrEntry 36 snmpUDPDomain 10.1.1.1:0 100 3 TrapSink
\ v2cExampleParams nonVolatile 255.255.255.255:0 2048
```

Note
- In the example above, the IP address for Cisco MNM is 10.1.1.1, and the \ character entered at the end of the first line indicates that the entire command should be entered on one line.
- The second field on each line (33, 34, 35 and 36 in the example) must be a value that is unique in the TargetAddrEntry section.

Step 8 Verify that you have entered the exact information specified. UNIX is case-sensitive, so make sure that commands are entered in the same case each time they are entered.

Step 9 Save the changes you made to the snmpd.cnf file.

Step 10 Determine the process ID of the SNMP daemon. From the Sun Solaris command line, enter the command

```
# ps -ef | grep snmpdm
```

The information that displays resembles the following:

```
root 565 1 0 Mar 20 ? 0:01 /opt/<BAMS>/bin/snmpdm -d
mgcusr 7463 23729 0 12:33:04 pts/13 0:00 grep snmpdm
```

The process ID of the snmpdm daemon is the second field on the line that ends with snmpdm -d. In this example, the process ID of the SNMP daemon is 565.

Step 11 Enter the following command to terminate the SNMP daemon:

```
# kill -9 SNMP-daemon-process-ID
```

Note The SNMP daemon restarts automatically after termination.

Configuring a Cisco HSI Server

Use the following procedure to configure an HSI server for network management:

Step 1 Access the Cisco HSI server in either of the following ways:

- Enter the command

  telnet *Cisco-<HSI-server>-IP-address*
- If the device has been deployed in Cisco MNM, in the Map Viewer, right-click the device and choose **Tools > Connection Service**.

  A Telnet window opens.

Step 2 Use the following command to become the root user:

```
su - root
```

Step 3 Enter the following command and press Enter:

```
cd /etc/srconf/agt
```

Step 4 Use a text editor to edit the snmpd.cnf file.

Step 5 Search for the keyword sysName and change the system name to the host name of the HSI server. The entry should be

```
sysName <HSI-server-hostname>
```

Step 6 Community strings can be found at snmpCommunityEntry. Verify that the following default community strings are present:

```
snmpCommunityEntry  t0000000 public public localSnmpID - - nonVolatile
snmpCommunityEntry  t0000001 sysadmin sysadmin localSnmpID - - nonvolatile
```

Note Do not change the default values or attempt to add more entries.

Step 7 Enter the following line after the existing snmpNotifyEntry lines:

```
snmpNotifyEntry 32 rambler trap nonVolatile
```

Step 8 Enter the following line after the existing snmpTargetAddrEntry lines:

```
snmpTargetAddrEntry stae3 snmpUDPDomain 10.1.1.1:0 100 3 mgr1 stpe2 \
nonVolatile 255.255.255.255:0 2048
```

Note

- In the example above, the IP address for Cisco MNM is 10.1.1.1, and the \ character entered at the end of the first line indicates that the entire command should be entered on one line.
- The second field on the line (34 in the example) must be a value that is unique in the TargetAddrEntry section.

Step 9 Verify that you have entered the exact information specified. UNIX is case-sensitive, so make sure that they are entered in the same case each time they are entered.

Step 10 Save the changes you made to the snmpd.cnf file.

Step 11 Determine the process ID. From the Sun Solaris command line, enter the command

```
# ps -ef | grep snmpdm
```

Information displays that resembles the following:

```
root 565 1 0 Mar 20 ? 0:01 /opt/<HSI>/bin/snmpdm -d
mgcusr 7463 23729 0 12:33:04 pts/13 0:00 grep snmpdm
```

The process ID of the snmpdm daemon is the second field on the line that ends with snmpdm -d. In this example, the process ID of the SNMP daemon is 565.

Step 12 Enter the following command to terminate the SNMP daemon:

```
# kill -9 SNMP-daemon-process-ID
```

Note The SNMP daemon restarts automatically after termination.