CHAPTER 3

Configuring Network Devices for Management

Introduction to Device Configuration

You must configure each network device for SNMP before it can be managed by CMNM. You must configure:

- SNMP community strings
- SNMP trap destination (that is, CMNM)
- Other miscellaneous SNMP settings

You must configure SNMP for the following devices:

- Cisco MGC
- Cisco SLT (2600)
- LAN switch (Catalyst 2900XL and Catalyst 5500)
- Cisco MGX 8260
- BAMS

Note If you plan to configure CMNM to forward traps to northbound systems, you should only configure SNMP Version 1 traps on network devices. CMNM only forwards SNMP Version 1 traps to northbound systems. For more information on forwarding traps, see the “Forwarding Traps to Other Systems” section on page 8-11.

Configuring the Cisco MGC

To configure a Cisco MGC for network management:

Step 1 Access the Cisco MGC by entering the command:

```
telnet Cisco-MGC-IP-address
```

Step 2 Type **su - root** to become the root user.

Step 3 Type **cd /opt/CiscoMGC/snmp**.

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 hostname of the Cisco MGC. The entry should be:

```
sysName Cisco-MGC-hostname
```

Step 6 Search for the keyword communityEntry and configure the read-only and read-write community string to be public. The entry should be:

```
communityEntry localSnmpID public Anyone localSnmpID default -
nonVolatile
```

Step 7 Search for the keyword snmpNotifyEntry and configure CMNM as the trap receiver. Add the following line after the existing snmpNotifyEntry line:

```
snmpNotifyEntry 32 rambler trap nonVolatile
```

Note In the example above, the second field on the line, 32, should have a value that is 1 greater than the existing line. The example above assumes that the existing line has 31 as the second field in the line.

Step 8 Search for the keyword snmpTargetAddrEntry and add the following line after the existing snmpTargetAddrEntry lines:

```
snmpTargetAddrEntry 33 snmpUDPDomain 10.1.1.1:0 100 3 rambler \
v1ExampleParams nonVolatile 255.255.255.255:0
```

Note In the example above, the IP address of the NMS is 10.1.1.1. The second field on the line, 33 in the example above, should have a value that is 1 greater than the existing line. The example above assumes that the existing line has 32 as the second field in the line.

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

Step 10 Signal the SNMP daemon to reread the SNMP configuration file. From the Sun Solaris command line, enter the command:

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

You see information that resembles the following:

```
root 565 1 0 Mar 20 ? 0:01 /opt/CiscoMGC/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 command:

```
kill -1 SNMP-daemon-process-ID
```

Configuring a Cisco SLT (2600)

To configure a Cisco SLT (a Cisco 2600 router) for network management:

Step 1 Access the Cisco SLT by entering the command:

```
telnet Cisco-SLT-IP-address
```

You see the password prompt.

Step 2 Enter the login password for the Cisco SLT.

You see the slt prompt.

Step 3 Enter the command **enable**.

You see the password prompt.

Step 4 Enter the enable password for the Cisco SLT.

You see the slt prompt.

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

You see the slt(config) prompt.

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 public RW
```

Step 7 Configure traps to be sent to CMNM.

a. To configure the Cisco SLT to send all types of traps, enter the command:

```
snmp-server enable traps
```

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

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

Step 8 Set the SNMP trap source, which specifies the Cisco SLT interface from which traps are sent. The SNMP trap source should be the interface with the IP address that the CMNM 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 SLT. If CMNM is configured to communicate with the Cisco SLT using IP address 10.2.2.2, then the trap interface on the Cisco SLT 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 4k by entering the command:

```
snmp-server packetsize 4096
```

Step 10 To exit configuration mode, press Ctrl+Z. Then enter the **write** command to write the configuration to flash memory.

Configuring a LAN Switch (Catalyst 2900XL)

To configure a LAN switch (Catalyst 2900XL) for network management:

Step 1 Access the LAN switch by entering the command:

```
telnet LAN-switch-IP-address
```

You see the password prompt.

Step 2 Enter the login password for the LAN switch.

You see the 2900xl prompt.

Step 3 Enter the command **enable**.

You see the password prompt.

Step 4 Enter the enable password for the LAN switch.

You see the 2900xl prompt.

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

You see the 2900xl(config) prompt.

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 public RW
```

Step 7 Configure traps to be sent to CMNM.

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 CMNM to which traps are sent, enter the command (in this example the IP address of the CMNM is 10.1.1.1):

```
snmp-server host 10.1.1.1 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 CMNM is configured to use for SNMP communications.

For example, suppose that the IP address 10.2.2.2 is assigned to interface VLAN1 on the LAN switch. If CMNM is configured to communicate with the LAN switch using IP address 10.2.2.2, then 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 4k by entering the command:

```
snmp-server packetsize 4096
```

Step 10 To exit configuration mode, press Ctrl+Z. Then enter the **write** command to write the configuration to flash memory.

Configuring the LAN Switch (Catalyst 5500)

To configure a LAN switch (Catalyst 5500) for network management:

Step 1 Access the LAN switch by entering the command:

```
telnet LAN-switch-IP-address
```

You see the password prompt.

Step 2 Enter the login password for the LAN switch.

You see the cat prompt.

Step 3 Enter the command **enable**.

You see the password prompt.

Step 4 Enter the enable password for the LAN switch.

You see the cat(enable) prompt.

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
```

Step 6 Configure traps to be sent to CMNM.

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 CMNM to which traps are sent, enter the command (in this example the IP address of the CMNM is 10.1.1.1):

```
set snmp trap 10.1.1.1 public
```

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

Configuring the Cisco MGX 8260

To configure a Cisco MGX 8260 for network management:

Step 1 Start the Cisco MGX 8260 Web Viewer application by entering the command:

```
netscape Cisco-MGX-8260-IP-address
```

The Cisco MGX 8260 Web Viewer application opens in the web browser.

Step 2 In the right pane, select **Node**, then **SNMP**.

Step 3 Set the SNMP community strings:

- Read-only: public
- Read-write: private

Step 4 Configure trap registration by configuring the IP address of the CMNM to which traps are sent. For example, if the IP address of the CMNM is 10.1.1.1, register the trap receiver as 10.1.1.1.

Configuring BAMS

To configure a BAMS 1.0 for network management:

Step 1 Access the BAMS server by entering the command:

```
telnet BAMS-server-IP-address
```

Step 2 Log in using the user ID acec.

Step 3 Navigate to the directory containing the configuration program by entering the command:

```
cd /opt/VSCcmp/bin
```

Step 4 Load the proper environment by entering the command:

```
. sym_defs
```

Step 5 Launch the BAMS system configuration interface by entering the command:

```
samari &
```

You see the BAMS system configuration interface (named CMP *BAMS-server-IP-address*).

Step 6 Select **System**, then **Trap Management**.

You see the SNMP Trap Configuration window.

Step 7 Select **Actions**, then **Add**.

You see the Add SNMP Trap window.

Step 8 Configure the IP address of the CMNM to which traps are sent. For example, if the IP address of the CMNM is 10.1.1.1, register the trap receiver as 10.1.1.1. Set the following information in the window:

Name: *hostname of the NMS*

Domain Name: *domain name of the NMS*

Trap Definition Address: *IP address of the CMNM*

Trap Destination Port: 162

SNMP Version: 2 is better, 1 is OK

Step 9 Click **OK** to save the trap receiver changes, select **File**, then **Exit** to close the SNMP Trap Configuration window.

Step 10 You can control the severity of the SNMP traps sent to the trap receiver. On the CMP *BAMS-server-IP-address* window, select **System**, then **Alarm Management**.

You see the Alarms Configuration window.

Step 11 Set the message forward level to minor.

If you set this level to informational or warning, a large number of traps of limited value are sent to the CMNM.

Step 12 For the changes to take effect, you must stop and restart the BAMS:

a. On the CMP *BAMS-server-IP-address* window, select **File**, then **Stop System**.

b. Wait for BAMS to stop; this may take a couple minutes. When it has stopped, select **File**, then **Start System**.