Avocent®

CCM

Installer/User Guide

INSTRUCTIONS

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

DANGEROUS VOLTAGE

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

POWER ON

This symbol indicates the principal on/off switch is in the on position.

POWER OFF

This symbol indicates the principal on/off switch is in the off position.

PROTECTIVE GROUNDING TERMINAL

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

CCM
Installer/User Guide

USA Notification

WARNING: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Notification

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Japanese Approvals

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

European Union

WARNING: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese Notification

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

Product Overview

Features and Benefits

Overview

The CCM console management appliance provides non-blocked access and control for devices such as serial-managed Linux (or other UNIX) servers, routers, power management devices and firewalls. This includes Avocent SPC power control devices that provide advanced power management.

- The CCM850 appliance has 8 serial ports. A single 10/100 Mbps Ethernet port provides network connectivity on each appliance. Two CCM850 appliances may be mounted in 1U of vertical space in a standard 19 inch rack.
- The CCM1650 appliance has 16 serial ports. A single 10/100 Mbps Ethernet port provides network connectivity on each appliance. Two CCM1650 appliances may be mounted in 1U of vertical space in a standard 19 inch rack.
- The CCM4850 appliance has 48 serial ports. A single 10/100/1000 Mbps Ethernet port provides network connectivity on each CCM appliance. One CCM4850 appliance may be mounted in 1U of vertical space in a standard 19 inch rack.

Each appliance has a console port that uses a Command Line Interface (CLI) for configuration, management and optionally, connection to other ports.

Serial device access options

You may choose from among several client application options to access the CCM appliance and its attached serial devices:

- The AVWorks® cross-platform management application that offers a built-in enhanced Telnet client and a Secure Shell (SSH) client
- Third party Telnet clients
- Third party SSH clients

Access to attached serial devices is also possible through the appliance serial CLI, plus PPP (Point to Point Protocol) and other types of dial-in connections to a modem on the console port.

When session sharing is enabled, the CCM appliance supports multiple concurrent sessions. Configured user access levels may be used as preemption criteria for serial port access.

User authentication and data security

The CCM user database supports up to 64 user accounts, which include usernames, passwords and/or keys, plus specifications of access rights/levels to CCM appliance ports and commands. User definitions may be changed at any time. You may choose to have user access authenticated locally at the CCM user database and/or at one or more RADIUS (Remote Access Dial-In User Service) servers. Data security may be enhanced using industry-standard SSH encryption.

Extensive command set

The CCM appliance offers a wide range of commands that allow administrators to easily configure, control and display information about the CCM appliance operating environment, including its ports, user accounts and active sessions. The serial CLI is always available on the unit's console port, and may be easily accessed during a session with an attached serial device.

The user interface also offers descriptive error message data and built-in command help information. On-board Trivial File Transfer Protocol (TFTP) support allows administrators to upload new functionality to CCM appliances in the field.

Port history

Each CCM port has a buffer that holds the most recent 64K bytes of online and offline serial data. A separate history command mode lets you navigate within a port's current history file and conduct tailored searches.

You may also configure the appliance to write serial port data to a file on an NFS server, thus preventing data loss due to overflow of the history buffer.

Safety Precautions

To avoid potential device problems, if the building has 3-phase AC power, ensure that a computer and its monitor (if used) are on the same phase. For best results, they should be on the same circuit.

To avoid potentially fatal shock hazard and possible damage to equipment, please observe the following precautions:

- Do not use a 2-wire extension cord in any product configuration containing this appliance.
- Test AC outlets at the computer and monitor (if used) for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup Uninterruptible Power Supply (UPS), power the computer, the monitor and the CCM appliance off the supply.

NOTE: The AC inlet is the main disconnect.

Rack mount safety considerations

- Elevated Ambient Temperature: If installed in a closed rack assembly, the operation temperature of the rack environment may be greater than room ambient. Use care not to exceed the rated maximum ambient temperature of the unit.

- Reduced Airflow: Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- Mechanical Loading: Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Consider equipment nameplate ratings for maximum current.
- Reliable Earthing: Reliable earthing of rack mounted equipment should be maintained. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

Using AVWorks Software

The AVWorks cross-platform management application may be used to manage CCM appliances and access attached devices. Using AVWorks software, you may perform most of the operations that are described in this manual. This manual describes how to manage a CCM appliance by entering commands using the CLI. The AVWorks Installer/User Guide describes how to manage a CCM appliance using the graphic interface.

CHAPTER 2

Installation and Configuration

Hardware Overview

This section describes the CCM appliance LEDs, buttons and connectors.

CCM850 and 1650 appliance hardware

Figure 2.1 shows the front panel of a CCM1650 appliance. (The front panels of the CCM850 appliance and the CCM1650 appliance contain the same LEDs and buttons.)

Figure 2.1: CCM1650 Appliance Front Panel

The lower left area of the front panel contains the following LEDs and buttons:

- The *POWER* LED illuminates when the CCM appliance is connected to a power source.
- The *ONLINE* LED illuminates steadily (not blinking) when the CCM appliance self-test and initialization procedures complete successfully.
- The *LINK* LED illuminates when the CCM appliance establishes a connection to the network.
- The *TRAFFIC* LED blinks when there is network traffic.
- The *100Mbps* LED illuminates when the CCM appliance is connected to a 100 Mbps LAN.
- The RESET button, when pressed, reboots the CCM appliance. See *Rebooting* on page 10.
- The INIT button, when pressed and held, restores the CCM factory default values. See *Reinitializing* on page 11.

Figure 2.2 shows the back panel of a CCM1650 appliance.

Figure 2.2: CCM1650 Appliance Back Panel

The back panel contains:

- RJ-45 port connectors for serial cabling (the CCM850 appliance has 8 port connectors, the CCM1650 appliance has 16 port connectors). The port number is adjadent to each connector.
- A LAN connector for a 10BaseT or 100BaseT interface cable.
- An RJ-45 CONSOLE PORT connector.

CCM4850 appliance hardware

Figure 2.3 shows the front panel of a CCM4850 network appliance.

Figure 2.3: CCM4850 Appliance Front Panel

The front panel contains 48 serial port connectors. The lower left area of the front panel contains the following LEDs, buttons and connectors.

The *ONLINE* LED illuminates steadily (not blinking) when the CCM self-test and initialization procedures complete successfully.

The *POWER* LED illuminates when the CCM appliance is connected to a power source and the power switch is on (|).

The RESET button reboots the CCM appliance when pressed. See *Rebooting* on page 10.

The INIT button restores the CCM factory defaults when pressed and held. See *Reinitializing* on page 11.

A console device may be connected to the RJ-45 CONSOLE PORT.

A 10BaseT, 100BaseT or 1000BaseT interface cable may be connected to the LAN PORT.

Two LEDs adjacent to the LAN PORT (*SPEED* and *LINK/TRAFFIC*) indicate the link speed and whether there is traffic on the link. Table 2.1 describes the possible values.

Table 2.1: CCM4850 Appliance LAN LED Values

SPEED LED	LINK/TRAFFIC LED	Description
Off	Off	No link
Off	On	Link at 10 Mbps
Green	On	Link at 100 Mbps
Orange	On	Link at 1000 Mbps
Off	Flashing	Traffic at 10 Mbps
Green	Flashing	Traffic at 100 Mbps
Orange	Flashing	Traffic at 1000 Mbps

Figure 2.4 shows the back panel of a CCM4850 appliance.

Figure 2.4: CCM4850 Appliance Back Panel

The back panel contains:

- The AC line cord connector.
- Outflow openings for the two internal fans.
- A DB-9 DEBUG PORT connector. This port should be used only on the advice and with the guidance of Technical Support.

Installing the CCM Appliance

WARNING: This unit is not user serviceable. To avoid electrical shock, do not attempt to open the unit or operate with the cover off. Do not attempt to make any repairs. See *Appendix F* on page 113 for information.

WARNING: The power outlet should be near the equipment and easily accessible.

To install the CCM appliance hardware:

1. Place the unit where you can connect cables between the serial devices and the CCM serial ports, and where you can connect a LAN interface cable between the Ethernet hub or switch and the CCM LAN connector.
2. Connect devices to the CCM serial ports; see *Device Cabling* on page 95 for cable information. Connect each serial device to its appropriate power source, following the device's documentation.

3. Attach a LAN interface cable to the LAN connector on the CCM appliance. A CAT 5 cable is required for 100BaseT operation. For CCM4850 appliances, a CAT 6 cable is required for 1000BaseT operation.
4. Insert the power cord into the back of the CCM appliance. Insert the other end of the power cord into a grounded electrical receptor.
5. Check that the *POWER* LED on the front of the unit is illuminated. If not, check the power cable to ensure that it is inserted snugly into the back of the unit. The *ONLINE* LED will illuminate within two to three minutes to indicate that the self-test is complete. If the *ONLINE* LED blinks, contact Technical Support for assistance.
6. For CCM850/1650 appliances, check that the *LINK* LED is illuminated.

   For CCM4850 appliances, check that the LAN port LEDs indicate that a 10, 100 or 1000 Mbps link exists.

   If there is no link, check the Ethernet cable to ensure that both ends are correctly inserted into their jacks.
7. Once the *POWER*, *ONLINE* and appropriate LEDs are illuminated, proceed with the configuration process (if you will be using BootP, remove power from the appliance).

Configuring the CCM Appliance

To configure the CCM appliance, you must specify a unique IP address, plus other network address information. This information will be stored in the CCM configuration database. During initial login, you will specify a password for the Admin user.

Configuring the network address settings

You may configure the CCM appliance network address settings using AVWorks software, BootP or the serial CLI on the console port.

To configure the network address settings using AVWorks software:

Using the AVWorks New Appliance Wizard is the easiest method to configure the CCM appliance network address settings. See the AVWorks Installer/User Guide for instructions. After the network address settings are configured, see *Initial CCM appliance login* on page 10.

To configure the network address settings using BootP:

1. Ensure that there is a BootP server on your network that is configured to correctly respond to a BootP request from the CCM appliance. BootP servers require the Ethernet MAC address of network devices. The Ethernet MAC address is printed on a label affixed to the appliance. See your BootP server's system administrator guide for information about configuring the BootP server.
2. After you have configured your network's BootP server with the CCM appliance Ethernet MAC address, IP address, subnet mask and gateway, restore power to the CCM appliance and wait for the *ONLINE* LED to illuminate. Once this occurs, the CCM appliance has completed the BootP protocol, obtained its network address information and stored these in FLASH.

3. You may verify that the BootP process was successful with a ping command, which tests network connectivity. The ping command is entered as:

   ```
   ping <ip_address>
   ```

   For example, the following command tests the network connectivity of a CCM appliance with the IP address 192.168.0.5.

   ```
   ping 192.168.0.5
   ```

4. If the CCM appliance completes the BootP successfully, you will see a display similar to the following.

   ```
   Pinging 192.168.0.5 with 32 bytes of data:
   Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
   Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
   Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
   Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
   ```

   If the CCM appliance did not successfully obtain its IP address with the BootP protocol, you will see a display similar to the following.

   ```
   Pinging 192.168.0.5 with 32 bytes of data
   Request timed out.
   Request timed out.
   Request timed out.
   Request timed out.
   ```

   In this case, check the address information provided to the BootP server to confirm it is correct. Verify that the Ethernet LAN adaptor cable is correctly installed on the CCM appliance and the Ethernet hub.

After the network address settings are configured successfully, launch a Telnet session to the assigned IP address. Then, see *Initial CCM appliance login* on page 10.

To configure the CCM appliance using the serial CLI:

1. Attach a compatible device to the console port. The compatible device types are: ASCII, VT52, VT100, VT102, VT220 and VT320.

   For cable and adaptor information, see *Device Cabling* on page 95. You may use any terminal emulation program that is available on your system.

2. Configure your terminal or terminal emulation program as follows.

Baud rate	9600
Bits per character	8
Stop bits	1
Flow control	None

3. Press the **Return** or **Enter** key until a prompt appears, requesting your username. If you do not receive a prompt after pressing the key five times, check your cable and serial settings to be sure that they are correct.
4. Proceed to *Initial CCM appliance login* on page 10.

Initial CCM appliance login

The CCM appliance ships with a single user defined in its user database. The first time you connect to the appliance, you are prompted for a username.

To log in to the CCM appliance for the first time:

1. At the Username prompt, type **Admin**. There is no factory default password for the Admin user. At the Password prompt, press **Return**.

   ```
   Username: Admin
   Password:
   Authentication Complete
   CCM configuration is required.
   ```

2. Once authentication completes, the CCM appliance prompts for any missing configuration values that are required for operation.

   If you already provided the IP address, subnet mask and gateway, you will not be prompted for those values again.

   If you have not already provided the network information, you will be prompted for them. Enter the addresses using standard dot notation.

   ```
   CCM configuration is required
   Enter CCM IP address > 192.168.0.5
   Enter CCM Subnet mask > 255.255.255.0
   Enter CCM Gateway address > 0.0.0.0
   ```

3. You are prompted for a new Admin password. Passwords are case sensitive and must contain 3-16 alphanumeric characters. You must enter the new password twice to confirm that you entered it correctly.

   ```
   Enter CCM New Admin Password > *****
   Confirm New Admin Password > *****
   ```

After you have provided the required configuration information, a confirmation message appears while the CCM appliance stores the values in its configuration database.

You have now completed the initial login, and you may enter additional commands at the CLI prompt (>). To configure other CCM appliance ports, see *Configuring Serial Port Settings* on page 15.

Rebooting and Reinitializing the CCM Appliance

You may reboot or reinitialize the CCM appliance by pressing a recessed button on the appliance front panel or by issuing a command.

Rebooting

During a reboot, any active Telnet sessions, including your own, are terminated. Any configuration changes that require a reboot will become effective when the reboot completes.

To reboot the appliance in hardware:

1. Locate the recessed RESET button on the front of the CCM appliance. An opened paper clip may be used to depress the button.
2. Insert the opened paper clip in the recess, then depress the button.

To reboot the appliance with a command:

Issue a Server Reboot command.

Reinitializing

Reinitializing the CCM appliance removes configured information. This may be useful when reinstalling the unit at another location in your network.You may erase the configuration database, which contains all nonvolatile data except the IP address, subnet mask and gateway. You may also erase both the configuration database and the network address information.

To reinitialize the CCM appliance in hardware:

1. Locate the recessed INIT button on the front of the CCM appliance. An opened paper clip may be used to depress the button.
2. Insert the end of the opened paper clip in the recess, then depress and hold the button. The *ONLINE* LED will blink, indicating an initialization has been requested. You have approximately seven seconds to release the button before any action is taken.

   After seven seconds, the *ONLINE* LED will blink more rapidly to confirm that the CCM configuration database has been erased. Continuing to hold the INIT button for a few more seconds will erase the IP address as well. The *ONLINE* LED will blink faster to confirm the deletion.

If any portion of FLASH is erased, the CCM appliance reboots when the INIT button is released.

To reinitialize the CCM appliance with a command:

1. Issue a Server Init command with the Config parameter if you wish to erase the configuration database but retain the network address information.
   -or-
   Use the All parameter if you wish to erase the configuration database and the network address information.
2. You are prompted to confirm or cancel the operation.

The appliance reboots after initializing the database and copying it to the configuration FLASH.

CHAPTER 3

Operations

Overview

The CCM console management appliance and its ports are easily configured and managed to meet your requirements for device connection, user authentication, access control, power status monitoring, port history information display and Simple Network Management Protocol (SNMP) compliance for use with third party network management products.

Configuring Global Settings

Generally, the CCM appliance-level commands affect console port operations, configure/initiate physical operations and enable/disable features.

Console port settings

The Server CLI command includes parameters that configure the console port:

- The terminal type to be used
- Enabling/disabling connections to devices from the console port - see *Connecting to devices from the console port* on page 18
- The modem initialization character - see *Configuring and using dial-in connections* on page 19

This command also covers the following:

- The CLI access character that will suspend a device session and place you in CLI command mode (this value may be overridden at the port level) - see *CLI Mode* on page 26
- Local port history file processing options during connection and when a session ends - see *Managing Port History* on page 33.
- The session time-out value, which indicates the period of inactivity that must occur before a session is ended (this value may be overridden at the port level) - see *Session time-out* on page 27

Network settings, updating firmware and rebooting/reinitializing the appliance

To change the CCM appliance IP, gateway or subnet addresses, use the Server Set command (page 71).

To update the boot or application firmware on the appliance, use the Server FLASH command (page 67).

The appliance may be rebooted or reinitialized by pressing a button on the appliance or by issuing a command; see *Rebooting and Reinitializing the CCM Appliance* on page 10.

Enabling/disabling features

Table 3.1: Appliance Feature Reference

For information about using this feature	See this section
Accessing a Network Time Protocol (NTP) server to update the time	*Updating the Appliance Clock* on page 14
Using an NFS server to store device session data	*NFS history files* on page 35
PPP	*Using PPP* on page 19
Using a RADIUS server for user authentication	*RADIUS authentication* on page 30
Security lock-out	*Using security lock-out* on page 32
Session sharing	*Session sharing* on page 23
SNMP	*Managing the CCM Appliance Using SNMP* on page 39
SSH	*Using SSH* on page 20

Updating the Appliance Clock

The CCM appliance supports the NTP protocol. When NTP is enabled, the real time clock on the CCM appliance will be updated immediately after NTP is enabled, each time the appliance reboots and optionally, at specified intervals.

You may specify one or two NTP servers to provide the time. An NTP server may be external or an internal server that you supply. The primary server will be queried for the time first. If it does not respond with a valid time, the secondary server will be queried.

To enable or disable NTP:

To enable NTP, issue an NTP command with the Enable parameter.

NTP ENABLE [IP=<*prim_add*>[,<*sec_addr*>]] [UPDATE=<*hours*>]

If this is the first time NTP is being enabled, you must specify at least one NTP server address.

If you want the time to be updated periodically, specify an update interval of up to 99 hours. If you specify a zero interval value (which is the default), the time will be updated only when the CCM appliance reboots.

When you enable NTP, you are prompted to confirm or cancel the operation.

To disable NTP, issue an NTP command with the Disable parameter.

NTP DISABLE

Configuring Serial Port Settings

You may configure a CCM port to support one of two types of target devices (TDs): SPC or console.

For more information about SPC power control devices, see the SPC Installer/User Guide.

A console TD may be a serial-managed Linux (or other Unix) server, router, firewall or other supported serial device.

By default, CCM ports are configured with the settings listed in Table 3.2.

Table 3.2: Default Port Settings

Parameter	Value
Target device	Console
Name	xx-xx-xx Pn (last 3 octets of MAC address plus the port number)
Baud rate	9600
Bits per character	8
Parity	None
Stop bits	1
Flow control	None
Time-out	15 minutes
CLI access character	Use Server CLI setting (^D)
Power	None

Most of these settings are standard serial port operating characteristics.

The CLI access character parameter specifies how you access the CLI. For more information, see *CLI Mode* on page 26.

The Power parameter instructs the CCM appliance to monitor the state of a specified RS-232 control signal. Signal transitions may be configured to trigger SNMP traps. The parameter value indicates an inbound control signal (CTS, DCD or DSR) and the state of that signal (low or high). When the defined signal is true, the CCM appliance interprets it as a power on condition for the attached device; when the signal is false, a power off condition for the device is assumed. The signal specified for flow control may not be used for power control, and vice versa.

Port groups

The CCM appliance supports access control groups which may include one or more serial ports. This feature allows a user account to be granted access to a group of ports using a single specification. Each port may belong to only one group (but multiple ports may belong to the same

group). One or more port groups may then be specified in a user account. A group name may contain up to eight characters.

Up to 8 port groups may be specified for a CCM850 appliance user, up to 16 port groups for a CCM1650 appliance user and up to 48 port groups for a CCM4850 appliance user.

For example, assume that ports 1, 2, 3 and 4 are assigned to a group named LINUX. Ports 5, 6, 7 and 8 are assigned to a group named ROUTERS.

Users who must be able to access all Linux devices can be granted this right by having the LINUX group specified in each of their user accounts. Those users will be able to access the devices connected to ports 1, 2, 3 and 4.

Users who must be able to access Linux and router devices can be granted this right by having both the LINUX and the ROUTERS groups specified in their user accounts. Those users will be able to access the devices connected to ports 1 through 8.

To configure TD=console serial port settings:

Issue a Port Set command. You may specify settings for one port, multiple ports or all ports.

PORT [<*port*>|ALL] SET TD=CONSOLE [NAME=<*name*>] [BAUD=<*baud*>] [SIZE=<*size*>] [PARITY=<*parity*>] [STOP=<*stop_bits*>] [FLOW=<*flow_ctrl*>] [TIMEOUT=<*time-out*>] [SOCKET=<*socket*>] [CHAR=^<*cli_char*>] [TOGGLE=NONE|DTR] [POWER=<*signal*>] [GROUP=<*group*>]

For more information and descriptions of all valid parameters, see *Port Set command* on page 61.

To configure TD=SPC ports and settings:

Issue a Port Set command with the TD=SPC parameter.

PORT <*port*> SET TD=SPC [NAME=<*name*>] [GROUP=<*group*>]

When a port is configured for an SPC power control device, you may specify only the Name and Group parameters; no other serial port settings may be specified with the Port Set command. However, you may use the SPC command to change certain configuration values for the SPC device.

SPC <*port*>|ALL [MINLOAD=<*amps*>] [MAXLOAD=<*amps*>]

Use an SPC Socket command to configure or control the state of the sockets on the SPC device.

SPC <*port*>|ALL [SOCKET <*socket*>] [WAKE=ON|OFF] [ONMIN=<*time*>] [OFFMIN=<*time*>] [POWER=ON|OFF|REBOOT]

For more information, see *SPC Command* on page 85 and *SPC Socket Command* on page 85.

NOTE: Users who wish to use the native command interfaces of the SPC device should specify TD=console.

To display serial port settings:

Issue a Show Port command.

SHOW PORT [<*port*>|ALL|NAMES|GROUPS]

When you request information about a port configured as TD=console, the display includes configuration information, current power status (if power status monitoring has been enabled), plus

transmit, receive and error counts. When you request information about a single port and a user is currently accessing that port, the display also includes the username, access rights and other information about the current session.

When you request information about a single port configured as TD=SPC, the display includes information configured with the SPC command. A Show Port All command will indicate which ports are SPC ports.

The display for Show Port Names includes the port numbers and names. If a port's name has not been changed with a Port Set command, the logical name is displayed. The display for Show Port Groups includes the port number and port group name, if assigned.

For more information, see *Show Port command* on page 77.

Connecting to Serial Devices

The CCM appliance offers several methods for connecting to attached serial devices: Telnet, serial CLI , PPP and SSH.

You may use the session sharing feature to permit multiple concurrent connections to a port. See *Session sharing* on page 23 for more information.

Connecting to devices using Telnet

Each CCM serial port is directly addressable through a unique TCP port that provides a connection to the attached serial device.

Plain text (non-encrypted) Telnet connections are enabled by default. For information about enabling both plain text Telnet and SSH connections, *Enabling plain text Telnet and SSH connections* on page 23 and *Server Security command* on page 70.

You may access the CCM appliance and its ports using the AVWorks software Telnet client or third party Telnet client applications. Third party Telnet applications may be used in combination with AVWorks software or standalone.

AVWorks software Telnet client

Each CCM appliance ships with the AVWorks cross-platform management application. AVWorks software provides a convenient way to select a CCM appliance or an attached device and launch a Telnet session to manage it.

AVWorks software includes a built-in Serial Console Viewer Telnet application that offers several features not found in other Telnet clients. For maximum flexibility, AVWorks software allows you to associate a unique Telnet client with each CCM port. AVWorks software also provides built-in support for SSH2.

You may specify the built-in Telnet client or a third party Telnet client. For more information, see the AVWorks Installer/User Guide.

Standalone third party Telnet clients

You may use third party Telnet clients to access the CCM appliance directly without AVWorks software.

To connect to a device using Telnet:

Type **telnet,** followed by the CCM appliance IP address and the appropriate TCP port, which by default is 3000 plus the physical port number, in decimal format. (The TCP port number may be changed for any CCM port.)

For example, the following Telnet command connects to the serial device attached to physical port 4 of the CCM appliance.

```
telnet 192.168.0.5 3004
```

If an authentication method other than None has been configured for the CCM appliance, you will be prompted for a username and password. Once authentication completes, your connection is confirmed. When you successfully connect to the serial device, you will see a display similar to the following.

```
Username: Myname
Password: ******
Authentication Complete
Connected to Port: 7 9600,8,N,1,XON/XOFF
```

If the authentication method is configured as None, you may Telnet and connect to a serial device without entering credentials; however, credentials are always required when connecting to the CCM CLI.

NOTE: When using AVWorks software, the configuration of the credential caching feature may affect whether you are prompted for a username and password. See the AVWorks Installer/User Guide for more information.

Data entered at the Telnet client is written to the attached serial device. Any data received by the CCM appliance from the serial device is output to your Telnet client.

Connecting to devices from the console port

You may connect to a serial device from the console port, using a local terminal or a local PC using a terminal emulation program. If you connect an external modem to the console port, you may also access devices through a remote terminal or PC that can dial into the external modem. For information about modem connections, see *Configuring and using dial-in connections* on page 19 and *Server CLI command* on page 65.

To connect to a device from the console port:

1. Issue a Server CLI command, using the Connect parameter to enable the use of the Connect command from the console port. (This need only be done one time.)

   ```
   SERVER CLI CONNECT=ON
   ```

2. Issue a Connect command to the desired port.

   CONNECT [<*port*>] [EXCLUSIVE]

The optional Exclusive parameter requests exclusive access to the port. This is valid only if the port is not currently in use. See *Session sharing* on page 23 for more information.

If you do not specify a port, a menu will be displayed, listing the ports that are available for serial connection. Enter a port number or name, or press **Enter** to cancel the command. If a valid port is specified, a message *Connected to port ...* appears. This message includes the port name plus the configured settings for baud, data bits, parity, stop bits and flow control.

3. To end a device session that was initiated with a Connect command, issue a Disconnect command.

   DISCONNECT

For more information, see *Server CLI command* on page 65, *Connect Command* on page 53 and *Disconnect Command* on page 54.

Configuring and using dial-in connections

You may attach an external modem to the console port for dial-in serial CLI access to the CCM appliance. This may be used as a backup connection if the appliance is not accessible from the network. It may also be used as a primary connection at remote sites that do not have Ethernet network capability. The modem must be Hayes compatible.

To specify a modem initialization string:

1. Issue a Server CLI command, using the Modeminit parameter to specify the modem initialization string.

   SERVER CLI MODEMINIT="<*string*>"

   The string must be enclosed in quotes and must include at least the command settings ATV1 and S0=1, which cause the modem to issue verbose response strings and autoanswer the phone on the first ring. For more information, see *Server CLI command* on page 65.

   The modem initialization string is sent to the cabled modem when any of the following conditions occur:

   - CCM appliance initialization
   - Detection of a transition of DSR from low to high
   - Completion of a call when DCD changes from high to low

2. Upon successful modem connection, press the **Enter** key until the login prompt appears.

To display modem configuration information:

Issue a Show Server CLI command.

SHOW SERVER CLI

For more information, see *Show Server CLI command* on page 81.

Using PPP

The CCM appliance supports remote PPP access using an autoanswer modem that answers calls and establishes the PPP protocol with a dial-in client. You may establish Telnet or SSH connections over PPP.

PPP dial-in may be used to access a remote CCM appliance that does not warrant a WAN (Wide Area Network) link to the Ethernet interface. The PPP dial-in may also be used to access a subnet containing remote devices in the event of a WAN link failure. In this case, the PPP provides an alternate path to one or more remote devices.

To use PPP, you must configure a modem in autoanswer mode on the console port; see *Configuring and using dial-in connections* on page 19. Once the PPP connection is established, you must launch an application that connects to the CCM appliance or to one of its ports. The PPP connection is only a communications interface to the CCM appliance.

The CCM appliance implements a PPP server that uses CHAP (Challenge Authentication Protocol). Passwords are not accepted in the clear on PPP connections.

To enable or disable a PPP server on the console port:

1. To enable a PPP server on the console port, issue a Server PPP command with the Enable parameter.

   SERVER PPP ENABLE LOCALIP=<*local_ip*> REMOTEIP=<*rem_ip*> [MASK=<*subnet*>]

   You must specify local and remote IP addresses to be used for the CCM appliance and client ends of the PPP connection respectively. You are prompted to confirm or cancel the changes.
2. To disable a PPP server, issue a Server PPP command with the Disable parameter.

   SERVER PPP DISABLE

For more information, see *Server PPP command* on page 68.

To display PPP configuration information:

Issue a Show Server PPP command.

SHOW SERVER PPP

For more information, see *Show Server PPP command* on page 81.

Using SSH

The CCM console management appliance supports version 2 of the SSH protocol (SSH2). The CCM SSH server operates on the standard SSH port 22. The shell for this connection provides a CLI prompt as if you had established a Telnet connection on port 23. The shell request for this connection is for CLI access.

SSH connections to specific serial ports may be made on TCP ports that are numbered with values 100 greater than the standard 30xx Telnet ports for the CCM appliance. For example, if port 7 is configured for Telnet access on port 3007, then port 3107 will be a direct SSH connection for port 7. When SSH is enabled, Telnet port 23 connections will be accepted from other clients if the Server Security command includes the Encrypt=SSH,None parameter, which indicates that both SSH and plain text connections will be allowed. Connecting to Telnet port 23 may also be tunneled through a connection to SSH port 22.

SSH server keys

When SSH is enabled for the first time, all sessions are terminated and the CCM appliance generates an SSH server key. The key generation process may take up to three minutes. The key is computed at random and is stored in the CCM configuration database.

In most cases, the SSH server key should not be modified because most SSH clients will associate the key with the IP address of the CCM appliance. During the first connection to a new SSH server, the client will display the SSH server's key. You will be prompted to indicate if it should be stored on the SSH client. After the first connection, most SSH clients will validate the key when connecting to the CCM appliance. This provides an extra layer of security because the SSH client can verify the key sent by the server each time it connects.

When you disable SSH and later reenable it, you may either use the existing server key or compute a new one. If you are reenabling the same server at the same IP address, it is recommended that you use the existing key, as SSH clients may be using it for verification. If you are moving the CCM appliance to another location and changing the IP address, you may wish to generate a new SSH server key.

Authenticating an SSH user

SSH is enabled and disabled with the Server SSH command. When you enable SSH, you may specify the authentication method(s) that will be used for SSH connections. The method may be a password, an SSH key or both. A user's password and SSH key are specified with a User Add or User Set command. All SSH keys must be RSA keys. DSA keys are not supported.

Table 3.3 lists and describes the valid SSH authentication methods that may be specified with a Server SSH command.

Table 3.3: SSH Authentication Methods

Method	Description
PW (default)	SSH connections will be authenticated with a username/password. With this method, a user's definition must include a valid password in order for that user to authenticate an SSH session.
KEY	SSH connections will be authenticated with an SSH key. With this method, a user's definition must include valid SSH key information in order for that user to authenticate an SSH session. Key authentication is always local; RADIUS is not supported. For more information, see *SSH user keys* on page 22.
PW|KEY or KEY|PW	SSH connections will be authenticated with either a username/password or an SSH key. If a user has only a password defined, that user must authenticate an SSH session with a username/password. If a user has only an SSH key defined, that user must authenticate an SSH session using the key. If a user has both a password and an SSH key defined, that user may use either a username/password or the SSH key to authenticate an SSH session. This method allows the administrator to define how each user will authenticate an SSH session based on information provided in the User Add/Set command. PW authentication will be local or RADIUS as specified in the Auth parameter of the Server Security command. Key authentication is always local.

Table 3.3: SSH Authentication Methods (Continued)

Method	Description
PW&KEY or KEY&PW	SSH connections will be authenticated using both a username/password and an SSH key. With this method, a user's definition must include a password and SSH key information for that user to authenticate an SSH session. PW authentication will be local or RADIUS as specified in the Auth parameter of the Server Security command. Key authentication is always local.

A user's access rights are determined from the authentication method used. SSH key authentication always uses the access rights from the local user database. Depending on the server authentication mode specified with the Server Security command, SSH password authentication will use either the access rights from the local user database or the values returned by the RADIUS server.

With either of the "or" methods (PW|KEY and KEY|PW), the user access rights are determined from the method used to authenticate the user.

With either of the "and" methods (PW&KEY and KEY&PW), the user access rights are determined from the first method specified. If PW&KEY is specified, the access rights from the password authentication will be used. If KEY&PW is specified, the access rights from the key authentication will be used.

For more information, see *Using Authentication Methods* on page 30.

SSH user keys

A user's SSH key is specified in a User Add or User Set command. You may define a key even if SSH is not currently enabled. The key may be specified in one of two ways:

- When using the SSHKEY and FTPIP keyword pair to define the network location of a user's SSH key file, the SSHKEY parameter specifies the name of the uuencoded (Unix to Unix encoded) public key file on an FTP server. The maximum file size that can be received is 4K bytes. The FTPIP parameter specifies the FTP server's IP address.

  When this method is specified, the CCM appliance initiates an FTP client request to the specified IP address. The CCM appliance then prompts the user for an FTP username and password for connection. When connected, the CCM appliance will GET the specified key file and the FTP connection will be closed. The CCM appliance then stores the SSH key with the username in the CCM user database.
- When using the KEY keyword to specify the SSH key, the KEY parameter specifies the actual uuencoded SSH key. This is for configurations that do not implement an FTP server. The CCM appliance stores the specified key in the CCM user database.

The CCM appliance processes a uuencoded SSH2 public key file with the format described in the IETF document draft-ietf-secshpublickeyfile-02. The key must follow all format requirements. The UNIX ssh-keygen2 generates this file format. The CCM appliance also processes a uuencoded SSH1 public key file. The UNIX ssh-keygen generates this file format.

To enable SSH session access to the CCM appliance:

1. Issue a Show Server Security command to ensure that you are using an authentication method other than None.

   SHOW SERVER SECURITY

2. Issue a Server SSH command with the Enable parameter. You may also specify an authentication method.

   SERVER SSH ENABLE AUTH=<*auth*>

   If an authentication method is not specified, the previous authentication parameter will be used. The default value is AUTH=PW.

3. If you are enabling SSH for the first time, you are advised that all other CCM appliance sessions will be terminated. Enter **Y** to continue or **N** to cancel.
4. If you are reenabling SSH, you are prompted to use the existing SSH server key or generate a new key. Enter **Y** to use the existing key or **N** to generate a new key.

For more information, see *Server SSH command* on page 75.

To disable SSH session access to the CCM appliance:

Issue a Server SSH command with the Disable parameter.

SERVER SSH DISABLE

When SSH is disabled, the CCM appliance operates in plain text mode.

To display SSH information:

Issue a Show Server Security command.

SHOW SERVER SECURITY

If SSH is enabled, the display will include SSH2. Regardless of whether SSH is enabled, the display will indicate the authentication method that was specified with the Server SSH command.

Enabling plain text Telnet and SSH connections

Plain text (non-encrypted) Telnet connections are enabled by default.

If you enable SSH connections using the Server Security command and the Encrypt=SSH parameter, plain text Telnet connections will be disabled. However, if you enable SSH connections with the Server SSH command, both plain text and SSH connections will be allowed.

To enable both Telnet and SSH connections:

Issue a Server Security command, indicating Encrypt=SSH,None.

Session sharing

Session sharing allows multiple concurrent sessions to the same attached device.

- The CCM850 appliance allows up to 16 total concurrent sessions, with up to four concurrent sessions per port.

- The CCM1650 appliance allows up to 32 total concurrent sessions, with up to four concurrent sessions per port.
- The CCM4850 appliance allows up to 96 total concurrent sessions, with up to four concurrent sessions per port.

You may:

- Disable sharing. In this case, only one session per port may be active at a time.
- Enable automatic session sharing. In this case, a user will automatically be connected to a port even if it is in use (with restrictions noted in the following examples).
- Enable session sharing with the query option. In this case, when a port is in use, the session originator (the user who initiated the first session) must grant permission before other users are able to join a session on that port.

Session sharing and the preemption of device sessions are also affected by a user's configured access level. There are three access levels, with the following hierarchy:

Appliance Administrator > Administrator > User

For example, assume user A is currently accessing a device, and user B wishes to access the same device. If user B's access level is equal to or higher than user A's access level, then user B may be allowed to preempt user A's device session. See *Access levels* on page 29 for more information.

Any user may also request exclusive access to a port if there is no other existing connection to that port. This is done on the login screen by adding the E parameter after the username or by adding the Exclusive parameter with the Connect command.

The following examples show the interaction between share mode and access levels.

Session sharing examples

These examples illustrate session sharing and preemption for one port and two users. Assume this port is currently in use by the session originator (SO). Another user, the requesting user (RU), wants to connect to the same port. For simplicity, also assume that if RU is allowed to connect, it will not exceed the maximum allowable number of sessions per port or sessions per appliance.

Example 1 - SO's access level is higher than RU's access level.

Share mode = Query
SO is connected non-exclusively

SO will be prompted to approve sharing the connection.

If SO approves, then RU will be connected to the port.
If SO does not approve, then RU will not be connected to the port.

Share mode = Query
SO is connected exclusively

RU will not be connected to the port.

Share mode = Disabled or Auto

RU will not be connected to the port. (In this case, it does not matter whether SO is connected exclusively or non-exclusively.)

Example 2 - RU's access level is equal to or higher than SO's access level

Share mode = Disabled
-or-
SO is connected exclusively

RU is prompted with preemption choices E, N and D.

If RU replies with **E**, then SO will be preempted/disconnected and RU will be connected exclusively to the port.

If RU replies with **N**, then SO will be preempted/disconnected and RU will be connected non-exclusively to the port.

If RU replies with **D**, SO will remain connected and RU will not be connected to the port.

Share mode = Auto or Query
SO is connected non-exclusively

RU is prompted with preemption choices E, N, S and D.

If RU replies with **E**, then SO will be preempted/disconnected and RU will be connected exclusively to the port.

If RU replies with **N**, then SO will be preempted/disconnected and RU will be connected non-exclusively to the port.

If RU replies with **S** and Share Mode = Auto, SO will remain connected and RU will be connected to the port.

If RU replies with **S** and Share Mode = Query, SO will be prompted to approve sharing the connection.

If SO approves, RU will be connected to the port.

If SO does not approve, RU will not be connected to the port.

If RU replies with **D**, SO will remain connected and RU will not be connected to the port.

Example 3 - Ending shared sessions

In a shared session, if the SO quits the session, the next user sharing the session will become the SO. If the SO is logged out by another user, all sessions that are shared with the SO will be terminated, as well as the SO's session.

To enable/disable session sharing:

To disable session sharing, issue a Server Share command with the Disable parameter.
-or-
To enable automatic sharing, specify the Auto parameter.
-or-
To enable sharing only with the permission of the session originator, specify the Query parameter. This is the default value.

To initiate a device session with exclusive access:

At the Username: prompt, enter your username, followed by an **E** or **e**.
-or-
If device connections from the console port are enabled, enter a Connect command, followed by a port number or name, then the Exclusive parameter.

NOTE: A request for an exclusive connection is valid only when there are no other users currently using the port.

To display share mode information:

Issue a Show Server command. The display will indicate the share mode.

CLI Mode

While you are connected to an attached serial device, you may enter CLI mode and enter CCM appliance commands.

To enter or exit CLI mode when connected to a serial device:

1. To enter CLI mode, type the CLI access character, which is **Ctrl-D** by default. At the CLI prompt (>), you may enter CCM commands.
2. To exit CLI mode and return to the session with the attached device, issue a Resume command.
   RESUME

For more information, see *Resume Command* on page 64.

To change the CLI access character:

Issue a Server CLI command or a Port Set command, using the Char parameter to specify the CLI access character.

SERVER CLI CHAR=^<*char*>
- or -
PORT SET CHAR=^<*char*>

If you issue a Port Set command with Char=None, then the CLI access character specified in the Server CLI command will be used. You may use the Port Set command to override the Server CLI access character on a per-port basis.

For more information, see *Server CLI command* on page 65 and *Port Set command* on page 61.

To display CLI access character information:

Issue a Show Server CLI command.

SHOW SERVER CLI

For more information, see *Show Server CLI command* on page 81.

Ending Device Sessions

To end your session:

Enter CLI mode and issue a Quit command.
- or -
If you initiated the device session with a Connect command, enter CLI mode and issue a Disconnect command.
- or -
Allow the port to time-out due to inactivity. In this case, a notification message is issued and the serial CLI session returns to CLI mode. This time-out may occur while you are in CLI mode.
- or -
For modem connections, if a carrier drop occurs, the serial CLI session is automatically logged off.

If you end a shared session and you were the session originator, the next user sharing the session becomes the session originator.

For more information, see *Quit Command* on page 64 and *Disconnect Command* on page 54.

To end another user's session:

Issue a User Logout command, specifying the name of the user to be logged out.

A message is sent and the connection is dropped.

If you are logged out by another user during a shared session and you are the session originator, all the sessions that share with you will also be logged out.

For more information, see *User Logout command* on page 88. For information about session sharing, see *Session sharing* on page 23.

Session time-out

The CCM console management appliance monitors data traffic when you are connected to an attached serial device. You may specify a time-out value with the Server CLI command. You may also specify a time-out value for each port with the Port Set command. When no data is received from the connected user for the configured number of minutes, the connection is terminated.

The following time-out values are used:

- For a Telnet session, the Server CLI time-out value is used.
- For a serial port session, if the port's configured time-out value is zero, the Server CLI time-out value is used, even if it is also zero.
- For a serial port session, if the port's configured time-out value is non-zero, that value is used.

Managing User Accounts

The CCM user database can store information for up to 64 user accounts.

To add a user:

Issue a User Add command.

USER ADD <*username*> [PASSWORD=<*pwd*>] [SSHKEY=<*keyfile*>] [FTPIP=<*ftpadd*>] [KEY=<*sshkey*>] [ACCESS=<*access*>] [GROUP=<*group1*>[,<*group2*>...]]

You must specify a username. You must also specify a password or SSH user key information, or you may specify both. You may also include an access level/access rights and group names. For more information, see *Using SSH* on page 20, *Access rights and levels* on page 28, *User Add command* on page 87 and *Port groups* on page 15.

To change a user's configuration information:

Issue a User Set command.

USER SET <*username*> [PASSWORD=<*pwd*>] [SSHKEY=<*keyfile*>] [FTPIP=<*ftpadd*>] [KEY=<*sshkey*>] [ACCESS=[+|–]<*access*>] [GROUP=[+|–]<*group1*>[,<*group2*>...]]

You may change your own password at any time. You must have USER access rights to change another user's password or to change any user's SSH user key information and access rights.

To remove an SSH user key or password, specify Key="" or Password="". You cannot remove both the password and the SSH key from a user's definition; one must remain in the user database. Also, you cannot remove a user's key or password if that removal would result in no valid users having USER access rights.

For more information, see *Using SSH* on page 20, *Access rights and levels* on page 28 and *User Set command* on page 89.

To delete a user:

Issue a User Delete command.

USER DELETE <*username*>

For more information, see *User Delete command* on page 88.

To display user configuration information:

1. To display information about one user, issue a Show User command, specifying the username.
   SHOW USER <*username*>
2. To display information about all users, issue a Show User command with the All parameter.
   SHOW USER ALL

For more information, see *Show User command* on page 83.

Access rights and levels

Most CCM appliance commands require the user to have the appropriate permission to issue CCM appliance commands. Permissions are expressed as access rights or access levels. The access rights/levels for each command are listed in Table 4.4 on page 47. Table 3.4 describes the access rights a user may be given.

Table 3.4: Access Rights

Access Right	Description
PCON	The Port Configuration access right allows the user to modify port settings. Grant PCON access only to users who need to issue the Port Set command.
SCON	The Server Configuration access right allows the user to change the CCM configurations, including setting the IP address and updating the program load in FLASH. Grant SCON access only to users who need to administer the CCM appliance.
SMON	The Server Monitor access right allows the user to view CCM appliance status and monitor serial port activity. Grant SMON access only to users who need to assist other users in accessing attached serial devices.
USER	The USER access right allows the user to modify the user database. Grant USER access only to users who need to add users, change user specifications or delete users. At least one user must have USER access rights; otherwise, the user database cannot be changed.
BREAK	The BREAK access right allows the user to send a serial break sequence to the attached serial device. On certain devices, this sequence has a special meaning. Grant BREAK access only to users who need to use the Port Break command.
P	The Port access right gives a user access to one or more serial ports and the attached serial devices. You may grant Port access rights to specific ports (Pn), a range of ports (Px-y) or all ports (PALL).

Access levels

When you specify a user's permissions, you may either indicate the individual rights as listed in Table 3.4 or you may indicate a predefined access level. The APPLIANCEADMIN and ADMIN levels are equivalent to the following individual specifications:

- The APPLIANCEADMIN level is equivalent to PALL, USER, SCON, SMON, PCON and BREAK
- The ADMIN level is equivalent to PALL, USER, SMON, PCON and BREAK

The third level (that is, not APPLIANCEADMIN or ADMIN) is user. For preemption purposes, the following hierarchy is used: APPLIANCEADMIN > ADMIN > user.

Session sharing is affected by access levels; see *Session sharing* on page 23 for more information.

To manage a user's access rights/levels:

1. To configure a user's access rights/level, issue a User Add command, using the Access parameter to specify the rights or a level.

   USER ADD <*username*> ACCESS=<*access*>

2. To change a user's access rights/level, issue a User Set command, using the Access parameter to specify the rights or a level.

   USER SET <*username*> ACCESS=<*access*>

3. To display the access rights and level for one or all users, issue a Show User command.

   SHOW USER <*username*>|ALL

For more information, see *Managing User Accounts* on page 27 plus *User Add command* on page 87, *User Set command* on page 89 and *Show User command* on page 83.

Using Authentication Methods

The CCM appliance supports several methods for authenticating users: local, RADIUS and none. Multiple connection and authentication methods may operate concurrently. By default, authentication is performed at the local CCM user database.

Local authentication

Local authentication uses the CCM appliance internal user database to authenticate users. You may optionally specify both local and RADIUS authentication, in either order. In this case, authentication will be attempted initially on the first method specified. If that fails, the second method will be used for authentication.

RADIUS authentication

RADIUS authentication uses an external third party RADIUS server containing a user database to authenticate CCM appliance users. The CCM appliance, functioning as a RADIUS client, sends usernames and passwords to the RADIUS server. If a username and password do not agree with equivalent information on the RADIUS server, the CCM appliance is informed and the user is denied CCM access. If the username and password are successfully validated on the RADIUS server, the RADIUS server returns an attribute that indicates the access rights defined for that username.

To use RADIUS authentication, you must specify information about the primary RADIUS server and optionally, a secondary RADIUS server to be used as a backup.

The RADIUS server definition values specified in CCM appliance commands must match corresponding values configured on the RADIUS server. On the RADIUS server, you must include CCM appliance-specific information: the list of valid users and their access rights for the CCM appliance. Each user-rights attribute in the RADIUS server's dictionary must be specified as a string containing the user's access rights for the CCM appliance, exactly matching the syntax used in the CCM User Add command.

Consult your RADIUS administrator's manual for information about specifying users and their attributes. The exact process depends on the RADIUS server you are using.

You may optionally specify both RADIUS and local authentication, in either order. In this case, authentication will be attempted initially on the first method specified. If that fails, the second method will be used for authentication.

When port group names are used, the CCM appliance will parse group names coming from a RADIUS server, and allow access according to group content.

No authentication

When authentication is disabled, users are not authenticated. Telnet sessions to serial ports are accepted immediately, and users are not prompted for a username or password. In this case, users are granted access only to the port to which they are connected, including Break access.

Connections to the Telnet port (23), serial CLI and PPP are still authenticated using the local CCM user database, even when authentication is expressly disabled. Generally, these communications paths are used only by administrators, and authentication is enforced in order to establish appropriate access rights.

Authentication may not be disabled when SSH session access is enabled.

Authentication summary

Table 3.5 indicates how authentication is performed according to the authentication method specified and the type of connection to the CCM appliance.

Table 3.5: Authentication Method Summary

Mode	Connection Type and Authentication Action
Local	All sessions are authenticated using the CCM user database.
RADIUS	Telnet and SSH sessions are authenticated using RADIUS. Serial CLI sessions are authenticated using the CCM user database.
Local,RADIUS	Telnet and SSH sessions are authenticated using the CCM user database. If that fails, authentication uses RADIUS. Serial CLI sessions are authenticated using the CCM user database.
RADIUS,Local	Telnet and SSH sessions are authenticated using RADIUS. If that fails, authentication uses the CCM user database. Serial CLI connections are authenticated using the CCM user database.
None	Telnet to serial port sessions use no authentication. Telnet CLI and serial CLI sessions are authenticated using the CCM user database. This authentication mode cannot be used for SSH connections.

To specify the authentication method:

1. For RADIUS authentication, issue a Server RADIUS command.

   SERVER RADIUS PRIMARY|SECONDARY IP=<*radius_ip*> SECRET=<*secret*> USER-RIGHTS=<*attr*> [AUTHPORT=<*udp*>] [TIMEOUT=<*time-out*>] [RETRIES=<*retry*>]

   You must specify the server's IP address, the UDP port to be used and a "secret" to be used. You must also specify a user-rights attribute value that matches a value in the RADIUS server's dictionary.

   You may also use this command to delete a RADIUS server definition.

   SERVER RADIUS PRIMARY|SECONDARY DELETE

   For more information, see *Server RADIUS command* on page 69.

2. Issue a Server Security command, using the Authentication parameter to specify the authentication method. Use the Encrypt parameter to enable plain text Telnet connections, SSH connections or both.

   SERVER SECURITY AUTHENTICATION=<*auth*> ENCRYPT=<*conns*>

   You may optionally specify both RADIUS and local authentication, in either order. In tis case, authentication will be attempted initially on the first method specified. If that fails, the second method will be used for authentication.

   When SSH session access is enabled, you must specify an authentication mode other than None.

3. You are prompted to save the information. Enter **Y** to confirm or **N** to cancel.

To display authentication configuration information:

1. Issue a Show Server Security command.

   SHOW SERVER SECURITY

   The display includes the current CCM appliance authentication settings that were configured with the Server Security command. If SSH access has been enabled, the display indicates SSH2. Regardless of whether SSH is enabled, the display includes the authentication method specified with the Server SSH command.

2. To display CCM RADIUS settings that were configured with the Server RADIUS command, issue a Show Server RADIUS command.

   SHOW SERVER RADIUS

For more information, see *Server Security command* on page 70, *Show Server Security command* on page 82, *Show Server RADIUS command* on page 81 and *Using SSH* on page 20.

Using security lock-out

When the security lock-out feature is enabled, a user account will be locked-out after five consecutive authentication failures. A successful authentication will reset the counter to zero. You may configure a lock-out period of 1-999 hours. A lock-out period of zero disables the feature; that is, user accounts will not be locked-out.

A locked account will remain locked until the specified time elapses, the CCM appliance is power-cycled or the account is unlocked by an administrator with the User Unlock command. A user with the ADMIN access level may unlock all users except a user with the APPLIANCEADMIN level. A user with the APPLIANCEADMIN level may unlock all users.

To enable or disable security lock-out:

1. To enable security lock-out, issue a Server Security command, using the Lockout parameter with a value between 1-999.
2. To disable security lock-out, issue a Server Security command, using the Lockout=0 parameter.

To unlock a locked-out user:

Issue a User Unlock command with the username.

Managing Port History

Each CCM appliance serial port has a circular history buffer that contains the latest 64K bytes of data received from the attached serial device. You may enable the NFS feature, which will write buffered data to a file on an NFS server. Port history information may be useful for auditing and troubleshooting.

Using the local history buffer

The history buffer begins filling with data received from attached devices upon completion of CCM appliance initialization, even if no user is connected. When you connect to a serial port, the data that was received from the attached serial device prior to the connection is available in the buffer. Once online, new data continues to be stored in the buffer. You may choose whether to display the history buffer's content automatically when you connect and whether to keep or discard the history buffer's content at the end of a session.

When more than 64K bytes of data are sent to the history buffer, data at the top of the buffer is discarded to make room for the new data. As a result, the buffer always contains the most recent 64K bytes of port history.

Using port history mode commands

Once you are in port history mode, you may issue the commands listed in Table 3.6. Only the first letter of the command is required.

Table 3.6: Port History Mode Commands

Command	Description
Bottom	**B** sets the view location to the bottom of the file minus 23 history display lines, if available.
Clear	**C** clears the port history buffer.
Help	**H** displays a summary of the port history commands.
Next	**N** increments the current history display line by the number of lines per page and outputs a new history display page.
Prev	**P** decrements the current history display line by the number of lines per page and outputs a new history display page.
Quit	**Q** returns to the normal CLI.
Resume	**R** leaves port history mode and CLI mode and resumes the session with the attached serial device. This single command is equivalent to sequentially using the Quit and Resume commands.

Table 3.6: Port History Mode Commands (Continued)

Command	Description
Search	**S** searches the port history buffer for a specified text string. Search strings with embedded spaces must be enclosed in quotes. By default, the search is case sensitive. To ignore case, enter **-i** before the string. To specify direction, type **-u** to search up from the current line toward the top of the buffer or **-d** to search down from the current line toward the bottom of the buffer. The search direction remains in effect for subsequent searches until you change the search direction. If the string is found, the current history display line is set to the line containing the string, and the unit outputs a history display page. If the string is not found, an error message is displayed, no other information is output and the current history display line is not changed. Entering the Search command with no parameters searches again for the previous string in the same direction as the previous search.
Top	**T** sets the current history display line to one and outputs a history display page.

The following examples assume the user is in port history mode.

The following command searches the history buffer in the upward direction for the string Abort Process.

```
PORT HISTORY> s -u "Abort Process"
```

The following command searches the history buffer for the string Process, ignoring case.

```
PORT HISTORY> s -i Process
```

For more information, see *Server CLI command* on page 65 and *Port History command* on page 59.

To access port history mode:

Issue a Port History command.

PORT HISTORY

The PORT HISTORY > prompt appears.

To control the port history buffer display when you connect:

Issue a Server CLI command, using the History parameter to specify the Hold or Auto option:

```
SERVER CLI HISTORY=HOLD|AUTO
```

- If Hold is specified, the number of bytes in the history buffer is displayed, but none of the history data is output. In this case, you must access the CLI and use the Port History command to view the port's history buffer content. This is the default mode.
- If Auto is specified, the number of bytes in the history buffer is displayed and the entire content of the buffer is output to the Telnet session. In this mode, the history buffer's content may be reviewed in the Telnet client's scrolling window. You may also use the Port History command to view the port's history buffer content.

To control the port history buffer content when you end a session:

Issue a Server CLI command, using the History parameter to specify the Clear or Keep option:

SERVER CLI HISTORY=CLEAR|KEEP

- If Clear is specified, the port history buffer is cleared and all data is discarded at the end of a session.
- If Keep is specified, the port history buffer's content is retained at the end of a session.

To clear and discard all data in a port history buffer:

Issue a Clear command while you are in port history mode.

CLEAR

- or -

Issue a Server CLI command, indicating History=Clear.

SERVER CLI HISTORY=CLEAR

In this case, the port's history buffer is cleared at the end of each device session.

NFS history files

When the NFS feature is enabled on the CCM appliance and on a port, port history data is written to a file on an NFS server, in addition to the local history buffer on the CCM appliance. Each serial port has its own file(s) on the NFS server where data is written. The NFS server must support NFSv3 (RFC1813).

Timestamps

Timestamps are written to the history file in the format: YYYY-MM-DD HH:MM:SS, where the hour (HH) is in 24-hour format. Each timestamp is preceded and followed by a carriage return and linefeed (**CR**+**LF**). The timestamp date/time uses the current time on the CCM appliance, which is assumed to be UTC (Universal Coordinated Time). You may display the current time on the CCM appliance at any time by entering a Show Server command.

A timestamp is inserted at the beginning of the file and whenever the file is opened for data to be written, but not more frequently than once every second.

If the CCM appliance is unable to send incoming data to the NFS server file quickly enough (for example, due to network load or server speed), an overrun may occur in the history accumulation buffer, and older data will be discarded to accommodate new incoming data. If this occurs, the location in the history file where the data was lost will indicate <<data lost due to overrun>> appended to the timestamp.

Enabling NFS on the CCM appliance

To use NFS, you must first enable NFS on the CCM appliance by identifying the address and mount point of the NFS server, plus the file type and the protocol.

NOTE: The NFS server's system administrator must make the appropriate configuration changes to allow the CCM appliance to access a specific subdirectory in the NFS server's file system (the mount point). This may or may not allow the CCM appliance to access and/or create subdirectories within the mounted subdirectory. This will affect what may be specified in the Port NFS command's file parameter.

The valid file types are:

- Linear - A file will be opened for writing at the end (appended); this is the default
- Daily - A new file will be created every midnight

By default, the TCP network protocol is used for communications between the CCM appliance and the NFS server. You may use the Protocol parameter to specify the UDP or TCP protocol.

To enable/disable NFS on the CCM appliance:

1. To enable NFS on the appliance, issue an NFS command with the Enable parameter.

   NFS ENABLE [IP=<*nfs_server*>] [MOUNT=<*mount*>] [FTYPE=LINEAR|DAILY] [PROTOCOL=TCP|UDP]

   If this is the first time you are enabling NFS on the appliance, you must include the IP address of the NFS server and a valid mount point. You may also specify the file type and protocol.

   You may also use the NFS Enable command to change the current IP address, mount point, file type or protocol.

   The values will be displayed and you will be prompted to confirm.

   If a mount operation is not immediately successful, it will be retried every 60 seconds for approximately 15 minutes. If an existing mount is lost, the CCM appliance will automatically attempt to restore it.

   If an error occurs, the display may include a numeric value and a text message. See *NFS Error Codes and Port Status* on page 105 for descriptions.
2. To disable NFS, issue an NFS command with the Disable parameter.

   NFS DISABLE

   If you later enable NFS again on the appliance, the server address, mount point, file type and protocol values at the time of disabling will be used if new values are not specified with the enable command.

For more information, see *NFS Command* on page 54.

To check the NFS mount status:

Issue a Show NFS command. (You may also issue the NFS Enable command without additional parameters to verify an existing mount.)

Enabling NFS on the CCM appliance ports

After NFS is successfully enabled on the CCM appliance, you may enable and configure NFS on the individual ports.

If an error occurs, it may include a numeric value and a text message. See *NFS Error Codes and Port Status* on page 105 for descriptions.

NFS filenames

When you enable NFS on one or all ports, you may specify a filename, which must be unique for each port. If the daily file type was configured with the NFS Enable command, the filename must

be also be unique for each day. You may use the substitution strings listed in Table 3.7 as part of the filename specification, regardless of the file type.

Table 3.7: Substitution Strings in NFS Filename Specification

2-Character String	Substituted Value	Example (Port 7 on January 8, 2004)
%d	Day of month (01-31)	08
%D	Same as %m-%d-%y	01-08-04
%F	Same as %Y-%m-%d (this is the ISO 8601 date format)	2004-01-08
%j	Julian day of year (001-366)	008
%m	Month (01-12)	01
%y	Year without century (00-99)	04
%Y	Year with century (2004-9999)	2004
%#	Port number (01-nn)	07
%%	%	%

If you do not specify a filename, the default is interpreted according to the configured file type:

- If the file type is linear, the default is equivalent to P%#.hst. The resulting filename for each port will include the port number.
- If the file type is daily, the default is equivalent to P%#_%F.hst. The resulting daily filename for each port will include the port number and the date.

Using the default filenames is the most convenient way to ensure that all filenames will be unique for each port (and for each day, if the file type is daily).

However, if you choose to specify a filename rather than use the defaults, it must meet the following criteria:

- The filename must be different from the filename specified for any other port on the CCM appliance. Using the port number substitution string (%#) in the filename specification is one way to accomplish this.

  If you are enabling NFS on all ports by including the All parameter, and you also include the File parameter with a nondefault specification (that is, a specification other than File=), the filename specification must explicitly include the %# port number substitution string.
- If the file type is daily, the filename specification must also include one or more of the date substitution strings so that the resulting filename is different each day.

If you specify a nondefault filename, and later wish to use the default filename, you may change it by issuing a Port NFS Enable command with a File= or File="" parameter.

If you specify a nondefault filename, and later attempt to change the file type from linear to daily, the request will be rejected if the filename specification does not include a date substitution string.

When writes will occur

When you enable NFS on a port, you may configure a buffer size and a time interval, which will be used to determine when accumulated data is written to the NFS server file.

- If you configure a buffer size of zero bytes and a time interval of zero seconds, data will be written to the file as soon as the data is available (not to exceed one write per second).
- If you configure a buffer size of zero bytes and a non-zero time interval, accumulated data will be written to the file each time the specified interval elapses (unless 3584 or more bytes accumulate in the buffer before an interval elapses, in which case the data will be written then).
- If you configure a non-zero buffer size and a time interval of zero seconds, data will be written when the specified number of bytes has accumulated, regardless of elapsed time. (If you configure a size value larger than 3584, the data will be written whenever 3584 or more unwritten bytes accumulate.)

To display NFS configuration information and mount status:

Issue a Show NFS command. The display will include the status of the mount operation. For more information, see *Show NFS command* on page 76.

SHOW NFS

To enable/disable and configure NFS on a port:

1. To enable NFS on one or all ports, issue a Port NFS command with the Enable parameter.

   PORT <*port*>|ALL NFS ENABLE [FILE=<*file*>] [SIZE=<*bytes*>] [TIME=<*sec*>]

   You may specify a filename or use default values; see *NFS filenames* on page 36.You may also configure size and time thresholds; see *When writes will occur* on page 38.
2. To disable NFS on one or all ports, issue a Port NFS command with the Disable parameter.

   PORT NFS DISABLE

For more information, see *Port NFS command* on page 60.

To display NFS port history file information:

Issue a Show Port command. The display includes the current port NFS status, which covers the most recent 15 minutes or since NFS history was most recently enabled for that port.

SHOW PORT

-or-

Issue a Show NFS command. In addition to displaying the current NFS mount status, this command will also show any port error status other than *No Recent Errors Detected*.

SHOW NFS

NFS Error Codes and Port Status on page 105 describes the error codes that may be displayed.

Managing the CCM Appliance Using SNMP

The CCM console management appliance provides a set of commands that create and manage SNMP structures for use by third party network management products. These commands cover the following operations:

- Enabling and disabling SNMP UDP port 161 SNMP processing
- Defining read, write and trap community names
- Defining and deleting up to four SNMP management entity IP addresses
- Enabling and disabling SNMP traps
- Defining and deleting up to four trap destination IP addresses
- Defining, copying and deleting up to ten alert strings for each port

By default, SNMP is enabled but no traps are enabled and no trap destinations are defined.

To enable or disable SNMP processing:

1. To enable SNMP processing, issue a Server SNMP command with the Enable parameter. This is the default setting.

   SERVER SNMP ENABLE

2. To disable SNMP processing, issue a Server SNMP command with the Disable parameter.

   SERVER SNMP DISABLE

For more information, see *Server SNMP command* on page 72.

To specify SNMP community names:

Issue a Server SNMP Community command, using the Readcomm, Writecomm and Trapcomm parameters to specify community names.

NOTE: The default community names are “public”; if you enable SNMP, you are encouraged to change the community values to prevent access to the MIB.

SERVER SNMP COMMUNITY READCOMM=<*name*> WRITECOMM=<*name*> TRAPCOMM=<*name*>

Although all three community names default to public, if you specify a trap community name with this command, it must be different from the read and write community names.

For more information, see *Server SNMP Community command* on page 73.

To add or delete SNMP management entity addresses:

1. To add an SNMP management entity address, issue a Server SNMP Manager command with the Add parameter and the management entity’s IP address. You may define up to four SNMP management entity addresses, using separate commands.

   SERVER SNMP MANAGER ADD <*ip_address*>

When you define at least one SNMP manager, SNMP requests are processed if they are from one of the defined SNMP managers. If a request is not from one of the defined SNMP managers, the SNMP request is discarded.

2. To delete an SNMP management entity address, issue a Server SNMP Manager command with the Delete parameter and the management entity's IP address.

   SERVER SNMP MANAGER DELETE <*ip_address*>

If no management entities are defined, any SNMP manager may access the MIB. For more information, see *Server SNMP Manager command* on page 73.

To enable or disable SNMP traps:

1. To enable SNMP traps, issue a Server SNMP Trap command with the Enable parameter.

   SERVER SNMP TRAP ENABLE

   The CCM appliance will display a numbered list of traps that are currently disabled with a prompt requesting you to select trap(s) to enable. Indicate the traps to be enabled by entering a trap's list number, several numbers separated by commas, a range of numbers separated by a dash or a combination of numbers with commas and dashes. To enable all traps, type **ALL**. To cancel the command, press **Enter**.

   - or -

   To enable all SNMP traps, issue a Server SNMP Trap command with the Enable and All parameters. In this case, the numbered list is not displayed.

   SERVER SNMP TRAP ENABLE ALL

2. To disable SNMP traps, issue a Server SNMP Trap command with the Disable parameter.

   SERVER SNMP TRAP DISABLE

   The CCM appliance will display a numbered list of traps that are currently enabled with a prompt requesting you to select trap(s) to disable. Indicate the traps to be disabled by entering a trap's list number, several numbers separated by commas, a range of numbers separated by a dash or a combination of numbers with commas and dashes. To disable all traps, type **ALL**. To cancel the command, press **Enter**.

   - or -

   To disable all SNMP traps, issue a Server SNMP Trap command with the Disable and All parameters. In this case, the numbered list is not displayed.

   SERVER SNMP TRAP DISABLE ALL

For more information, see *Server SNMP Trap command* on page 74 and *Supported Traps* on page 100.

To add or delete SNMP trap destination addresses:

1. To add an SNMP trap destination address, issue a Server SNMP Trap Destination command with the Add parameter and the destination's IP address. You may define up to four destination addresses, using separate commands.

   SERVER SNMP TRAP DESTINATION ADD <*ip_address*>

2. To delete an SNMP trap destination address, issue a Server SNMP Trap Destination command with the Delete parameter and the destination's IP address.

   SERVER SNMP TRAP DESTINATION DELETE <*ip_address*>

For more information, see *Server SNMP Trap Destination command* on page 75.

To add, copy or delete port alert strings:

1. To add a port alert string, issue a Port Alert Add command, specifying the port and a 3-32 character string. You may define up to ten strings for each port, using separate commands.

   The alert string will only generate a trap if the PortAlert trap is enabled with a Server SNMP Trap command.

   PORT <*port*> ALERT ADD "<*string*>"

2. To delete a port alert string, issue a Port Alert Delete command, specifying a port.

   PORT <*port*> ALERT DELETE

   The CCM appliance displays a numbered list of alert strings that have been defined for the specified port with a prompt requesting you to select alert string(s) to delete. Indicate the alert strings to be deleted by entering an alert string's list number, several numbers separated by commas, a range of numbers separated by a dash or a combination of numbers with commas and dashes. To delete all alert strings, type **ALL**. To cancel the command, press **Enter**.

3. To copy the defined alert strings from one port to another port, issue a Port Alert Copy command, specifying the ports to be copied to and from.

   PORT <*to_port*> ALERT COPY <*from_port*>

   At the confirmation prompt, press **Y** to confirm or **N** to cancel. When the copy operation occurs, all previously defined strings on the port being copied to will be replaced.

For more information, see *Port Alert Add command* on page 57, *Port Alert Copy command* on page 57 and *Port Alert Delete command* on page 58.

To display SNMP configuration information:

Issue a Show Server SNMP command.

SHOW SERVER SNMP

The display includes information specified with the Server SNMP, Server SNMP Community, Server SNMP Manager, Server SNMP Trap and Server SNMP Trap Destination commands.

For more information, see *Show Server SNMP command* on page 82.

To display port alert string information:

Issue a Show Port Alert command, specifying a port.

SHOW PORT <*port*> ALERT

The display lists all the port's defined alert strings.

For more information, see *Show Port command* on page 77.

CHAPTER 4

Using CCM Appliance Commands

Accessing the CLI

You may access the CLI in three ways: using the Telnet CLI, using the console port or entering the CLI access character during a session to a serial device. When the CLI is accessed, its prompt appears (>), indicating you may type a command.

Entering Commands

At the command prompt, type a command and then press **Return** or **Enter**. When the key is pressed, the command line comprises all characters to the left of the cursor. The character at the cursor and any characters to the right of the cursor are ignored. Table 4.1 lists the line editing operations for VT100 compatible devices.

Table 4.1: Line Editing Operations for VT100 Compatible Devices

Operation	Action
Backspace	The character immediately before the cursor is erased and all text at and to the right of the cursor moves one character to the left.
Left Arrow	If the cursor is not at the beginning of the line, the cursor moves one character to the left. If the cursor is at the beginning of the line, no action is taken.
Right Arrow	If the cursor is not at the end of the line, the cursor moves one character to the right. If the cursor is at the end of the line, no action is taken.
Up Arrow	The CLI maintains a buffer containing the last 16 typed command lines. If there is a previous command line, it will be output as the current command line and may be edited. If there is no previous command line in the command line buffer, the command line is set to blanks and you may enter a new command.
Down Arrow	The next command in the CLI command line buffer is made available for edit. If there is no next command line, the command line is set to blanks and you may enter a new command.
Delete	The character at the cursor position is deleted and all characters to the right of the cursor position are moved left one character.

Table 4.2 lists the line editing operations for ASCII TTY devices. There is no command line buffer available on an ASCII TTY device.

Table 4.2: Line Editing Operations for ASCII TTY Devices

Operation	Action
Backspace	Erases the last character typed.
Esc	Erases the current command line.

When commands take effect

Each command is completely processed before the next command may be entered. Some commands prompt for confirmation before they are processed. In these cases, you must confirm or cancel by entering **Y** or **N** respectively.

If you enter a Server FLASH command or if you change the CCM appliance IP address with a Server Set command, a reboot is required before the change becomes effective. In these cases, the CCM database is updated when you enter the command and you are prompted that the change will not take effect until the CCM appliance reboots. You may choose to reboot at that time, or you may decline. When the unit reboots, your session and all other sessions on the CCM appliance are terminated.

Understanding Conventions

This section describes the parts of a CCM appliance command and the conventions used in this document to describe a command's syntax.

Command syntax

A command may have four types of syntax: positional commands, positional parameters, keyword parameters and keyword values. The following examples demonstrate the syntax types.

The following Set Port command changes the baud rate and flow control settings for port 2.

```
> PORT 2 SET BAUD=57600 FLOW=XONXOF
```

Table 4.3: Command Syntax Types in Example Command

Value	Syntax
PORT	Positional command.
2	Positional parameter that indicates the port number for the command.
SET	Positional command that indicates port settings are to be changed.
BAUD	Keyword parameter, which is always followed by an equal (=) sign.
57600	Keyword value indicating the baud rate value for the BAUD keyword parameter.
FLOW	Keyword parameter, which is always followed by an equal (=) sign.

Table 4.3: Command Syntax Types in Example Command (Continued)

Value	Syntax
XONXOF	Keyword value.

Not every command will contain all syntax types. For example, the following command reboots the CCM appliance.

```
>SERVER REBOOT
```

In this case, both SERVER and REBOOT are positional commands.

In most cases, one or more spaces separate positional commands, positional parameters and keyword parameters.

For most positional commands, positional parameters or keyword parameters, you only need to enter the first three characters. The exceptions are:

- When you specify a terminal type with the Type parameter in the Server CLI command, you must enter all characters.
- When you specify an authentication method with the Auth parameter in the Server SSH command, you must enter all characters.
- When you specify control signal monitoring with the Power parameter in the Port Set command, you must enter all characters.
- When you specify the console port in commands such as Port Set and Show Port, you must enter the capitalized abbreviation **CON**.

Port names may contain up to 32 characters, and must be unique; two ports on the same appliance cannot have the same name. Port names are case sensitive. The name cannot begin with a number or a space, nor can it contain a double quote (“) or comma (,). The name cannot be Names, All, Set or Alert (in any case or any shortened form). If the name contains spaces, enclose the name in double quotes whenever it is used in commands.

With the exception of usernames, passwords, port names and group names, commands are not case sensitive; they may be entered in uppercase, lowercase or a combination. For example, all of the following commands are correct.

```
> PORT 2 SET BAUD=57600 FLOW=XON
> POR 2 SET BAU=57600 FLOW=XON
> por 2 Set Baud=57600 flow=xon
> port 2 set baud=57600 flow=xon
```

NOTE: Usernames and passwords are case sensitive. These values are stored exactly as you enter them. For example, the username “Ann” must be entered with an uppercase “A” and all other letters lowercase. The username “ANN” will not be accepted as the username “Ann.” Usernames and passwords must contain 3-16 alphanumeric characters.

Any syntax errors are displayed, and where applicable, the error is underlined.

In the following example, the keyword parameter “baud” is misspelled. Even if more than three characters are entered, they must all be correct.

```
> port 2 Set Baux=57600 flow=xon
             ----
ERR 26 - SET keyword parameter invalid
```

In the following example, the keyword value “576” is not valid. Numeric keyword values must be fully specified and may not be shortened to three characters.

```
> POR 2 SET BAUD=576 FLOW=XON
                  ---
ERR 27 - SET keyword value invalid
```

In the following example, there are spaces between BAUD, the equal sign and the value 57600. Spaces are not permitted between keyword parameters and their values.

```
> POR 2 SET BAUD = 57600 FLOW=XON
            ------------
ERR 26 - SET keyword parameter invalid
```

Command displays

For commands that display information, if the information spans more than one screen, -*More*- will appear on the last line. You may:

Press the **Spacebar** to see the next screen.
-or-
Enter **Ctrl-J**, **Ctrl-M** or press **Enter** to see the next line.
-or-
Enter **q** to quit.

Syntax conventions

This manual uses the following command syntax conventions:

- Brackets [ ] surround optional keywords and values.
- Angle brackets < > surround user-supplied positional parameters and keyword parameter values.
- In most cases, choices are separated by a vertical bar |. The description indicates if you may specify more than one of the choices and how to separate multiple values. The exception is the Server SSH command. In this case, the vertical bar is specified on the command line when you wish to enable the “password or key” method (PW|KEY) or the “key or password” method (KEY|PW).

Command Summary

Table 4.4 lists the CCM appliance commands, including a brief description plus the required access rights and level.

Table 4.4: CCM Appliance Command Summary

Command	Description, Access Right and Access Level
Connect	Accesses devices from the console port. Access right: port-specific Access level: ADMIN or APPLIANCEADMIN (Users who do not have the ADMIN or APPLIANCEADMIN level must have the appropriate port access configured to issue this command.)
Disconnect	Ends a device session initiated with Connect command. Access right: port-specific Access level: ADMIN or APPLIANCEADMIN (Users who do not have the ADMIN or APPLIANCEADMIN level must have the appropriate port access configured to issue this command.)
Help	Displays information about commands. Access right: none needed Access level: all
NFS	Enables/disables using an NFS server to hold device session data. Access right: SCON Access level: APPLIANCEADMIN
NTP	Enables/disables using an NTP server to update the time on the appliance. Access right: SCON Access level: APPLIANCEADMIN
Port Alert Add	Adds a port alert string. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Port Alert Copy	Copies a port's alert strings to another port. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Port Alert Delete	Deletes one or more port alert strings. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Port Break	Sends a break signal to the attached device. Access right: BREAK Access level: ADMIN or APPLIANCEADMIN
Port History	Accesses the port history buffer. Access right: none needed Access level: all

Table 4.4: CCM Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
Port Logout	Terminates the CCM session on a specified port. Access right: USER Access level: ADMIN or APPLIANCEADMIN
Port NFS	Enables/disables the NFS feature on a port. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Port Set	Changes port settings. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Port Set In/Out	Specifies how carriage returns and linefeeds are treated in incoming or outgoing serial data. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Quit	Terminates the current CCM session. Access right: none needed Access level: all
Resume	Resumes device connection after being in CLI mode. Access right: none needed Access level: all
Server CLI	Specifies the console port type, CLI access character; enables/disables device connection from the console port; specifies a modem initialization string; specifies port history mode operations and a port time-out value. Access right: SCON Access level: APPLIANCEADMIN
Server FLASH	Updates the unit's FLASH. Access right: SCON Access level: APPLIANCEADMIN
Server Init	Reinitializes the CCM appliance. Access right: SCON Access level: APPLIANCEADMIN
Server PPP	Enables/disables a PPP server on the console port. Access right: SCON Access level: APPLIANCEADMIN
Server RADIUS	Specifies RADIUS server parameters. Access right: SCON Access level: APPLIANCEADMIN
Server Reboot	Reboots the unit. Access right: SCON Access level: APPLIANCEADMIN

Table 4.4: CCM Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
Server Security	Specifies the user authentication mode, enables/disables security lock-out and connection methods. Access right: SCON Access level: APPLIANCEADMIN
Server Set	Changes the CCM appliance network configuration. Access right: SCON Access level: APPLIANCEADMIN
Server Share	Enables/disables session sharing on the appliance. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP	Enables/disables UDP port 161 SNMP processing. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Community	Defines read, write and trap SNMP community strings. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Manager	Defines/deletes SNMP management entities. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Trap	Enables/disables SNMP traps. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Trap Destination	Defines/deletes destinations for enabled SNMP traps. Access right: SCON Access level: APPLIANCEADMIN
Server SSH	Enables/disables SSH session access to the CCM appliance and specifies the SSH authentication method. Access right: SCON Access level: APPLIANCEADMIN
Show NFS	Displays NFS configuration information and mount status. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show NTP	Displays NTP configuration information. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Port	Displays port configuration information and statistics. Access right: SMON Access level: ADMIN or APPLIANCEADMIN

Table 4.4: CCM Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
Show Port In|Out	Displays how carriage returns and linefeeds are treated. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server	Displays CCM appliance configuration, statistics and session information. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server CLI	Displays information specified with the Server CLI command. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server PPP	Displays PPP settings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server RADIUS	Displays RADIUS settings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server Security	Displays authentication and lock-out settings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server SNMP	Displays SNMP configuration information. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show User	Displays user configuration and session information. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
SPC	Changes SPC port settings. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
SPC Socket	Changes SPC socket settings or states. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
User Add	Adds a new user. Access right: USER Access level: ADMIN or APPLIANCEADMIN
User Delete	Deletes a user. Access right: USER Access level: ADMIN or APPLIANCEADMIN

Table 4.4: CCM Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
User Logout	Terminates a user's session. Access right: USER Access level: ADMIN OR APPLIANCEADMIN (An ADMIN level user may issue this command for users with any level other than APPLIANCEADMIN.)
User Set	Changes a user's configuration information. Access right: USER Access level: ADMIN or APPLIANCEADMIN
User Unlock	Unlocks a locked-out user. Access right: USER Access level: ADMIN or APPLIANCEADMIN (An ADMIN level user may issue this command for users with any level other than APPLIANCEADMIN.)

CHAPTER 5

CCM Appliance Commands

Connect Command

The Connect command establishes a connection from the console port of the CCM appliance to a device attached to a serial port on that CCM appliance. To use this command, you must have previously issued a Server CLI command with the Connect=On parameter. For more information, see *Connecting to Serial Devices* on page 17.

Your ability to connect to another port is also affected by session sharing. For more information, see *Session sharing* on page 23.

When the connect completes successfully, the message Connected to port x: will be displayed, followed by the values for port_number,baud,bits_per_character,parity,stop_bits,flow_control.

Access right: port-specific
Access level: ADMIN, APPLIANCEADMIN or users with access to port

Syntax

CONNECT [<*port*>] [EXCLUSIVE]

Table 5.1: Connect Command Parameters

Parameter	Description
<*port*>	Port number or name. If omitted, a menu will be displayed, listing all ports that are available for serial connection (this excludes SPC ports, ports to which you are already connected and ports you do not have permission to access). At the prompt, enter a port number or name. You may also press **Enter** to cancel the command.
EXCLUSIVE	Requests exclusive access to the port. This will initially be accommodated only if the port is not currently in use.

Example

The following command establishes a connection from the CCM appliance console port to port 6.

```
> connect 6
```

Disconnect Command

The Disconnect command terminates a session with a serial device that was previously initiated with a Connect command.

Access right: port-specific
Access level: ADMIN, APPLIANCEADMIN or others with access to port

Syntax

DISCONNECT

Help Command

The Help command displays information about CCM appliance commands. The display may span more than one screen; see *Command displays* on page 46 for more information.

Access right: none needed
Access level: none needed

Syntax

HELP [<*command_name*>]

Table 5.2: Help Command Parameter

Parameter	Description
<*command_name*>	Command name. Default: Displays list of all commands

Examples

The following command displays information about the Show Server CLI command.

```
help sho ser cli
```

The following command displays a list of all commands.

```
help
```

The following command displays a list of all commands that begin with Server.

```
help server
```

NFS Command

The NFS command enables or disables use of the NFS feature on the CCM appliance, and specifies the location of the NFS server, its mount point, the type of files that will be created and the protocol to be used. For more information, see *NFS history files* on page 35.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

NFS ENABLE [IP=<*nfs_server*>] [MOUNT=<*mount*>] [FTYPE=LINEAR|DAILY] [PROTOCOL=TCP|UDP]
-or-
NFS DISABLE

Table 5.3: NFS Command Parameters

Parameter	Description
ENABLE	Enables NFS on the appliance.
IP=<*nfs_server*>	IP address of the NFS server, in IP dot notation. The NFS server must support NFSv3 (RFC1813). This parameter is required if NFS is being enabled for the first time.
MOUNT=<*mount*>	Mount point (subdirectory location) on the NFS server. This parameter is required if NFS is being enabled for the first time. The NFS server must be configured to allow the CCM appliance to access this file system location.
FTYPE=LINEAR|DAILY	Linear indicates a file will be opened on the NFS server for writing at the end (appended). Daily indicates a new file will be created on the NFS server every midnight. For either file type, if the file being opened does not already exist, it will be created. If the file already exists, it will be opened for writing at the end (appended). Default = Linear
PROTOCOL=TCP|UDP	Specifies the network protocol to be used between the CCM appliance and the NFS server. Default = TCP
DISABLE	Disables NFS on the appliance.

Examples

The following command enables the use of the NFS on the CCM appliance. The NFS server is located at IP address 192.168.52.50, and files will be created under the subdirectory c/ccm_history every midnight.

```
nfs enable ip=192.168.52.50 mount=c/ccm_history ftype=daily
```

The following command disables using the NFS feature on the CCM appliance. If NFS is later enabled again without additional parameters, the previously configured values will be used.

```
nfs disable
```

NTP Command

The NTP command enables or disables use of the Network Time Protocol on the CCM appliance, and specifies the location of the NTP server that will supply the time to the CCM appliance. For more information, see *Updating the Appliance Clock* on page 14.

When you enable NTP, you are prompted to confirm or cancel the operation.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

NTP ENABLE [IP=<*prim_add*>[,<*sec_addr*>]] [UPDATE=<*hours*>]
-or-
NTP DISABLE

Table 5.4: NTP Command Parameters

Parameter	Description
ENABLE	Enables NTP on the appliance.
IP=<*prim_add*> ,<*sec_addr*>	IP address of the first NTP server to contact to obtain the time and optionally, the IP address of the second NTP server to contact if a valid time is not received from the first server. At least a primary address is required if NTP is being enabled for the first time.
UPDATE=<*hours*>	Interval for sending a time request to the NTP server and then updating the clock. Valid values are 0-99 hours. A zero value indicates that the time should be requested and the clock updated when the CCM appliance reboots. Regardless of this parameter's value, the clock is updated immediately when the NTP Enable command is issued. Default = 0 (update immediately and then only upon reboot)
DISABLE	Disables NTP on the appliance.

Example

The following command enables use of NTP on the CCM appliance. The time requests will first be made to the NTP server at IP address 192.168.50.200. If a valid time is not acquired from that server, the secondary NTP server at 192.168.50.220 will be contacted. The time will be updated immediately and then every two hours.

```
ntp enable ip=192.168.50.200,192.168.50.220 upd=2
```

Port Commands

The Port command has several forms, as listed in Table 5.5.

Table 5.5: Port Command Summary

Command	Description
Port Alert Add	Adds a port alert string to a specified port.
Port Alert Copy	Copies port alert strings from one port to another port.
Port Alert Delete	Deletes one or more port alert strings from a specified port.
Port Break	Sends a serial break signal to the attached device.

Table 5.5: Port Command Summary (Continued)

Command	Description
Port History	Accesses a port's history mode.
Port Logout	Terminates the CCM session on a specified port.
Port NFS	Enables or disables using the NFS feature on a port.
Port Set	Changes CCM serial port settings for one or all ports.
Port Set In/Out	Specifies how carriage returns and linefeeds are treated in incoming or outgoing serial data.

Port Alert Add command

The Port Alert Add command adds a port alert string to a specified port. Each port may have up to ten port alert strings. Duplicate strings are not allowed on the same port. To generate a trap, the Server SNMP Trap command must be issued to enable the PortAlert trap. For more information, see *Managing the CCM Appliance Using SNMP* on page 39.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*> ALERT ADD "<*string*>"

Table 5.6: Port Alert Add Command Parameters

Parameter	Description
<*port*>	Port number or name.
<*string*>	3-32 character string. If the string contains embedded spaces, it must be enclosed in quotes.

Port Alert Copy command

The Port Alert Copy command copies the alert strings from one port (from_port) to another (to_port). Any alert strings that were previously defined on the to_port will be deleted. When you enter this command, you are prompted to confirm or cancel the copy operation.

For more information, see *Managing the CCM Appliance Using SNMP* on page 39.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*to_port*> ALERT COPY <*from_port*>

Table 5.7: Port Alert Copy Command Parameters

Parameter	Description
<*to_port*>	Port number or name where alert strings will be copied.
<*from_port*>	Port number or name from which alert strings will be copied.

Example

The following command copies the alert strings defined on port 1 to port 17, replacing any previously defined alert strings on port 17.

```
port 17 alert copy 1
```

Port Alert Delete command

The Port Alert Delete command deletes one or more alert strings from a port. When you issue this command, a numbered list of defined alert strings is displayed, from which you choose those to be deleted. You may enter one or more numbers separated by commas, a range of numbers separated by a hyphen or type **ALL** to specify all strings. Pressing **Enter** cancels the command.

For more information, see *Managing the CCM Appliance Using SNMP* on page 39.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*> ALERT DELETE

Table 5.8: Port Alert Delete Command Parameter

Parameter	Description
<*port*>	Port number or name.

Example

The following command deletes defined alert strings from port 26.

```
> PORT 26 ALERT DELETE
Alert-strings assigned to port 26:
1) The first alert string
2) The second alert string
3) The third alert string
4) The fourth alert string
Select Alert-string(s) to delete>
```

The alert string numbers specified at the prompt will be deleted.

Port Break command

The Port Break command sends a serial break signal to the device to which you are attached.

Access right: BREAK
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT BREAK

Port History command

The Port History command accesses a serial port's history mode while you are attached to the port. When you are in history mode, the PORT HISTORY> prompt appears, and you may search the port's history buffer for specified strings.

For more information, see *Managing Port History* on page 33.

Access right: none needed
Access level: all

Syntax

PORT HISTORY

When you are in port history mode, you may issue the commands listed in Table 3.6 on page 33.

Examples

The following command accesses the serial port's history mode.

```
> port history
```

In history mode, the following command searches the history buffer in the downward direction for the string "connected to," ignoring case.

```
PORT HISTORY > s -d -i "connected to"
```

Port Logout command

The Port Logout command terminates the CCM appliance session on a specified port. If more than one session is active on the port, all sessions are logged out.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*> LOGOUT

Table 5.9: Port Logout Command Parameter

Parameter	Description
<*port*>	Port number or name.

Port NFS command

The Port NFS command enables or disables using the NFS feature on a port, and specifies NFS parameters. For more information, see *NFS history files* on page 35.

NOTE: If you are enabling NFS on a port, an NFS Enable command must have successfully completed before the Port NFS command will be accepted.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*>|ALL NFS ENABLE [FILE=<*file*>] [SIZE=<*bytes*>] [TIME=<*sec*>]
-or-
PORT <*port*>|ALL NFS DISABLE

Table 5.10: Port NFS Command Parameters

Parameter	Description
ENABLE	Enables NFS on the specified port.
port	Port name or number.
ALL	Indicates that the following parameters should be applied to all ports.
FILE=<*file*>	Filename specification, up to 32 characters. This must result in a unique filename for the port (and a unique daily port file if the file type is daily). Substitution strings may be used; see Table 3.7 on page 37. Default = "" (P%#.hst if file type is linear, P%#_%F.hst if file type is daily)
SIZE=<*bytes*>	Number of bytes that will be buffered on the CCM appliance before being written to the NFS server file. This threshold is used with the Time value to determine when accumulated data will be written. Valid values are 0-3584 bytes. Default = 0 bytes
TIME=<*sec*>	Maximum number of seconds that will be allowed to elapse before buffered data will be written to the NFS server file. This threshold is used with the Size value to determine when accumulated data will be written. Valid values are 0-65536 seconds. Default = 1 second
DISABLE	Disables NFS on the specified port.

Examples

The following command enables NFS on port 3, using the default filename specification, and setting a size threshold of 20 bytes and a time threshold of zero. With this configuration, data will be buffered according to the non-zero threshold value, 20 bytes, then it will be written to the NFS history file. The history file will be named P03.hst if the file type is linear, or P03_<4-digit year>-<2-digit_month>-<2-digit_day> if the file type is daily.

```
port 3 nfs ena size=20 time=0 file=
```

The following command enables NFS on port 7, using a substitution string within the filename specification, and setting zero thresholds for both size and time. (This configuration will not be acceptable if the file type is daily, because the file specification does not include a date substitution string that would make each daily file uniquely named.) Assuming the file type is linear, data will be written to the NFS server file named ccm_1_P07 as soon as it is available, because both thresholds are zero.

```
port 7 nfs ena size=0 time=0 file=ccm_1_%#
```

Port Set command

The Port Set command changes serial port settings in the CCM configuration database. At least one keyword parameter and value must be specified. Some changes become effective upon the next connection to the port.

For more information, see *Configuring Serial Port Settings* on page 15.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT [<*port*>|ALL] SET
[TD=<*device*>] [NAME=<*name*>] [BAUD=<*baud*>] [SIZE=<*size*>] [PARITY=<*parity*>]
[STOP=<*stopbits*>] [FLOW=<*signal*>] [TIMEOUT=<*time-out*>] [SOCKET=<*socket*>]
[CHAR=^<*cli_char*>] [TOGGLE=NONE|DTR] [POWER=<*signal*>] [GROUP=<*group*>]

Table 5.11: Port Set Command Parameters

Parameter	Description
<*port*>	A port number, port name or CON. Default = port to which you are attached
ALL	Indicates that the port settings that follow should be applied to all ports except the console port.
TD=<*device*>	Target device type. Valid values are Console and SPC. If SPC is specified, only the Name and Group parameters may be specified with this command. This parameter is not valid for the console port. Default = Console
NAME=<*name*>	Port name, up to 32 characters. The name cannot be Names, All, Set or Alert (in any case or any shortened form) or CON. The name must be unique; two ports cannot have the same name. Port names are case sensitive. The name cannot begin with a number or a space, nor can it contain a double quote (“) or comma (,). If the name contains spaces, enclose the name in double quotes. To return a port name to its default value, specify Name=“”. This parameter is not valid for the console port. Default = last 3 octets of MAC address, followed by P and the port number
BAUD=<*baud*>	Baud rate. Valid values are: 50, 75, 110, 134, 150, 200. 300, 600, 1200, 2400, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 57600 and 115200. Default: = 9600

Table 5.11: Port Set Command Parameters (Continued)

Parameter	Description
SIZE=<*size*>	Number of data bits per character. Valid values are 7 and 8. Default = 8
PARITY=<*parity*>	Parity. Valid values are: None — No parity. Even — Even parity. Odd — Odd parity. Mark — Mark parity. Space — Space parity. Default = None
STOP=<*stopbits*>	Number of stop bits per character. Valid values are 1 and 2. Default = 1
FLOW=<*signal*>	Flow control signal. For hardware flow control, be sure the control signals are correctly wired, or data loss may occur. The flow control signal cannot also be used for power status monitoring. Valid values are: XONXOF — Software XON/XOFF flow control. RTSCTS — Hardware RTS/CTS flow control. DTRDCD — Hardware DTR/DCD flow control. None — No flow control. Default = None
TIMEOUT=<*time-out*>	Number of time-out minutes in the range 0-90. If no data is received or transmitted during a Telnet session for the specified period, the session will time-out. A zero value indicates no time-out. The new value does not affect an active session; it takes effect in subsequent sessions. This value overrides the time-out value set with a Server CLI command. Default = use value set with Server CLI command
SOCKET=<*socket*>	TCP port that must be entered on the Telnet client to connect to this serial port. The new value becomes effective in subsequent sessions. When SSH is enabled, the CCM appliance automatically adds 100 to the specified value. When All is specified, port 1 will be assigned the specified socket value plus 1, port 2 will be assigned the specified value plus 2, and so on. When All is specified and SSH is enabled, port 1 will be assigned the specified socket value plus 101, port 2 will be assigned the specified value plus 102, and so on. When both plain text Telnet and SSH connections are enabled, the +100 value will not appear in displays. This parameter is not valid for the console port. Default = 3000 plus the port number, 3100 plus the port number if SSH is enabled; see above for action taken if All is specified

Table 5.11: Port Set Command Parameters (Continued)

Parameter	Description
CHAR=^<*cli_char*>	CLI access character in the range A to _ (underscore) or None. (The allowable ASCII range is 0x41-0x5F and 0x61-0x7A.) The CLI access character, when pressed simultaneously with the **Ctrl** key during a session with an attached serial device, will suspend the session with the device and place you in CLI command mode. If None is specified, the value specified in the Char parameter of the Server CLI command will be used. Default = None
TOGGLE=NONE|DTR	When set to DTR, the CCM appliance will toggle the port's DTR-out signal off for 1/2 second each time a connection is made to the port. This toggle is required to awaken the console port of some devices. This parameter is not valid for the console port. Default = None
POWER=<*signal*>	Control signal to monitor and the state that indicates the target device has power on. The entire value must be specified; abbreviations are not allowed. The power status monitoring signal cannot also be used for flow control. This parameter is not valid for the console port. Valid values are: None Disables power status monitoring. HICTS CTS high indicates power on. LOCTS CTS low indicates power on. HIDCD DCD high indicates power on. LODCD DCD low indicates power on. HIDSR DSR high indicates power on. LODSR DSR low indicates power on. Default = None
GROUP=<*group*>	Group name, up to 8 characters. Group names are case sensitive. If the name contains spaces, enclose the name in double quotes. A port may belong to only one group (multiple ports may belong to the same group). If the port was previously assigned to a group and a Port Set command is issued with a different group specification, the most recent group name is assigned. This parameter is not valid for the console port.

Example

The following command sets a baud rate of 57600 and enables XON/XOFF flow control on port 2.

```
> port 2 set baud=57600 flow=xonxof
```

Port Set In/Out command

The Port Set In/Out command specifies how carriage returns (CR) and linefeeds (LF) are treated in incoming or outgoing serial data on one or all ports.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT [<*port*>|ALL] SET IN|OUT [CR=<*cr*>] [LF=<*lf*>|CRLF=CR]

Table 5.12: Port Set In/Out Command Parameters

Parameter	Description
<*port*>	Port number or name. Default = port to which you are attached
ALL	Indicates that the port settings that follow should be applied to all ports except the console port.
IN|OUT	Either IN to specify translation for incoming data or OUT to specify translation for outgoing data.
CR=<*cr*>	Translation to be made for carriage returns. Valid values are: CR=CR Carriage return is treated as a carriage return. CR=LF Carriage return is treated as a linefeed. CR=STRIP Carriage return is stripped. CR=CRLF Carriage return is treated as a carriage return and linefeed. Default = CR=CR
LF=<*lf*>|CRLF=CR	Translation to be made for linefeeds. Valid values are: LF=LF Linefeed is treated as a linefeed. LF=CR Linefeed is treated as a carriage return. LF=STRIP Linefeed is stripped. CRLF=CR Linefeed is stripped only if it is preceded by a carriage return. This LF setting cannot be specified with any other LF setting. Default = LF=LF

Quit Command

The Quit command terminates the current CCM appliance session and terminates your Telnet connection to the unit.

Access right: none needed
Access level: all

Syntax

QUIT

Resume Command

The Resume command exits the CLI and resumes your connection to the attached serial device. The history buffer contains any data received while you were in CLI mode.

Access right: none needed
Access level: all

Syntax

RESUME

Server Commands

The Server command has several forms, as listed in Table 5.13.

Table 5.13: Server Command Summary

Command	Description
Server CLI	Specifies the console port type, CLI access character, modem initialization string, port history mode operations and port time-out value. It also enables/disables device connection from the console port.
Server FLASH	Updates the unit's FLASH.
Server Init	Reinitializes the CCM appliance.
Server PPP	Enables/disables PPP connections to the console port.
Server RADIUS	Specifies RADIUS server parameters.
Server Reboot	Reboots the unit.
Server Security	Specifies user authentication method, enables/disables security lock-out and enables/disables connection methods.
Server Set	Changes the CCM appliance network configuration.
Server Share	Specifies session sharing settings.
Server SNMP	Enables/disables UDP port 161 SNMP processing.
Server SNMP Community	Defines read, write and trap SNMP community strings.
Server SNMP Manager	Defines/deletes SNMP management entities.
Server SNMP Trap	Enables/disables SNMP traps.
Server SNMP Trap Destination	Defines/deletes destinations for enabled SNMP traps.
Server SSH	Enables/disables SSH session access to the CCM appliance and specifies the SSH authentication method.

Server CLI command

The Server CLI command:

- Specifies the console port type
- Specifies the CLI access character
- Enables or disables device connection from the console port
- Specifies a modem initialization string
- Specifies port history mode operations
- Specifies a port time-out value

At least one parameter must be specified.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER CLI [TYPE=<*type*>] [CHAR=^<*char*>] [CONNECT=ON|OFF] [HISTORY=HOLD|AUTO,CLEAR|KEEP] [MODEMINIT="<*string*>"] [TIMEOUT=<*time-out*>]

Table 5.14: Server CLI Command Parameters

Parameter	Description
TYPE=<*type*>	Terminal type to be used on the console port. The entire name of the type must be specified; abbreviations are not permitted. Valid types are: ASCII, VT52, VT100, VT102, VT220 and VT320. Default: ASCII
CHAR=^<*char*>	CLI access character in the range A through _ (underscore). (The allowable ASCII range is 0x41-0x5F and 0x61-0x7A.) The CLI access character, when pressed simultaneously with the **Ctrl** key during a session with an attached serial device, will suspend the session with the device and place you in CLI command mode. This value will be used if a port's Port Set command contains a Char=None parameter. Default = ^d
CONNECT=ON|OFF	Enables or disables the ability to use the Connect command from the console port. When enabled, a console port user may use the Connect command to establish a connection to the serial device attached to another CCM appliance serial port. When disabled, you cannot use the Connect command from the console port. Default = ON
HISTORY=HOLD|AUTO ,CLEAR|KEEP	Port history file processing options during connection (Hold or Auto) and when a session ends (Clear or Keep): Hold Upon connection you are informed of how much data is in the history buffer, but the data is not displayed. Auto Upon connection you are informed of how much data is in the history buffer, and it is then displayed. Clear The history buffer's content is cleared when a session ends. Keep The history buffer's content is retained when a session ends. You cannot specify both Clear and Keep or both Hold and Auto. Default = HOLD,CLEAR
MODEMINIT="<*string*>"	Modem initialization string, enclosed in quotation marks. Must contain at least ATV1 and S0=1. Default = "" (no modem is attached to the console port)

Table 5.14: Server CLI Command Parameters (Continued)

Parameter	Description
TIMEOUT=<*time-out*>	Number of time-out minutes in the range 0-90. If no data is received or transmitted during a Telnet session for the specified period, the session will time-out. A zero value indicates no time-out. This value is used for any CCM port that does not have a time-out value set with the Port Set command, during a Telnet session to port 23 or an SSH session to port 22. Default = 15 minutes

Server FLASH command

The Server FLASH command updates the CCM appliance program images in FLASH memory. You may wish to use this command to update the program with new features or to install a later release of the program.

There are two program images that you may update in the CCM appliance FLASH. The boot image file (ccm50bt.img) contains the CCM appliance startup and self-test logic. The application image (ccm50app.img) contains the program that provides CCM appliance functionality.

You will need a TFTP server. Download the latest FLASH image from the Avocent web site (www.avocent.com), and save the image file to the appropriate directory on the TFTP server.

NOTE: Powering down a system in the middle of a boot FLASH update may render the unit inoperable. To update the bootstrap, it is recommended that the unit be placed on a UPS under controlled conditions to avoid interruption of the boot FLASH update process.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER FLASH BOOT|APP HOSTIP=<*tftp_add*> IMAGE=<*host_file*>

Table 5.15: Server FLASH Command Parameters

Parameter	Description
BOOT|APP	Indicates either the boot image should be updated or the application image should be updated.
HOSTIP=<*tftp_add*>	IP address of TFTP server host.
IMAGE=<*host_file*>	Name of file on TFTP server host containing the image file.

Example

The following command updates the boot image program using the image filename c:\winnt\system32\drivers\ccm50bt.img, which is located on the TFTP server host located at 192.168.1.16.

```
> ser fla app hostip=192.168.1.16
c:\winnt\system32\drivers\ima=ccm50bt.img
```

Server Init command

The Server Init command reinitializes the CCM appliance configuration database, that is, restores it to default values. You may choose to retain only the network address information.

When you enter this command, you are prompted to confirm or cancel the reinitialization.

You may also reinitialize the CCM appliance in hardware. See *Reinitializing* on page 11 for more information.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER INIT CONFIG|ALL

Table 5.16: Server Init Command Parameter

Parameter	Description
CONFIG	Reinitializes the appliance but retains the IP address, subnet mask and gateway.
ALL	Reinitializes the appliance, including the network address information.

Server PPP command

The Server PPP command enables or disables the PPP server on the console port. For more information and requirements, see *Using PPP* on page 19 and *Configuring and using dial-in connections* on page 19.

Once the PPP server has been configured with this command by specifying the required addresses and masks, those values remain in the database. Later, if you disable the PPP server and wish to reenable it with the same addresses, you don't need to specify the address values again.

When you enter this command, you are prompted to confirm or cancel the specified changes.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER PPP DISABLE|ENABLE
[LOCALIP=<*local_ip*>] [REMOTEIP=<*rem_ip*>] [MASK=<*subnet*>]

Table 5.17: Server PPP Command Parameters

Parameter	Description
DISABLE|ENABLE	Disables or enables the PPP server.
LOCALIP=<*local_ip*>	IP address to be used to connect the CCM appliance over the PPP connection. Must be on same subnet as REMOTEIP address.

Table 5.17: Server PPP Command Parameters (Continued)

Parameter	Description
REMOTEIP=<*rem_ip*>	IP address to assign to the PPP client end of the PPP connection. Must be on same subnet as LOCALIP address.
MASK=<*subnet*>	Subnet mask for the PPP dial-in client.

Examples

The following command enables the PPP server with a local IP address of 192.168.0.1, a remote IP address of 192.168.0.2 and a subnet mask of 255.255.255.0.

```
> ser ppp ena loc=192.168.0.1 rem=192.168.0.2 mas=255.255.255.0
```

The following command enables the PPP server with previously configured IP and subnet mask values. This form of the command would not be valid unless the IP and subnet mask values had been previously configured.

```
> server ppp enable
```

Server RADIUS command

The Server RADIUS command defines or deletes RADIUS parameters for the CCM RADIUS client. For more information, see *RADIUS authentication* on page 30.

When you enter this command, you are prompted to confirm or cancel the specified changes.

NOTE: The IP, Secret and User-Rights parameters are required only when you are first defining RADIUS server values. If you later wish to change other parameters with a subsequent Server RADIUS command, the current IP, Secret, and User-Rights values will be used, unless you change them also.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER RADIUS PRIMARY|SECONDARY
IP=<*radius_ip*> SECRET=<*secret*> USER-RIGHTS=<*attr*>
[AUTHPORT=<*udp*>] [TIMEOUT=<*time-out*>] [RETRIES=<*retry*>]
- or -
SERVER RADIUS PRIMARY|SECONDARY DELETE

Table 5.18: Server RADIUS Command Parameters

Parameter	Description
PRIMARY| SECONDARY	Indicates either the primary RADIUS server or the secondary RADIUS server is being defined or deleted.
IP=<*radius_ip*>	IP address of the RADIUS authentication server.

Table 5.18: Server RADIUS Command Parameters (Continued)

Parameter	Description
SECRET=<*secret*>	8-24 character text string for shared secret with the RADIUS server. Enclose the string in quotes if it contains spaces.
USER-RIGHTS=<*attr*>	Attribute number defined on the RADIUS server, in the range 1-255.
AUTHPORT=<*udp*>	UDP port for RADIUS authentication server, in the range 1-65535. This value is usually 1645, but may be 1812. Default = 1645
TIMEOUT=<*time-out*>	Number of seconds to wait for a response from the RADIUS server, in the range 1-60. Default = 5
RETRIES = <*retry*>	Number of attempts to make to authenticate a user after a time-out, in the range 1-10. Default = 3
DELETE	Deletes a primary or secondary RADIUS server definition. If a primary server is deleted, and a secondary server was configured, that secondary server becomes the new primary server.

Examples

The following command specifies primary RADIUS server information; default values will be used for the UDP port, time-out and retries values.

```
> ser radius primary ip=192.168.0.200 secret=ThePrimaryRadSecret user-
rights=86
```

The following command deletes the primary RADIUS server definition.

```
> ser radius primary del
```

Server Reboot command

The Server Reboot command reboots the CCM appliance. During a reboot, any active Telnet sessions, including your own, are terminated, and all users are informed accordingly. Any configuration changes that require a reboot will become effective when the reboot completes.

When you enter this command, you are prompted to confirm or cancel the reboot.

You may also reboot the appliance by pressing the RESET button on the front panel. See *Rebooting* on page 10 for more information.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER REBOOT

Server Security command

The Server Security command specifies the authentication method, enables/disables access methods and enables/disables security lock-out. For more information, see *Using Authentication*

Methods on page 30, *Enabling plain text Telnet and SSH connections* on page 23 and *Using security lock-out* on page 32.

When you enter this command, you are prompted to confirm or cancel the specified information.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SECURITY [AUTHENTICATION=<*auth*>] [ENCRYPT=<*conns*>] [LOCKOUT=<*hours*>]

Table 5.19: Server Security Command Parameters

Parameter	Description
AUTHENTICATION=<*auth*>	Authentication method. You may specify multiple values (other than None), separated by commas. Valid values are: LOCAL Use the local CCM user database to authenticate users. RADIUS Use the previously defined RADIUS server(s) to authenticate users. NONE Do not authenticate users. This method cannot be used when SSH access is enabled, and it cannot be combined with other authentication methods. Default = LOCAL
ENCRYPT=<*conns*>	Enables/disables plain text Telnet or SSH connections. You may enable both by specifying both values, separated by a comma. Valid values are: SSH Enables SSH connections. None Enables plain text Telnet connections. Default = None
LOCKOUT=<*hours*>	Enables or disables security lock-out. To enable, specify the number of hours in the lock-out period, in the range 1-999. To disable, specify a zero value. Default = 0 (disabled)

Server Set command

The Server Set command changes CCM appliance address settings. You may specify one, two or all three parameters. A reboot is required if you change the IP address.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SET [IP=<*ip_address*>] [MASK=<*subnet*>] [GATEWAY=<*gtwy*>]

Table 5.20: Server Set Command Parameters

Parameter	Description
IP=<*ip_address*>	IP address.

Table 5.20: Server Set Command Parameters

Parameter	Description
MASK=<*subnet*>	Subnet mask for the subnet on which the CCM appliance resides.
GATEWAY=<*gtwy*>	IP address of default gateway for routing IP packets.

Server Share command

The Server Share command configures the share mode. For more information, see *Session sharing* on page 23.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SHARE [DISABLE|AUTO|QUERY]

Table 5.21: Server Share Command Parameter

Parameter	Description
DISABLE	Disables session sharing. Only one connection per port will be allowed.
AUTO	Enables automatic session sharing (subject to preemption based on access level).
QUERY	Enables session sharing when permission is obtained from the session originator (subject to preemption based on access level). This is the default value.

Server SNMP command

The Server SNMP command enables or disables SNMP UDP port 161 SNMP processing. When you disable SNMP processing, you may still enable and disable traps with the Server SNMP Trap command.

For more information, see *Managing the CCM Appliance Using SNMP* on page 39.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP ENABLE|DISABLE

Table 5.22: Server SNMP Command Parameter

Parameter	Description
ENABLE|DISABLE	Enables or disables SNMP processing. Default = Enabled

Server SNMP Community command

The Server SNMP Community command defines read, write and trap SNMP community strings. Community names are case sensitive.

NOTE: The default community names are “public”; if you enable SNMP, you are encouraged to change the community values to prevent access to the MIB.

For more information, see *Managing the CCM Appliance Using SNMP* on page 39.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP COMMUNITY [READCOMM=<*name*>] [WRITECOMM=<*name*>] [TRAPCOMM=<*name*>]

Table 5.23: Server SNMP Community Command Parameters

Parameter	Description
READCOMM=<*name*>	1-64 alphanumeric character read community name. Default = public
WRITECOMM=<*name*>	1-64 alphanumeric character write community name. Default = public
TRAPCOMM=<*name*>	1-64 alphanumeric character trap community name. If you specify this parameter, the name must be different from the read and write community names. Default = public

Server SNMP Manager command

The Server SNMP Manager command defines or deletes SNMP management entities. You may define up to four management entities. If you delete all SNMP managers (or never add any), the CCM appliance may be accessed using SNMP from any IP address.

For more information, see *Managing the CCM Appliance Using SNMP* on page 39.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP MANAGER ADD|DELETE <*ip_address*>

Table 5.24: Server SNMP Manager Command Parameters

Parameter	Description
ADD|DELETE	Adds or deletes the specified SNMP management entity.
<*ip_address*>	IP address of SNMP management entity.

Example

The following command adds an SNMP management entity with the IP address of 192.168.0.1.

```
server snmp manager add 192.168.0.1
```

Server SNMP Trap command

The Server SNMP Trap command enables or disables SNMP traps. When you issue this command with the Enable parameter, the CCM appliance displays a numbered list of all currently disabled traps. When you issue this command with the Disable parameter, a numbered list of all currently enabled traps is displayed.

You may indicate the traps to be enabled/disabled by entering a single number, several numbers separated by commas, a range of numbers separated by a dash or a combinations of numbers separated by commas and dashes. You may also type **ALL** to select all traps in the list or press **Enter**, which cancels the operation.

If you specify **ALL** on the command line, the numbered list is not displayed.

If you enable a trap but there is no trap destination configured for it, a warning will be issued. In this case, issue a Server SNMP Trap Destination command.

NOTE: By default, all traps are disabled. The PortAlert trap must be enabled for port alert processing to be performed.

For more information, see *Managing the CCM Appliance Using SNMP* on page 39 and *Supported Traps* on page 100.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP TRAP [ENABLE|DISABLE] [ALL]

Table 5.25: Server SNMP Trap Command Parameter

Parameter	Description
ENABLE|DISABLE	Enable generates a numbered list of currently disabled traps from which you choose those to enable. Disable generates a numbered list of currently enabled traps from which you choose those to disable.

Example

The following command enables the linkUp, UserDeleted and UserLogin SNMP traps.

```
server snmp trap enable
Traps now disabled:
1) linkUp        4) UserLogin
2) UserAdded     5) ImageUpgradeStarted
3) UserDeleted
Select trap(s) to enable>1,3-4
```

Server SNMP Trap Destination command

The Server SNMP Trap Destination command defines or deletes destinations for enabled SNMP traps. Once you define destinations for enabled SNMP traps, when a trap occurs, the CCM appliance will generate SNMP trap messages to each defined SNMP trap destination. You may define up to four trap destinations, using separate commands.

For more information, see *Managing the CCM Appliance Using SNMP* on page 39.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP TRAP DESTINATION ADD|DELETE <*ip_address*>

Table 5.26: Server SNMP Trap Destination Command Parameters

Parameter	Description
ADD|DELETE	Defines or deletes the specified destination.
<*ip_address*>	IP address of trap destination.

Server SSH command

The Server SSH command enables or disables SSH session access to the CCM appliance and specifies the SSH authentication method. When you enable SSH, all CCM sessions will be terminated if a CCM SSH server key must be generated. You must also have previously specified an authentication method other than None with the Server Security command.

If you enable plain text Telnet connections with a Server Security command, enabling SSH session access with the Server SSH command will add that as a valid connection method (both plain text and SSH connections will be allowed.)

For more information, see *Using SSH* on page 20.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SSH ENABLE|DISABLE [AUTH=<*auth*>]

Table 5.27: Server SSH Command Parameters

Parameter	Description
ENABLE|DISABLE	Enables or disables SSH session access to the CCM appliance.

Table 5.27: Server SSH Command Parameters (Continued)

Parameter	Description
AUTH=<*auth*>	SSH authentication methods. You must enter the entire value; abbreviations are not permitted. Valid values are: PW — Password authentication. KEY — Key authentication. PW|KEY — Password or key authentication. KEY|PW — Key or password authentication. PW&KEY — Password and key authentication. KEY&PW — Key and password authentication. Default = PW

Show Commands

The Show command has several forms, as listed in Table 5.28.

Table 5.28: Show Command Summary

Command	Description
Show NFS	Displays NFS mount status and configured values.
Show NTP	Displays configured NTP values.
Show Port	Displays port information.
Show Port In/Out	Displays how carriage returns and linefeeds are treated.
Show Server	Displays CCM configuration information and statistics.
Show Server CLI	Displays CCM CLI settings.
Show Server PPP	Displays CCM PPP settings.
Show Server RADIUS	Displays CCM RADIUS settings.
Show Server Security	Displays CCM authentication, connection and security lock-out settings.
Show Server SNMP	Displays SNMP configuration information.
Show User	Displays user configuration and session information.

A Show command display may span more than one screen. See *Command displays* on page 46 for more information.

Show NFS command

The Show NFS command displays NFS configuration information and the current mount status. If a mount error occurred, the display also includes the error message returned by the NFS server.

If NFS has never been enabled on the appliance, the default values will be displayed. If NFS was previously enabled and successfully configured, then later disabled, the display will retain the configured address, mount point and file type values.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW NFS

Show NTP command

The Show NTP command displays NTP configuration information.

If NTP has never been enabled on the appliance, the default values will be displayed. If NTP was previously enabled and successfully configured, then later disabled, the display will retain the configured address and update values, and the status will remain Success.

If a second IP address was not configured, None will be indicated for that value. If a request for the time from the first server is successful, the second server's status will indicate Not attempted.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW NTP

Show Port command

The Show Port command displays configuration and status information about one or all ports.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW PORT [<*port*>] [ALL|NAMES|GROUPS|ALERT]

Table 5.29: Show Port Command Parameter

Parameter	Description
<*port*>	A port number, port name or CON. If the port name contains spaces, it must be enclosed in double quotes. Default = your port
ALL	Displays information about all ports.
NAMES	Displays a list of port numbers and associated names.
GROUPS	Displays a list of port numbers and the group name assigned to each port (if any).
ALERT	Displays a port's alert strings.

The display for the console port will not include values for the socket, power, TD, toggle, name or group fields.

Table 5.30 lists the display fields for a Show Port command that specifies a single port configured as TD=console. A Show Port All command displays the items listed in the first six rows of the table (Port through Power fields).

Table 5.30: Show Port Command Display Fields for TD=Console

Field	Content
Port	Port number.
Serial Port Settings	Comma-separated string of port values: baud rate, number of bits, parity, stop bits, flow control, socket number, time-out value and CLI access character (from Port Set command). The CLI character is preceded by POR CLI= if it was defined with a Port Set command or by SER CLI= if it was defined with a Server CLI command.
TX Bytes	Number of bytes transmitted.
RX Bytes	Number of bytes received.
Errors	Number of TX/RX parity and framing errors.
Toggle	Toggle value (from Port Set command).
Power	Device power status, if monitoring is enabled. ON indicates the device is on, OFF indicates the device is off.
Power Signal	Signal and state being monitored for device power status (from Port Set command). If monitoring is disabled, this field indicates None.
Port name	Port name assigned with the Port Set command or the default name (last three octets of MAC address plus the port number).
Group	Group names.
Port NFS	ENABLE indicates NFS is enabled, DISABLE indicates NFS is disabled (from Port NFS command).
File	NFS filename (from Port NFS command).
Size threshold	NFS size threshold (from Port NFS command).
Time threshold	NFS time threshold (from Port NFS command).
Port NFS Status	Status of NFS history file operations. See *NFS port status values* on page 111 for more information.
Current file	Current NFS filename.
User *	Username (from User Add command).
Level *	User's access level (from User Add and User Set Access commands).

Table 5.30: Show Port Command Display Fields for TD=Console (Continued)

Field	Content
Access *	User's access rights (from User Add and User Set Access commands).
Port Access *	Indicates if a user may connect to the port BY GROUP or BY PORT. If there is any group defined for any ports (which can be determined with a Show Port Groups command), each user may connect BY GROUP, unless a user's access rights include PALL, in which case, a user may connect BY PORT. If a user is assigned an empty group (with no ports in it) or no groups at all, that user may lose access to any port once there is a group defined for any port.
Locked *	Indicates if the port is LOCKED or UNLOCKED. If security lock-out is disabled, N/A is displayed. See *Using security lock-out* on page 32 for more information.
Last Login *	System up time value when the user logged in.
Duration *	Duration of user's session.
* Displayed only when the command specifies a single port that has a current connection.	

Table 5.31 lists the display fields for a Show Port command (that specifies a single port or All) for ports that were configured as TD=SPC.

Table 5.31: Show Port Command Display Fields for TD=SPC

Parameter	Description
Status	ONLINE indicates the SPC device is powered up, OFFLINE indicates the SPC device is powered down.
Version	SPC device firmware version.
Sockets	Number of sockets on the SPC device.
Minload	Minimum load amp value (from SPC command).
Maxload	Maximum load amp value (from SPC command).
Wake	Wakeup state for socket (from SPC command).
ON Min	Minimum On time (from SPC command).
OFF Min	Minimum Off time (from SPC command).

The Show Port Names command displays a list of port numbers and their names. If a port has not been assigned a name with the Port Set command, the default name is displayed.

The Show Port Groups command displays a list of port numbers and group assignments.

The Show Port Alert command displays a port's alert strings.

Show Port In/Out command

The Show Port In/Out command displays the translation settings for all ports. These translation settings indicate how carriage returns and linefeeds are treated in incoming and outgoing serial data.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW PORT IN|OUT

Show Server command

The Show Server command displays CCM appliance configuration information, statistics and the current time.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER

Table 5.32: Show Server Command Display Fields

Field	Content
Server	IP address (from initial configuration or Server Set command).
Mask	Subnet mask (from initial configuration or Server Set command).
Gateway	Gateway IP address (from initial configuration or Server Set command).
Up Time	Days, hours, minutes and seconds since unit was rebooted.
MAC	Ethernet MAC address.
S/N	Serial number.
Port	Port number.
Username	Username (from User Add command).
Duration	Duration of session.
Socket	Telnet socket number.
From Socket	Telnet client IP address with socket number in parentheses.
IP Input and Output	Network IP statistics, including number of packets delivered, discarded and fragments.
TCP	Network TCP statistics, including in segs, out segs, errors and retransmissions.
UDP	Network UDP statistics, including in, out, errors and no port events.
BOOT	BIOS/Bootstrap version, date and time.

Table 5.32: Show Server Command Display Fields (Continued)

Field	Content
APP	Application version that is running, plus its date and time.
Share Mode	DISABLE, AUTO or QUERY (from Server Share command).

Show Server CLI command

The Show Server CLI command displays the serial CLI settings.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER CLI

Table 5.33: Show Server CLI Command Display Fields

Field	Contents
CLI Port	Console port terminal type.
Access Character	Control character used to access the CLI.
History	Indicates whether a port's history buffer content is displayed (auto) or not displayed (hold) when a user connects to the port, and whether the buffer content is cleared (clear) or kept (keep) when a session ends.
Connect	Indicates whether a valid user on the console port may use the Connect command.
Modeminit string	String used to initiate modem connections on the console port.
Server CLI Timeout	Session time-out value, shown in full minute or minute:second form (for example, 3m for 3 minutes, 3:30 for 3 minutes, 3 seconds.

Show Server PPP command

The Show Server PPP command displays the current PPP settings that were configured with the Server PPP command.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER PPP

Show Server RADIUS command

The Show Server RADIUS command displays the current CCM RADIUS settings that were configured with the Server RADIUS command.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER RADIUS

Show Server Security command

The Show Server Security command displays the current authentication, connection and lock-out settings that were configured with the Server Security and Server SSH commands.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER SECURITY

Table 5.34: Show Server Security Command Display Fields

Field	Contents
Authentication	Configured authentication method(s). This includes the SSH authentication method configured with the Server SSH command (or the default value), regardless of whether SSH is enabled.
Encryption	Configured connection methods.
Lockout	Configured security lock-out state (Enabled or Disabled). If Enabled, the number of hours in the lock-out period is included.
Fingerprint (Hex)	SSH key MD5 hash.
Fingerprint (BB)	SSH key bubble babble.

Show Server SNMP command

The Show Server SNMP command displays SNMP configuration information.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER SNMP

Table 5.35: Show Server SNMP Command Display Fields

Field	Contents
Server SNMP	ENABLE if SNMP processing is enabled, DISABLE if SNMP processing is disabled (from Server SNMP command).
Read Community	Read community name (from Server SNMP Community command).

Table 5.35: Show Server SNMP Command Display Fields (Continued)

Field	Contents
Write Community	Write community name (from Server SNMP Community command).
Trap Community	Trap community name (from Server SNMP Community command).
SNMP Managers	SNMP management entity IP addresses (from Server SNMP Manager command). If no SNMP managers have been added or if they are all deleted, this field will indicate (none).
Trap Dests	Destinations for enabled SNMP traps (from Server SNMP Trap Destination command).
Enabled Traps	Names of SNMP traps that have been enabled (from Server SNMP Trap command).

Show User command

The Show User command displays information about one or all users.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW USER [<*username*>|ALL]

Table 5.36: Show User Command Parameter

Parameter	Description
<*username*>	Username. Default: user currently logged in
ALL	Requests a display of all defined users.

The Show User command display for one user includes the information in Table 5.37.

Table 5.37: Show User Command Display Fields

Field	Contents
User	Username.
Level	User's access level. If a level was not configured, access rights determine the level: Users with SCON access => APPLIANCEADMIN. Users with USER or PCON but not SCON => ADMIN. Otherwise, USER level is assigned.
Access	User's access rights.
Groups	User's groups or blank if no groups.

Table 5.37: Show User Command Display Fields (Continued)

Field	Contents
Port Access	Indicates if the user may connect to ports BY GROUP or BY PORT. If there is any group defined for any ports (which can be determined with a Show Port Groups command), each user may connect BY GROUP, unless a user's access rights include PALL, in which case, a user may connect BY PORT. If a user is assigned an empty group (with no ports in it) or no groups at all, that user may lose access to any port once there is a group defined for any port.
Locked	YES if user is locked-out, NO if not.
Last Login	System up time value when the user logged in.
Port	Serial port to which user is connected.
Username	Username.
Duration	Duration of user's session.
Socket	Telnet socket number.
From Socket	Telnet client IP address and socket number.

There may be a difference between the display for a Show User command (without a username) and Show User <*current_username*>. If you do not specify a username, the command displays the current user credentials; with a username, the information comes from the database.

For example, assume username Admin is logged in with Access=PALL. Then, a User Set Admin Access=–PALL command is issued and the database is modified. A Show User command (without a username) will display the access as PALL, while a Show User Admin command will display the new access without PALL.

A Show User All command display includes the information in Table 5.38.

Table 5.38: Show User All Command Display Fields

Field	Contents
User	Username.
Pass	YES if user has a password defined, NO if not.
Key	YES if user has an SSH key defined, NO if not.
Lock	YES if user is locked-out, NO if not.
Level	User's access level. If a level was not configured, access rights determine the level: Users with SCON access => APPLIANCEADMIN. Users with USER or PCON but not SCON => ADMIN. Otherwise, USER level is assigned.
Access	User's access rights.

SPC Command

The SPC command changes settings for an SPC power control device.

NOTE: To access the control screen or command line interface provided by the SPC device, this command should not be used, and the CCM appliance port to which the SPC device is attached should be configured as TD=Console. When TD=SPC is configured, you cannot connect to the SPC device; all SPC device operations are performed from the CCM appliance CLI.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SPC <*port*>|ALL [MINLOAD=<*amps*>] [MAXLOAD=<*amps*>]

Table 5.39: SPC Command Parameters

Parameter	Description
<*port*>|ALL	Port number, port name or All, which indicates that the settings that follow should be applied to all ports configured as TD=SPC. If the name contains spaces, it must be enclosed in double quotes.
MINLOAD=<*amps*>	Minimum load in amperes in the range 0-30. A zero value indicates no minimum load. Default = 0
MAXLOAD=<*amps*>	Maximum load in amperes in the range 0-30. A zero value indicates no maximum load. Default = 0

The following command sets a maximum load of 20 amps for the SPC device attached to the port named spc3 on the CCM appliance.

```
spc spc3 max=20
```

SPC Socket Command

The SPC Socket command changes the settings or state for one or more sockets on an SPC power control device.

NOTE: For standalone use of the SPC device, this command should not be used, and the CCM appliance port to which the SPC device is attached should be configured as TD=Console.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SPC <*port*>|ALL [SOCKET <*socket*>] [WAKE=ON|OFF] [ONMIN=<*time*>] [OFFMIN=<*time*>] [POWER=ON|OFF|REBOOT]

Table 5.40: SPC Socket Command Parameters

Parameter	Description
<*port*>|ALL	Port number, port name or All, which indicates that the settings/operations that follow should be applied to all ports configured as TD=SPC. If the name contains spaces, it must be enclosed in double quotes.
SOCKET <*socket*>	Socket number.
WAKE=ON|OFF	State that the socket will enter when the SPC device is powered up. Default = On
ONMIN=<*time*>	Minimum amount of time that a socket will stay on before it may be turned off. The value may be specified with S for seconds, M for minutes or H for hour. Valid values are: 0S, 15S, 30S, 45S, 60S, 75S, 90S, 105S. 1M, 2M, 3M, 4M, 5M, 10M, 15M, 30M, 60M. 1 H. Default = 0S
OFFMIN=<*time*>	Minimum amount of time that a socket will stay off before it may be turned on. The value may be specified with S for seconds, M for minutes or H for hour. Valid values are: 0S, 15S, 30S, 45S, 60S, 75S, 90S, 105S. 1M, 2M, 3M, 4M, 5M, 10M, 15M, 30M, 60M. 1 H. Default = 0S
POWER=ON|OFF| REBOOT	ON causes the specified socket(s) to turn on (after the time specified in Offmin). OFF causes the specified socket(s) to turn off (after the time specified in Onmin). REBOOT causes the specified socket(s) to turn off, then on.

Example

The following command turns on all sockets on the SPC power control device attached to port 6 of the CCM appliance. The sockets will turn on based on their Offmin values.

```
spc 6 socket all on
```

User Commands

The User command has several forms, as listed in Table 5.41.

Table 5.41: User Command Summary

Command	Description
User Add	Adds a new user to the user database.
User Delete	Deletes a user from the user database.
User Logout	Terminates a user's active session.
User Set	Changes a user's configuration information.

Table 5.41: User Command Summary (Continued)

Command	Description
User Unlock	Unlocks a locked-out user.

User Add command

The User Add command adds a new user to the CCM user database. The user database holds a maximum of 64 user definitions. For more information, see *Managing User Accounts* on page 27 and *Access rights and levels* on page 28.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

USER ADD <*username*> [PASSWORD=<*pwd*>] [SSHKEY=<*keyfile*>] [FTPIP=<*ftpadd*>] [KEY=<*sshkey*>] [ACCESS=<*access*>] [GROUP=<*group1*>[,<*group2*>...]]

Table 5.42: User Add Command

Parameter	Description
<*username*>	3-16 alphanumeric character username. Usernames are case sensitive. A username cannot be All.
PASSWORD=<*pwd*>	3-16 alphanumeric character password. Passwords are case sensitive.
SSHKEY=<*keyfile*>	Name of uuencoded public key file on an FTP server. The maximum file size that may be received is 4K bytes. If this parameter is specified, you must also specify the FTPIP parameter.
FTPIP=<*ftpadd*>	FTP server's IP address. If this parameter is specified, you must also specify the SSHKEY parameter.
KEY=<*sshkey*>	Uuencoded SSH key.
ACCESS=<*access*>	Command and port access rights or level. You may specify multiple access rights, separated by commas, or a level. Valid values for access rights are: P<*n*> Access to the specified port number. P<*x-y*> Access to the specified range of ports. PALL Access to all ports. USER User configuration access rights. PCON Port configuration access rights. SCON Configuration access rights. SMON Monitor access rights. BREAK Can issue Port Break command. Valid values for access levels are: ADMIN PALL, USER, SMON, PCON and BREAK access rights. APPLIANCEADMIN PALL, USER, SCON, SMON, PCON and BREAK access rights. Default = PALL,SMON

Table 5.42: User Add Command (Continued)

Parameter	Description
GROUP=<*group*>	Name of port group to which the user will be assigned. Up to 8 port groups, separated by commas, may be defined for a CCM850 appliance user, up to 16 port groups for a CCM1650 appliance user and up to 48 groups for a CCM4850 appliance user.

Examples

The following command adds the username JohnDoe, with the password secretname, access to ports 2, 5, 6 and 7 and user and monitor access rights.

```
> user add JohnDoe password=secretname access=P2,5-7,user,smon
```

The following command adds the username JaneDoe, with access to all ports. The name of the SSH public user key file is ccm_key2.pub. This file is located on the FTP server at IP address 10.0.0.3.

```
> user add JaneDoe ssh=ccm_key2.pub ftp=10.0.0.3 access=pall
```

The following command adds the username JDoe, with the password mysecret and the Appliance Administrator access level, which enables access to all ports and CCM appliance commands.

```
> user add JDoe pas=mysecret access=applianceadmin
```

The following command adds the username JohnD with the password pword and the Administrator access level. JohnD is assigned to the port groups Dev1 and Dev2.

```
user add JohnD password=pword access=adm group=Dev1,Dev2
```

User Delete command

The User Delete command removes a username entry from the CCM user database. The username will no longer be used to authenticate a session with the CCM appliance.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

USER DEL <*username*>

Table 5.43: User Delete Command Parameter

Parameter	Description
<*username*>	Username to be deleted.

User Logout command

The User Logout command terminates a user's active sessions on the CCM appliance. If the specified user has no active sessions, an error message is displayed. For all active sessions that are terminated, a message is sent to the Telnet client and the Telnet connection is dropped.

Access right: USER
Access level: ADMIN (may log out all except APPLIANCEADMIN) or APPLIANCEADMIN

Syntax

USER LOGOUT <*username*>

Table 5.44: User Logout Command Parameter

Parameter	Description
<username>	Username to be logged out.

User Set command

The User Set command changes a user's configuration in the user database. For more information, see *Managing User Accounts* on page 27 and *Access rights and levels* on page 28.

You may delete a user's password or key; however, each user must have a password or a key, so you cannot remove both. Also, you cannot remove a user's password or key if that action would result in no users having USER access rights.

Access right: none to change your own password, USER to change anything else
Access level: none to change your own password, ADMIN or APPLIANCEADMIN to change anything else

Syntax

USER SET <*username*> [PASSWORD=<*pwd*>] [SSHKEY=<*keyfile*>] [FTPIP=<*ftpadd*>] [KEY=<*sshkey*>] [ACCESS=<*access*>] [GROUP=<*group*>]

Table 5.45: User Set Command Parameters

Parameter	Description
<*username*>	Username. This parameter may be omitted only if you are modifying your own password.
PASSWORD=<*pwd*>	New 3-16 alphanumeric character password. Passwords are case sensitive. This parameter is required when changing another user's password. The password is displayed on the screen. For security, clear your screen display after issuing this command. To delete a password, specify Password =“”.
SSHKEY=<*keyfile*>	Name of uuencoded public key file on an FTP server. The maximum file size that may be received is 4K bytes.
FTPIP=<*ftpadd*>	FTP server's IP address.
KEY=<*sshkey*>	Uuencoded SSH key. To delete an SSH key (whether it was originally specified with the SSHKEY and FTPIP parameters or with the KEY parameter), specify Key=“”.

Table 5.45: User Set Command Parameters (Continued)

Parameter	Description
ACCESS=<*access*>	Command and port access rights or level. You may specify multiple access rights, separated by commas, or a level. If specifying access rights, you may use one of three forms: ACCESS=<*access*> to specify all access rights. ACCESS=+<*access*> to specify only access rights to be added. ACCESS=–<*access*> to specify only access rights to be deleted. Valid values for access rights are: P<n> Access to the specified port number. P<x-y> Access to the specified range of ports. PALL Access to all ports. USER User configuration access rights. PCON Port configuration access rights. SCON Configuration access rights. SMON Monitor access rights. BREAK Can issue Port Break command. Valid values for access levels are: ADMIN PALL, USER, SMON, PCON and BREAK access rights. APPLIANCEADMIN PALL, USER, SCON, SMON, PCON and BREAK access rights. Default = PALL,SMON
GROUP=<*group*>	Port group name. You may specify multiple groups, separated by commas. You may use one of three forms: GROUP=<*group*> to specify all the port groups to which this user will belong. GROUP=+<*group*> to specify only port groups to be added. GROUP=–<*group*> to specify only port groups to be deleted. Up to 8 port groups, separated by commas, may be defined for a CCM850 appliance user, up to 16 port groups for a CCM1650 appliance user and up to 48 groups for a CCM4850 appliance user.

Examples

The following command sets the access rights for JohnDoe, enabling access to all ports with configuration and monitoring access rights.

```
> user set JohnDoe access=pall,scon,smon
```

The following command removes the server configuration and port configuration access right for JohnDoe, and leaves any other previously configured access rights intact.

```
> user set JohnDoe access=-SCON,PCON
```

The following command deletes the SSH key information for JohnDoe. The command will complete successfully only if JohnDoe has a password configured in a previous User Add or User Set command, and if there are other users with User access rights.

```
> user set JohnDoe key=""
```

The following command adds the groups Dev3 and Dev4 for JohnD. He may now access the ports defined in groups Dev3 and Dev4 as well as ports in other groups that were previously configured for him.

```
> user set JohnD group=+Dev3,Dev4
```

User Unlock command

The User Unlock command unlocks a user who was previously locked-out. After this command completes, the user will be able to attempt login authentication again.

Access right: USER
Access level: ADMIN (may unlock all except APPLIANCEADMIN) or APPLIANCEADMIN

Syntax

USER UNLOCK <*username*>

Table 5.46: User Logout Command Parameter

Parameter	Description
<username>	Username to be unlocked.

APPENDICES

Appendix A: Technical Specifications

Table A.1: CCM Appliance Technical Specifications

Item	CCM850 Appliance	CCM1650 Appliance	CCM4850 Appliance
Device Ports			
Number	8	16	48
Type	Serial ports	Serial ports	Serial ports
Connectors	Serial port RJ-45	Serial port RJ-45	Serial port RJ-45
Console Port			
Number	1	1	1
Connector	Serial port RJ-45	Serial port RJ-45	Serial port RJ-45
Network Connection			
Number	1	1	1
Type	Ethernet: IEEE 802.3, 10BaseT Fast Ethernet: IEEE 802.3U, 100BaseT	Ethernet: IEEE 802.3, 10BaseT Fast Ethernet: IEEE 802.3U, 100BaseT	Ethernet: IEEE 802.3, 10BaseT Fast Ethernet: IEEE 802.3U, 100BaseT Gigabit Ethernet: IEEE 802.ab, 1000BaseT
Connector	RJ-45	RJ-45	RJ-45
Dimensions			
H x W x D	4.45 x 22.23 x 20.32 cm 1U form factor (1.75 x 8.75 x 8.00 in)	4.45 x 22.23 x 20.32 cm 1U form factor (1.75 x 8.75 x 8.00 in)	4.45 x 44.45 x 25.40 cm 1U form factor (1.75 x 17.50 x 10.00 in)
Weight (without cables)	5 lbs (2.3 kg)	5 lbs (2.3 kg)	5 lbs (2.27 kg)
Heat Dissipation	75 BTU/hr	102 BTU/hr	205 BTU/hr
Airflow	2.5 cfm	2.5 cfm	14 cfm
Power Consumption	22 W	30 W	60 W

Table A.1: CCM Appliance Technical Specifications (Continued)

Item	CCM850 Appliance	CCM1650 Appliance	CCM4850 Appliance
AC-input power	45 W maximum	45 W maximum	90 W maximum
AC-input maximum	90 to 267 VAC	90 to 267 VAC	100 to 240 VAC
AC-input current rating	0.5 A	0.5 A	1 A maximum
AC-input cable	18 AWG three-wire cable, with a three-lead IEC-320 receptacle on the power supply end and a country dependent plug on the power resource end		
Frequency	50 to 60 Hz	50 to 60 Hz	50 to 60 Hz
Temperature Operating	0° to 40° Celsius (32° to 104° Fahrenheit)	0° to 40° Celsius (32° to 104° Fahrenheit)	0° to 55° Celsius (32° to 131° Fahrenheit)
Temperature Nonoperating	-20° to +65° Celsius (-4° to +149° Fahrenheit)	-20° to +65° Celsius (-4° to +149° Fahrenheit)	-40° to +70° Celsius (-40° to +158° Fahrenheit)
Humidity	10% to 90% noncondensing	10% to 90% noncondensing	10% to 90% noncondensing
Safety and EMC Approvals and Markings	ANSI/UL 60950-1, CSA C22.2 No. 60950-1-CAN/CSA (UL cUL Listed), IEC 60950-1 (2001-10), CENELEC EN 60950-1		
Regulatory Compliance	FCC P. 15 Class A, ICES-003, EN 55022: 1998 Class A, EN 61000-3-3, AS/NZS CISPR 22, CNS 13438 - Issued: 1997/01/01, VCCI V-3/02.04 Class A, EN 55024-1998 The products herewith comply with the requirements of the Low Voltage Directive, 73/23/EEC and the EMC Directive 89/336/EEC, including amendments by the CE-marking Directive 93/68/EEC		

Appendix B: Device Cabling

Each CCM appliance serial port has an RJ-45 connector for attaching a serial device. Table B.1 lists the pin assignments.

Table B.1: Port Pin Assignments

Pin Number	RS-232 Signal	Direction	Description
1	RTS	Output	Request to Send
2	DSR	Input	Data Set Ready
3	DCD	Input	Data Carrier Detect
4	RD	Input	Receive Data
5	TD	Output	Transmit Data
6	GND	(N/A)	Signal Ground
7	DTR	Output	Data Terminal Ready
8	CTS	Input	Clear to Send
NOTE: RI (Ring Indicate) is not supported			

Modular adaptors are available to convert RJ-45 modular jacks to standard pinout configurations. Adaptors are available for use with:

- CAT 5 cable (and CAT 6 cable for CCM4850 appliances).
- Serial reversing cable. Reversing adaptors and cables are recommended for distances greater than 100 feet.

Adaptors for use with CAT 5 and CAT 6 cable

Table B.2 lists the adaptors available for use with CAT 5 and CAT 6 cable.

Table B.2: Adaptors for Use with CAT 5 and CAT 6 Cable

Part Number	Description
210122	RJ-45 to DB-9M (DTE) Adaptor
210120	RJ-45 to DB-9F (DCE) Adaptor
210124	RJ-45 to DB-25M (DTE) Adaptor
210123	RJ-45 to DB-25M (DCE) Adaptor
210125	RJ-45 to DB-25F (DTE) Adaptor
210121	RJ-45 to DB-25F (DCE) Adaptor

Table B.2: Adaptors for Use with CAT 5 and CAT 6 Cable (Continued)

Part Number	Description
210127	RJ-45 to RJ-45 Male Adaptor for Cisco and Sun Netra console port
750238	CAT 5 Serial Starter Kit - includes all the above adaptors

Figure B.1 shows the pin assignments for the adaptors listed in Table B.2.

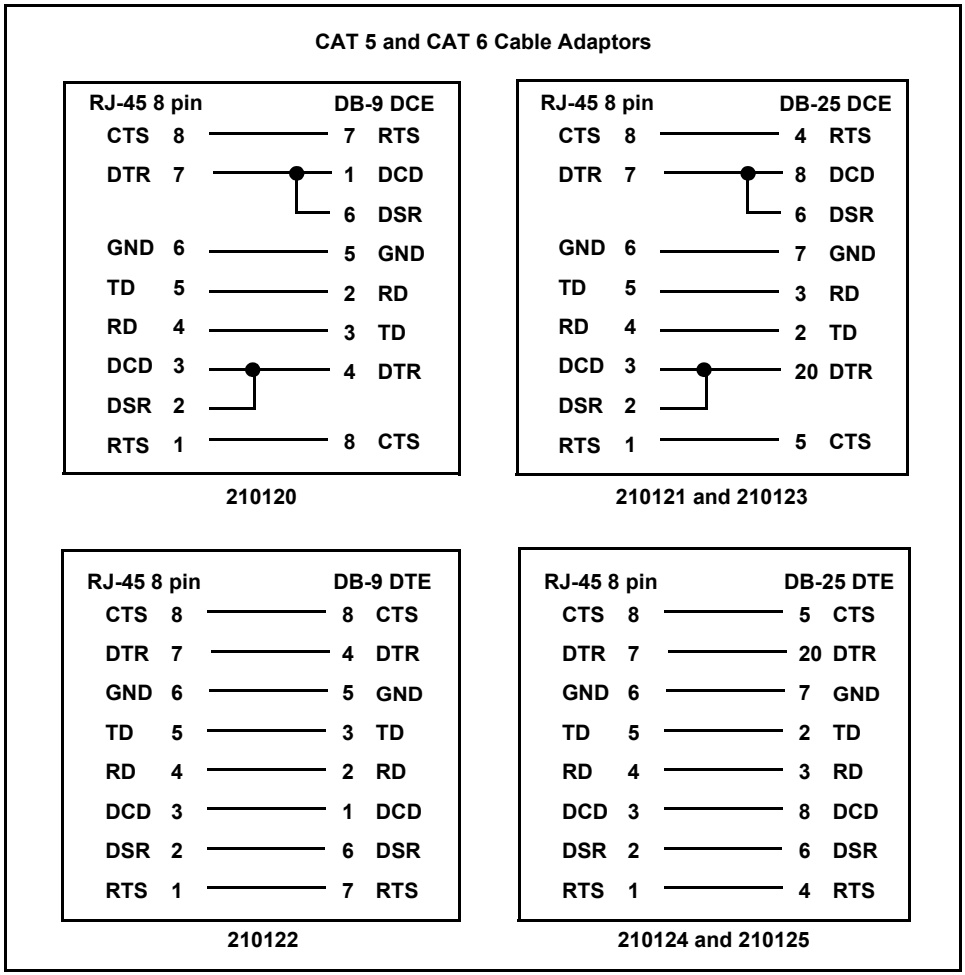

Figure B.1: CAT 5 and CAT 6 Cable Adaptor Pin Assignments

Reversing adaptors and cables

Table B.3 lists the reversing adaptors and reversing cables available for the appliance.

Table B.3: Reversing Adaptors and Cables

Part Number	Description
210094	RJ-45 to DB-9M (DTE) Adaptor
210095	RJ-45 to DB-9F (DCE) Adaptor
210090	RJ-45 to DB-25M (DTE) Adaptor
210092	RJ-45 to DB-25M (DCE) Adaptor
210091	RJ-45 to DB-25F (DTE) Adaptor
210093	RJ-45 to DB-25F (DCE) Adaptor
210105	RJ-45 to RJ-45 Male Adaptor for Cisco and Sun Netra console port
690226	10 foot 8-wire Reversing Modular Cable
690227	25 foot 8-wire Reversing Modular Cable
690228	75 foot 8-wire Reversing Modular Cable
750122	Wiring Starter Kit (8-wire) - includes all the above adaptors and one 690226 cable

Figure B.2 shows the pin assignments for the adaptors listed in Table B.3.

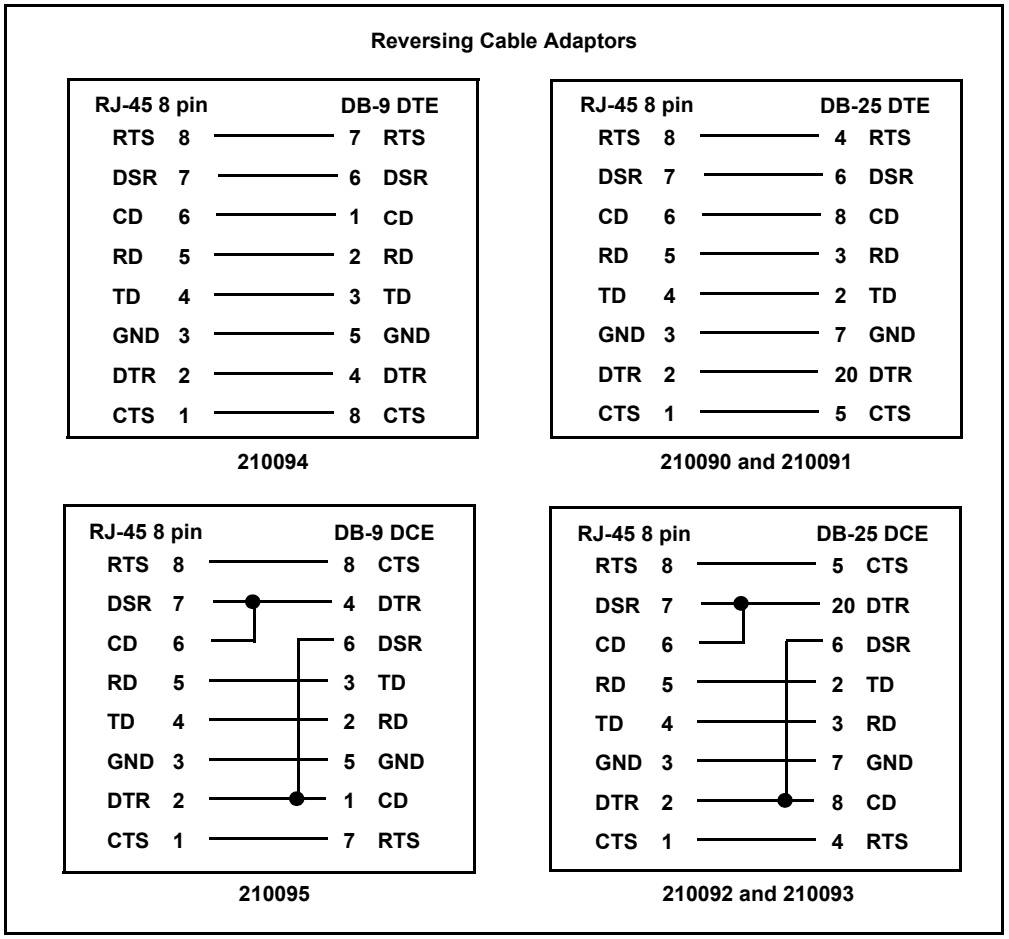

Figure B.2: Reversing Cable Adaptor Pin Assignments

If you choose to use a third party reversing cable, make sure the cable is reversing, as shown in Figure B.3.

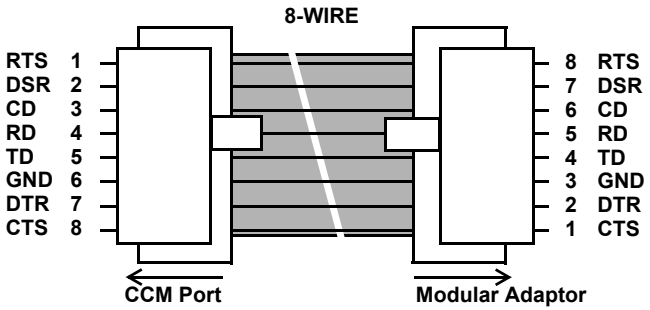

Figure B.3: 8-wire RJ-45 Reversing Cable

Appendix C: Supported Traps

The CCM appliance supports the following MIB2 traps:

- authenticationFailure
- linkUp
- linkDown
- coldStart

Table C.1 lists the supported enterprise traps. The Avocent web site (www.avocent.com) contains the complete trap MIB.

Table C.1: CCM Appliance Enterprise Traps

Trap	Description and Variable(s)
AggregatedServer StatusChanged	The status of one or more servers (connections paths) has changed. The appliance always sends this trap upon bootup. Thereafter, it sends the trap when there is a change in connection path status, and will include only those paths whose status has changed. Variable(s): connection path(s)
ConfigurationFile Loaded	The CCM appliance has loaded a configuration file. This trap applies to AVWorks software. Variables: initiating username and name of loaded file
FactoryDefaultsSet	The CCM appliance has received a command to set itself to factory default values. (The appliance sends this trap after receiving the command, but before actually reverting to factory default values.)
ImageUpgradeResults	An image upgrade has ended. Variables: result (successful or error code), initiating username, image type (boot or application), upgrade version number and running version number (if the upgrade was successful, the two version numbers will match)
ImageUpgradeStarted	The CCM appliance has started an image upgrade. Variables: initiating username, image type (boot or application), new version number, current version number
NFSDisableRqstd	A request has been made to disable NFS. Variable: requesting username
NFSEnableRqstd	A request has been made to enable NFS. Variable: requesting username
NFSMountedOK	NFS is enabled and the mount operation has completed successfully.
NFSMountFailedGave Up	NFS is enabled but repeated mount attempts have failed. No additional mount retries will be performed. Variables: primary and secondary NFS error codes (see *NFS Error Codes and Port Status* on page 105)

Table C.1: CCM Appliance Enterprise Traps (Continued)

Trap	Description and Variable(s)
NFSMountFailed Retrying	NFS is enabled and the first mount attempt failed. Additional mount retries are still being performed. Variables: primary and secondary NFS error codes (see *NFS Error Codes and Port Status* on page 105)
NFSMountLost1stRetry Failed	NFS is enabled and a mount completed successfully. That mount was lost and the first attempt to reestablish that mount has now failed. Additional retries are being performed. Variables: primary and secondary NFS error codes (see *NFS Error Codes and Port Status* on page 105)
NFSMountLostGaveUp	NFS is enabled and a mount completed successfully. That mount was lost and repeated attempts to reestablish that mount have failed. No addition mount retries will be performed. Variables: primary and secondary NFS error codes (see *NFS Error Codes and Port Status* on page 105)
NFSMountLostRetrying	NFS is enabled and a mount completed successfully; however, that mount has now been lost and is being retried. Variables: primary and secondary NFS error codes (see *NFS Error Codes and Port Status* on page 105)
NFSMountVerifiedOK	NFS is enabled and has successfully verified the mount in response to a subsequent NFS Enable command.
NFSPortDisableRqstd	An NFS Port Disable command has been issued. Variables: initiating username and CCM appliance port number
NFSPortEnableRqstd	An NFS Port Enable command has been issued. Variables: initiating username and CCM appliance port number
NFSPortFileClosed	NFS has closed the history file on the NFS server. Variable: CCM appliance port number
NFSPortFileOpenOK	NFS is enabled on the port and has successfully opened the history file on the NFS server. Variable: CCM appliance port number
NFSPortNeedsMount	NFS is enabled on the port, but a mount is required (using an NFS Enable command) before the port can open and/or write to the history file on the NFS server. Variables: CCM appliance port number, port error status (see *NFS Error Codes and Port Status* on page 105) plus primary and secondary NFS error codes (see *NFS Error Codes and Port Status* on page 105)
NFSPortNoRecent Errors	NFS is enabled on the port and has successfully opened the history file on the NFS server; however, an NFSPortWriteError and/or an NFSPortOverrunError trap was previously sent for that port. A successful write to the file has since been performed and 15 minutes have subsequently elapsed without any errors being encountered. Variable: CCM appliance port number

Table C.1: CCM Appliance Enterprise Traps (Continued)

Trap	Description and Variable(s)
NFSPortOpenFailGave Up	NFS is enabled on the port, but repeated attempts to open the history file on the NFS server have failed. No additional file open retries will be performed. Variables: CCM appliance port number, port error status (see *NFS Port Status Values* on page 111) plus primary and secondary NFS error codes (see *NFS Error Codes* on page 105)
NFSPortOpenFail Retrying	NFS is enabled on the port, but the first attempt to open the history file on the NFS server has failed. Additional file open retries are being performed. Variables: CCM appliance port number, port error status (see *NFS Port Status Values* on page 111) plus primary and secondary NFS error codes (see *NFS Error Codes and Port Status* on page 105)
NFSPortOverrunError	NFS is enabled on the port and has successfully opened the history file on the NFS server; however, an overrun error occurred when writing to that file. Variables: CCM appliance port number, port error status (see *NFS Port Status Values* on page 111) plus primary and secondary NFS error codes (see *NFS Error Codes and Port Status* on page 105)
NFSPortWriteError	NFS is enabled on the port and has successfully opened the history file on the NFS server; however, an error occurred when writing to that file. Variables: CCM appliance port number, port error status (see *NFS Port Status Values* on page 111) plus primary and secondary NFS error codes (see *NFS Error Codes and Port Status* on page 105)
NFSUnmountedOK	NFS is disabled and the unmount operation has completed successfully.
PortAlert	The CCM appliance detected a port alert string on a serial port. Variables: server name, port number and port alert string
PortPowerOffDetect	The CCM appliance detected that a port's power on/off control signal is in the state indicating power is off. This trap is sent upon initialization if the condition is detected. Subsequent traps are sent only if this signal changes state. Variables: server name and port number
PortPowerOnDetect	The CCM appliance detected that a port's power on/off control signal is in the state indicating power is on. This trap is sent upon initialization if the condition is detected. Subsequent traps are sent only if this signal changes state. Variables: server name and port number
RebootStarted	The CCM appliance is rebooting. Variable: initiating username
SerialSessionStarted	A serial session has started. Variables: username, server name and port number
SerialSessionStopped	A serial session has stopped. Variables: username, server name and port number
SerialSession Terminated	Another user has terminated a serial session. Variables: initiating username, terminated username, server name and port number

Table C.1: CCM Appliance Enterprise Traps (Continued)

Trap	Description and Variable(s)
SpcDeviceOffline	An SPC power control device is offline. Variables: SPC device location name and CCM appliance port number
SpcDeviceOnline	An SPC power control device is online. Variables: SPC device location name and CCM appliance port number
SpcLoginErr	The CCM appliance was unable to log in to the SPC device using the username configured in the appliance. Variables: SPC device location, CCM appliance port number and username
SpcSocketOff Command	A command was issued to turn off an SPC device socket. Variables: username who issued the command, name of server attached to SPC device socket, SPC device location name, CCM appliance port number and SPC device socket number
SpcSocketOffSenseFail	An SPC device has detected an off sense failure for a socket. This occurs when a socket should be in the off state, but is actually in the on state. Variables: name of server attached to the SPC device socket, SPC device location name, CCM appliance port number and SPC device socket number
SpcSocketOn Command	A command was issued to turn on an SPC device socket. Variables: username who issued the command, name of server attached to SPC device socket, SPC device location name, CCM appliance port number and SPC device socket number
SpcSocketOnSenseFail	An SPC device has detected an on sense failure for a socket. This occurs when a socket should be in the on state, but is actually in the off state. Variables: name of server attached to the SPC device socket, SPC device location name, CCM appliance port number and SPC device socket number
SpcSocketReboot Command	A command was issued to reboot an SPC power control device socket. Variables: username who issued the command, name of server attached to the SPC device socket, SPC device location name, CCM appliance port number and SPC device socket number
SpcStatusSocketOff	An SPC device socket has changed to the off state. Variables: name of server attached to the SPC device socket, SPC device location name, CCM appliance port number and SPC device socket number
SpcStatusSocketOn	An SPC power control device socket has changed to the on state. Variables: name of server attached to the SPC device socket, SPC device location name, CCM appliance port number and SPC device socket number
SpcTotalLoadHigh	An SPC device has exceeded the maximum threshold for total load amperage. Variables: SPC device location name and CCM appliance port number
SpcTotalLoadLow	The total load amperage on an SPC device has gone below the minimum threshold. Variables: SPC device location name and CCM appliance port number

Table C.1: CCM Appliance Enterprise Traps (Continued)

Trap	Description and Variable(s)
UserAdded	A new user has been added to the CCM appliance user database. Variables: initiating username and new username
UserAuthentication Failure	A user failed to authenticate with the CCM appliance. Variable: username
UserDatabaseFile Loaded	The CCM appliance has loaded a user database file. This trap applies to AVWorks software. Variables: initiating username and name of loaded file
UserDeleted	A user has been deleted from the CCM appliance user database. Variables: initiating username and deleted username
UserLocked	A user account has been locked. Variables: client IP address, locked username and reason
UserLogin	A user logged in to the CCM appliance. Variable: username
UserLogout	A user logged out of the CCM appliance. Variable: username
UserModified	A user's definition has been modified in the CCM appliance user database. Variables: initiating username and modified username
UserUnlocked	A user account has been unlocked. Variables: client IP address, initiating username, unlocked username and reason

Appendix D: NFS Error Codes and Port Status

Table D.1 describes the error codes that may be reported by the CCM appliance for NFS history file operations. Your display may also have additional descriptive information.

Table D.1: NFS Error Codes

Error Code	Description
1	An unidentified error was encountered. Check the console output for possible additional information.
2	Internal CCM mount or unmount error.
3	The file type is incompatible with the port filename.
4	A port history filename error occurred.
5	A port history file write error occurred.
6	A port history file overrun error occurred.
7	From the remote procedure call: arguments cannot be encoded.
8	From the remote procedure call: the result cannot be decoded.
9	From the remote procedure call: unable to send.
10	From the remote procedure call: unable to receive.
11	From the remote procedure call: a time-out occurred.
12	From the remote procedure call: RPS versions were incompatible.
13	From the remote procedure call: an authentication error occurred.
14	From the remote procedure call: a program was unavailable.
15	From the remote procedure call: a program/version mismatch occurred.
16	From the remote procedure call: a procedure was unavailable.
17	From the remote procedure call: the server cannot decode the arguments.
18	From the remote procedure call: a remote system error occurred.
19	From the remote procedure call: an unknown host was encountered.
20	From the remote procedure call: a port mapper failure occurred.
21	From the remote procedure call: the program was not registered.
22	From the remote procedure call: the RPC failed due to an unspecified error.
23	From the remote procedure call: an unknown protocol was encountered.

Table D.1: NFS Error Codes (Continued)

Error Code	Description
24	From the remote procedure call: an unspecified error occurred.
25	From the remote procedure call: the remote address was unknown.
26	From the remote procedure call: an unspecified error occurred.
27	From the remote procedure call: broadcasting is not supported.
28	From the remote procedure call: the name-to-address translation failed.
29	From the remote procedure call: an unspecified error occurred.
30	From the remote procedure call: an asynchronous error occurred.
31	From the remote procedure call: an asynchronous error occurred.
32	The operation was not permitted.
33	No such file or directory could be located.
34	An I/O error occurred.
35	No such device or address could be located.
36	A bad file number was encountered.
37	Out of memory.
38	Permission was denied.
39	The file already exists.
40	A cross-device link was encountered.
41	No such device could be located.
42	The specification is not a directory.
43	The specification is a directory.
44	An invalid argument was encountered.
45	The file was too large.
46	There is no space left on the device.
47	This is a read-only file system.
48	There were too many links.
49	The network is down.

Table D.1: NFS Error Codes (Continued)

Error Code	Description
50	The network is unreachable.
51	The network dropped the connection because of a reset.
52	The software caused a connection abort.
53	The connection was reset by a peer.
54	No buffer space is available.
55	The transport endpoint is already connected.
56	The transport endpoint is not connected.
57	Cannot send after a transport endpoint shutdown.
58	The connection timed-out.
59	The connection was refused.
60	The host is down.
61	There is no route to the host.
62	A stale NFS file handle was encountered.
63	The operation was not allowed because the caller is either not a privileged user (root) or not the owner of the operation's target.
64	The specified file or directory name does not exist.
65	A hard I/O error (such as a disk error) occurred while processing the requested operation.
66	The specified device or address does not exist.
67	The operation was not allowed because the caller does not have the correct permission to perform the requested operation. (This error differs from error 63, which is restricted to owner or privileged user permission failures.)
68	The specified file already exists.
69	For NFSv3: an attempt was made to perform a cross-device hard link. For NFSv4: an attempt was made to perform an operation between different FSIDs.
70	The specified device could not be located.
71	The caller specified a non-directory in a directory operation.
72	The caller specified a directory in a non-directory operation.

Table D.1: NFS Error Codes (Continued)

Error Code	Description
73	An invalid argument or unsupported argument was supplied for an operation. For example, attempting a READLINK on an object other than a symbolic link. NFSv3 example: attempting to SETATTR with a time field on a server that does not support the operation. NFSv4 example: specifying a value for an enum field that is not defined in the protocol (such as nfs_ftype4).
74	For NFSv2: The operation caused a file to grow beyond the server's limit. For NFSv3 and NFSv4: The operation would have caused a file to grow beyond the server's limit.
75	For NFSv2: The operation caused the server's file system to reach its limit. For NFSv3 and NFSv4: The operation would have caused the server's file system to exceed its limit.
76	For NFSv2: A write operation was attempted on a read-only file system. For NFSv3 and NFSv4: A modifying operation was attempted on a read-only file system.
77	For NFSv3 and NFSv4: Too many hard links exist.
78	The filename in the operation was too long.
79	An attempt was made to remove a directory that was not empty.
80	For NFSv2: The client's disk quota on the server has been exceeded. For NFSv3 and NFSv4: The user's resource limit on the server has been exceeded.
81	The file handle specified in the arguments was invalid - it either no longer exists or access to it has been revoked.
82	The file handle specified in the arguments referenced a file on a nonlocal file system on the server (that is, there were too many levels of remote in the path).
83	The server's write cache used in the WRITECACHE call was flushed to the disk.
84	The file handle failed internal consistency checks.
85	An update synchronization mismatch was detected during a SETADDR operation.
86	For NFSv3, the READDIR or READDIRPLUS cookie is stale. For NFSv4, the READDIR cookie is stale.
87	The operation is not supported.
88	For NFSv3: the buffer or request is too small. For NFSv4: the encoded response to a READDIR request exceeds the size limit set by the initial request.
89	An error occurred n the server which does not map to any of the legal NFS protocol error values. The client should translate this into an appropriate error. UNIX clients may choose to translate this to EIO.
90	An attempt was made to create an object of a type not supported by the server.

Table D.1: NFS Error Codes (Continued)

Error Code	Description
91	The server initiated the request, but was not able to complete in a timely manner. The client should wait and then try the request with a new RPC transaction ID. For example, this error should be returned from a server that supports hierarchical storage and receives a request to process a file that has been migrated. In this case, the server should start the immigration process and respond to the client with the error. For NFSv4: this error may also occur when a necessary delegation recall makes processing a request in a timely manner impossible.
92	The attributes compared were the same as provided in the client's request. This error is returned by the NVERIFY operation.
93	An attempt to lock a file was denied. Since this may be a temporary condition, the client is encouraged to retry the lock request until the lock is accepted.
94	A lease has expired that is being used in the current operation.
95	A read or write operation was attempted on a locked file.
96	The server is in its recovery or grace period, which should match the server's lease period.
97	The file handle provided is volatile and has expired at the server.
98	At attempt to OPEN a file with a share reservation has failed because of a share conflict.
99	The security mechanism being used by the client for the operation does not match the server's security policy. The client should change the security mechanism being used and retry the operation.
100	The SETCLIENTID operation has found that a client ID is already in use by another client.
101	The server has exhausted available resources while processing the COMPOUND procedure, and cannot continue processing operations within the COMPOUND procedure.
102	The file system that contains the current file handle object has been relocated or migrated to another server. The client may determine the new file system location by obtaining the *fs_locations* attribute for the current file handle.
103	The logical current file handle value (or the saved file handle value in the case of RESTOREFH) has not been properly set. This may have resulted from a malformed COMPOUND operation (that is, no PUTFH or PUTROOTFH before an operation that requires the current file handle to be set).
104	The server has received a request that specifies an unsupported minor version. The server must return a COMPOUND4res with a zero length operation result array.
105	A client ID not recognized by the server was used in a locking or SETCLIENTID_CONFIRM request.
106	A state ID generated by an earlier server instance was used.
107	A state ID that designates the locking state for a lockowner-file at an earlier time was used.

Table D.1: NFS Error Codes (Continued)

Error Code	Description
108	A state ID generated by the current server instance (that does not designate any locking state either current or superseded) for a current lockowner-file pair was used.
109	The sequence number in a locking request is neither the next expected number nor the last number processed.
110	The attributes compared were not the same as provided in the client's request. This error is returned by the VERIFY operation.
111	A lock request is operating on a sub-range of a current lock for the lock owner and the server does not support this type of request.
112	The current file handle provided for a LOOKUP is not a directory but a symbolic link. This error is also issued if the final component of the OPEN path is a symbolic link.
113	The RESTOREFH operation does not have a saved file handle (identified by SAVEFH) to operate on.
114	A lease being renewed is associated with a file system that has been migrated to a new server.
115	A specified attribute is not supported by the server. This does not apply to the GETATTR operation.
116	A reclaim of the client state has fallen outside of the server's grace period. As a result, the server cannot guarantee that a conflicting state has not been provided to another client.
117	The reclaim provided by the client does not match any of the server's state consistency checks and is bad.
118	The reclaim provided by the client has encountered a conflict and cannot be provided. This could indicate a misbehaving client.
119	The server encountered an XDR decoding error while processing an operation.
120	A CLOSE was attempted and file locks would exist after the CLOSE.
121	The client attempted a READ, WRITE, LOCK or SETATTR operation that was not sanctioned by the state ID passed (for example, writing to a file opened only for reading).
122	An owner, owner group or ACL attribute value cannot be translated to local representation.
123	A UTF-8 string contains a character that is not supported by the server in the context in which it is being used.
124	A name string in a request contains valid UTF-8 characters supported by the server, but the name is not supported by the server as a valid name for the current operation.
125	The range for a LOCK, LOCKT or LOCKU operation is not appropriate for the allowable range of offsets for the server.
126	The server does not support the atomic upgrade or downgrade of locks.

Table D.1: NFS Error Codes (Continued)

Error Code	Description
127	An illegal operation value has been specified in the *arg op* field of a COMPOUND or CB_COMPOUND procedure.
128	The server determined a file locking deadlock condition for a blocking lock request.
129	The operation cannot be successfully processed because a file used in the operation is currently open.
130	Due to administrator intervention, the lock owner's record locks, share reservations and delegations have been revoked by the server.
131	The callback path is down.
132	The NFS server does not support the TCP protocol for this service. To resolve this, issue an NFS Enable command with the Protocol=UDP parameter.
9999	No error.

NFS port status values

Table D.2 describes the port status values that may be reported by the CCM appliance for NFS history file operations.

Table D.2: NFS Port Status Values

Value	Description
1	Mount needed
2	Error opening history file - still retrying
3	Error opening history file - gave up
4	Current write error encountered (on most recent write to file)
5	Recent write error encountered (most recent write succeeded)
6	Current overrun encountered and no recent write errors have occurred (unable to write to the file fast enough)
7	Recent overrun encountered and no recent write errors have occurred (unable to write to the file fast enough)
9999	No recent errors

Appendix E: Ports Used

Table E.1 lists the UDP and TCP port numbers used by the CCM appliance and the attached servers/devices. The values assume a default configuration; some values are configurable.

Table E.1: Ports Used by CCM Appliance

Port Type and Number	Direction	Used for
TCP 22	Inbound on appliance	SSH2, if enabled
TCP 23	Inbound on appliance	Telnet
UDP 69	Inbound on appliance and outbound on device	TFTP
TCP/UDP 111	Outbound on device	NFS, if enabled
UDP 123	Outbound on device	NTP, if enabled
UDP 161	Inbound on appliance	SNMP, if enabled
TCP/UDP 2049	Outbound on device	NFS, if enabled
UDP 3211	Inbound on appliance	Secure protocol used by AVWorks software
TCP 3211	Inbound on appliance	Secure protocol used by AVWorks software
TCP 3001-30xx	Inbound on appliance	Telnet serial sessions with ports
TCP 3101-31xx	Inbound on appliance	SSH serial sessions with ports

Appendix F: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service.

To resolve an issue:

1. Check the pertinent section of the manual to see if the issue can be resolved by following the procedures outlined.
2. Check our web site at www.avocent.com/support to search the knowledge base or use the on-line service request.
3. Call the Avocent Technical Support location nearest you.

INDEX

H

I

L

M

N

P

Q

R

S

T

U

Avocent®

The Power of Being There®

For Technical Support:

Email: support@avocent.com
www.avocent.com

Avocent Corporation
4991 Corporate Drive
Huntsville, Alabama 35805-6201 USA
Tel: +1 256 430 4000
Fax: +1 256 430 4031

Avocent International Ltd.
Avocent House, Shannon Free Zone
Shannon, County Clare, Ireland
Tel: +353 61 715 292
Fax: +353 61 471 871

Avocent Asia Pacific
Singapore Branch Office
100 Tras Street, #15-01
Amara Corporate Tower
Singapore 079027
Tel: +656 227 3773
Fax: +656 223 9155

Avocent Germany
Gottlieb-Daimler-Straße 2-4
D-33803 Steinhagen
Germany
Tel: +49 5204 9134 0
Fax: +49 5204 9134 99

Avocent Canada
20 Mural Street, Unit 5
Richmond Hill, Ontario
L4B 1K3 Canada
Tel: +1 877 992 9239
Fax: +1 877 524 2985

590-434-001B