

Out-of-Band Management

Note Out-of-band management requires the optional Cisco network management module (NMM).

This chapter describes how to manage your hub or hub stack using the management console.

Managing Your Hub or Hub Stack

Note To understand how the type of hub connection used in the installation plays a role in managing the hub stack, see the “Building a Hub Stack” section in the “Installing the FastHub” chapter.

It is important to understand that you can manage the hub stack at three levels:

- Port (Port Configuration menu and Port Statistics Report)
At the port level, you can enable or disable ports and examine individual port statistics to monitor individual-user or workgroup traffic.
- Unit (Unit Configuration menu, Unit Statistics Report, Unit Addressing Report)
At the unit level, you can select any unit within the hub stack and examine the unit’s port statistic totals to monitor network traffic through the unit.

Configuring the FastHub Console Port for Terminal or Modem Connection

- Hub stack (Stack (RMON) Statistics Report)

At the hub-stack level, you can examine the entire hub stack's statistics to monitor the total traffic passing through the hub stack.

Configuring the FastHub Console Port for Terminal or Modem Connection

Note See the section “Connecting to a Terminal or Modem” in the “Installing the FastHub” chapter for information on connecting the terminal or modem.

The FastHub console port must be configured to the same baud rate and character format as the terminal or modem. Although the match-baud-rate option (auto baud, configured through the Console Port menu) matches the baud rate when the FastHub is answering an incoming call, the FastHub does not change from its configured rate when dialing out. In addition, the FastHub only matches a baud rate lower than its configured rate. When it completes a call and disconnects, the FastHub always returns to the last configured baud rate.

Following are the default characteristics for the FastHub console port:

- 9600 baud
- Eight data bits
- One stop bit
- Parity: none

Use the Console Port menu to change any defaults.

Note If you change any of the console port defaults, make sure that you also change the terminal or modem configuration.

Using the Management Console

The management console is a menu-driven interface, as shown in Figure 4-1. Management console screens include menus through which the configuration of the FastHub can be modified and menus that present network conditions and statistics.

Keyboard Characteristics

The management console has the following standard keyboard characteristics:

To move the menu cursor: Use the left, right, up, or down arrow keys.

To select a menu item: Position the cursor on the command or its parameter value and press Enter.

To move to the beginning or end of a text field: Use the Home and End keys, respectively. Use the right and left arrow keys to move the text-edit cursor.

To move to the OK and Cancel buttons: Use the Tab key.

To cancel the current menu selection and return to the Main Menu from a submenu, use the Esc key.

Accessing Online Help

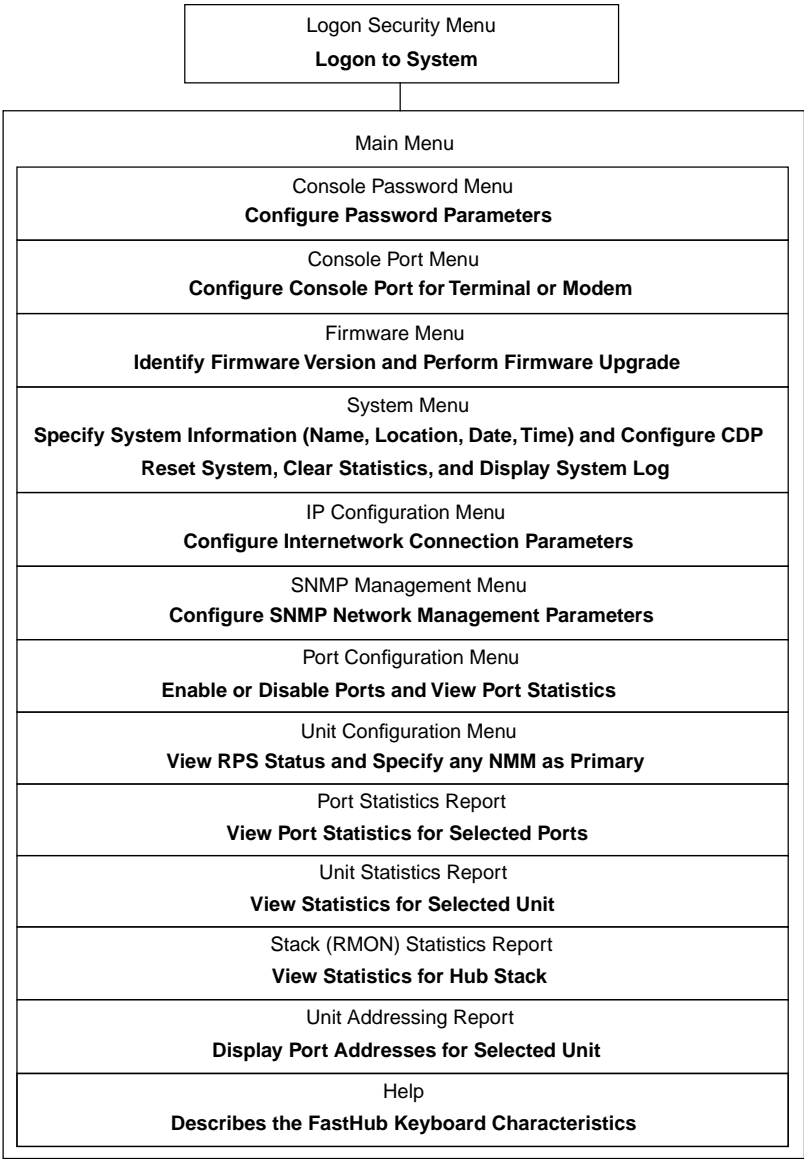
To access Help information for an item, select the item, then press either the F3 or ? key.

Unit and Port Numbering Conventions

Unit numbers shown in the management console screens reflect the actual physical positions of the units in the hub stack. The management console uses a unit numbering convention, assigning hubs unit numbers from the bottom up—the hub at the bottom of the stack is unit 1, the hub above unit 1 is unit 2, and so on.

The Port Selection and Port Statistics screens reflect the actual physical positions of the ports in each unit. The base configuration ports are numbered from 1 to 16, left to right. If a 100BaseTX/16 port expansion module is installed, its ports are numbered from 17 to 32, left to right.

Figure 4-1 Management Console Menu Screen Descriptions



NM3193

Resetting the FastHub

This section describes the various methods of resetting the FastHub.

Note Disconnecting the power cord or an expansion cable causes a reset as described in this section. These descriptions are included for informational purposes only. These are not recommended methods of resetting the system.

Through Management Console

There are three ways to reset the FastHub through the management console System menu.

- Reset system
 - Resets the FastHub hardware and firmware.
 - Does not run the NMM POST.
 - Retains all configured system parameters.
 - Clears all network-related statistics.

- Reset to factory defaults

Use this type of reset when moving the hub from one network to another or when the current configuration no longer suits your network.



Caution Resetting to factory defaults is not reversible; all system parameters revert to factory defaults, and the original configuration is irrecoverable.



Caution Resetting to factory defaults causes all ports to come up enabled. Ports that were previously disabled through “Port status” are enabled after the reset.

- Resets the FastHub hardware and firmware.
- Does not run the NMM POST.

Using the Management Console

- All configured system parameters revert to their factory defaults (see Table 4-1 for factory default settings).
- Clears all network-related statistics.
- Reset repeater
 - Resets the FastHub hardware.
 - Does not run the NMM POST.
 - Retains all configured system parameters.
 - Does not clear network-related statistics.

NMM Front-Panel Reset

The FastHub can be reset through the reset button on the NMM front panel.

- Resets the FastHub hardware and firmware.
- Runs the NMM POST.
- Retains all configured system parameters.
- Clears all network-related statistics.

Unplugging Power Cord

Unplugging the FastHub rear-panel power cord initiates a reset.

- Resets the FastHub hardware and firmware.
- Runs the NMM POST.
- Retains all configured system parameters.
- Clears all network-related statistics.

Disconnecting Expansion Cable

Disconnecting any FastHub rear-panel expansion cable connection initiates a reset.

- Resets the FastHub hardware.
- Does not run the NMM POST .

- Retains all configured system parameters.
- Clears all network-related statistics.

Removing or Inserting an NMM

- Does not reset the FastHub hardware or firmware.
- Runs the NMM POST.
- Retains all configured system parameters.
- Clears all network related statistics.

Default Parameters

Table 4-1 lists management console menu items and, if applicable, their default settings. The items are listed in the sequence that they appear in the management console menu tree (see Figure 4-1).

Table 4-1 Default Configuration Settings

Menu Item	Default Setting	Management Console Menu
Password intrusion threshold	None	Console Password
Silent time upon intrusion detection	None	Console Password
Modify password	—	Console Password
Baud rate	9600	Console Port
Data bits	8	Console Port
Stop bits	1	Console Port
Parity setting	None	Console Port
Match remote baud rate (auto baud)	Enabled	Console Port
Auto answer	Enabled	Console Port
Time delay between dial attempts	300 seconds	Console Port
Number for dial-out connection	—	Console Port

Using the Management Console

Menu Item	Default Setting	Management Console Menu
Initialization string for modem	0	Console Port
Upgrade status	–	Firmware
Primary supervisor	–	Firmware
Standby supervisor	–	Firmware
Supervisor boot version	–	Firmware
Supervisor mgmt version	–	Firmware
Upgrade auto distribution	Enabled	Firmware
Server accept TFTP upgrade requests	Enabled	Firmware
Name or IP address of TFTP server	–	Firmware
Filename for firmware upgrade	–	Firmware
Initiate TFTP upgrade	–	Firmware
Initiate XMODEM upgrade	–	Firmware
Name of system	–	System
Contact name	–	System
Location	–	System
Date	–	System
Time	–	System
Management console inactivity timeout	None	System
Use Cisco Discovery Protocol (CDP)	Enabled	System
CDP message interval	60 seconds	System
Reset system	–	System
Reset to factory defaults	–	System
Reset repeater	–	System
Display Supervisor log	–	System
Display CDP neighbors	–	System
IP address of system	0.0.0.0 or no IP address	IP Configuration
IP subnet mask	0.0.0.0 or no mask	IP Configuration

Management Console Screens

Menu Item	Default Setting	Management Console Menu
IP address of default gateway	0.0.0.0 or no gateway address	IP Configuration
IP address of DNS server 1	0.0.0.0 or no IP address	IP Configuration
IP address of DNS server 2	0.0.0.0 or no IP address	IP Configuration
DNS domain name	–	IP Configuration
Use routing information protocol	Enabled	IP Configuration
READ community string	0	SNMP Management
WRITE community string	0	SNMP Management
Authentication trap generation	Enabled	SNMP Management
Write manager names	0	SNMP Management
Trap manager names	0	SNMP Management
Trap manager community strings	0	SNMP Management
Port name	–	Port Configuration
Port status (port enabled or disabled)	Enabled	Port Configuration
RPS status	–	Unit Configuration
Power source	–	Unit Configuration
Supervisor	–	Unit Configuration
Boot version	–	Unit Configuration
Mgmt version	–	Unit Configuration
Current Primary Supervisor is unit	–	Unit Configuration
Clear statistics	–	Stack (RMON) Statistics Report

Management Console Screens

This section describes the management console screens.

Management Console Screens

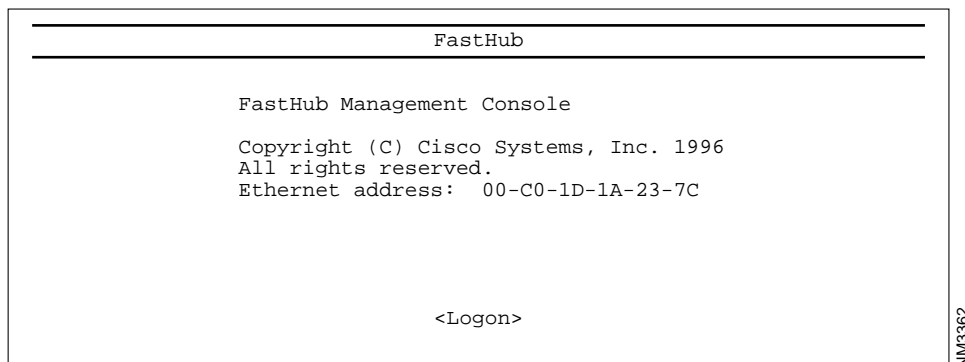
Note Depending on your system configuration, the actual screens might appear different from what is presented here.

Logging On to the Management Console

Although you can assign a password to limit access to the management console, it is not required (the password prompt does not display if a password has not been assigned).

To logon (see Figure 4-2), select Logon, and press Return. The Main Menu is displayed.

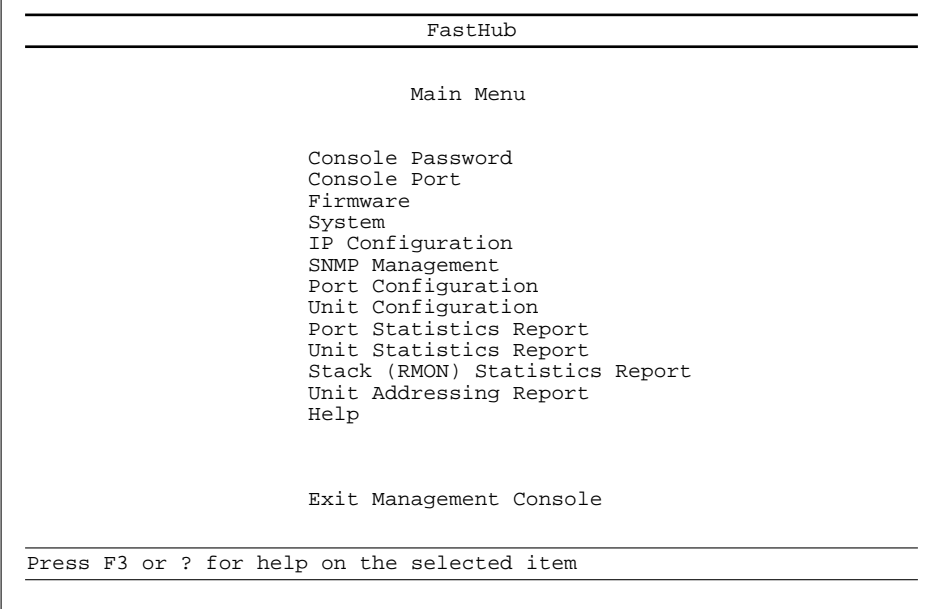
Figure 4-2 Logon Screen



NM3362

Main Menu

Select one of the Main Menu items (see Figure 4-3), and press Return. Selecting the Exit Management Console option returns you to the Logon Security Menu. The other menu options are described in the following sections.

Figure 4-3 Main Menu

The screenshot shows a terminal window titled "FastHub" with a "Main Menu". The menu items are: Console Password, Console Port, Firmware, System, IP Configuration, SNMP Management, Port Configuration, Unit Configuration, Port Statistics Report, Unit Statistics Report, Stack (RMON) Statistics Report, Unit Addressing Report, and Help. At the bottom, there is an option to "Exit Management Console" and a prompt to "Press F3 or ? for help on the selected item".

```
FastHub

Main Menu

Console Password
Console Port
Firmware
System
IP Configuration
SNMP Management
Port Configuration
Unit Configuration
Port Statistics Report
Unit Statistics Report
Stack (RMON) Statistics Report
Unit Addressing Report
Help

Exit Management Console

Press F3 or ? for help on the selected item
```

NM3363

Console Password Menu

Use the Console Password menu (see Figure 4-4) to configure the management console logon parameters.

Figure 4-4 Console Password Menu

```
FastHub

Console Password

Password intrusion threshold      [None ]
Silent time upon intrusion detection [None ]
Modify password                  [      ]

< Exit >

Press F3 or ? for help on the selected item
```

NM3364

Password intrusion threshold. Enter the number of failed logon attempts allowed before the management console shuts down for a configured duration.

Silent time upon intrusion detection. Enter the number of minutes during which the management console is unavailable after password intrusion threshold has been exceeded.

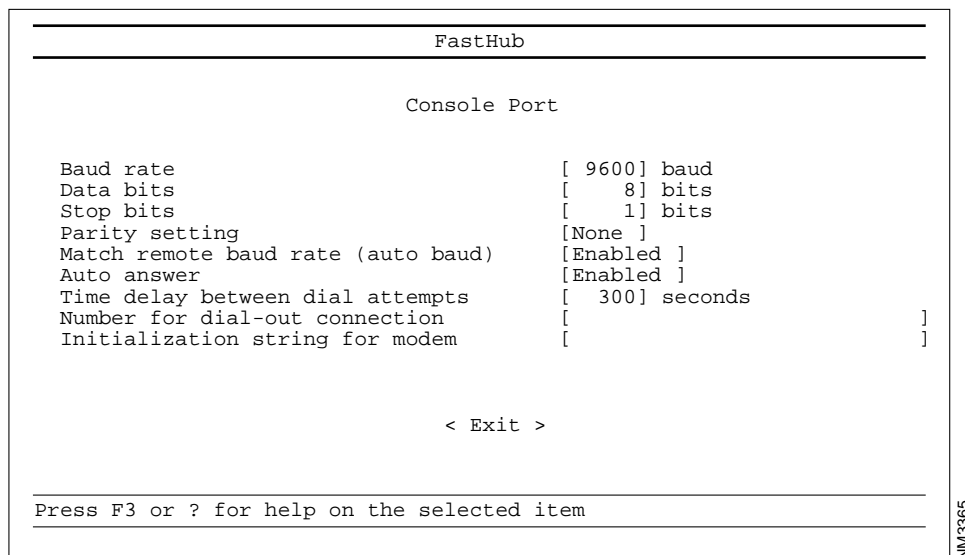
Modify password. Change your logon password.

Exit. Return to Main Menu.

Console Port Menu

Use the Console Port menu (see Figure 4-5) to configure the NMM console port.

Figure 4-5 Console Port Menu



The screenshot shows a terminal window titled "FastHub" with a "Console Port" menu. The menu lists several configuration options with their current values in brackets. At the bottom, there is an "< Exit >" option and a footer instruction "Press F3 or ? for help on the selected item".

FastHub	
Console Port	
Baud rate	[9600] baud
Data bits	[8] bits
Stop bits	[1] bits
Parity setting	[None]
Match remote baud rate (auto baud)	[Enabled]
Auto answer	[Enabled]
Time delay between dial attempts	[300] seconds
Number for dial-out connection	[]
Initialization string for modem	[]
< Exit >	
Press F3 or ? for help on the selected item	

NM/3365

Baud rate. Enter the signal speed for the console port.

Data bits. Enter the number of data bits for the console port.

Stop bits. Enter the number of stop bits for the console port.

Parity setting. Enter the parity setting for the console port.

Match remote baud rate (auto baud). Enable or disable auto-baud detect for the console port. When enabled, the console port automatically determines the baud rate of an incoming call and switches to that baud rate.

Auto answer. Enable or disable auto-answer for the console port. When auto-answer is enabled, the system automatically answers incoming calls on a modem attached to the console port.

Management Console Screens

Time delay between dial attempts. Enter the time in seconds that the management console delays before each attempted dial-out connection.

Number for dial-out connection. Enter the number used for dial-out connection.

Initialization string for modem. Enter a modem initialization string.

Exit. Return to Main Menu.

Firmware Menu

Use the Firmware menu (see Figure 4-6) to display system firmware version levels, identify which unit houses the primary NMM, and perform firmware upgrades.

Figure 4-6 Firmware Menu

```
FastHub

Firmware

Upgrade status: Factory installed
Primary supervisor: Unit 1 Boot version: 0.10 Management version: 1.00

Server accept TFTP upgrade requests      [Enabled ]
Name or IP address of TFTP server        [           ]
Filename for firmware upgrades           [           ]

Actions
-----
Initiate TFTP upgrade
Initiate XMODEM upgrade

< Exit >

Press F3 or ? for help on the selected item
```

NM3366

Upgrade status. Displays the date and time of the last firmware upgrade and the IP address of the TFTP server where the upgrade file resided. Also indicates whether the upgrade was successful.

Primary supervisor. Identifies which unit in the hub stack houses the NMM serving as the primary supervisor.

Boot version. Displays the version number of the bootstrap firmware on the primary NMM.

Management version. Displays the version number of the management firmware on the primary NMM.

Server accept TFTP upgrade requests. This is the first of three items used to configure a Trivial File Transfer Protocol (TFTP) upgrade. The TFTP upgrade is the in-band upgrade method discussed in detail in the *Catalyst FastHub 100+ Series MIB Reference Manual*. Use this item to specify whether the FastHub accepts TFTP write requests from the management console.

Name or IP address of TFTP server. This is the second of three items used to configure a TFTP upgrade. Use this item to name the TFTP server from which the firmware file is downloaded.

Filename for firmware upgrade. This is the third item used to configure a TFTP upgrade. Use this item to specify the name of the firmware upgrade file downloaded from the server.

Initiate TFTP upgrade. Initiate the TFTP upgrade process. Note that the second confirmation prompt allows you to verify the upgrade file path, filename, and the server address.

Initiate XMODEM upgrade. Initiate an out-of-band firmware upgrade. The XMODEM protocol is used to perform this upgrade.

Exit. Return to Main Menu.

System Menu

Use the System menu (see Figure 4-7) to do the following:

- Designate system name and location and network administrator name
- Set system date and time
- Specify management console timeout period
- Configure Cisco Discovery Protocol (CDP) and display CDP neighbor
- Reset the system
- Display Supervisor log information

Figure 4-7 System Menu

```
FastHub
-----
System

Name of system          [                ]
Contact name            [                ]
Location                [                ]
Date                   [Jan 22 2010 ]
Time                   [20:39:34]
Management Console inactivity timeout [None   ]
Use Cisco Discovery Protocol (CDP)    [Enabled ]
CDP message interval   [  60] seconds

                        Actions
-----
Reset system           Reset repeater
Reset to factory defaults Display Supervisor log
Display CDP neighbors

                        < Exit >

-----
Press F3 or ? for help on the selected item
-----
```

NM3367

Name of system. Enter a name for the system.

Contact name. Enter the name of the person or organization responsible for administering the system.

Location. Enter the location of the system.

Date. Set the system date.

Time. Set the system time.

Management console inactivity timeout. Enter the number of minutes that the management console can go without activity, after which it will be unavailable and password needs to be reentered.

Cisco Discovery Protocol (CDP) status. Enable or disable CDP on this hub or hub stack. Using CDP, the FastHub can advertise its existence to other devices and receive information about other devices on the same LAN.

CDP message interval. Enter the interval in seconds that CDP messages are generated on this hub or hub stack.

Reset system. Resets the FastHub hardware and firmware, does not run the NMM POST, retains all configured system parameters, and clears all network related statistics.

Reset to factory defaults. Resets the FastHub hardware and firmware, does not run the NMM POST, changes all configured system parameters to their factory defaults, and clears network related statistics.

Reset repeater. Resets the FastHub hardware, does not run the NMM POST, retains all configured system parameters, and retains all network related statistics.

Display Supervisor log. Displays supervisor log information.

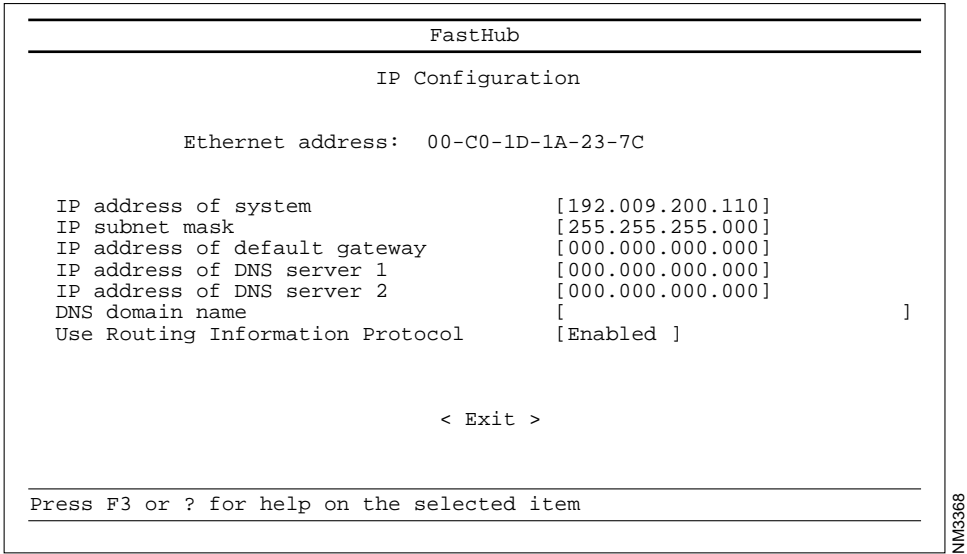
Display CDP neighbors. Displays CDP cache information.

Exit. Return to Main Menu.

IP Configuration Menu

Use the Internet Protocol (IP) Configuration menu (see Figure 4-8) to configure internetwork connection parameters.

Figure 4-8 IP Configuration Menu



- Ethernet address.** Displays the Ethernet address of the system.
- IP address of system.** Enter the system IP address.
- IP subnet mask.** Enter a subnet mask for the system.
- IP address of default gateway.** Enter the IP address of the default gateway.
- IP address of DNS server 1.** Enter the IP address of Domain Name System (DNS) server 1.
- IP address of DNS server 2.** Enter the IP address of DNS server 2.
- DNS domain name.** Enter the DNS domain name.

Use Routing Information Protocol. Enable or disable the Routing Information Protocol (RIP) listener. The RIP listener automatically discovers IP gateways.

Exit. Return to Main Menu.

SNMP Management Menu

Use the SNMP Management menu (see Figure 4-9) to configure SNMP network management parameters. The read and write community strings are used by the SNMP agent to control requests for information about, and access to, management information for the repeater.

Figure 4-9 SNMP Management Menu

FastHub			
SNMP Management			
READ community string	[*****]
WRITE community string	[*****]
Authentication trap generation	[Enabled]
Write manager names:			
[]	[]
TRAP manager names:			
[]	[]
TRAP manager community strings:			
[]	[]
< Exit >			
Press F3 or ? for help on the selected item			

NM3369

Management Console Screens

READ community string. Enter the SNMP-agent read (Get) community string. The community string serves as a password to authenticate messages sent between the FastHub and the SNMP agent.

WRITE community string. Enter the SNMP-agent write (Set) community string. The community string serves as a password to authenticate messages sent between the FastHub and the SNMP agent.

Authentication trap generation. Enable or disable the generation of SNMP authentication traps. An authentication trap alerts a management workstation of SNMP requests that do not carry a valid read (Get) or write (Set) community string.

Write manager names. Identify which management workstations are allowed to issue write (Set) requests to the FastHub. Either the name or IP address of the management workstation can be entered. You can define up to four workstations. If no name or address is defined, then any management workstation can set the MIB objects.

Trap manager names. Identify which management workstations receive SNMP traps (alerts) from the FastHub. Either the name or IP address of the management workstation can be entered. You can define up to four workstations. If no name or IP address is defined, the FastHub does not send any traps.

Trap manager community strings. Enter the community string that accompanies an SNMP trap sent to each trap management workstation. The community string serves as a password to authenticate messages sent between the FastHub and the management workstation.

Exit. Return to Main Menu.

Port Configuration Menu

When you select the Port Configuration menu, first the Port Selection screen (see Figure 4-10) is displayed. Enter the desired unit number and port number. If port 1 on unit 1 was selected, the following Port Configuration menu (see Figure 4-11) is displayed.

Use the Port Configuration menu to enable or disable ports and display port statistics.

Note To enable or disable the uplink port or view uplink port statistics, select port 16 from the Port Selection screen.

Figure 4-10 Port Selection Screen

FastHub																		
Port Selection																		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	UNIT	3	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	UNIT	2	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Mgmt	UNIT	1

Select unit number: [1]
 Select port number: [1]

NM3372

Figure 4-11 Port Configuration Menu

FastHub		
Port Configuration - Port 1 on unit 1		
Port linkbeat status	No-linkbeat	
Port autopartition status	Not-autopartitioned	
Port connector type	RJ45	
Last source address	Unaddressed	
Source address changes	0	
Port name	[]	
Port status	[Enabled]	
<Previous port>	<Next port>	<Goto port...>
<Port statistics>	<Unit configuration>	< Exit >
Press F3 or ? for help on the selected item		

NM3370

Management Console Screens

Port linkbeat status. Indicates whether link pulses are being received by this port.

Port autopartition status. Indicates whether the port is currently autopartitioned. Autopartitioned ports are automatically reconnected when the fault is rectified. Frequent partitions can indicate that the port is not terminated correctly or a connected device is faulty.

Port connector type. Indicates the port connector type.

Last source address. Indicates the MAC address of the last frame received at this port.

Source address changes. Indicates the number of different source addresses received at this port.

Port name. Enter a name for a designated port.

Port status. Enable or disable the port. A disabled port does not transmit or receive.

Previous port. Go to the Port Configuration screen for the port numerically before this port.

Next port. Go to the Port Configuration screen for the port numerically after this port.

Goto port.... Go to the Port Configuration screen for a specific port.

Port statistics. View the Port Statistics Report for the currently selected port. The Port Statistics Report presents frame transmit and receive statistics. See the “Port Statistics Report” section in this chapter.

Unit configuration. Go to the Unit Configuration menu.

Exit. Return to Main Menu.

Unit Configuration Menu

Use the Unit Configuration menu (see Figure 4-12) to do the following:

- View redundant power supply (RPS) status
- Identify whether individual hub stack units are powered by the RPS or FastHub internal power supply
- Identify the units housing the primary NMM and standby NMM
- Specify a unit’s NMM as the primary NMM
- Display the primary NMM bootstrap and management firmware version numbers.

Figure 4-12 Unit Configuration Menu

FastHub				
Unit Configuration				
	Unit 1	Unit 2	Unit 3	Unit 4
RPS status	Failure	Failure	Not present	Not present
Power source	Internal	Internal	Internal	Internal
Supervisor	Primary			
Boot version	1.10			
Mgmt version	1.10			
Main board	0.00			
Expansion board	0.00	0.00	0.00	0.00

Select Primary Supervisor unit [1]

<Port configuration> <Unit addressing> < Exit >

Press F3 or ? for help on the selected item

NM3371

RPS status. Indicates whether an RPS is present and operational.

Power source. Indicates whether the power source is an RPS or the FastHub internal power supply.

Supervisor. Displays the unit number of the unit with the primary NMM.

Boot version. Displays the version number of the bootstrap firmware on the primary NMM.

Mgmt version. Displays the version number of the management firmware on the primary NMM.

Main board. Displays the revision number of the main board.

Expansion board. Displays the revision number of the port expansion module.

Select Primary Supervisor unit. Identify a unit's NMM as the primary NMM.

Port configuration. Go to Port Configuration menu (via Port Selection screen).

Unit addressing. Go to the Unit Addressing Report.

Exit. Return to Main Menu.

Port Statistics Report

When you select the Port Statistics Report, first the Port Selection screen (see Figure 4-13) is displayed. Enter the desired unit number and port number. If port 1 on unit 1 was selected, the following Port Statistics Report screen (see Figure 4-14) is displayed.

Use the Port Statistics Report selection to display port statistics for individual ports. The Port Statistics Report presents frame transmit and receive statistics. You cannot modify any parameters through this report.

Figure 4-13 Port Selection Screen

FastHub

Port Selection

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----

UNIT
3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----

UNIT
2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Mgmt
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	------

UNIT
1

Select unit number: [1]

Select port number: [1]

NM3372

Figure 4-14 Port Statistics Report

FastHub			
Port Statistics Report - Port 1 on unit 1			
<u>Receive Statistics</u>			
Total good frames	0	Runts	0
Total good octets	0	Collisions	0
Source address changes	0		
	0		
<u>Receive Errors</u>			
Autopartitions	0	Late collisions	0
Alignment errors	0	Jabber errors	0
FCS errors	0	Isolates	0
Frames too long	0	False carriers	0
Symbol errors	0	Short events	0
Data rate mismatches	0		
<div> <div><Previous port></div> <div><Next port></div> <div><Goto port...></div> </div> <div> <div><Port configuration></div> <div><Unit statistics></div> <div>< Exit ></div> </div>			
Press F3 or ? for help on the selected item			

NM3373

Receive Statistics

Total good frames. Total number of readable frames received by the port.

Total good octets. Total number of octets (bytes) received as part of good frames by the port.

Source address changes. Number of different source addresses received at this port.

Runts. Frames that are smaller than the minimum frame size for IEEE-802.3 standard frames. Runt frames typically are caused by collision fragments and are propagated through the network (runts are a normal part of IEEE 802.3 networks). If the number of runt frames exceeds the number of collisions, there is a problem with a transmitting device. Some protocols can also cause runt frames.

Collisions. Occur when two devices attempt to transmit at the same time (collisions are a normal part of 802.3 networks). If the collision count suddenly increases without an accompanying general increase in network traffic, you probably have a faulty device on your network. Check port collision statistics to find the port with the largest number of collisions. Ensure that the device connected to this port is operational and not in full-duplex mode.

Receive Errors

Autopartitions. Number of times the unit has automatically partitioned the segment attached to this port. Autopartitioned ports are automatically reconnected when the fault is rectified. Frequent partitions indicate that the port is not terminated correctly or that a connected device is faulty.

Alignment errors. Total number of alignment errors at the port. Alignment errors occur if all bytes are not received whole. Check the cable and the connected device. Verify the network configuration; see the “Making Network Connections” chapter, and ensure that cabling distances have not been exceeded and that the number of repeaters in the network does not exceed the maximum allowed.

FCS errors. Frame Check Sequence errors indicating that frames of data are being corrupted during transmission; this number should be a very small percentage of the total data traffic. Check the cable and the connected device. Verify the network configuration; see the “Making Network Connections” chapter, and ensure that cabling distances have not been exceeded and that the number of repeaters in the network does not exceed the maximum allowed.

Frames too long. Frames that exceed the maximum size for 802.3 frames. The frame might have been corrupted during transmission. Some network protocols can cause these frames.

Symbol errors. Total number of frames of valid length with at least one occurrence of an invalid data symbol.

Data rate mismatches. Number of frames whose timing no longer matches the transmit frequency. Check the transmitting device.

Late collisions. Collision outside the collision domain. These might occur if you have an oversized network or a segment that is longer than prescribed in 802.3. Verify the network configuration; see the “Making Network Connections” chapter and ensure that cabling distances have not been exceeded and that the number of repeaters in the network does not exceed the maximum allowed.

Jabber errors. Occur when data packets exceed the lengths prescribed in 802.3. Check port collision statistics to find the port with the largest number of jabber errors. Ensure that the device connected to this port is operational and that the connecting cable is not faulty.

Isolates. The number of times the port automatically isolates due to false carrier events. This is generally caused by a faulty cable.

False carriers. This statistic is generated when port cables are connected or disconnected, or when connected devices are powered on and off. It can also indicate a faulty cable.

Short events. Short events are smaller than runt frames. They often indicate network problems caused by externally generated noise. Check cable routing and reroute as necessary.

Previous port. Go to the Port Statistics Report for the port numerically before this port.

Goto port.... Go to the Port Statistics Report for a specific port.

Next port. Go to the Port Statistics Report for the port numerically after this port.

Port configuration. Go to the Port Configuration menu for the current port.

Unit statistics. View the Unit Statistics Report for frame transmit and receive statistics for the current unit. See the “Unit Statistics Report” section in this chapter.

Exit. Return to Main Menu.

Unit Statistics Report

When you select the Unit Statistics Report, first the Unit Selection screen (see Figure 4-15) is displayed. Enter the desired unit number. If unit 1 was selected, the following Unit Statistics Report screen (see Figure 4-16) is displayed.

Management Console Screens

Use the Unit Statistics Report selection to display port statistics for individual units. The Unit Statistics Report presents frame transmit and receive statistics. You cannot modify any parameters through this report.

Note If there is only one unit in the configuration, the Unit Selection screen (see Figure 4-15) does not display.

Figure 4-15 Unit Selection Screen

FastHub

Unit Selection

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----

UNIT 3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----

UNIT 2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Mgmt
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	------

UNIT 1

Select unit number: [1]

NM3374

Figure 4-16 Unit Statistics Report

FastHub			
Unit Statistics Report - unit 1 (16 ports)			
<u>Receive Statistics</u>			
Total good frames	287476845	Runts	22
Total good octets	4045611357	Collisions	0
Source address changes	0		
	0		
<u>Receive Errors</u>			
Autopartitions	0	Late collisions	0
Alignment errors	3734	Jabber errors	0
FCS errors	0	Isolates	0
Frames too long	0	False carriers	0
Symbol errors	0	Short events	0
Data rate mismatches	0		
<div> <div><Previous unit></div> <div><Next unit></div> <div><Goto unit...></div> </div> <div> <div><Port statistics></div> <div><RMON statistics></div> <div>< Exit ></div> </div>			
Press F3 or ? for help on the selected item			

NM3375

Receive Statistics

Total good frames. Total number of readable frames received by the unit.

Total good octets. Total number of octets (bytes) received as part of good frames by the unit.

Source address changes. Number of different source addresses received by this unit.

Runts. Frames that are smaller than the minimum frame size for 802.3 frames. Runt frames are typically caused by collision fragments and are propagated through the network (runts are a normal part of 802.3 networks). If the number of runt frames exceeds the number of collisions, there is a problem with a transmitting device. Some protocols can also cause runt frames.

Collisions. Occur when two devices attempt to transmit at the same time (collisions are a normal part of 802.3 networks). If the collision count suddenly increases without an accompanying general increase in network traffic, you probably have a faulty device on your network. Check port collision statistics to find the port with the largest number of collisions. Ensure that the device connected to this port is operational and not in full duplex mode.

Receive Errors

Autopartitions. Number of times the unit has automatically partitioned the segments attached to its ports. Autopartitioned ports are automatically reconnected when the fault is rectified. Frequent partitions indicate that a port is not terminated correctly or a connected device is faulty.

Alignment errors. Total number of alignment errors at the unit. Alignment errors occur if all bytes are not received whole. Check the cable and the connected device. Verify the network configuration; see the “Making Network Connections” chapter, and ensure that cabling distances have not been exceeded and that the number of repeaters in the network does not exceed the maximum allowed.

FCS errors. Frame Check Sequence errors indicating that frames of data are being corrupted during transmission; this number should be a very small percentage of the total data traffic. Check the cable and the connected device. Verify the network configuration; see the “Making Network Connections” chapter, and ensure that cabling distances have not been exceeded and that the number of repeaters in the network does not exceed the maximum allowed.

Frames too long. Frames that exceed the maximum size for 802.3 frames. The frame might have been corrupted during transmission. Some network protocols can cause these frames.

Symbol errors. Total number of frames of valid length with at least one occurrence of an invalid data symbol.

Data rate mismatches. Number of frames whose timing no longer matches the transmit frequency. Check the transmitting device.

Late collisions. Collisions outside the collision domain. These might occur if you have an oversized network or a segment that is longer than prescribed in 802.3. Verify the network configuration; see the “Making Network Connections” chapter, and ensure that cabling distances have not been exceeded and that the number of repeaters in the network does not exceed the maximum allowed.

Jabber errors. Occur when data packets exceed the lengths prescribed in 802.3. Check port collision statistics to find the port with the largest number of jabber errors. Ensure that the device connected to this port is operational and that the connecting cable is not faulty.

Isolates. Number of times the unit ports automatically isolate due to consecutive false carrier events. This is generally caused by a faulty cable.

False carriers. This statistic is generated when port cables are connected or disconnected, when connected devices are powered on and off, or it might indicate a faulty cable.

Short events. Short events are smaller than runt frames. They could indicate network problems caused by externally generated noise. Check cable routing and reroute as necessary.

Previous unit. Go to the Unit Statistics Report for the unit numerically before this unit.

Next unit. Go to the Unit Statistics Report for the unit numerically after this unit.

Goto unit.... Go to the Unit Statistics Report for a specific unit.

Port statistics. Go to the Port Statistics Report (via the Port Selection screen).

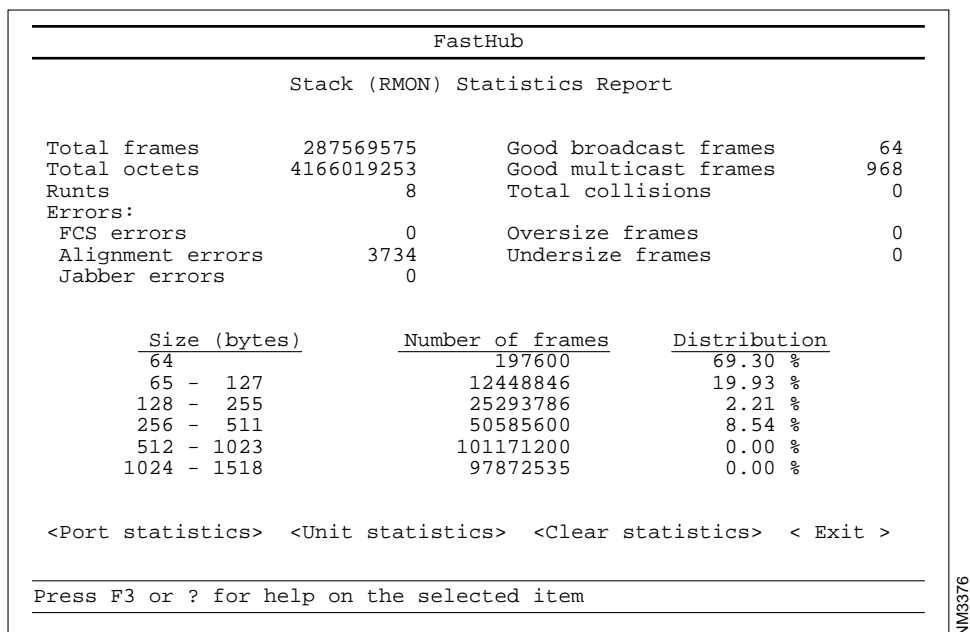
RMON statistics. View the stack (RMON) Statistics Report for frame and receive statistics for the entire hub stack. See the “Stack (RMON) Statistics Report” section in this chapter.

Exit. Return to Main Menu.

Stack (RMON) Statistics Report

Use the Stack (RMON) Statistics Report selection (see Figure 4-17) to display frame and receive statistics for the entire hub stack. You can also clear hub stack statistics through this report.

Figure 4-17 Stack (RMON) Statistics Report



Stack Statistics

Total frames. Total number of readable frames received by the hub stack. This is a good indication of the total amount of valid data traffic passing through the hub stack.

Total octets. Total number of octets (bytes) received as part of good frames by the hub stack.

Runts. Frames that are smaller than the minimum frame size for 802.3 frames. Runt frames typically are caused by collision fragments and are propagated through the network (runts are a normal part of IEEE 802.3 networks). If the number of runt frames exceeds the number of collisions, there is a problem with a transmitting device. Some protocols can also cause runt frames.

Good broadcast frames. Total number of broadcast frames received by the hub stack.

Good multicast frames. Total number of multicast frames seen at the hub stack.

Total collisions. Total number of collisions seen at the hub stack. Collisions occur when two devices attempt to transmit at the same time (collisions are a normal part of 802.3 networks). If the collision count suddenly increases without an accompanying general increase in network traffic, you probably have a faulty device on your network. Check port collision statistics to find the port with the largest number of collisions. Ensure that the device connected to this port is operational and not in full duplex mode.

Errors

FCS errors. Frame Check Sequence errors indicating that frames of data are being corrupted during transmission; this number should be a very small percentage of the total data traffic. Check the cable and the connected device. Verify the network configuration; see the “Making Network Connections” chapter, and ensure that cabling distances have not been exceeded and that the number of repeaters in the network does not exceed the maximum allowed.

Alignment errors. Total number of alignment errors for the hub stack. Alignment errors occur if all bytes are not received whole. Check the cable and the connected device. Verify the network configuration; see the “Making Network Connections” chapter, and ensure that cabling distances have not been exceeded and that the number of repeaters in the network does not exceed the maximum allowed.

Jabber errors. Occur when data packets exceed the lengths prescribed in 802.3. Check port collision statistics to find the port with the largest number of jabber errors. Ensure that the device connected to this port is operational and that the connecting cable is not faulty.

Oversize frames. Total number of frames that exceed the maximum size for 802.3 frames. The frames might have been corrupted during transmission. Some network protocols can cause these frames.

Management Console Screens

Undersize frames. The number of frames that are less than 64 octets long but are otherwise well formed.

Port statistics. Go to Port Statistics Report (via Port Selection screen).

Unit statistics. Go to Unit Statistics Report (via Unit Selection screen).

Clear statistics. Clears all statistics in the hub stack.

Exit. Return to Main Menu.

Unit Addressing Report

When you select the Unit Addressing Report, first the Unit Selection screen (see Figure 4-18) is displayed. Enter the desired unit number. If unit 1 was selected, the following Unit Addressing Report screen (see Figure 4-19) is displayed.

Use the Unit Addressing Report selection to display the port addresses for selected units. You cannot modify any parameters through this report.

Note If there is only one unit in the configuration, the Unit Selection screen (see Figure 4-18) does not display.

Figure 4-18 Unit Selection Screen

FastHub

Unit Selection

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	UNIT 3
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	UNIT 2
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	UNIT 1

Select unit number: [1]

NM3374

Figure 4-19 Unit Addressing Report

FastHub

Unit Addressing Report - unit 1 (16 ports)

Port	Source Address	Port	Source Address	Port	Source Address
1	Unaddressed	2	Unaddressed	3	Unaddressed
4	Unaddressed	5	Unaddressed	6	Unaddressed
7	Unaddressed	8	Unaddressed	9	Unaddressed
10	Unaddressed	11	Unaddressed	12	Unaddressed
13	Unaddressed	14	Unaddressed	15	Unaddressed
16	00-10-18-17-83-45				

<Previous unit>
<Next unit>
<Goto unit...>

<Unit configuration>
<Unit statistics>
< Exit >

* indicates address has changed more than once

Press F3 or ? for help on the selected item

NM3377

Management Console Screens

Port. Indicates port number on selected unit.

Source Address. Source address of port.

Previous unit. Go to the Unit Addressing Report for the unit numerically before this unit.

Next unit. Go to the Unit Addressing Report for the unit numerically after this unit.

Goto unit.... Go to the Unit Addressing Report for a specific unit.

Unit configuration. Go to Unit Configuration menu.

Unit statistics. Go to the Unit Statistics Report.

Exit. Return to Main Menu.

Help

The Help selection describes the FastHub management console keyboard characteristics.