C12kM Set Up

This chapter describes setup, configuration and starting procedures in the following sections:

Router Configuration

In order for C12kM to communicate with the Cisco 12000 series internet router, certain configuration tasks must be performed on the router. Until these configuration tasks are completed, C12kM cannot contact the Cisco 12000 series internet router, and no management can begin.

Before you can start using C12kM to manage Cisco 12000 series internet routers, the following conditions must apply:

- Ethernet—Management Ethernet port must be configured.
- Password—Current privileged command password must be configured.
- SNMP—Gigabit Route Processor (GRP) must be SNMP-manageable.
- Telnet—GRP should accept a telnet session.

To meet these requirements, perform the following tasks, as appropriate:

Step 1 If the Cisco 12000 series internet router does not have a configured management Ethernet port, then through the System Console enter commands as follows:

```
Router> enable
Password: <Enable Password>
Router# configure terminal
Router (config)# interface Ethernet 0
Router (config-if)# ip address <IP Address><Netmask>
```

```
Router (config-if)# exit
Router (config)# exit
Router#
```

This allows management connectivity through the Ethernet port on the GRP.

Ensure that the management workstation can telnet to the router (this may involve updating the routing table on the router).

Step 2 If the GRP does *not* currently accept telnet sessions, enter the following commands through the System Console:

Note This configuration assumes you have not configured usernames in Cisco IOS software.

```
Router> enable
Password: <Enable Password>
Router# configure terminal
Router (config)# line vty 0 4
Router (config-line)# password <Telnet Password>
Router (config-line)# login
Router (config-line)# exit
Router (config)# exit
Router#
```

The workstation running C12kM should now be able to ping the GRP.

Step 3 Open a telnet window.

If there is no current privileged command password, enter commands as follows:

```
Router> enable
Router# configure terminal
Router (config)# enable password <Enable Password>
```

Step 4 If the GRP is *not* SNMP-manageable, enter commands as follows:

```
Router> enable
Password: <Enable Password>
Router# configure terminal
Router (config)# snmp-server community <Read Only Community String> ro
Router (config)# snmp-server community <Read Write Community String> rw
Router (config)# exit
```

Enabling Traps

Traps should be enabled so that the Cisco 12000 series internet router sends traps to the C12kM server at the appropriate IP address. To enable traps to be sent to the appropriate C12kM server IP address, proceed as follows:

Step 1 Telnet to the Cisco 12000 series internet router and enter your login password.

Step 2 Enter the following:

```
enable
```

Step 3 Enter the enable password.

Step 4 Enter the following:

```
configure terminal
snmp-server enable traps
snmp-server host <IP Address of C12kM> server version 2c <ro Community String of GRP>
exit
```

Note To obtain help when using Cisco IOS commands, enter the command in question, followed by a question mark.

Setting Up a Workstation as a TFTP Server

Configuring a Trivial File Transfer Protocol (TFTP) server enables the configuration backup/restore to operate. Setting up a workstation as a TFTP server is presented in the following sections:

- Using Another Machine as a TFTP Server
- Setting Up TFTP
- Enabling the TFTP Daemon
- Creating the tftpboot Directory

Using Another Machine as a TFTP Server

Any network device can be used as a TFTP server. It is your responsibility to ensure that the network device is configured correctly. For example, when configuring Solaris devices you must have an empty file in the tftp boot directory with the following filename format, GRPaa.bb.cc.dd, where aa.bb.cc.dd is the IP address of the GRP card.

Note When the Manager is set up to be the TFTP server, C12kM ensures that the backup files exist and have the correct permissions.

Setting Up TFTP

TFTP enables you to transfer files to and from remote systems. The Configuration Backup/Restore window in C12kM allows you to back up and restore the configuration of C12kM. TFTP transfers the configuration files from a device to your system through the network.

Verify the following information:

- Daemon—TFTP daemon is enabled
- Environment—TFTP environment variable is set correctly
- Directory—tftpboot directory exists

Enabling the TFTP Daemon

The TFTP daemon must be enabled for C12kM to upload or download a configuration file.

If you are using standard Sun software, verify that the TFTP daemon (tftpd) is enabled as follows:

Step 1 Log in as a user with superuser rights.

Step 2 Edit the /etc/inetd.conf file using a text editor (such as vi).

Step 3 Look in the file /etc/inetd.conf for the line that invokes tftpd. When the line is commented out (starts with a pound sign **#** as in the following example), use a text editor to delete the pound sign.

```
#tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

Step 4 Save the changes in the edited file and exit.

Step 5 Reboot the system.

Step 6 Verify that the TFTP daemon is enabled by entering:

```
hostname# netstat -a | grep tftp
```

Output similar to the following appears:

```
*.tftp Idle
```

Note When there is no output, tftpd is not enabled. For additional information on TFTP, refer to the UNIX man pages on tftp and tftpd.

Creating the tftpboot Directory

The tftpboot directory stores configuration files from GRPs. To create the tftpboot directory, do the following:

Step 1 If the tftpboot directory does not exist, enter commands as follows to create the directory:

```
hostname# mkdir /tftpboot
```

Step 2 Modify the permissions by entering the following:

```
hostname# chmod 777 /tftpboot
```

Note All users accessing the tftpboot directory will have read, write, and execute permissions.

Starting a User Session

C12kM starts automatically when you start the Cisco EMF user session. To start a Cisco EMF/C12kM user session, do the following.

Note Cisco EMF must be running before starting a Cisco EMF user session.

Step 1 Log in as a user with superuser rights.

Step 2 If Cisco EMF is already started, proceed to step 3.

or

To run Cisco EMF, enter the following:

CEMF_ROOT`/bin/cemf start`

Note Replace `CEMF_ROOT` with the directory where Cisco EMF is installed.

Note Any type of user (not just superusers) can start a Cisco EMF user session.

Step 3 To start a Cisco EMF user session, enter commands as follows:

CEMF_ROOT`/bin/cemf session`

Step 4 Enter a username and a password. The default username is `admin`, and the default password is `admin`.

The Cisco EMF and C12kM processes start.

Stopping a C12kM User Session

When you stop Cisco EMF, you also stop the C12kM application. To stop the Cisco EMF/C12kM user session, proceed as follows:

Step 1 Quit any Cisco EMF/C12kM windows running.

When you quit the Launchpad window, your user session is terminated.

Step 2 Confirm your decision to quit the Cisco EMF system by clicking `OK`.

The Cisco EMF user session ends.

Stopping Cisco EMF

If you want to stop all Cisco EMF processes entirely, proceed as follows:

Step 1 Log in as a user with superuser rights.

Step 2 Enter commands as follows:

```
CEMF_ROOT/bin/cemf stop
```

Note Replace `CEMF_ROOT` with the directory where Cisco EMF is installed.

The Cisco EMF processes stop.

Checking the Status of C12kM

To check the status of Cisco EMF/C12kM, enter the following command:

```
CEMF_ROOT/bin/cemf query
```

Note Replace `CEMF_ROOT` with the directory where Cisco EMF is installed.

The message “CEMF Manager Initialized” is displayed. A list of running processes is also be displayed. If Cisco EMF is not active, this message appears: “CEMF Manager system not running”.

When you run a `cemf query`, verify that the process “CiscoCGMCon” is running. If this process is not running, C12kM might be installed incorrectly and may need to be reinstalled.