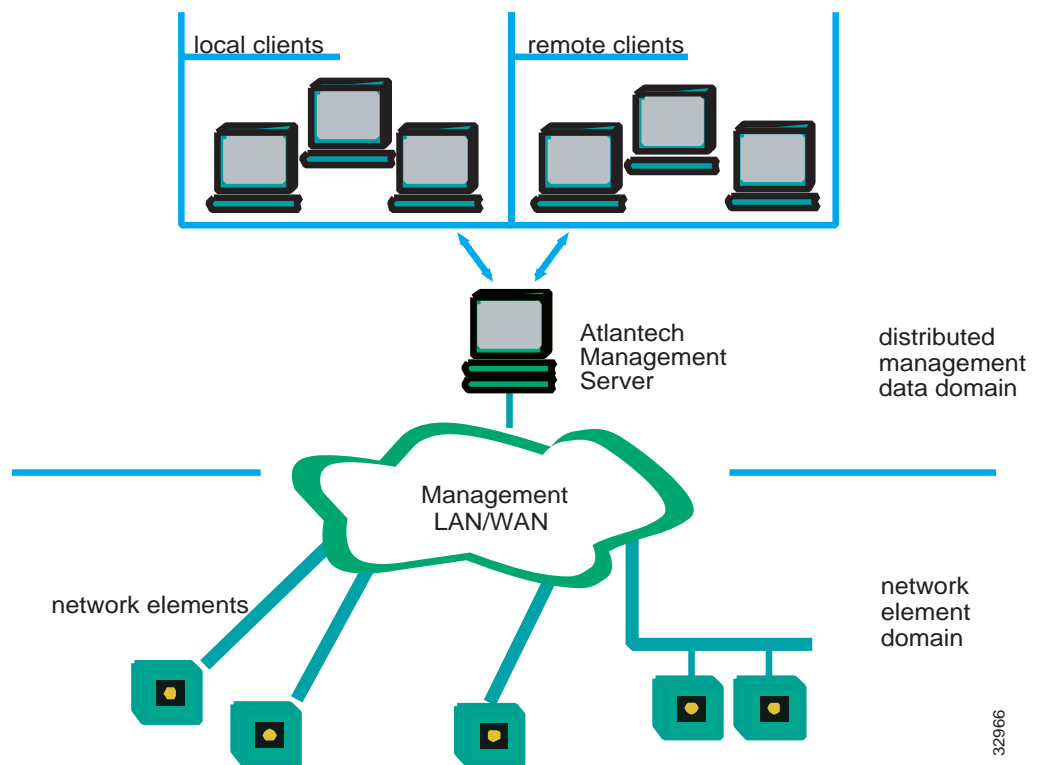# Installation

6400 SCM Deployment Options

The Cisco 6400 SCM can be deployed in a distributed manner, utilizing the power of multiple machines. Two types of installation (server and client) can be performed from the CD. Figure 1-1 shows a typical deployment.

Figure 1-1   **Server/Client Deployment**

Cisco 6400 SCM Server

Every Cisco 6400 SCM deployment must have a Cisco 6400 SCM server installed. The Cisco 6400 SCM server contains all the server processes which keep track of the current state of the network, such as models, user access, and events. The server also includes all client application windows.

Client Installations

A Cisco 6400 SCM deployment may have client installations on separate workstations. These client installations run Cisco 6400 SCM applications which access objects on the server. A client installation contains only those parts of the Cisco 6400 SCM system necessary to allow you to run a Cisco 6400 SCM user session. This user session communicates with the Cisco 6400 SCM server when required to retrieve management information. In this case, all window updates are processed locally on the client machine, freeing more resources on the Cisco 6400 SCM server to process network information.

The client install copies the client software onto the local machine; therefore, there is no need to mount files across the network. The only network traffic occurs when the client requires more data from the server.

Note   A Cisco 6400 SCM server installation also includes all files that run a Cisco 6400 SCM user session on the server system. The Cisco 6400 SCM system can therefore be installed on a single system with server and client functionality, and can be upgraded by adding separate client machines later as required.

System Requirements

The Cisco 6400 SCM is a CEMF-based solution and can be deployed in a number of configurations, from a 'single hardware system' solution to a multi-site distributed management system. All CEMF-based solutions run on Sun Solaris/SPARC hardware running the Solaris operating environment, release 2.6.

Use the Cisco 6400 SCM with the following Cisco 6400 IOS releases:

* IOS Version for NSP card — 12.0(3) DB

* IOS Version for NRP card —11.3(8) DB

Note   For large scale deployments, fault tolerant options (for example, Sun Netra FT1800) are available.

Minimum Server Requirements:

* Sun Ultra 60

* 1 CPU

* 256 MB RAM (512 MB recommended)

* 4GB disk + additional SCSI disk (internal or external)

* 17" color monitor

Note   The additional disk is for performance improvements of the database, not for additional storage capacity.

Note   The Sun Ultra 30 is also suitable - however, the Sun Ultra 60 provides extra options for future expansion (such as additional CPU) and is therefore recommended.

In larger deployments, CEMF-based solutions can run in a client-server configuration.

Typical Client Requirements:

- Sun Ultra 5 workstation

- 128 MB RAM (256 MB recommended)

- 4GB disk

- 17" color monitor

Note   If a number of graphically intensive applications are being ran on this workstation, it is helpful to use a Sun color card (for example, 24 bit color). A typical server installation requires 300MB of free disk space in a file system (for example, **/opt)**. An appropriate amount of free disk space for database files is also required.

For a small deployment (for example, trials), the typical client and server can run together on a single workstation. The requirements for this scenario are as follows:

- Sun Ultra 5 Workstation

- 256MB RAM

- 4GB disk

- 17" color monitor

Hardware Configuration Requirements

The following list of prerequisites must be met before the Cisco 6400 SCM can manage a Cisco 6400 UAC.

Perform these steps through a Console Terminal session to the Node Switch Processor (NSP):

Step 1   If there is currently no privileged command password:

Switch> **enable**

Switch# **config terminal**

Switch (config)# **enable password** *<ENABLE PASSWORD>*

Step 2   If the NSP does not have a configured management ethernet port:

Switch> **enable**

Password: *<ENABLE PASSWORD>*

Switch# **config terminal**

Switch (config)# **interface Ethernet 0/0/0**

Switch (config-if)# **ip address** *<ADDRESS> <NETMASK>*

Switch (config-if)# **exit**

Switch (config)# **exit**

Switch#

> **Note** Be sure that the 10BaseT ethernet port on the NSP is connected to the same network as the Cisco 6400 SCM.

The Ultra 60 running the Cisco 6400 SCM is now able to ping the NSP.

Step 3 If the NSP is not SNMP-manageable:

Switch> **enable**

Password: *<ENABLE PASSWORD>*

Switch# **config terminal**

Switch (config)# **snmp-server community** *<Read Only Community Name>* **ro**

Switch (config)# **snmp-server community** *<Read Write Community Name>* **rw**

Switch (config)# **exit**

Step 4 Check to see if the NSP accepts a telnet session by entering: **telnet** *<IP ADDRESS OF NSP> f*rom the Ultra 60 running the Cisco 6400 SCM. If the NSP does not accept a telnet session:

Switch> **enable**

Password: *<ENABLE PASSWORD>*

Switch# **config terminal**

Switch (config)# **line vty 0 4**

Switch (config-line)# **password** *<TELNET PASSWORD>*

Switch (config-line)# **login**

Switch (config-line)# **exit**

Switch (config)# **exit**

Switch#

Step 5 If WebConsole access is required, refer to CISCO NSP documentation for set up details.

Perform the following steps through a Console Terminal session to each NRP:

If there is currently no privileged command password:

Router> **enable**

Router# **config terminal**

Router (config)# **enable password** *<ENABLE PASSWORD>*

Step 6 When the NRP does not have a configured management ethernet port:

Router> **enable**

Password: *<ENABLE PASSWORD>*

Router# **config terminal**

Router (config)# **interface Ethernet 0/0/0**

Router (config-if)# **ip address** *<ADDRESS> <NETMASK>*

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

Router (config)# **exit**

Router#

Note   Make sure that the 10BaseT ethernet port on the NRP is connected to the same network as the Cisco 6400 SCM.

The Ultra 60 running the Cisco 6400 SCM is now able to ping the NRP.

Step 7   If the device is not SNMP-manageable:

Router> **enable**

Password: <*ENABLE PASSWORD*>

Router# **config terminal**

Router (config)# **snmp-server community** <*Read Only Community Name*> **ro**

Router (config)# **snmp-server community** <*Read Write Community Name*> **rw**

Router (config)# **exit**

Router#

Step 8   If the device is not set up to send SNMPv1 traps to the management station:

Router> **enable**

Password: <*ENABLE PASSWORD*>

Router# **config terminal**

Router(config)# **snmp-server host** <*management station ipaddress*> **version 1** <*Read Write Community Name*>

Router(config)# **exit**

Router#

Step 9   Check to see if the NRP accepts a telnet session by entering: **telnet** <*IP ADDRESS OF NRP*> from the Ultra 60 running the Cisco 6400 SCM. If the NRP does not accept a telnet session:

Router> **enable**

Password: <*ENABLE PASSWORD*>

Router# **config 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#

Enabling 6400 SCM Traps

Traps should be enabled so that the 6400 UAC sends traps to the SCM Server at the appropriate IP address.

To enable traps to be sent to the appropriate SCM server, proceed as follows:

Step 1   Telnet onto the 6400 (to the NSP and NRP), enter your login password (this is the 1st one in the NSP/NRP config EM screen)

Step 2   Type: enable

Step 3   Enter the enable password (this is the 2nd one in the NSP/NRP config EM screen)

Step 4   Type:

config t

snmp-server enable traps

snmp-server-host *<IP address of SCM Server> <read community name of NSP>*

Note   To get help when using IOS, type the word, followed by **?**.

License Requirements

The CEMF framework, upon which the Cisco 6400 SCM is based, requires a license key to operate. Please refer to the *CEMF Server User Guide* for details, or contact the Cisco Technical Assistance Center (TAC) for assistance.

Installing from a Remote CD-ROM Drive

To install software onto a system that does not have its own CD-ROM drive, you need to mount the CD on the remote system and then export the device to make it accessible over the network. These operations are done on the remote system where the CD-ROM drive exists. Finally, on the local system where the installation is to take place, you need to mount the remote CD.

Step 1   Insert the Cisco 6400 SCM CD into the CD-ROM drive on the remote host.

Step 2   Login as superuser on the remote host and see if the volume manager is running.
Enter **/usr/bin/ps -ef | grep vold**

When the Volume Manager is running, a message similar to this one is returned:

root 591 1 0 Feb 26 ? 0 :01 /usr/sbin/vold

Step 3   If a message similar to the one shown above is not displayed, start the Volume Manager:
Enter **/etc/rc2.d/S92volmgt start**

Step 4   Export the CD-ROM device on the remote host:

A) If they are not already running, start the NFS related daemons.
Enter **/usr/lib/nfs/nfsd 8**
Then enter **/usr/lib/nfs/mountd**

B) Share the mount point from the remote host.
Enter **share -F nfs -o ro /cdrom/cdrom0**

C) Verify that this host has now made the CD-ROM drive accessible.
Enter **share**
The listing displayed includes the **/cdrom** mount point.

Step 5   Mount the remote CD-ROM on the local host (on which the installation is to take place):

A) Create a mount point when none exists already.
Enter **mkdir /mnt/cdfiles**

B) Mount the remote directory.
Enter **mount -r** *<remote-host>* **: /cdrom/cdrom0 /mnt/cdfiles**

Note   Replace the *<remote-host>* with the host name of the remote device.

The contents of the CD are visible under the **/mnt/cdfiles** mount point.

Installing the Cisco 6400 SCM/Server Using avinstall

Note   The following process assumes that you have already installed the CEMF server from the CEMF CD-ROM and that you have a valid license key. Refer to the CEMF server installation user guide for further details.

To install a Cisco 6400 SCM using **avinstall:**

Step 1   Login as superuser.

Step 2   Insert the Cisco 6400 SCM CD. Change the directory into the cdrom area: **cd /cdrom/cdrom0**

Step 3   Stop CEMF processes if they are running. Enter: *<CEMFROOT>*/**bin/av stop**, where *<CEMFROOT>* is the CEMF installation path (for example, **/opt/av**).

Step 4   Run the install script **./avinstall**

A menu listing the SCM client and SCM server installation options (shown in Figure 1-2) appears:

Figure 1-2   Installation Options

Note   If the required CEMF server/client is not installed, the SCM installation option is not available.

Step 5   Select the installation you require.

The utility performs the appropriate installation.

Note   The Cisco 6400 SCM user guide is located on the CD-ROM in the docs subdirectory of the CD. The guide is in PDF format and can be read using the Acrobat Reader available from http://www.adobe.com/prodindex, or on the CD ROM, in the **acrobat** subdirectory.
To install the Acrobat Reader:
1) Change directory into the acrobat subdirectory on the CD ROM.
2) Run the install script, as follows: **INSTALL**, and follow the instructions given.
3) Add the 'bin' directory of the Acrobat installation to your UNIX search path.
4) To view the 6400 SCM User Guide from the CD ROM, type: **acroread /cdrom/cdrom0/docs/cisco6400scmv1_1userguide.pdf**.
Note that, in accordance with the defects listed above, the user guide PDF files are not installed during the installation process. Therefore, you may choose to view the PDF files directly from the CD, as shown above. Alternatively, you may choose to copy the PDF files from the CD ROM to a local directory on your workstation (for example, **mkdir** <*CEMFROOT*>/**docs**.
cp /cdrom/cdrom0/docs/cisco6400scmv1_1userguide.pdf <*CEMFROOT*>/**docs**).

Step 6   Once the installation is complete, exit the cdrom area by entering: **cd /** then remove the Cisco 6400 SCM CD ROM by entering: **eject cdrom**.

Step 7   Start the CEMF and 6400 SCM processes by entering: <*CEMFROOT*>/**bin/av start**.

Note   This automatically starts on a system restart.

Step 8   Initialize the system by entering <*CEMFROOT*> **av dataload**.

Step 9 Start the application set by entering *<CEMFROOT>*/**bin/avsession**.

The Cisco 6400 SCM is now ready to use.

De-Installing the Cisco 6400 SCM

All Cisco 6400 SCM processes stop and are de-installed when the avinstall script is run with the **-r** option.

Step 1 Log on to the machine as superuser with Cisco 6400 SCM installed.

Step 2 Insert the Cisco 6400 SCM CD. Change the directory into the cdrom area by entering: **cd /cdrom/cdrom0**.

Step 3 Run the de-installation script provided.
Enter **./avinstall -r**

A menu appears, listing SCM client and SCM server de-installation options (as shown in Figure 1-3).

Figure 1-3   De-Installation Options
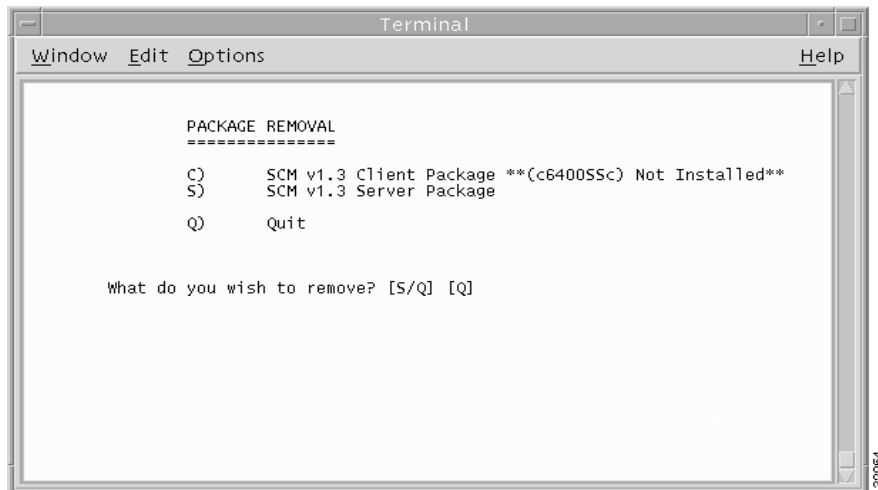
Note Figure 1-3 indicates that a client SCM is not installed on the system. However, a SCM server is installed on the system and can be de-installed through option S.

Step 4 Select the de-installation you require.

You are notified that the deinstallation is about to take place. When you proceed with the de-installation, the window scrolls through the software as it is deleted and the following message appears:

Message `Removal of <package> was successful.`

Setting Up a Workstation as a Trivial File Transfer Protocol (TFTP) Server

Configuring a TFTP Server

Configuring a TFTP server enables the configuration backup/restore to operate. This section describes how to configure the TFTP server to run on the SCM server.

Using Another Machine as the TFTP Server

Configuring the SCM server as a TFTP server is optional. You may alternatively choose to use a different machine as the TFTP server, or not to use the backup/restore functionality at all. If you decide to use another machine as a TFTP server, make sure that empty backup files exist on the TFTP server. You also need the appropriate permissions set to allow read and write access. The NSP backup files have the filename NSPaa.bb.cc.dd where aa.bb.cc.dd is the IP address of the NSP, and the NRP backup files have the filename NRPaa.bb.cc.dd where aa.bb.cc.dd is the IP address of the NRP. A backup file is created for the active NSP and each active NRP in the 6400 chassis.

Note   When the SCM server is set up to be the TFTP server, the SCM 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 the SCM allows you to backup and restore the configuration of a Cisco 6400 SCM (NSP and NRPs). TFTP transfers the configuration files from a device to your system through the network.

Verify the following information: that the TFTP daemon is enabled; that the TFTP environment variable is set correctly; and that a **tftpboot** directory exists.

Enabling the TFTP Daemon

The TFTP daemon must be enabled for the Cisco 6400 SCM to upload or download a configuration file.

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

Step 1   Log in as a superuser.

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), remove the pound sign with an editor.

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   Now verify that TFTP daemon is enabled by typing:

hostname# netstat -a | grep tftp

The output should be similar to the following:

*.tftp Idle

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

Creating the Tftpboot Directory

The tftpboot directory stores the configuration files from the Cisco 6400 SCM NSP and NRPs.

Step 1 When the tftpboot directory does not exist, use the following command to create the directory:

hostname# mkdir /tftpboot

Step 2 The tftpboot directory must have the appropriate permissions. Modify the permissions with the following command:

hostname# chmod 777 /tftpboot

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

Administering Cisco 6400 SCM Workstations

Starting Cisco 6400 SCM

The Cisco 6400 SCM software is automatically started during system boot-up. Otherwise, start the software as follows:

Step 1 Login as superuser.

Step 2 Enter *<CEMFROOT>***/bin/av start**. The Cisco 6400 SCM processes start.

Stopping the Cisco 6400 SCM

The Cisco 6400 SCM software is stopped during system shut down. Otherwise, stop the software as follows:

Step 1 Quit any Cisco 6400 SCM Launchpad sessions currently running.

Step 2 Login as superuser.

Step 3 Enter *<CEMFROOT>***/bin/av stop**.

The Cisco 6400 SCM processes cease.

Checking the Status of Cisco 6400 SCM

You can check the status of Cisco 6400 SCM as follows:

Step 1 Enter *<CEMFROOT>***/bin/av query**

Step 2 The system responds with a list of running processes when the Cisco 6400 SCM is active or with the following message when the SCM is inactive:

Message `Cisco 6400 SCM system not running`

Starting a Client Application

Note "Client" refers to both clients on the SCM server and clients on a remote host.

Start a client application as follows:

Step 1 Enter <*CEMFROOT*>/**bin/avsession**.

Step 2 You are prompted to enter a user name and password. The default user name is **admin** and the default password is also **admin**.