Initial Configuration

The Cisco 6400 Equipment Module supports the Cisco 6400 Universal Access Concentrator (UAC). The Cisco 6400 UAC is a multi-technology access concentrator that offers conventional ATM switching functions with full support for different QoS classes as well as a unique set of aggregation and routing capabilities, including:

- Convergence
- Aggregation
- Multiplexing
- Mapping
- Routing
- Bridging
- NRP SSG
- ATM PVC Range

The Equipment Module works directly with the Cisco 6400 UAC through FTP (or Telnet) and SNMP or TFTP and SNMP.

The Equipment Module provides an event logging daemon to track event log changes from the Cisco 6400. The daemon is started/stopped in the workstation boot and runs independently of Cisco Provisioning Center.

To configure this Equipment Module for use with Cisco Provisioning Center, you must complete the following steps.

Table 1-1 Cisco 6400 Equipment Module Configuration Task List

Task	Page Reference
Verify the software requirements	page 1-2
Verify hardware compatibility	page 1-2
Perform Cisco 6400 configuration	page 1-3
Perform Cisco Provisioning Center server configuration	page 1-12
Perform RADIUS server configuration	page 1-17

Software Requirements

This section outlines the software requirements that must be fulfilled for the correct operation of the Cisco 6400 Equipment Module. All software included in this section must be acquired independently of the Cisco 6400 Equipment Module.

Table 1-2 outlines the software requirements for the Cisco 6400 Equipment Module.

Table 1-2 Required Software

Vendor	Software	Version
Cisco	IOS (NRP-1)	12.1(1) to 12.2(2)B5
	IOS (NRP-2)	12.1(5) to 12.2(2)B2
	IOS (NRP-2SV)	12.2B to 12.2(4)B3
	IOS (NSP)	12.1(1) to 12.2(2)B5
Merit	RADIUS server	3.6B[1]

1. Installation of the Merit RADIUS server requires Solaris version 2.7 or higher and FTP/Telnet capability.

Hardware Compatibility

This section provides information about hardware compatible with the Cisco 6400 Equipment Module.

Network Interface Cards

The following network interface cards (referred to as “line cards”) are supported by the Cisco 6400 Equipment Module.

Table 1-3 Compatible Hardware

Chassis	Part Number	Card Type	Description
Cisco 6400 UAC	NLC-2DS3-BNC	DS3	2 port DS3 line card
	NLC-2OC3-SM	OC3	2 port OC-3/STM-1 Single Mode
	NLC-2OC3-MM	OC3	2 port OC-3/STM-1 Multi Mode
	NLC-1OC12-SM	OC12	1 Port OC12/STM-4 Single Mode

Initial Configuration

The Cisco 6400 UAC, and the Cisco Provisioning Center server must be initially configured to make the Cisco 6400 Equipment Module fully operational. The initial configuration required for this Equipment Module involves the following steps:

Cisco 6400 Configuration

The following steps must be completed by logging into the NRP and NSP on the Cisco 6400 and manually configuring the hardware via IOS.

1. Setting up the NRP
2. Setting up the NSP
3. RADIUS configuration
4. IOS Command Support Configuration

Cisco Provisioning Center Server Configuration

The following procedures should be completed by logging into the Cisco Provisioning Center server host machine and configuring the Cisco Provisioning Center server via a terminal window.

1. Receiving traps (optional)
2. Event logger daemon (optional)
3. Workstation upload configuration (required)
4. RADIUS configuration (optional)

RADIUS Server Configuration (Optional)

The following procedures are completed by logging into the RADIUS server host machine and configuring the RADIUS server via a terminal window.

1. Installing the RADIUS server
2. Starting the RADIUS daemon
3. Installing the Cisco 6400 Equipment Module Utility Package
4. Configuring the RADIUS clients file (for NRPs)

Cisco 6400 Configuration

Some initial configuration must be done for each Node Router Processor (NRP) and Node Switch Processor (NSP) individually in order to facilitate the creation, modification, deletion and management of DSL services using the Cisco 6400 Equipment Module. Before upload and provisioning functions of the NSP and NRP can occur, each NSP and NRP must have the following parameters configured:

- Management IP address for NRP and NSP. For the NRP2 card, you do not have to provide an IP address.
- Login name
- Login password
- Enable password
- SNMP agent enabled
- SNMP community strings

For more information on configuring the above parameters, refer to the appropriate Cisco 6400 user documentation.

Running-Config Autosave

You can configure the Cisco 6400 Equipment Module to automatically save the IOS running-config file of the Cisco 6400. By default, the running-config autosave feature is disabled.

To enable autosave, follow these steps:

Step 1 Navigate to the $CCP_CONFIG directory on the server.

Step 2 Open the syavconfig.site file with a text editor.

Step 3 Locate the following line:

```
C4.WriteNVRAM = 0
```

Step 4 To enable autosave, change the value of the C4.WriteNVRAM variable to 1:

```
C4.WriteNVRAM = 1
```

Step 5 Save and exit the file.

Step 6 Have the Cisco Provisioning Center server read the configuration file:

```
SYnpt -r
```

Note The running-config autosave feature can have a performance impact on heavily loaded NRP cards.

Configuring the NRP

Each NRP requires initial configuration in order to communicate with the Cisco Provisioning Center server. An NRP must be configured to enable the following features:

- single hop and multihop tunneling (optional)
- event logging (optional)
- authentication (required)

Optionally, you can configure a first generation NRP card (NRP) as redundant for failure protection. Second generation NRP cards (NRP2) do not support redundancy.

Event Logger Requirements

You must set up each Cisco 6400 NRP before launching the event logger. For more information on configuring the NRP, refer to the appropriate Cisco 6400 user documentation. The following procedure uses an NRP and NRP2 to illustrate the configuration process. The procedure for configuring each NRP is identical but the method for accessing NRPs and NRP2s is different (these procedures are outlined in the following two sections). Configuration requires a thorough understanding of Cisco IOS software.

If you are configuring an NRP, follow the procedure outlined in "Accessing the NRP" to access it. If you are configuring an NRP2, follow the procedure outlined in "Accessing the NRP2" to access it. After you have accessed the NRP, continue with the NRP configuration by following the procedure outlined in "Configuring the NRP".

Accessing the NRP

Perform the following procedure to access the NRP.

Step 1 Log in to the Cisco 6400 by using telnet and the management IP address of the NRP:

```
telnet <ip_address>8
```

Step 2 Enter the username and password.

Step 3 The user EXEC prompt (*Router*>) will appear. Configuration changes must be made from enable mode. To enter enable mode from the user EXEC prompt, issue the following commands:

```
Router>enable
password:password
```

Accessing the NRP2

NRP2 cards do not have an IP address assigned to them and must be accessed through the NSP. Perform the following procedure to access the NRP2.

Step 1 Log in to the Cisco 6400 by using telnet and the management IP address of the NSP:

```
telnet <ip_address>
```

Step 2 Enter the username and password.

Step 3 The user EXEC prompt (*Router*>) will appear. Configuration changes must be made from enable mode. To enter enable mode from the user EXEC prompt, issue the following commands:

```
Router>enable
password:password
```

Step 4 Enter the following command to access the NRP2 through the NSP:

```
nrps<Slot_Number>
```

where:

Slot_Number—The slot number of the NRP2.

Configuring the NRP

To configure the NRP, perform the following procedure.

Step 1 Enter configuration mode.

```
config terminal
```

Step 2 Enable Event Logger requirements by entering the following IOS commands:

```
snmp-server community PUBLIC RO
snmp-server community PRIVATE RW
snmp-server trap-timeout 10
snmp-server enable traps config
snmp-server enable traps snmp
snmp-server host <IP Address> traps version 2c PUBLIC udp-port 5999
exit
```

where:

IP Address—The IP address of the Cisco Provisioning Center server host.

Note You can enable other traps in addition to the ones specified in the above example. For a complete list of traps, refer to the appropriate Cisco 6400 user documentation.

Step 3 Verify the NRP configuration by issuing the following command:

```
show running-config
```

Step 4 Save the configuration by entering the following command:

```
write memory
```

If you have enabled the running-config autosave feature, you do not need to perform this step. For more information on running-config autosave, see the "Running-Config Autosave" section on page 1-4.

Configuring Tunnel Awareness

You can configure each NRP to be aware of single hop and multihop tunnels. Tunnels that are created using L2TP are used by Virtual Private Dial-Up Networking (VPDN) to extend a PPP session across a wide area network. NRPs must be configured to look for tunnel definitions on a L2TP Network Server (LNS). Perform the following procedure at the privileged EXEC prompt to enable VPDN:

Step 1 Enter global configuration mode:

```
config terminal
```

Step 2 Enable VPDN and inform a router to look for tunnel definitions on an LNS:

```
vpdn enable
```

Step 3 Enable multihop tunneling:

```
vpdn multihop
```

Step 4 Specify how the NAS is to perform VPDN tunnel authorization searches:

```
vpdn search-order multihop-hostname domain
```

Configuring NRP Redundancy

As a failure prevention measure, NRPs can operate in redundant mode. In redundant mode, one NRP is configured as the primary NRP and a second NRP is configured as the secondary. Redundant NRP cards must occupy adjacent slots (i.e.: 1 and 2, or 3 and 4). Redundancy is transparent since both NRPs share the same IP address. In redundant mode, when a connection is provisioned on the primary NRP, it will be mirrored on the secondary NRP in case the primary card fails. It is also possible to swap the roles of each NRP between primary and secondary.

If you require a pair of NRPs to operate in redundant mode, you must do so using the following IOS commands on the NRP.

Change to Redundancy mode from Global mode using the following IOS command:

```
redundancy
```

In redundancy mode, configure a redundant pair using the following command:

```
associate subslot <slot_number_1>/0 <slot_number_2>/0
```

Where:

<slot_number_1>—the slot number of the primary NRP

<slot_number_2>—the slot number of the secondary NRP

For example, the following IOS command will configure slots one and two on the NRP as a redundant pair:

```
redundancy
associate subslot 1/0 2/0
```

For NRP redundancy to work properly, you must configure Cisco Provisioning Center to autosave to memory the IOS running-config file that the Cisco 6400 Equipment Module uses. For more information on configuring Cisco Provisioning Center to automatically save the IOS running-config file, see the "“Running-Config Autosave” section on page 1-4."

For more information on NRP redundancy, consult the appropriate Cisco documentation.

Note NRP2 cards cannot be configured to operate in redundant mode.

Note When the primary NRP becomes inactive, services are moved to the backup NRP. However, once the primary NRP is re-activated, Cisco Provisioning Center does not move services back to the primary NRP from the backup NRP. The primary NRP does not act as a backup NRP in this case. For more information, consult the appropriate Cisco documentation.

Configuring Username Authentication

Configuration of the username authentication system is optional when logging into the NRP. The NRP acts as a client NAS (Network Access Server). The NAS is the aggregation point of PPP sessions into an L2TP tunnel. To configure the username authentication system for the NAS, enter the following IOS commands at the privileged EXEC prompt:

Step 1 Enter global configuration mode:

```
config terminal
```

Step 2 Specify the host name or user name and a password in the following format:

```
username <name> [ no password | password <encryption type>
<password>]
```

where:

name—A username or the machine name

encryption type—A number that represents a certain encryption type - 0 indicates a cleartext password

password—A unique password

for example:

```
username C4 password 0 ABCPassword
```

Note For more information on configuring an NRP as a NAS, refer to the appropriate Cisco user documentation.

Matching VC Traffic Parameters for CNX

The Cisco 6400 Equipment Module will reuse existing VC Class traffic parameters when the C4_vcclassname attribute is null and the given traffic parameters match an existing VC Class. To enable the Cisco 6400 Equipment Module to compare given VC class parameters with existing VC Classes, the C4.CompareCNX_VCClass configuration flag in the syavconfig.site file must be set to a value of 1. Setting this value to 0 (zero) disables this comparison functionality and tells Cisco Provisioning Center to use the VC class provided by name.

To set the C4.CompareCNX_VCClass configuration flag, follow these steps:

Step 1 Ensure that the Cisco Provisioning Center server environment is sourced and the server is not running.

Step 2 Navigate to the $CCP_CONFIG directory on the server.

Step 3 Open the syavconfig.site file with a text editor.

Step 4 Locate the following line:

```
C4.CompareCNX_VCClass = 0
```

Step 5 Set the value of the C4.CompareCNX_VCClass flag to 1 to enable the matching feature. Set the value to 0 (zero) to disable the feature.

Step 6 Save and exit the file.

Step 7 Start the Cisco Provisioning Center server:

SYnpt -sS

Robust CNX Provisioning

When you create a PVC on the NRP, the Cisco 6400 Equipment Module performs a test in the network interface to detect if the PVC already exists in the NRP, but is not present in the Cisco 6400 Equipment Module database. When this out-of-sync condition occurs, Cisco Provisioning Center sends an error message, and forces a rollback of the transaction.

This test uses the IOS command show atm pvc <vpi>/<vci> | include exist which detects the IOS response that the PVC does not exist. When it does exist, no response is sent. The error message is in the following format:

"Failed to create CNX <vpi>/<vci> on subinterface ATM0/0/0.<subif>. Reason: the CNX exists but was not uploaded"

Configuring the NSP

You must configure the Cisco 6400 NSP before launching the event logger. For more information on configuring the NSP, refer to the appropriate Cisco 6400 user documentation. The following procedure uses an NSP to illustrate the configuration process. Configuration requires a thorough understanding of Cisco IOS software.

To configure the NSP:

Step 1 Log in to the Cisco 6400 by using telnet and the IP address of the NSP:

```
telnet <ip_address>
```

Step 2 Enter the username and password.

Step 3 The user EXEC prompt (*Switch*>) will appear. Configuration changes must be made from enable mode. To enter enable mode from the user EXEC prompt, issue the following commands:

```
Switch>enable
password:password
```

Step 4 Enter configuration mode.

```
config terminal
```

Step 5 Enable Upload and Event Logger requirements by entering the following IOS commands in succession:

```
snmp-server community PUBLIC RO
snmp-server community PRIVATE RW
snmp-server trap-timeout 10
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps chassis-fail
snmp-server enable traps chassis-change
snmp-server host <IP Address> traps version 2c PUBLIC udp-port 5999
exit
```

where:

IP Address—The IP address of the Cisco Provisioning Center server host with Event Logger.

Step 6 Verify the NSP configuration by issuing the following command:

```
show running-config
```

Step 7 Save the configuration by entering the following command:

```
write memory
```

If you have enabled the running-config autosave feature, you do not need to perform this step. For more information on running-config autosave, see the "Running-Config Autosave" section on page 1-4.

Note You can enable other traps in addition to the ones specified in the above example. For a complete list of traps, refer to the appropriate Cisco 6400 user documentation.

Configuring Username Authentication

Configuration of the username authentication system is recommended when logging into the NSP. The NSP acts as a client NAS (Network Access Server). To configure the username authentication system for the NAS, enter the following IOS commands at the privileged EXEC prompt:

Step 1 Enter global configuration mode:

```
config terminal
```

Step 2 Specify the host name or user name and a password in the following format:

```
username <name> [ no password | password <encryption type>
<password>]
```

where:

name—A username or the machine name

encryption type—A number that represents a certain encryption type - 0 indicates a cleartext password

password—A unique password

for example:

```
username C4 password 0 ABCPassword
```

Note For more information on configuring an NSP as a NAS, refer to the appropriate Cisco User Documentation.

RADIUS Configuration (Optional)

Before the provisioning of services can occur, you individually configure each NRP to recognize and communicate with the RADIUS server. Configuration of each NRP involves three steps:

1. New model identification—Enable the AAA access control model on each NRP.
2. Default authentication—Specify the default authentication protocol to be used in order to authenticate users.
3. Network Access Server (NAS) port format—Specify the ATM VC extended format for the NAS port field. This format is denoted by the letter "d".

Configuring RADIUS Awareness

An awareness of the RADIUS server must be established on the Cisco 6400 to allow the exchange of authorization and authentication information. This process must be done for each NRP within the Cisco 6400. The configuration is implemented using Cisco IOS commands on the router. To configure an NRP to be aware of a RADIUS server, issue the following IOS commands at the privileged EXEC prompt:

```
aaa new-model
aaa authentication ppp default group radius
aaa nas port extended
radius-server attribute nas-port format d
```

Configuring RADIUS Access

Once each NRP installed with the Cisco 6400 has been configured to be aware of a RADIUS server, further configuration must be done to specify the location of the RADIUS server host, the authentication and accounting port addresses on the server host, and the RADIUS password. These steps are required for the NRP to recognize a specific RADIUS server and where it is located. To configure RADIUS access, issue the following IOS commands at the privileged EXEC prompt:

```
radius-server host <ip address> auth-port 1645 act-port 1646
radius-server key <key>
```

where:

ip address—The IP address of the RADIUS server

key—The encryption key used on the RADIUS server. This encryption key must be identical in IOS and in the RADIUS server clients file. For more information, consult your RADIUS documentation.

Configuring Additional IOS Commands

You can configure the Cisco 6400 Equipment Module to support the *oam-pvc 0* IOS command when provisioning a VC class. To support this IOS command, you set the C4.supportExtraIOSCommands variable in the syavconfig.site file to a value of 1. Setting this variable to a value of 0 (zero) disables the IOS command support.

To configure the Cisco 6400 Equipment Module to support the additional IOS command, complete the following steps:

Step 1 Ensure that the Cisco Provisioning Center server environment is sourced and the server is not running.

Step 2 Navigate to the $CCP_CONFIG directory on the server.

Step 3 Open the syavconfig.site file with a text editor.

Step 4 Locate the following line:

```
C4.supportExtraIOSCommands = 0
```

Step 5 Set the value of the C4.supportExtraIOSCommands variable to 1.

If you want to disable the IOS command support, set the value of the C4.supportExtraIOSCommands variable to 0 (zero).

Step 6 Save and exit the file.

Step 7 Start the Cisco Provisioning Center server:

```
SYnpt -sS
```

Cisco Provisioning Center Server Configuration

The Cisco Provisioning Center server must be initially configured to communicate with the Cisco 6400 and, optionally, one or more RADIUS servers. This section outlines the procedures required to complete this configuration and enable upload.

Receiving Traps (Optional)

The Cisco Provisioning Center server system file must be configured to receive traps from the Cisco 6400. To configure the Cisco Provisioning Center server for communication with the Cisco 6400, complete the following steps:

Step 1 Log in as the root user on the Cisco Provisioning Center server.

Step 2 Open the /etc/services file with a text editor and add the following line:

```
c4trapd     5999/udp
```

This line specifies that when the C4trapd program is running, it uses the port # 5999 and udp protocol for communication with the Cisco 6400.

Step 3 Save and exit the /etc/services file.

Step 4 Find the process ID number for inetd.

```
ps -ef | grep inetd
```

Step 5 Kill the inetd process:

```
kill -HUP pid
```

where:

pid—the process ID.

Step 6 Restart the inetd process:

```
inetd -s
```

Event Logger Daemon

An event logging daemon must be installed on the Cisco Provisioning Center server host for any event logging to become operational. The event logger is distributed through the Cisco 6400 Equipment Module installation procedure. The event logger is a standalone daemon independent of Cisco Provisioning Center functions. Launching Cisco Provisioning Center does not activate the event logger, and shutting down Cisco Provisioning Center does not terminate the event logger. The event logger will continue to log events from the Cisco 6400 if Cisco Provisioning Center is shut down. When Cisco Provisioning Center is restarted, the Cisco Provisioning Center server system file will update the log files by checking in the event log directory.

Step 1 The Cisco 6400 UAC and the Cisco Provisioning Center server system file must be properly configured before the event logger can be used. You must launch the event logger separately by issuing the following command at the command line in the Cisco Provisioning Center runtime environment:

```
c4trapd -f $CCP_LOG/event/C4eventLog
```

Workstation Upload Configuration

The Cisco 6400 Equipment Module supports both FTP and TFTP to upload the hardware configuration. By default, FTP is used. If you require TFTP, you must first enable it on the Cisco Provisioning Center server. For both FTP and TFTP clients, you need to set the upload configuration variables in the FTP/TFTP Access Configuration File.

Enabling TFTP on the Cisco Provisioning Center Server

If you require TFTP enabled on the Cisco Provisioning Center server, perform the following procedure. This procedure is not required if you intend to use FTP.

Step 1 Log in as root on the Cisco Provisioning Center server.

Step 2 Ensure that you have write access to /etc/inetd.conf. If not, change the permissions by issuing the following command:

```
chmod u+w /etc/inetd.conf
```

Step 3 Edit the /etc/inetd.conf file by changing the following line from:

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

to:

```
tftp dgram udp wait root /usr/sbin/in.tftp in.tftp
```

This will enable the TFTP daemon in insecure mode.

Step 4 Verify the workstation is TFTP enabled by issuing the following command:

```
ps -ef | grep inetd
```

If your workstation outputs an inetd process like the following:

```
root 136  1  0  Apr 17 ?    0:12 /usr/sbin/inetd -s
```

where the second column (136) is the process ID (PID), then TFTP is already enabled. Force the TFTP daemon to re-read the inetd.conf file by issuing the following command:

```
kill -HUP <pid>
```

where *pid* is the inetd process ID.

If your workstation does not output an inetd process, start the inetd process by issuing the following command:

```
inetd -s
```

Step 5 Verify that TFTP is enabled by issuing the following command:

```
netstat -a | grep tftp
```

Step 6 If TFTP is enabled, you should see the following output:

```
*.tftp Idle
```

FTP/TFTP Access Configuration File

To enable FTP upload, you must define three configuration variables: C4_USER, C4_PASSWORD, and C4_FTP. The user and password combination must correspond to a valid UNIX user account on the workstation which has write permission in the /tmp directory. This account enables FTP to retrieve the running configuration from the Cisco 6400.

To enable TFTP upload, you do not uncomment the C4_USER and C4_PASSWORD variables. The C4_FTP variable must be uncommented and set to FALSE.

Optionally, for both FTP and TFTP, you can set the variable C4_IPADDRESS that points to the IP address of the Cisco Provisioning Center host machine. This is required when there are multiple IP addresses for Cisco Provisioning Center servers in the network, or when a firewall is performing IP address translation.

The configuration variables are contained in a configuration file and must be set before the Cisco Provisioning Center server starts.

For example, the C4FTPAccess.config for an FTP configuration may look as follows:

```
C4_USER = <username>
    C4_PASSWORD = <password>
C4_FTP = TRUE
#C4_IPADDRESS =
```

Or, the configuration file for a TFTP configuration may look as follows:

```
#C4_USER =
    #C4_PASSWORD =
C4_FTP = FALSE
C4_IPADDRESS = <ip_address>
```

The variables can also be manually set outside of the configuration file. In this case, these variables override the variables set in the configuration file.

To set the Cisco 6400 upload configuration variables, follow the steps:

Step 1 Ensure that the Cisco Provisioning Center server environment is sourced and the server is not running.

Step 2 Navigate to the $CCP_CONFIG directory on the server.

Step 3 Open the C4FTPAccess.config file with a text editor.

Step 4 Uncomment the required Cisco 6400 upload configuration variables, and provide values:

```
C4_USER = ftp_user_name
C4_PASSWORD = ftp_user_password
C4_FTP = TRUE | FALSE
C4_IPADDRESS = ip_address
```

where:

ftp_user_name—the user name for your FTP account (FTP only)

ftp_user_password —the password for your FTP account (FTP only)

TRUE | FALSE—set to TRUE to enable FTP for upload. Set to FALSE if you want to use TFTP.

ip_address—The IP address of the Cisco Provisioning Center host machine is required when there are multiple IP addresses for *Cisco Provisioning Center* servers in the network. Otherwise, this attribute is optional.

Step 5 Save and exit the file.

Step 6 Start the Cisco Provisioning Center server:

```
SYnpt -sS
```

Setting the Maximum Number of Network Interface Executors

You can set the maximum number of Network interface (NIF) executors in concurrent provisioning on a per site basis by editing the C4.NIFMaxSiteExecutors variable in the syavconfig.site. The default value of this variable is 5. The minimum allowed value is 1. The maximum value is determined by the value of the SYSSR.flowCOntrol variable.

To set the maximum number of NIF executors in concurrent provisioning, complete the following steps:

Step 1 Ensure that the Cisco Provisioning Center server environment is sourced and the server is not running.

Step 2 Navigate to the $CCP_CONFIG directory on the server.

```
cd $CCP_CONFIG
```

Step 3 Open the syavconfig.site file with a text editor.

```
vi syavconfig.site
```

Step 4 Locate the following line:

```
C4.NIFMaxSiteExecutors = 5
```

Step 5 Set the C4.NIFMaxSiteExecutors variable to the required value.

Step 6 Save and exit the file.

Step 7 Start the Cisco Provisioning Center server:

```
SYnpt -sS
```

Configuring CNX VC Class Autogeneration

You can configure CNX VC Class autogeneration by editing the C4.disableVCClassAutogenerate variable in the syavconfig.site. The default value of this variable is 0, which indicates that VC Class autogeneration is enabled. To disable CNX VC Class autogeneration, the variable must be set to 1.

To configure CNX VC Class autogeneration, complete the following steps:

Step 1 Ensure that the Cisco Provisioning Center server environment is sourced and the server is not running.

Step 2 Navigate to the $CCP_CONFIG directory on the server.

```
cd $CCP_CONFIG
```

Step 3 Open the syavconfig.site file with a text editor.

```
vi syavconfig.site
```

Step 4 Locate the following line:

```
C4.disableVCClassAutogenerate = 0
```

Step 5 To disable the feature, set the C4.disableVCClassAutogenerate variable to a value of 1.

```
C4.disableVCClassAutogenerate = 1
```

Step 6 Save and exit the file.

Step 7 Start the Cisco Provisioning Center server:

```
SYnpt -sS
```

Setting the Maximum Number of Concurrent Getter Processes

To set the maximum number of concurrent getter processes, you set the C4upl.getterLimit configuration variable to indicate the number of concurrent sessions that Cisco 6400 Equipment Module will use at any one time. The maximum number of concurrent processes that Cisco 6400 EM supports is 100.

To set the maximum number of concurrent getter processes, complete the following steps:

Step 1 Ensure that the Cisco Provisioning Center server environment is sourced and the server is not running.

Step 2 Navigate to the $CCP_CONFIG directory on the server.

```
cd $CCP_CONFIG
```

Step 3 Open the syavconfig.site file with a text editor.

```
vi syavconfig.site
```

Step 4 Locate the following line:

```
C4upl.getterLimit = 5
```

Step 5 Edit the file to set the C4upl.getterLimit variable to the appropriate value.

Step 6 Save and exit the file.

Step 7 Start the Cisco Provisioning Center server:

```
SYnpt -sS
```

Setting Getter Timeout Time

To set the getter timeout time, you set the C4.getterTimeout configuration variable to indicate the amount of time (in seconds) the Cisco 6400 Equipment Module will wait before individual getters (both Fabric and Service) will time out. The default value is 60.

To set the getter timeout time, complete the following steps:

Step 1 Ensure that the Cisco Provisioning Center server environment is sourced and the server is not running.

Step 2 Navigate to the $CCP_CONFIG directory on the server.

```
cd $CCP_CONFIG
```

Step 3 Open the syavconfig.site file with a text editor.

```
vi syavconfig.site
```

Step 4 Locate the following line:

```
C4.getterTimeout = 60
```

Step 5 Edit the file to set the C4.getterTimeout variable to the appropriate value.

Step 6 Save and exit the file.

Step 7 Start the Cisco Provisioning Center server:

```
SYnpt -sS
```

Merit RADIUS Configuration

Configuration of the Merit RADIUS server is an integral part of provisioning Layer Two Tunneling Protocol (L2TP) single hop services on Cisco 6400 UAC equipment. The RADIUS server carries information on subscriber service lists and L2TP tunnels. The server acts as a repository of tunnels. Each tunnel has a Service Name key used to bind subscribers to the tunnel.

The Cisco 6400 Equipment Module uses a Merit RADIUS server for service pre-authorization. Data transfer between the Cisco Provisioning Center server host and the Merit server host is accomplished through FTP and TELNET sessions.

Merit RADIUS Installation

Installing the RADIUS Server

To install the Merit RADIUS server, perform the following steps on the host where the RADIUS server is to be installed. It is assumed that you have obtained a copy of the Merit RADIUS server software independently of Cisco Provisioning Center.

Step 1 Log in as root.

Step 2 Display the admintool interface by entering

```
admintool
```

Step 3 Select **Groups** from the **Browse** pull-down menu.

Step 4 Select **Add** from the **Edit** pull-down menu

Step 5 Table 1-4 specifies the values that should be entered during the setup of the group account.

Table 1-4 Group Attribute Values

Attribute	Description	Sample Value
Group Name	Required. Specifies a name used by the system to identify a user's group. A group name is a text string composed of lowercase alphabetical characters (a-z) and digits (0-9). A group name can be 1-8 characters.	staff
Group ID	Required. Specifies a group identification number used by the system to create a user's primary group. By default the next available number displays here.	102, 103
Members List	Optional. Specifies users or groups who belong to this group. If there is more than one member in the list, then separate names with a comma but do not use any spaces.	bill,bob,barney

Step 6 Select **Users** from the **Browse** pull-down menu.

Step 7 Select **Add** from the **Edit** pull-down menu. Table 1-5 specifies the values that should be entered during the setup of the group account.

Table 1-5 User Attribute Values

Attribute	Description	Sample Value
User Name	Required. Specifies the login name the operating system will use to identify this user. The user name must be a unique name composed of uppercase or lowercase alphabetical characters (a-z) or digits (0-9). A user name can be 1-8 characters long.	meritP
User ID	Required. Specifies a number by which the operating system can identify a user. The user's UID is typically a number between 100 and 60000.	1003, 1004
Primary Group	Required. Specifies a group number or a group name.The operating system will assign the group number to files created by the user.	staff
Secondary Groups	Optional. Specifies other groups this user will belong to.	
Comment	Optional. Specifies notes about this user account.	
Login Shell	Required. Specifies a login shell for the user. The Korn shell is mandatory.	Korn
Password	Required. Specifies the means by which a user sets up a password.	Select Normal Password from the drop-down menu and enter a password for the user.
Min Change	Optional. Specifies the minimum number of days allowed between password changes.	
Max Change	Optional. Specifies the maximum number of days a user can go without having to set up a new password.	
Max Inactive	Optional. Specifies the maximum number of days the user account can be inactive before the user must set up a new password.	
Expiration Date	Optional. Specifies the expiration day, month, and year for a user's password.	

Table 1-5 User Attribute Values (continued)

Attribute	Description	Sample Value
Warning	Optional. Specifies when users will start receiving warning messages about their password expiring.	
Create Home Dir	Required. Specifies whether or not the user's home directory is to be set up automatically. By default, the user's home directory is set up automatically.	/usr/private/etc/raddb
Path	Required. Specifies the path for the user's home directory. The path is where admintool will place the user's initialization files. If Create Home Dir is selected you must specify a path.	/usr/private/etc

Step 8 Exit the admintool interface and login as the user you just created (i.e.: **meritP**):

```
su - meritP
```

Step 9 Change to the directory where the Merit RADIUS server is to be installed.

```
cd /usr/private/etc
```

Step 10 Copy the Merit RADIUS server file (c4MeritRadius3.6B.tar) from the $CCP_MNG/utility directory into the current directory.

Step 11 Extract the Merit RADIUS server according to the directions in the Merit RADIUS README file (RadiusInstall.README) found in the $CCP_MNG/utility directory. This will install the software.

Starting the RADIUS Daemon

Step 1 Ensure that you are in the directory where the Merit RADIUS server is installed.

```
cd /usr/private/etc
```

Step 2 Start the Merit daemon:

```
$ ./radiusd
```

Testing the RADIUS Server

It is recommended that you test the Merit RADIUS server to determine whether the server is operational and to determine if the server will correctly authenticate a user.

Step 1 Login as the user **meritP**:

```
su - meritP
```

Step 2 Navigate to the directory containing the Merit server installation:

```
cd /usr/private/etc
```

Step 3 Issue the radcheck command to determine whether the Merit server is operational:

```
radcheck -p 1645 -r 1 <hostname>
```

The server is working if a similar output to the following is displayed:

```
 MF: vp=1703/1692 auth=2/1 waldo=1/1 redo=0/0
 DNS-MF: client=2/0 addr=78/78 name=78/77
 CLIENT-MF: vendor=10/0 vendor_list=158/157 (found=1)
 auth queue: 1/1/(1/0), acct queue: 0/0/(0/0), maxtime: 0
(000107.143023)
 auth stats: 2/0/0, acct stats: 0/0/0
 authfile: 2, clients: 1, users: 1, 000107.143022
 fsmid: STD, dictid: 1.14, vendid: 1.4
 cleanup_delay: 6, avg-delay 1 (of 100)
 Version 3.6B  sun

 "hostname(1645)" is responding
```

Step 4 Authenticate a sample user by using the radpwtst command:

```
radpwtst -p 1645 -s <hostname> -r 1 -w smart -u ppp smartuser
```

If authentication is successful, the server will prompt:

```
"smartuser" authentication OK
```

Automating RADIUS Server Startup

You can enable the RADIUS server to start up automatically when the system is booted. To automate the Merit RADIUS server startup process, follow the following procedure on the RADIUS server host:

Step 1 Add the following entries into the /etc/services file on the Merit RADIUS server host:

```
# RADIUS protocol
radius                                          1645/udp
radacct                         1646/udp
```

Step 2 Add the following entry in the /etc/inetd.conf file on the Merit RADIUS server host:

```
radius dgram udp wait meritP /usr/private/etc/radiusd radiusd
```

Installing the Cisco 6400 Equipment Module Utility Package

The Cisco 6400 Equipment Module includes a utilities package that must be installed separately on the RADIUS server host if you are doing your own installation of a RADIUS server. This package must be installed in the utility directory under the database directory. The package includes the C4buildDBM, C4userFilter, and C4userMerge executables.

To install the package, complete the following procedure:

Step 1 Navigate to the database directory on the RADIUS server host:

```
cd usr/private/etc/raddb
```

Step 2 Copy the C4buildDBM, C4userFilter, and C4userMerge executables from the Cisco Provisioning Center server host. These files are contained in the c4Utils.tar file located in the $CCP_BIN directory on the Cisco Provisioning Center server host. Copy the tar file over to the RADIUS server host.

```
cp /net/host/disk2/SY/Activator/Server/sys/bin/c4Utils.tar.
```

Step 3 Extract the utilities.

```
tar xvf c4Utils.tar
```

Note Ensure that the RADIUS server database directory is the login directory for RADIUS server user accounts. By doing this, you avoid having to modify scripts to change from the working directory to the database directory when an FTP or TELNET session is initialized.

Configuring the RADIUS Clients File

In order to enable the RADIUS server to allow an NRP authorization request from the Cisco 6400, the NRP must be recognized as a client of the RADIUS server. The clients file must specify the IP address of each NRP that intends to use the RADIUS server for user authorization and authentication. The structure of the clients file will be similar to the following dialog:

```
#Client Name       Key             [type]          [version] [prefix]
#----------------  --------------- --------------- --------- --------
192.1.10.151        password       type = Merit:PROXY
#10.1.2.3:256       test            type = nas      v2        pfx
#pm1                 %^$%#*(&!(*&)+  type=nas                  pm1.
```

Note The key specified in the RADIUS clients file must be identical to the key specified for the RADIUS server in the NRP IOS as outlined in the section "Configuring RADIUS Access".

For more information on configuring the Merit RADIUS server clients file, visit the Merit Server AAA Configuration clients file page at http://www.merit.edu/aaa/clients.html.