

Out-of-Band Management

This chapter describes how to manage your FastHub or FastHub stack by using the BMM management console, a menu-driven interface for network configuration and management. This chapter also provides information about how FastHub connections affect network management, explains unit and port numbering conventions, and lists management console defaults.

How FastHub Connections Affect Network Management

When a FastHub is hotswapped, the FastHub stack reconfigures itself in less than 1 second (300 msec). During this period, all packets received by the hub stack are dropped. However, the end-station protocols retransmit the lost packets; no connections are lost, and there is no degradation in network performance. If a BMM is present, all configured system parameters are retained; however, all network-related statistics are cleared.



Caution If you remove a FastHub with a BMM and there is no backup BMM in the FastHub stack, you lose manageability for the entire stack.

Unit and Port Numbering Conventions

The physical position of the units in a FastHub stack and the expansion cable connections between units determine how they appear to the BMM management interface. The BMM management console assigns FastHub unit numbers from the bottom up—the FastHub at the bottom of the stack is unit 1, the FastHub above unit 1 is unit 2, and so on. If you have four units in a stack and you remove unit 3 and connect the expansion cable from unit 2 to unit 4, the BMM renumbers unit 4 as unit 3.

Default Parameters

The Port Selection menu and Repeater Port Statistics report 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.

The Bridge Port Selection menu and Bridge Port Statistics Report reflect the physical positions of the BMM ports. BMM ports are identified from left to right as port A (10BaseT) and port B (100BaseT).

Default Parameters

Table 3-1 lists the default settings for the network management console parameters and the menus you use to set them. The items are listed in the sequence that they appear in the management console menu tree (see Figure 3-1).

Table 3-1 **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
Initialization string for modem	0	Console Port
Upgrade status	–	Firmware
Primary supervisor	–	Firmware

Table 3-1 Default Configuration Settings (Continued)

Menu Item	Default Setting	Management Console Menu
Standby supervisor	–	Firmware
Supervisor boot version	–	Firmware
Supervisor mgmt version	–	Firmware
Server accept TFTP upgrade requests	Enabled	Firmware
Name or IP address of TFTP server	–	Firmware
Filename for firmware upgrade	–	Firmware
Name of system	–	System
Contact name	–	System
Location	–	System
System up time	0d 0h 0m 0s	System
Management console inactivity timeout	None	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
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	public	SNMP Management
WRITE community string	private	SNMP Management
Authentication trap generation	Enabled	SNMP Management
linkUp/linkDown trap generation	Enabled	SNMP Management
Write manager names	0	SNMP Management
Trap manager names	0	SNMP Management
Trap manager community strings	0	SNMP Management

Default Parameters

Table 3-1 Default Configuration Settings (Continued)

Menu Item	Default Setting	Management Console Menu
Port linkbeat status	No-linkbeat	Repeater Port Configuration
Port autopartition status	Not-autopartitioned	Repeater Port Configuration
Port connector type	RJ45	Repeater Port Configuration
Last source address	Unaddressed	Repeater Port Configuration
Source address changes	0	Repeater Port Configuration
Port name	–	Repeater Port Configuration
Port status (port enabled or disabled)	Enabled	Repeater Port Configuration
RPS status	–	Repeater Unit Configuration
Power source	–	Repeater Unit Configuration
Supervisor	–	Repeater Unit Configuration
Boot version	–	Repeater Unit Configuration
Mgmt version	–	Repeater Unit Configuration
Main board	–	Repeater Unit Configuration
Expansion board	–	Repeater Unit Configuration
Select Primary Supervisor unit	1	Repeater Unit Configuration
Bridging mode	Fragment free	Bridge Configuration
Use of Store-and-Forward for multicast	Disabled	Bridge Configuration
Accelerated Contention Resolution (10-Mbps port)	Disabled	Bridge Configuration
IEEE-802.1d STP State	Forwarding	Bridge Port Configuration
IEEE-802.1d STP Forward Transitions	0	Bridge Port Configuration
Port name	–	Bridge Port Configuration
Port status	Enabled	Bridge Port Configuration
Port priority (Spanning Tree)	128	Bridge Port Configuration
Path cost (Spanning Tree)	100	Bridge Port Configuration
Half-duplex back-pressure enhancement	Disabled	Bridge Port Configuration

Table 3-1 Default Configuration Settings (Continued)

Menu Item	Default Setting	Management Console Menu
Full duplex	Disabled	Bridge Port Configuration
Accelerated Contention Resolution	Disabled	Bridge Port Configuration
Flood unknown unicast	Enabled	Bridge Port Addressing
Flood unregistered multicast	Enabled	Bridge Port Addressing
Registered multicast addresses	–	Multicast Registration
Action upon exceeding broadcast threshold	Block	Broadcast Storm Control
Generate alert when threshold exceeded	Enabled	Broadcast Storm Control
Broadcast threshold	500	Broadcast Storm Control
Broadcast re-enable threshold	250	Broadcast Storm Control
Capturing frames to the Monitor	Disabled	Monitoring Configuration
Monitor port assignment	–	Monitoring Configuration
Port A assigned to capture list	Disabled	Monitoring Configuration
Port B assigned to capture list	Disabled	Monitoring Configuration
Port R assigned to capture list	Disabled	Monitoring Configuration
Bridge ID	–	Spanning-Tree Configuration
Designated root	–	Spanning-Tree Configuration
Number of member ports	0	Spanning-Tree Configuration
Max age (sec)	20	Spanning-Tree Configuration
Forward delay (sec)	15	Spanning-Tree Configuration
Topology changes	0	Spanning-Tree Configuration
Spanning-Tree Algorithm & Protocol	Enabled	Spanning-Tree Configuration
Bridge priority	32768 (8000 hexadecimal)	Spanning-Tree Configuration
Max age when operation as root	20	Spanning-Tree Configuration
Hello time when operating as root	2	Spanning-Tree Configuration
Forward delay time when operating as root	15	Spanning-Tree Configuration

Management Levels

Table 3-1 Default Configuration Settings (Continued)

Menu Item	Default Setting	Management Console Menu
Address aging time	300 seconds (5 minutes)	Spanning-Tree Configuration
Port A uses Cisco Discovery Protocol (CDP)	Enabled	Cisco Discovery Protocol Configuration
Port B uses Cisco Discovery Protocol (CDP)	Enabled	Cisco Discovery Protocol Configuration
Port R uses Cisco Discovery Protocol (CDP)	Enabled	Cisco Discovery Protocol Configuration
CDP message interval	30	Cisco Discovery Protocol Configuration
Use Cisco Group Management Protocol (CGMP)	Enabled	Cisco Group Management Protocol Configuration
CGMP Router Hold Time	90	Cisco Group Management Protocol Configuration

Management Levels

Using the BMM management console, you can perform FastHub stack network management at system, repeater, and bridge levels. Within the repeater level, you can manage the network and view statistics at port, unit, and FastHub stack levels. The bridge level allows you to configure bridging for individual ports or the entire module. Table 3-2 describes each management level.

Table 3-2 Network Management Levels

Management Level	Actions	Menu or Report Name
System	Enter system-wide parameters for a FastHub.	Console Password menu Console Port menu Firmware menu System menu IP Configuration menu SNMP Management menu

Table 3-2 Network Management Levels (Continued)

Management Level	Actions	Menu or Report Name
Repeater		
Port	Enable or disable repeater ports and examine individual port statistics to monitor individual-user or workgroup traffic.	Port Configuration menu Port Statistics Report
Unit	Monitor the network traffic through a selected FastHub by examining the port statistic totals of the unit.	Unit Configuration menu Unit Statistics Report Unit Addressing Report
Stack	Examine stack statistics to monitor the traffic passing through the stack.	Stack (RMON) Statistics Report
Bridge		
Port	Configure bridging options on a port-by-port basis and examine individual port statistics.	Port Configuration menu Port Addressing menu Port Statistics Report
Module	Display and configure global bridging options.	Bridge Configuration menu Multicast Registration menu Broadcast Storm Control menu Monitoring Configuration menu Spanning-Tree Protocol menu Cisco Discovery Protocol menu Cisco Group Management Protocol menu Bridge Port Status Report Bridge Port Addressing Report Bridge Exception Statistics Report Bridge Utilization Statistics Report

Using the Keyboard

Table 3-3 shows how to use a standard keyboard to control the management console interface and access online help.

Table 3-3 Management Console Standard Keyboard Characteristics

Task	Key
Move the menu cursor.	Left, right, up, or down arrow keys.
Select a menu item.	Position the cursor on the command or its parameter value, and press Enter.
Move to the beginning of a text field.	Home key.
Move to the end of a text field.	End key.
Move the text-edit cursor.	Right and left arrow keys.
Move to the OK and Cancel buttons.	Tab key.
Cancel the current selection.	^X keys.
Access Help information for an item.	Select the item, then press either the F3 or ? key.

Help

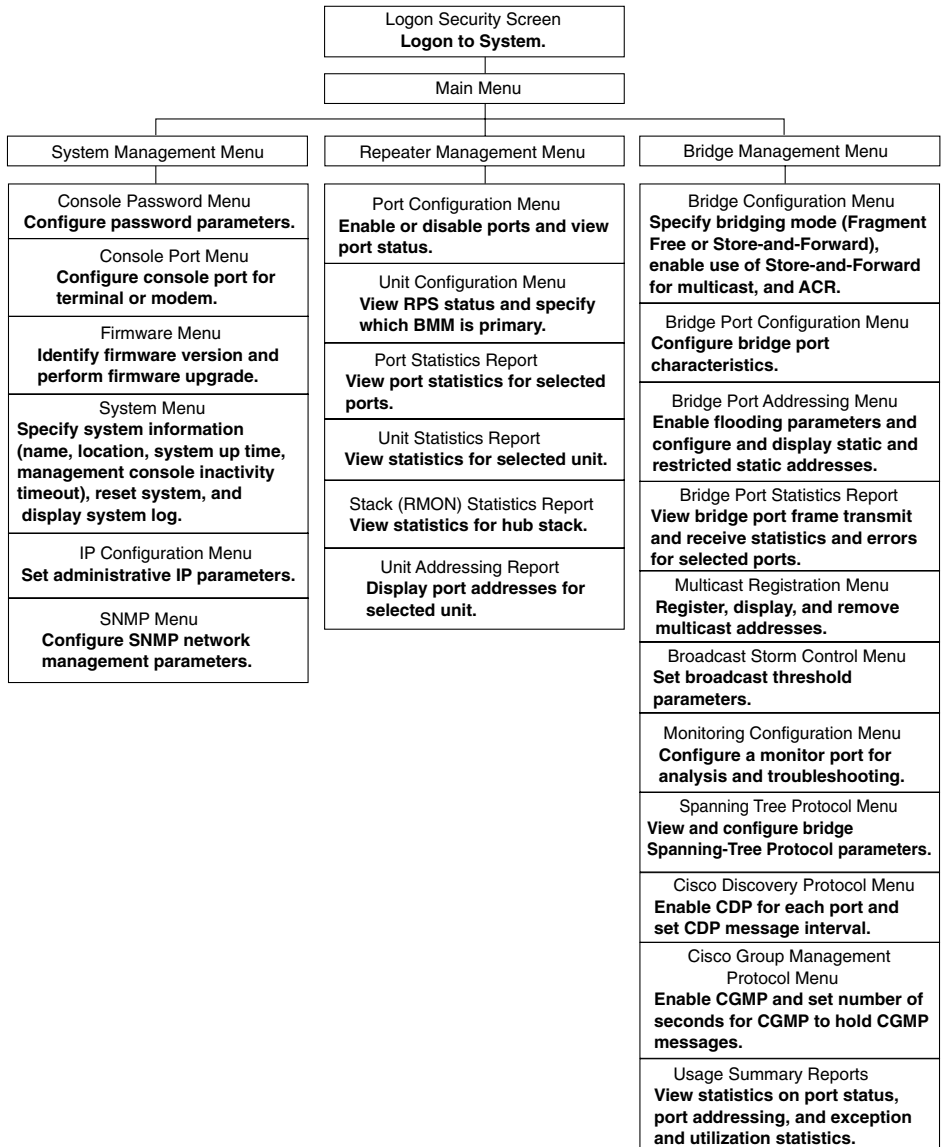
Select **F3** or **?** on the console keyboard to view Help information on a displayed menu or report item. Press **Return** to exit the Help screen.

Console Menus and Reports

Figure 3-1 shows the menus and reports for configuring and displaying FastHub and BMM options, conditions, and statistics, and the actions associated with each.

Note Depending on your system configuration, the actual console screens might appear differently from what is presented in this guide.

Figure 3-1 Management Console Menu and Report Descriptions



HT10112

Logging In 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 log in (see Figure 3-2), select Logon, and press Return. The Main Menu is displayed.

Figure 3-2 **Log-In Screen**

```
FastHub

FastHub Management Console

Copyright (C) Cisco Systems, Inc. 1997
All rights reserved.

Ethernet address: 00-C0-1D-80-19-39

1 user(s) now active on Management Console.

Password:      [                ]

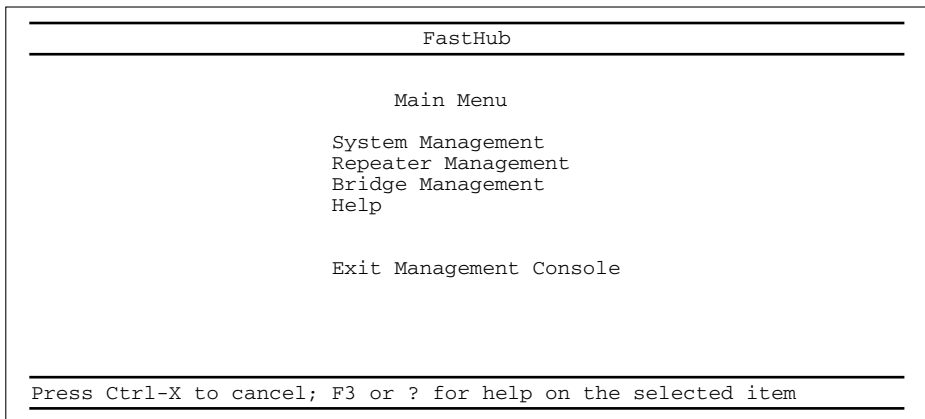
                < Logon >
```

NM5185

Main Menu

Select one of the Main Menu items (see Figure 3-3), and press Return. Select Help on the Main Menu to display a description summary of the FastHub management console, including instructions for using the keyboard and how to read and modify command parameters. Select the Exit Management Console option to return to the Log-In Security Menu. The other menu options are described in the following sections.

Figure 3-3 Main Menu

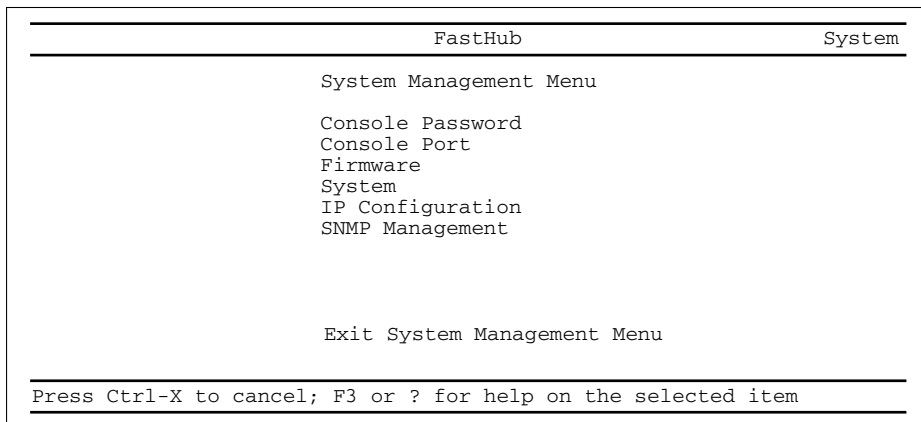


NM5186

System Management Menu

The first top-level menu, the System Management Menu, provides access to menus used to enter system-wide parameters for the FastHub (see Figure 3-4). Select one of the System Management menu items, and press Return. Select the Exit System Management Menu to return to the Main Menu. The other menu options are described in the following sections.

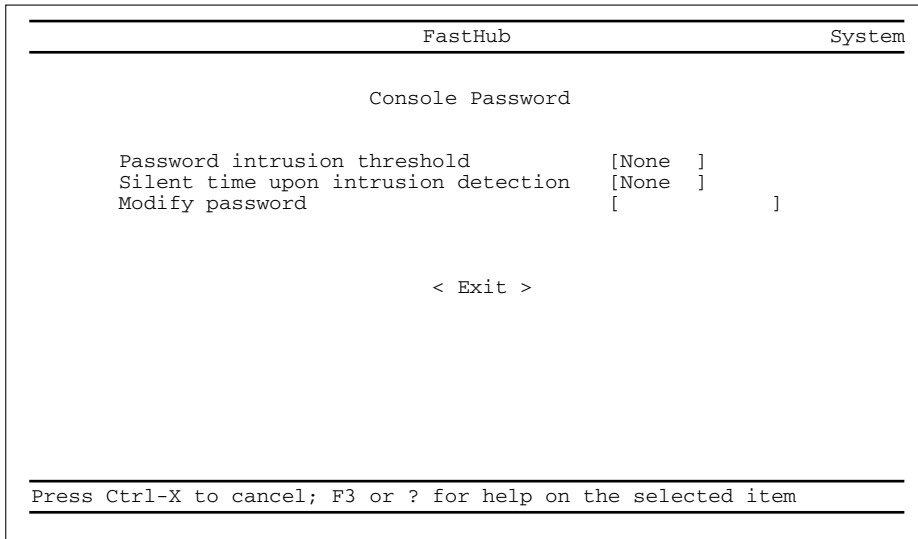
Figure 3-4 System Management Menu



Console Password Menu

Use the Console Password menu to configure the management console log-in parameters (see Figure 3-5).

Figure 3-5 Console Password Menu



NM5190

Password intrusion threshold—Enter the number of failed log-in attempts allowed before the management console shuts down for a configured duration. Valid values range from 0 to 65,500.

Silent time upon intrusion detection—Enter the number of minutes during which the management console is unavailable after password intrusion threshold has been exceeded. Valid values range from 0 to 65,500 minutes.

Modify password—Change your log-in password. Passwords can be between four and eight characters.

Exit—Return to the Main Menu.

Console Port Menu

Use the Console Port menu (see Figure 3-6) to configure the BMM console port.

Figure 3-6 Console Port Menu

```
FastHub                                     System
-----
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 Ctrl-X to cancel; F3 or ? for help on the selected item
-----
```

NM5191

Baud rate—Enter the signal speed for the console port. The baud rates are 2,400, 9,600, 19,200, 38,400, and 57,600.

Data bits—Enter the number of data bits for the console port. The valid values are 7 or 8 bits.

Stop bits—Enter the number of stop bits for the console port. The valid values are 1 or 2 bits.

Parity setting—Enter the parity setting for the console port. The valid values are None, Odd, Even, Mark, and Space.

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 enabled, the system automatically answers incoming calls on a modem attached to the console port.

Time delay between dial attempts—Enter the time in seconds that the management console waits before each attempted dial-out connection. Valid values range from 1 to 65,500 seconds.

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

Initialization string for modem—Enter a modem initialization string with up to 48 characters.

Exit—Return to the Main Menu.

Firmware Menu

Use the Firmware menu (see Figure 3-7) to display system firmware version levels, to identify which unit houses the primary BMM, and to perform firmware upgrades.

Figure 3-7 Firmware Menu

```
FastHub                                     System
-----
Firmware

Upgrade status: Factory installed
Primary supervisor: Unit 1 Boot version: 1.05 Management version: 3.00

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 Ctrl-X to cancel; F3 or ? for help on the selected item
-----
```

NM5192

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 FastHub unit in the stack houses the BMM serving as the primary management supervisor.

Boot version—Displays the version number of the bootstrap firmware on the primary BMM.

Management version—Displays the version number of the management firmware on the primary BMM.

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 “Management Console-Directed In-Band Upgrade” section of the “Troubleshooting” chapter. 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, the filename, and the server address. Refer to the “Management Console-Directed In-Band Upgrade” section in the “Troubleshooting” chapter for details.

Initiate XMODEM upgrade—Initiate the XMODEM upgrade process. You are then prompted to enter an appropriate-application specific command to upgrade the firmware. Refer to the “Out-Of-Band Upgrade” section in the “Troubleshooting” chapter for details.

Exit—Return to the Main Menu.

System Menu

Use the System menu (see Figure 3-8) to do the following:

- Designate system name and location and network administrator name
- Display the amount time the system has been powered up and running
- Specify management console timeout period
- Reset the system
- Reset the repeater hardware
- Display Supervisor log information

Figure 3-8 System Menu

```
FastHub                                     System
-----
System

Name of system                             [BMM           ]
Contact name                               [Alex         ]
Location                                   [California   ]
System up time                             0d 01h 30m 35s
Management Console inactivity timeout     [None        ]

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

      < Exit >

-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
```

NM5193

Name of system—Enter a name for the system, using up to 255 characters.

Contact name—Enter the name of the person or the organization responsible for administering the system, using up to 255 characters.

Location—Enter the location of the system, using up to 255 characters.

System up time—Displays the amount time the system has been running since power up.

Management Console inactivity timeout—Enter the number of minutes that the management console can go without activity. After this period, it is unavailable, and you need to reenter a password. Valid values range from 30 to 65,500 minutes.

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

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

Display Supervisor log—Displays supervisor log information.

Exit—Return to the Main Menu.

IP Configuration Menu

Use the Internet Protocol (IP) Configuration menu (see Figure 3-9) to configure internetwork connection parameters.

Figure 3-9 IP Configuration Menu

```
FastHub                                     System
-----
IP Configuration

Ethernet address: 00-C0-1D-1A-23-7C

IP address of system                        [172.020.128.086]
IP subnet mask                              [255.255.255.000]
IP address of default gateway               [172.020.128.001]
IP address of DNS server 1                 [171.069.002.132]
IP address of DNS server 2                 [198.092.030.032]
DNS domain name                            [cisco.com      ]
Use Routing Information Protocol            [Enabled ]

< Exit >

-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
-----
```

NM5194

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 the Main Menu.

SNMP Management Menu

Use the SNMP Management menu (see Figure 3-10) 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 3-10 SNMP Management Menu

```

FastHub                                     System
-----
SNMP Management

READ community string                       [***** ]
WRITE community string                       [***** ]
Authentication trap generation              [Enabled ]
linkUp/linkDown trap generation             [Enabled ]

Write manager names:
[          ] [          ] [          ] [          ]

TRAP manager names:
[          ] [          ] [          ] [          ]

TRAP manager community strings:
[          ] [          ] [          ] [          ]

< Exit >

Press Ctrl-X to cancel; F3 or ? for help on the selected item
    
```

NM5195

READ community string—Enter the SNMP-agent read (Get) community string, using up to 32 characters. 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, using up to 32 characters. 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.

linkUp/linkDown trap generation—Enable or disable the generation of SNMP linkUp and linkDown traps. A linkUp trap alerts a management workstation that a link has become suspended or disabled. A linkDown trap indicates that a link that was suspended or disabled is now enabled.

Write manager names—Identify which management workstations can issue write (Set) requests to the BMM. Enter either the name or the IP address of the management workstation. You can specify up to four workstations, using up to 255 characters. If no name or address is defined, any management workstation can set the MIB objects.

Trap manager names—Identify which management workstations receive SNMP traps (alerts) from the BMM. Enter either the name or the IP address of the management workstation. You can specify up to four workstations, using up to 255 characters. If no name or IP address is defined, the BMM 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 BMM and the management workstation. You can use up to 255 characters.

Exit—Return to the Main Menu.

Repeater Management Menu

The second top-level menu, the Repeater Management Menu, provides access to menus and reports that allow you to enter and display repeater-specific parameters for the FastHub (see Figure 3-11). Select one of the Repeater Management menu items, and press Return. Select the Exit Repeater Management Menu to return to the Main Menu. The other menu options are described in the following sections.

Figure 3-11 Repeater Management Menu

FastHub	Repeater
Repeater Management Menu	
Port Configuration	
Unit Configuration	
Port Statistics Report	
Unit Statistics Report	
Stack (RMON) Statistics Report	
Unit Addressing Report	
Exit Repeater Management Menu	
Press Ctrl-X to cancel; F3 or ? for help on the selected item	

NIM5188

Figure 3-13 Repeater Port Configuration Menu

```

FastHub                                     Repeater
-----
Repeater 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 Ctrl-X to cancel; F3 or ? for help on the selected item
    
```

NM5197

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

Port autopartition status—Indicates whether the port is autopartitioned. Autopartitioned ports are automatically reconnected when the fault is rectified. Frequent partitions can indicate that the port is not terminated correctly or that 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, using up to 60 characters.

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

Previous port—Go to the Repeater Port Configuration menu for the port numerically before this port.

Next port—Go to the Repeater Port Configuration menu for the port numerically after this port.

Goto port...—Go to the Repeater Port Configuration menu for a specific port.

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

Unit configuration—Go to the Repeater Unit Configuration menu.

Exit—Return to the Main Menu.

Repeater Unit Configuration Menu

Use the Repeater Unit Configuration menu (see Figure 3-14) to do the following:

- View redundant power system (RPS) status
- Identify whether FastHub stack units are powered by the RPS or the FastHub internal power supply
- Identify the units housing the primary BMM and the standby BMM
- Specify the primary BMM
- Display the primary BMM bootstrap and management firmware version numbers
- Display the firmware version numbers of the optional expansion boards

Figure 3-14 Repeater Unit Configuration Menu

	Unit 1	Unit 2	Unit 3	Unit 4
RPS status	Connected	Connected	Not present	Not present
Power source	Internal	Internal	Internal	Internal
Supervisor	*Primary	*Standby		
Boot version	1.05	1.05		
Mgmt version	3.00	3.00		
Main board	0.00	0.00	0.00	
Expansion board	0.00	0.00	0.00	0.00

Select Primary Supervisor unit [1]

<Port configuration> <Unit addressing> < Exit >

*indicates bridge module

Press Ctrl-X to cancel; F3 or ? for help on the selected item

NM5198

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 FastHub containing the primary BMM.

Boot version—Displays the version number of the bootstrap firmware on the primary BMM.

Mgmt version—Displays the version number of the management firmware on the primary BMM.

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—Specify a BMM in a FastHub as the primary BMM.

Port configuration—Go to Repeater Port Configuration menu (via Repeater Port Selection menu).

Unit addressing—Go to the Repeater Unit Addressing Report.

Exit—Return to the Main Menu.

Repeater Port Statistics Report

When you select the Repeater Port Statistics Report, the Port Selection menu is displayed (see Figure 3-15). After you select a unit number and a port number, the Repeater Port Statistics Report is displayed. For example, if you select port 1 on unit 1, the Repeater Port Statistics Report shown in Figure 3-16 is displayed.

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

Figure 3-15 Port Selection Menu

FastHub																Repeater																																		
Port Selection																																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15px;">1</td><td style="width: 15px;">2</td><td style="width: 15px;">3</td><td style="width: 15px;">4</td><td style="width: 15px;">5</td><td style="width: 15px;">6</td><td style="width: 15px;">7</td><td style="width: 15px;">8</td><td style="width: 15px;">9</td><td style="width: 15px;">10</td><td style="width: 15px;">11</td><td style="width: 15px;">12</td><td style="width: 15px;">13</td><td style="width: 15px;">14</td><td style="width: 15px;">15</td><td style="width: 15px;">16</td> <td style="width: 15px;"></td> </tr> </table>																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																																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15px;">1</td><td style="width: 15px;">2</td><td style="width: 15px;">3</td><td style="width: 15px;">4</td><td style="width: 15px;">5</td><td style="width: 15px;">6</td><td style="width: 15px;">7</td><td style="width: 15px;">8</td><td style="width: 15px;">9</td><td style="width: 15px;">10</td><td style="width: 15px;">11</td><td style="width: 15px;">12</td><td style="width: 15px;">13</td><td style="width: 15px;">14</td><td style="width: 15px;">15</td><td style="width: 15px;">16</td> <td style="width: 15px;"></td> </tr> </table>																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																																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15px;">17</td><td style="width: 15px;">18</td><td style="width: 15px;">19</td><td style="width: 15px;">20</td><td style="width: 15px;">21</td><td style="width: 15px;">22</td><td style="width: 15px;">23</td><td style="width: 15px;">24</td><td style="width: 15px;">25</td><td style="width: 15px;">26</td><td style="width: 15px;">27</td><td style="width: 15px;">28</td><td style="width: 15px;">29</td><td style="width: 15px;">30</td><td style="width: 15px;">31</td><td style="width: 15px;">32</td> <td style="width: 15px;"></td> </tr> <tr> <td style="width: 15px;">1</td><td style="width: 15px;">2</td><td style="width: 15px;">3</td><td style="width: 15px;">4</td><td style="width: 15px;">5</td><td style="width: 15px;">6</td><td style="width: 15px;">7</td><td style="width: 15px;">8</td><td style="width: 15px;">9</td><td style="width: 15px;">10</td><td style="width: 15px;">11</td><td style="width: 15px;">12</td><td style="width: 15px;">13</td><td style="width: 15px;">14</td><td style="width: 15px;">15</td><td style="width: 15px;">16</td> <td style="width: 15px;">Mgmt</td> </tr> </table>																17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Mgmt	Unit 1
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32																																			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Mgmt																																		
Select unit number: [1] Select port number: [1]																																																		

NM/5196

Figure 3-16 Repeater Port Statistics Report

FastHub		Repeater	
Repeater 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		
<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		
<Previous port>	<Next port>	<Goto port...>	
<Port configuration>	<Unit statistics>	< Exit >	
Press Ctrl-X to cancel; F3 or ? for help on the selected item			

NNM5199

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 IEEE-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 times a frame check sequence (FCS) error occurs and the number of bits is not byte-aligned (the number of received bits does not divide evenly into bytes). The FCS error is not recorded when an alignment error occurs. Check the cable and the connected device. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure 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. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure that the number of repeaters in the network does not exceed the maximum allowed.

Frames too long—Frames that exceed the maximum size for IEEE-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 IEEE 802.3. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure 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 IEEE 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—Statistic 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 Repeater Port Statistics Report for the port numerically before this port.

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

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

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

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

Exit—Return to the Main Menu.

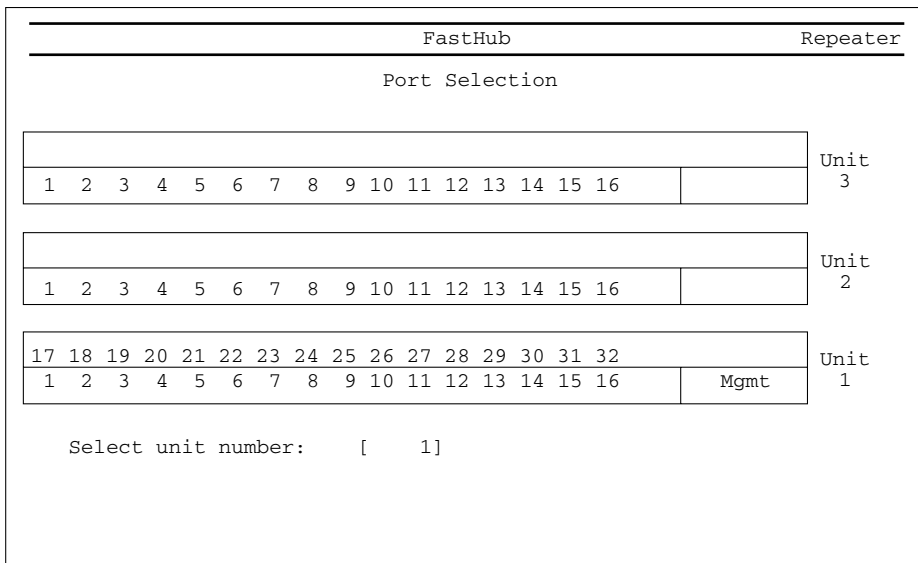
Repeater Unit Statistics Report

When you select the Repeater Unit Statistics Report, the Repeater Unit Selection menu is displayed (see Figure 3-17). After you select a unit number, the Repeater Unit Statistics Report is displayed. For example, if you select unit 1, the Repeater Unit Statistics Report shown in Figure 3-18 is displayed.

Use the Repeater Unit Statistics Report selection to display port statistics for individual units. The Repeater 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 Repeater Unit Selection menu does not display.

Figure 3-17 Repeater Unit Selection Menu



NM/5200

Figure 3-18 Repeater Unit Statistics Report

FastHub		Repeater	
Repeater 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	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		
<Previous unit>	<Next unit>	<Goto unit...>	
<Port statistics>	<RMON statistics>	< Exit >	
Press Ctrl-X to cancel; F3 or ? for help on the selected item			

NM5201

Receive Statistics

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

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

Source address changes—Number of different source addresses received by the FastHub unit.

Runts—Frames that are smaller than the minimum frame size for IEEE-802.3 frames. Runt frames are typically 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 IEEE-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 times a frame check sequence (FCS) error occurs and the number of bits is not byte-aligned (the number of received bits does not divide evenly into bytes). The FCS error is not recorded when an alignment error occurs. Check the cable and the connected device. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure 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. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure that the number of repeaters in the network does not exceed the maximum allowed.

Frames too long—Frames that exceed the maximum size for IEEE-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 IEEE 802.3. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure 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—Statistic generated when port cables are connected or disconnected, when connected devices are powered on or off, or when a cable is faulty.

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 Repeater Unit Statistics Report for the unit numerically before this unit.

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

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

Port statistics—Go to the Port Statistics Report (Port Selection menu).

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

Exit—Return to the Main Menu.

Repeater Stack (RMON) Statistics Report

Use the Repeater Stack (RMON) Statistics Report to display frame and receive statistics for the entire FastHub stack (see Figure 3-19). You can also clear stack statistics through this report.

Figure 3-19 Repeater Stack (RMON) Statistics Report

FastHub		Repeater	
Repeater Stack (RMON) Statistics Report			
Total frames	287569575	Good broadcast frames	64
Total octets	4166019253	Good multicast frames	968
Runts	8	Total collisions	0
Errors:		Oversize frames	0
FCS errors	0	Undersize frames	0
Alignment errors	0		
Jabber errors	0		
<u>Size (bytes)</u>		<u>Number of frames</u>	
64		197600	
65 - 127		12448846	
128 - 255		25293786	
256 - 511		50585600	
512 - 1023		101171200	
1024 - 1518		97872535	
		<u>Distribution</u>	
		69.30 %	
		19.93 %	
		2.21 %	
		8.54 %	
		0.24 %	
		1.53 %	
<Port statistics> <Unit statistics> <Clear statistics> < Exit >			
Press Ctrl-X to cancel; F3 or ? for help on the selected item			

NM5202

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 FastHub stack.

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

Runts—Frames that are smaller than the minimum frame size for IEEE-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 FastHub stack.

Good multicast frames—Total number of multicast frames seen at the FastHub stack.

Total collisions—Total number of collisions seen at the FastHub stack. Collisions occur when two devices attempt to transmit at the same time (collisions are a normal part of IEEE-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. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure that the number of repeaters in the network does not exceed the maximum allowed.

Alignment errors—Total number of times a frame check sequence (FCS) error occurs and the number of bits is not byte-aligned (the number of received bits does not divide evenly into bytes). The FCS error is not recorded when an alignment error occurs. Check the cable and the connected device. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure 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 IEEE 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 IEEE-802.3 frames. The frames might have been corrupted during transmission. Some network protocols can cause these frames.

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

Port statistics—Go to Repeater Port Statistics Report (via Repeater Port Selection menu).

Unit statistics—Go to Repeater Unit Statistics Report (via Repeater Unit Selection menu).

Clear statistics—Clears all statistics in the FastHub stack.

Exit—Return to the Main Menu.

Repeater Unit Addressing Report

When you select the Repeater Unit Addressing Report, the Repeater Unit Selection menu is displayed (see Figure 3-20). After you select a unit number, the Repeater Unit Addressing Report is displayed. For example, if you select unit 1, the Repeater Unit Addressing Report shown in Figure 3-21 is displayed.

Use the Repeater 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 Repeater Unit Selection does not display.

Figure 3-20 Repeater Unit Selection Menu

FastHub																Repeater
Port Selection																
																Unit
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16																3
																Unit
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16																2
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32																Unit
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16															Mgmt	1
Select unit number: [1]																

NM5200

Figure 3-21 Repeater Unit Addressing Report

FastHub		Repeater	
Repeater Unit Addressing Report - unit 1 (16 ports)			
<u>Port</u>	<u>Source Address</u>	<u>Port</u>	<u>Source Address</u>
1	Unaddressed	2	Unaddressed
* 4	00-60-70-CB-F3-02	5	Unaddressed
7	Unaddressed	8	Unaddressed
10	Unaddressed	11	Unaddressed
13	Unaddressed	14	Unaddressed
16	Unaddressed		
		3	Unaddressed
		6	Unaddressed
		9	Unaddressed
		12	Unaddressed
		15	Unaddressed
<Previous unit> <Next unit> <Goto unit...> <Unit configuration> <Unit statistics> < Exit >			
* indicates address has changed more than once			
Press Ctrl-X to cancel; F3 or ? for help on the selected item			

NME203

Port—Port number on selected unit.

Source Address—Source address of port.

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

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

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

Unit configuration—Go to the Repeater Unit Configuration menu.

Unit statistics—Go to the Repeater Unit Statistics Report.

Exit—Return to the Main Menu.

Bridge Management Menu

The third top-level menu, the Bridge Management Menu, provides access to menus and reports that allow you to enter and display bridge-specific parameters for the FastHub (see Figure 3-22). Select one of the Bridge Management menu items, and press Return. Select the Exit Bridge Management Menu to return to the Main Menu. The other menu options are described in the following sections.

Figure 3-22 Bridge Management Menu

```

FastHub                                     Bridge
-----
Bridge Management Menu
Bridge Configuration
Port Configuration
Port Addressing
Port Statistics Report
Multicast Registration
Broadcast Storm Control
Monitoring Configuration
Spanning-Tree Protocol
Cisco Discovery Protocol
Cisco Group Management Protocol
Usage Summary

Exit Bridge Management Menu
-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
    
```

NM5189

Bridge Configuration Menu

Use the Bridge Configuration menu to enable Store-and-Forward mode for multicast signalling (see Figure 3-23).

Figure 3-23 Bridge Configuration Menu

```
FastHub                               Bridge
-----                               -----
                                     Bridge Configuration
Bridging mode                         [Store-and-Forward]
Use of Store-and-Forward for multicast [Disabled]
Accelerated Contention Resolution (10 Mbps port) [Disabled]

                                     <Exit>

-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
-----
```

NM5204

Bridging mode—Select a bridging mode: FragmentFree or Store-and-Forward.

Use of Store-and-Forward for multicast—Enable or disable the store-and-forward mode for multicast frames.

Accelerated Contention Resolution (10-Mbps port)—Enable or disable the use of Accelerated Contention Resolution (ACR), to discard frames early when a port is congested and limit the number of frames queued on a port.

Exit—Return to the Bridge Management menu.

Bridge Port Configuration Menu

When you select the Bridge Port Configuration menu, the Bridge Port Selection menu is displayed (see Figure 3-24). After you select a port, the Bridge Port Configuration menu is displayed. For example, if you select port B, the Bridge Port Configuration – port B menu is displayed (see Figure 3-25). Use the Bridge Port Configuration menu to view the status and configure port characteristics for selected ports.

Figure 3-24 Bridge Port Selection Menu

FastHub	Bridge
Bridge Port Selection	
	Unit 1
R	A B

Select port: A (10BaseT bridge port)
 B (100BaseTX bridge port)
 R (Internal bridge to repeater)

NM15205

Figure 3-25 Bridge Port Configuration—Port B Menu

```

FastHub                                     Bridge
-----
Bridge Port Configuration - port B

10BaseTX bridge port
802.1d STP State                               Forwarding
802.1d STP Forward Transitions                 1

Port name                                     [port B      ]
Port status                                   [Enabled]
Port priority (Spanning Tree)                 [ 128] (80 hex)
Path cost (Spanning Tree)                     [ 100]
Half duplex back pressure enhancement         [Disabled]
Full duplex                                    [Disabled]
Accelerated Contention Resolution              [Disabled]

<Previous port>    <Next port>    <Goto port...>
<Port addressing> <Port statistics> < Exit >

Press Ctrl-X to cancel; F3 or ? for help on the selected item
    
```

NM5206

100BaseTX bridge port—Displays the selected port type. This option appears as **10BaseT bridge port** for the Bridge Port Configuration – Port A menu and **internal bridge to repeater** for the Bridge Port Configuration – port R menu.

802.1d STP State—Displays the current Spanning-Tree Protocol state.

802.1d STP Forward Transitions—Displays the number of times Spanning-Tree Protocol changed forwarding states. An increase in this number might indicate that Spanning-Tree Protocol detected a network loop.

Port name—Specify a name for a selected port, using up to 60 characters.

Port status—Enable or disable the selected port. A disabled port does not transmit or receive. A disabled port must be explicitly enabled to restore operation.

Port priority (Spanning Tree)—Define which port remains enabled by Spanning-Tree Protocol if two ports form a loop.

Path cost (Spanning Tree)—Define the Spanning-Tree Protocol path cost of the selected port.

Half-duplex back-pressure enhancement—Enable or disable back pressure mode for a port in half-duplex mode. When back pressure is enabled and no port receive buffers are available, the BMM forces a signal collision. The collision causes the transmitting device to resend dropped frames immediately, which increases performance. You can enable back pressure on a per-port basis for all ports operating in half-duplex mode.

Full duplex—Enable or disable the operation of full-duplex mode for the selected port. Full duplex can double port bandwidth by allowing simultaneous signal transmitting and receiving.

Accelerated Contention Resolution—Set the Accelerated Contention Resolution (ACR) level to one of four options: Disabled, Adaptive, Moderately Aggressive, or Aggressive. ACR discards frames early when a port is congested and limits the number of frames queued on a port.

Previous port—Go to the Bridge Port Configuration menu for the port alphabetically before this port.

Next port—Go to the Bridge Port Configuration menu for the port alphabetically after this port.

Goto port...—Go to the Bridge Port Configuration menu for a specific port.

Port addressing—Go to the Bridge Port Addressing menu. See the “Bridge Port Addressing Menu” section in this chapter.

Port statistics—Go to the Bridge Port Statistics Report. See the “Bridge Port Statistics Report” section in this chapter.

Exit—Return to the Bridge Management menu.

Bridge Port Addressing Menu

When you select the Bridge Port Addressing menu, the Bridge Port Selection menu is displayed (see Figure 3-24). After you select a port, the Bridge Port Addressing menu is displayed. For example, if you select port B, the Bridge Port Addressing – port B menu is displayed (see Figure 3-26). Use the Bridge Port Addressing menu to define static unicast and multicast addresses.

Figure 3-26 Bridge Port Addressing Menu

```
FastHub                                     Bridge
-----
Bridge Port Addressing - port B

Address : Unaddressed

Flood unknown unicasts                     [Enabled]
Flood unregistered multicasts              [Enabled]

Actions
-----
Add a static addresses      Define restricted static address
List addresses              Erase an address
Remove all addresses

<Previous port>           <Next port>           <Goto port...>
<Port configuration>     <Port statistics>     < Exit >

Press Ctrl-X to cancel; F3 or ? for help on the selected item
```

NM45207

Address—Displays the selected port address.

Flood unknown unicast—Enable or disable transmitting frames with unknown unicasts to the selected port.

Flood unregistered multicast—Enable or disable transmitting frames with unregistered multicast destination addresses to the selected port.

Add a static address—Add a static unicast address to the address table of the selected port. An error message is generated if the address table is full.

Define restricted static address—Add or replace a restricted static unicast address to the address table of the selected port. After entering the new address, you are prompted to enter the port numbers allowed to send to the address. Separate port numbers by commas or spaces. The default is to allow all ports to send to the address. An error message is generated if the address table is full.

List addresses—Display the Bridge Port Address List (see port B example in Figure 3-27). All static and dynamic addresses associated with the selected port are listed.

Erase an address—Erase a dynamic or static address that belongs to the current port. Enter the address using six hexadecimal octets, in the format hh hh hh hh hh hh.

Remove all addresses—Remove all dynamic and static addresses currently associated with the selected port. You are prompted for a confirmation before each address is removed.

Previous port—Go to the Bridge Port Addressing menu for the port alphabetically before this port.

Next port—Go to the Bridge Port Addressing menu for the port alphabetically after this port.

Goto port...—Go to the Bridge Port Addressing menu for a specific port.

Port configuration—Go to the Bridge Port Configuration menu.

Port statistics—Go to the Bridge Port Statistics Report. See the “Bridge Port Statistics Report” section in this chapter.

Exit—Return to the Bridge Management menu.

Figure 3-27 Bridge Port Address List—Port B

```
FastHub
-----
Bridge Port Address List - port B

Dynamic      00-C0-1D-99-03-61  Unrestricted
Dynamic      00-60-70-CB-C7-B1  Unrestricted
Dynamic      00-60-70-CB-F3-02  Unrestricted
Dynamic      00-C0-1D-E4-43-F8  Unrestricted
Dynamic      00-60-5C-F4-00-76  Unrestricted
Dynamic      00-00-00-03-CD-8A  Unrestricted
Dynamic      00-00-00-03-CD-8B  Unrestricted
Dynamic      00-00-00-03-DA-7A  Unrestricted
Dynamic      00-C0-1D-E4-52-43  Unrestricted
Dynamic      00-00-00-03-CA-12  Unrestricted
Dynamic      00-00-00-03-CE-7C  Unrestricted
Dynamic      00-00-24-24-88-8E  Unrestricted
Dynamic      00-C0-1D-C0-A1-81  Unrestricted
Dynamic      00-00-00-03-DA-CB  Unrestricted
Dynamic      00-00-00-03-CA-13  Unrestricted

          < More >                                < Exit >

-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
-----
```

NW5208

Bridge Port Statistics Report

When you select the Bridge Port Statistics Report, the Bridge Port Selection menu is displayed (see Figure 3-24). After you select a unit number and a port number, the Bridge Port Statistics Report is displayed. For example, if you select port B on unit 1, the Bridge Port Statistics Report is displayed (see Figure 3-28).

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

Figure 3-28 Bridge Port Statistics Report

FastHub		Bridge	
Bridge Port Statistics Report - port B			
<u>Receive Statistics</u>		<u>Transmit Statistics</u>	
Total good frames	0	Total good frames	0
Total octets	0	Total octets	0
Broadcast/multicast frames	0	Broadcast/multicast frames	0
Broadcast/multicast octets	0	Broadcast/multicast octets	0
Frames forwarded	0	Deferrals	0
Frames filtered	0	Single collisions	0
Runt frames	0	Multiple collisions	0
No buffer discards	0	Excessive collisions	0
		Queue full discards	0
<u>Receive Errors:</u>		<u>Transmit Errors:</u>	
FCS errors	0	Late collisions	0
Alignment errors	0	Excessive deferrals	0
Giant frames	0	Jabber errors	0
		Other transmit errors	0
<Previous port>	<Next port>	<Goto port...>	
<Port configuration>	<Port addressing >	< Exit >	
Press Ctrl-X to cancel; F3 or ? for help on the selected item			

NMS209

Receive Statistics

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

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

Broadcast/multicast frames—Total number of broadcast and multicast frames received as part of the good frames received by the port.

Broadcast/multicast octets—Total number of broadcast and multicast octets received as part of the good frames received by the port.

Frames forwarded—Total number of received frames that are forwarded.

Frames filtered—Total number of received frames that are filtered.

Runt frames—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 (runt frames 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.

No buffer discards—Total number of received frames that are discarded due to a lack of bridge forwarding frame buffer resources.

Receive 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. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure that the number of repeaters in the network does not exceed the maximum allowed.

Alignment errors—Total number of times a frame check sequence (FCS) error occurs and the number of bits is not byte-aligned (the number of received bits does not divide evenly into bytes). The FCS error is not recorded when an alignment error occurs. Check the cable and the connected device. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure that the number of repeaters in the network does not exceed the maximum allowed.

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

Transmit Statistics

Total good frames—Total number of readable frames transmitted by the port.

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

Broadcast/multicast frames—Total number of broadcast and multicast frames transmitted as part of the good frames transmitted by the port.

Broadcast/multicast octets—Total number of broadcast and multicast octets transmitted as part of the good frames transmitted by the port.

Deferrals—Total number of frames delayed on their first transmission attempt because the network medium is busy.

Single collisions—Total number of successfully transmitted frames that are inhibited by one collision.

Multiple collisions—Total number of successfully transmitted frames that are inhibited by more than one collision.

Excessive collisions—Total number of frames for which transmission fails due to excessive collisions. The threshold is 16 in a normal mode of operation and 4 in ACR mode.

Queue full discards—Total number of frames that cannot be transmitted because the port transmit queue is full.

Transmit Errors

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 IEEE 802.3. See the “Installation” chapter in this guide and also check that cabling distances described in the *FastHub 300 Series Installation and Configuration Guide* have not been exceeded. Verify the network configuration; ensure that the number of repeaters in the network does not exceed the maximum allowed.

Excessive deferrals—Total number of frames for which transmission is deferred for an excessive period of time.

Jabber errors—Occur when data packets exceed the lengths prescribed in IEEE 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.

Other transmit errors—Total number of frames for which transmission fails because of an internal MAC sublayer transmit error.

Previous port—Go to the Bridge Port Statistics Report for the port alphabetically before this port.

Next port—Go to the Bridge Port Statistics Report for the port alphabetically after this port.

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

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

Port addressing—Go to the Bridge Port Addressing menu for the current port.

Exit—Return to Bridge Management Menu.

Multicast Registration Menu

Use the Multicast Registration Menu to define the sets of ports to receive multicast streams, such as those carrying video images (see Figure 3-29). Select one or more multicast address(es) and specify the ports to which traffic destined for these addresses should be forwarded. Each multicast address might represent, for example, a shared destination for a video stream.

The total number of multicast addresses you can add is limited to the space available in the BMM static address table. A separate menu is provided for configuring the broadcast address.

Figure 3-29 Bridge Multicast Registration Menu

```

FastHub                                     Bridge
-----                                     -----
Multicast Registration
Registered multicast addresses: 14

Actions
-----
Register a multicast   List all multicast addresses
Delete a multicast     Erase all multicast addresses

< Exit >

-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
-----

```

NMS268

Registered multicast addresses—Displays the number of registered multicast addresses.

Register a multicast—Register or replace a multicast address. You are prompted for the multicast address to register and the list of ports where frames destined for the registered address are forwarded. Enter the address using six hexadecimal octets, in the format hh hh hh hh hh hh.

After entering the new address, you are prompted to enter the destination port numbers. Separate port numbers by commas or spaces. The default is to forward all frames destined for this address to all ports. If the static address table is full, an error message is displayed.

List all multicast addresses—List all BMM multicast addresses. The addresses are displayed in the Bridge Multicast Registration report (see Figure 3-30).

Delete a multicast—Delete a registered multicast address. Enter the address using six hexadecimal octets, in the format hh hh hh hh hh hh. You can only delete registered addresses. If you attempt to delete a nonregistered multicast address, an error message indicates that the nonregistered multicast address cannot be erased.

Erase all multicast—Delete all registered multicast addresses. You are prompted for a confirmation before each address is removed.

Exit—Return to the Bridge Management Menu.

Figure 3-30 Bridge Multicast Registration Report

```
FastHub                               Bridge
-----                               -----
Bridge Multicast Registration
Registered multicast addresses: 14
Address                               Destination
00-C0-1D-00-00-01                      B
00-C0-1D-34-AE-36                      A,B
* 00-C0-1D-04-56-56                    B

< More >                               < Exit >

* denotes an address with source port filtering
Press Ctrl-X to cancel; F3 or ? for help on the selected item
```

NM0213

Bridge Broadcast Storm Control Menu

Use the Broadcast Storm Control Menu (see Figure 3-31), to generate SNMP alerts and to inhibit the forwarding of broadcast packets when an excessive number arrive from a given port.

Figure 3-31 Bridge Broadcast Storm Control Menu

```

FastHub                                     Bridge
-----
Broadcast Storm Control

Action upon exceeding broadcast threshold    [ Block]
Generate alert when threshold exceeded       [Disabled]
Broadcast threshold                          [ 500]
Broadcast re-enable threshold                [ 250]

< Exit >

Press Ctrl-X to cancel; F3 or ? for help on the selected item
    
```

NM5211

Action upon exceeding broadcast threshold—Define the action to take when the number of broadcast packets reaches the broadcast threshold. The bridge can block or ignore the broadcast storm. During blocking, the bridge drops all broadcast packets received from a port when the rate of broadcast packets exceeds the broadcast threshold. The bridge begins forwarding again when the rate of broadcast packets received drops below the re-enable threshold. The broadcast rate is measured by the number of broadcast packets received from a port in 1 second.

Generate alert when threshold exceeded—Enable or disable the bridge to generate SNMP alerts (traps). When enabled, the bridge generates an SNMP trap to a management station if broadcast storm control is enabled and the broadcast threshold is exceeded on a

port. The action the bridge takes on the port is independent from the generation of the trap. The bridge can generate a maximum of one broadcast control trap per port every 30 seconds.

Broadcast threshold—Set the broadcast threshold. This measurement is the number of packets per second arriving on a port. When this threshold is exceeded, the system blocks the forwarding of packets on the port and generates an SNMP alert, if configured to do so. The broadcast rate is the number of broadcast packets received from a port in 1 second. If the broadcast rate exceeds the specified threshold and broadcast storm control is enabled, the bridge can generate an alert or block broadcast packets received from the port. Valid values range from 10 to 14,400.

Broadcast re-enable threshold—Define when to automatically disable broadcast storm control. The system can continue to forward packets received from a blocked port only when the number of broadcast packets received from the port drops below this re-enable threshold. The re-enable threshold is relevant only if you choose to block broadcast forwarding to control broadcast storms. Valid values range from 10 to 14,400.

Exit—Return to the Bridge Management Menu.

Bridge Monitoring Configuration Menu

Use the Monitoring Configuration Menu (see Figure 3-32) to enable port monitoring, select a monitor port, and specify which ports to monitor by assigning them to a capture list. When monitoring is enabled and configured, a copy of all incoming and outgoing traffic on the monitored ports is routed to the monitor port for analysis and troubleshooting.

Note Monitoring occurs only if frame monitoring is enabled, the port to which monitored frames are sent is identified, and the capture list contains at least one port.

Figure 3-32 Monitoring Configuration Menu

```

FastHub                                     Bridge
-----
Monitoring Configuration

Capturing frames to the Monitor             [Enabled ]
Monitor port assignment                       [C ]
Port A assigned to capture list              [Disabled]
Port B assigned to capture list              [Disabled]
Port R assigned to capture list              [Disabled]

< Exit >

-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
  
```

NM5212

Capturing frames to the Monitor—Enable or disable frame monitoring (capturing) from ports you added to the capture list.

Monitor port assignment—Define the port to which captured frames are to be sent.

Port A assigned to capture list—Select port A to be monitored.

Port B assigned to capture list—Select port B to be monitored.

Port R assigned to capture list—Select the BMM internal port to be monitored.

Exit—Return to the Bridge Management Menu.

Spanning-Tree Protocol Menu

Use the Spanning-Tree Protocol menu to display and configure bridge Spanning-Tree Protocol parameters (see Figure 3-33).

Figure 3-33 Bridge Spanning-Tree Protocol Menu

```

FastHub                                     Bridge
-----
Spanning-Tree Configuration

Bridge ID:                                8000 00-C0-1D-84-19-39
Designated root:                          8000 00-C0-1D-80-19-39
Number of member ports                    11   Root port                               B
Max age (sec)                             20   Root path cost                               100
Forward Delay (sec)                       15   Hello time (sec)                             2
Topology changes                           2   Last Topology Change                         0d00h00m55s

Spanning-Tree Algorithm & Protocol         [Enabled]
Bridge priority                             [ 32768] (8000 hex)
Max age when operation as root              [ 20]   second(s)
Hello time when operating as root           [ 2]   second(s)
Forward delay when operating as root        [ 15]   second(s)
Address aging time                          [ 300]  second(s)

                                     < Exit >

-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
-----

```

NM5210

Bridge ID—Displays the BMM bridge identifier that is used by the Spanning-Tree Protocol. The first two octets indicate the bridge priority value and the last six octets are the unique MAC address for the bridge.

Designated root—Displays the bridge identifier that the Spanning-Tree Protocol discovered as the root bridge. If Spanning-Tree Protocol is disabled, the designated root is displayed as NA (not applicable).

Number of member ports—Displays the number of bridged ports configured with Spanning-Tree Protocol.

Max age (sec)—Displays the current aging interval used to time out old Spanning-Tree Protocol messages. The value, measured in seconds, is established by the root bridge. Valid values range from 6 to 40 seconds.

Forward Delay (sec)—Displays the amount of time ports wait before they transition to a Spanning-Tree Protocol forwarding state. This value, measured in seconds, is established by the root bridge. The pre-forwarding state includes listening and learning states; therefore, 2 seconds must pass before an interactive (blocking) port can forward frames. The Forward Delay value also accelerates the aging of dynamic addresses during a bridge topology change. Valid values range from 4 to 30 seconds.

Topology changes—Displays the number of bridge topology changes, including the number of times ports transition between the Spanning-Tree Protocol blocking state and forwarding state. When Spanning-Tree Protocol is disabled, this value is displayed as NA.

Spanning Tree Algorithm & Protocol—Enable or disable the Spanning-Tree Protocol. When enabled, Spanning-Tree Protocol keeps redundant ports in a standby (suspended) status and automatically enables them when needed.

Bridge priority—Set a two-octet bridge priority value in the loop-free Spanning Tree topology to force a bridge to be the root bridge or a designated bridge. Set the root bridge to the lowest value (the highest priority). Valid priority values are from 0 to 65,535 (FFFF hexadecimal); zero has the highest priority.

Max age when operation as root—Specify the time, in seconds, for the *max age* interval when this bridge is the root bridge. The root bridge configures a timer value that all other bridges use to determine when to discard old bridge configuration messages from the root. Valid values range from 6 seconds to 40 seconds.

Hello time when operating as root—Specify the time interval between bridge configuration messages sent out by the root bridge. Valid values range from 1 to 10 seconds.

Forward delay when operating as root—Specify the amount of time the root bridge allows ports to remain in spanning-tree learning and listening states. Twice this amount of time must elapse before a port in a blocking state can transition to the forwarding state. Valid values range from 4 to 30 seconds.

Address aging time—Specify the amount of time an unused dynamic address is held in the bridge address table before it is automatically removed. When a bridge topology change occurs, dynamic addresses use the current forward-delay parameter as a timeout value to age more rapidly. Valid values range from 10 to 1,000,000 seconds (roughly 11 days and 13 hours).

Exit—Return to the Bridge Management Menu.

Cisco Discovery Protocol Configuration Menu

Use the Cisco Discovery Protocol Configuration menu to display Cisco Discovery Protocol (CDP) configuration and status information (see Figure 3-34).

Figure 3-34 Cisco Discovery Protocol Configuration Menu

```
FastHub                               Bridge
-----                               -----
Cisco Discovery Protocol Configuration

Port A uses Cisco Discovery Protocol (CDP)      [Enabled ]
Port B uses Cisco Discovery Protocol (CDP)      [Enabled ]
Port R (Internal) uses Cisco Discovery Protocol (CDP) [Enabled ]
CDP message interval                          [  30] seconds

                Actions
                -----
                Display CDP neighbors

                < Exit >

-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
```

NM5451

Port A uses Cisco Discovery Protocol (CDP)—Enable or disable the use of CDP on the 10BaseT port. Using CDP, the FastHub can advertise its existence to other devices and receive information about other devices on the same LAN.

Port B uses Cisco Discovery Protocol (CDP)—Enable or disable the use of CDP on the 100BaseTX port.

Port R (Internal) uses Cisco Discovery Protocol (CDP)—Enable or disable the use of CDP on the BMM internal port.

CDP message interval—Set the amount of time between generated CDP messages. The interval can range from 5 to 254 seconds.

Display CDP neighbors—Display the CDP Device Neighboring Information report, which lists the addresses of neighboring devices that are discovered by CDP (see Figure 3-35). You cannot modify any parameters through this report.

Exit—Return to the Bridge Management Menu.

Figure 3-35 CDP Device Neighboring Information Report

```

FastHub
-----
CDP device neighboring information
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, P - Repeater,      H - Host, I - IGMP
DeviceID      Address      Holdtime Capability Platform      Port ID
-----
< More >
< Exit >
-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
    
```

NM5450

More—Displays any additional cached addresses of neighboring devices that are discovered by CDP.

Exit—Return to the Cisco Discovery Protocol Configuration Menu.

Cisco Group Management Protocol Configuration Menu

Use the Cisco Group Management Protocol Configuration menu to display Cisco Group Management Protocol (CGMP) configuration and status information (see Figure 3-36).

Figure 3-36 Cisco Group Management Protocol Configuration Menu

```
FastHub                               Bridge
-----                               -----
Cisco Group Management Protocol Configuration

Use Cisco Group Management Protocol (CGMP)      [Enabled ]
CGMP Router Hold Time                          [ 300 ]

                                     < Exit >

-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
-----
```

NM5449

Use Cisco Group Management Protocol (CGMP)—Enable or disable the use of CGMP on the BMM.

CGMP Router Hold Time—Specify the amount of time to hold CGMP messages. Multicast routers that support CGMP send CGMP join messages to advertise themselves to the bridges within a network. The bridges hold the CGMP messages for a the time period specified by the CGMP router hold time. If the router hold time expires before a bridge receives another CGMP message from the same router, the bridge discards the CGMP information. Valid values range from 5 to 900 seconds.

Exit—Return to the Bridge Management Menu.

Usage Summary Report

Use the Usage Summary Report (see Figure 3-37) to display the following report types:

- Port Status
- Port Addressing
- Exception Statistics
- Utilization Statistics

You cannot modify any parameters through these reports. Select Exit to return to the Bridge Management menu. The other menu options are described in the following sections.

Figure 3-37 Usage Summary Report

```

FastHub                                     Bridge
-----
Bridge Usage Summary

Port Status Report
Port Addressing Report
Exception Statistics Report
Utilization Statistics Report

< Exit >

-----
Press Ctrl-X to cancel; F3 or ? for help on the selected item
    
```

NM5214

Port Status Report

Use the Port Status Report menu to display a summary of all ports configured by the Bridge Port Configuration menu (see Figure 3-38).

Figure 3-38 Port Status Report

FastHub		Bridge
Bridge Port Status Report		
Port	Port Name	Status
A (10BaseT)	port a	Suspended-linkbeat
B (100BaseT)	port b	Suspended-linkbeat
R (Internal)	port r	Enabled
<Port Addressing>		<Exception Statistics>
<Utilization Statistics>		< Exit >
Press Ctrl-X to cancel; F3 or ? for help on the selected item		

NM5215

A (10BaseT)—Displays the name and status of the 10BaseT, Ax port.

B (100BaseT)—Displays the name and status of the 100BaseT, Bx port.

R (Internal)—Displays the name and status of the BMM internal port.

Port Addressing—Go to the Bridge Port Addressing Report. See the “Bridge Port Addressing Report” section in this chapter.

Exception Statistics—Go to the Bridge Exception Statistics Report. See the “Bridge Exception Statistics Report” section in this chapter.

Utilization Statistics—Go to the Bridge Utilization Statistics Report. See the “Bridge Utilization Statistics Report” section in this chapter.

Exit—Return to the Bridge Usage Summary menu.

Bridge Port Addressing Report

Use the Port Addressing Report menu to display a summary of all ports configured by the Bridge Port Configuration menu (see Figure 3-39).

Figure 3-39 Bridge Port Addressing Report

FastHub		Bridge	
Bridge Port Addressing Report			
Port	Addresses		
A (10BaseT)	Static	00-C0-1D-33-44-55	
B (100BaseT)	Dynamic	00-A0-24-69-13-33	
R (Internal)	Dynamic	38	Static 0
<Port status>		<Exception Statistics>	
<Utilization Statistics>		< Exit >	
Press Ctrl-X to cancel; F3 or ? for help on the selected item			

NM5216

A (10BaseT)—Displays the address types and quantity of each address type on the 10BaseT, Ax port. If space allows, a port address is also displayed.

B (100BaseT)—Displays the address types and quantity of each address type on the 100BaseT, Bx port. If space allows, a port address is also displayed.

R (Internal)—Displays the address types and quantity of each address type on the BMM internal port. If space allows, a port address is also displayed.

Port Status—Go to the Bridge Port Status Report.

Exception Statistics—Go to the Bridge Exception Statistics Report. See the “Bridge Exception Statistics Report” section in this chapter.

Utilization Statistics—Go to the Bridge Utilization Statistics Report. See the “Bridge Utilization Statistics Report” section in this chapter.

Exit—Return to the Bridge Usage Summary menu.

Bridge Exception Statistics Report

Use the Bridge Exception Statistics Report menu to display the number of receive errors and transmit errors for each port configured by the Bridge Port Configuration menu (see Figure 3-40).

Figure 3-40 Bridge Exception Statistics Report

FastHub		Bridge
Bridge Exception Statistics Report (Frame count)		
Port	Receive Errors	Transmit Errors
A (10BaseT)	0	0
B (100BaseT)	0	0
R (Internal)	13	35
<Port status>		<Port Addressing>
<Utilization Statistics>		< Exit >
Press Ctrl-X to cancel; F3 or ? for help on the selected item		

NM5217

- A (10BaseT)**—Displays the receive errors and transmit errors of the 10BaseT, Ax port.
- B (100BaseT)**—Displays the receive errors and transmit errors of the 100BaseT, Bx port.
- R (Internal)**—Displays the receive errors and transmit errors of the BMM internal port.
- Port Status**—Go to the Bridge Port Status Report.
- Port Addressing**—Go to the Bridge Port Addressing Report.

Utilization Statistics—Go to the Bridge Utilization Statistics Report. See the “Bridge Utilization Statistics Report” section in this chapter.

Exit—Return to the Bridge Usage Summary menu.

Bridge Utilization Statistics Report

Use the Bridge Utilization Statistics Report menu to display the frame-count statistics generated by the bridge (see Figure 3-41).

Figure 3-41 Utilization Statistics Report

FastHub		Bridge	
Bridge Utilization Statistics Report (Frame count)			
Port	Receive	Forward	Transmit
A (10BaseT)	4871212	539552	1046
B (100BaseT)	14690268	12519430	373
R (Internal)	0	0	0
<Port status>		<Port Addressing>	
<Exception Statistics>		< Exit >	
Press Ctrl-X to cancel; F3 or ? for help on the selected item			

NM5218

A (10BaseT)—Displays the total number of received, forwarded, and transmitted frames for the 10BaseT, Ax port.

B (100BaseT)—Displays the total number of received, forwarded, and transmitted frames for the 100BaseT, Bx port.

R (Internal)—Displays the total number of received, forwarded, and transmitted frames for the BMM internal port.

Port Status—Go to the Bridge Port Status Report.

Port Addressing—Go to the Bridge Port Addressing Report.

Exception Statistics—Go to the Bridge Exception Statistics Report.

Exit—Return to the Bridge Usage Summary menu.

