IBM BladeCenter
Management Module
BladeCenter T Management Module
Advanced Management Module
BladeCenter T Advanced Management Module

Command-Line Interface Reference Guide

IBM BladeCenter
Management Module
BladeCenter T Management Module
Advanced Management Module
BladeCenter T Advanced Management Module

Command-Line Interface Reference Guide

Note: Before using this information and the product it supports, read the general information in Appendix A, “Getting help and technical assistance,” on page 147 and Appendix B, “Notices,” on page 149.

Sixth Edition (August 2006)

Contents

Chapter 1. Introduction 1
Before you begin 2

Chapter 2. Using the command-line interface 3
Command-line interface guidelines 3
Selecting the command target 4
Commands and user authority 5
Cabling the management module 11
Networked connection 11
Direct connection 11
Serial connection (advanced management module only) 12
Starting the command-line interface 12
Telnet connection 13
Serial connection 13
Secure Shell (SSH) connection 13
BladeCenter unit configuration 14
Configuring the management module 14
Starting an SOL session 16
Ending an SOL session 16

Chapter 3. Command reference 17
Built-in commands 18
env (environment) command 18
help command 22
history command 23
list (system physical configuration) command 24
Common commands 25
health command 25
identify (location LED) command 28
info (configuration information) command 29
update (update firmware) command 30
Configuration commands 33
alertentries command 34
clear command (management modules other than the advanced management module) 39
clear command (advanced management module only) 40
dhcpinfo command 42
displaysd command (advanced management module only) 43
dns command 43
ifconfig command (management modules other than the advanced management module) 45
ifconfig command (advanced management module only) 49
ldapcfg command (advanced management module only) 54
nat command (advanced management module only) 55
portcfg command (advanced management module only) 57
ports command (advanced management module only) 59
read command (advanced management module only) 66
service command (advanced management module only) 66
slp command (advanced management module only) 67
smtp command 68
snmp command 69
sol (serial over LAN) command 75
sshcfg command (advanced management module only) 79

tcpcmdmode command (management modules other than the advanced management module) . . . 79
tcpcmdmode command (advanced management module only) . . . 81
telnetcfg (Telnet configuration) command . . . 82
uplink (management module failover) command . . . 83
users command (management modules other than the advanced management module) . . . 84
users command (advanced management module only) . . . 95
write command (advanced management module only) . . . 104
Event-log commands . . . 104
clearlog command . . . 104
displaylog command . . . 105
Power-control commands . . . 106
boot command . . . 107
fuelg command (management modules other than the advanced management module) . . . 107
fuelg command (advanced management module only) . . . 110
power command . . . 114
reset command . . . 116
Session commands . . . 118
console command . . . 118
exit command . . . 119
kvm (keyboard, video, mouse) command (advanced management module only) . . . 119
mt (media tray) command (advanced management module only) . . . 120
System management commands (for BladeCenter T only) . . . 122
alarm command . . . 122

Chapter 4. Error messages . . . 127
Common errors . . . 128
alarm command errors . . . 129
alertentries command errors . . . 130
boot command errors . . . 130
clear command errors . . . 130
clearlog command errors . . . 131
console command errors . . . 131
dhcpinfo command errors . . . 131
displaylog command errors . . . 131
displaysd command errors . . . 132
dns command errors . . . 132
fuelg command errors . . . 132
health command errors . . . 133
identify command errors . . . 133
ifconfig command errors . . . 133
info command errors . . . 135
kvm command errors . . . 136
ldapcfg command errors . . . 136
list command errors . . . 136
mt command errors . . . 136
nat command errors . . . 136
portcfg command errors . . . 137
ports command errors . . . 137
power command errors . . . 137
read command errors . . . 138
reset command errors . . . 138
service command errors . . . 138

slp command errors 138
smtp command errors 139
snmp command errors 139
sol command errors 139
sshcfg command errors 140
tcpcmdmode command errors 141
telnetcfg command errors 141
update command errors 141
uplink command errors 143
users command errors 143
write command errors 146

Appendix A. Getting help and technical assistance 147
Before you call 147
Using the documentation 147
Getting help and information from the World Wide Web 147
Software service and support 148
Hardware service and support 148
IBM Taiwan product service 148

Appendix B. Notices 149
Trademarks. 149
Important notes 150
Product recycling and disposal 151
Battery return program 152
Electronic emission notices 153
Federal Communications Commission (FCC) statement 153
Industry Canada Class A emission compliance statement 153
Australia and New Zealand Class A statement 153
United Kingdom telecommunications safety requirement 153
European Union EMC Directive conformance statement 154
Taiwanese Class A warning statement 154
Chinese Class A warning statement 154
Japanese Voluntary Control Council for Interference (VCCI) statement 154

Index 155

Chapter 1. Introduction

The IBM® BladeCenter® management-module command-line interface (CLI) provides direct access to BladeCenter management functions as an alternative to using the Web-based user interface. Using the command-line interface, you can issue commands to control the power and configuration of the management module and other components that are in a BladeCenter unit.

All IBM BladeCenter units are referred to throughout this document as the BladeCenter unit. All management modules are referred to throughout this document as the management module. Unless otherwise noted, all commands can be run on all management module and BladeCenter unit types.

The command-line interface also provides access to the text-console command prompt on each blade server through a serial over LAN (SOL) connection. See the *IBM BladeCenter Serial Over LAN Setup Guide* for information about SOL and setup instructions.

You access the management-module CLI by establishing a Telnet connection to the IP address of the management module or through a Secure Shell (SSH) connection. You can initiate connections from the client computer using standard remote communication software; no special programs are required. Users are authenticated by the management module before they can issue commands. You enter commands one at a time; however, you can use command scripting to enter multiple commands. The interface does not support keyboard shortcuts, except for the special key sequence (pressing “Esc” then “(”) that terminates an SOL session.

The most recent versions of all BladeCenter documentation are available from http://www.ibm.com/bladecenter/.

Before you begin

Hardware and software required for the command-line interface are as follows:

Hardware:

No special hardware is required to use the management-module command-line interface.

To use the SOL feature, an Ethernet I/O module that supports SOL must be installed in I/O-module bay 1. You can use the console command to control a blade server through SOL only on blade server types that support SOL functionality and have an integrated system management processor firmware level of version 1.00 or later. See the *IBM BladeCenter Serial Over LAN Setup Guide* for information.

Firmware:

Make sure you are using the latest versions of device drivers, firmware, and BIOS code for your blade server, management module, and other BladeCenter components. Go to http://www.ibm.com/bladecenter/ for the latest information about upgrading the device drivers, firmware, and BIOS code for BladeCenter components. The latest instructions are in the documentation that comes with the updates.

The management-module CLI is supported by BladeCenter management-module firmware level version 1.08 or later. All versions of BladeCenter T management-module firmware support the command-line interface. The SOL feature has additional firmware requirements. See the *IBM BladeCenter Serial Over LAN Setup Guide* for information.

Chapter 2. Using the command-line interface

The IBM management-module command-line interface (CLI) provides a convenient method for entering commands that manage and monitor BladeCenter components. This chapter contains the following information about using the command-line interface:

- "Command-line interface guidelines"
- "Selecting the command target" on page 4
- "Commands and user authority" on page 5
- "Cabling the management module" on page 11
- "Starting the command-line interface" on page 12
- "BladeCenter unit configuration" on page 14
- "Configuring the management module" on page 14
- "Starting an SOL session" on page 16
- "Ending an SOL session" on page 16

See Chapter 3, "Command reference," on page 17 for detailed information about commands that are used to monitor and control BladeCenter components. Command-line interface error messages are in Chapter 4, "Error messages," on page 127. See the *IBM BladeCenter Serial Over LAN Setup Guide* for SOL setup instructions and the documentation for your operating system for information about commands you can enter through an SOL connection.

Command-line interface guidelines

All commands have the following basic structure:

```
command -option parameter
```

Some commands do not require options and some command options do not require parameters. You can add multiple options to a command on one line to avoid repeating the same command. Options that display a value and options that set a value must not be used together in the same command. Some examples of valid command option syntax are:

- *command*
- *command -option_set*
- *command -option_set parameter*
- *command -option1_set parameter -option2_set parameter*

For example, `telnetcfg -t 360`.

The information for each option is returned in the order in which it was entered and is displayed on separate lines.

Observe the following general guidelines when using the command-line interface:

- Case sensitivity

  All commands, command options, and pre-defined command option parameters are case sensitive.

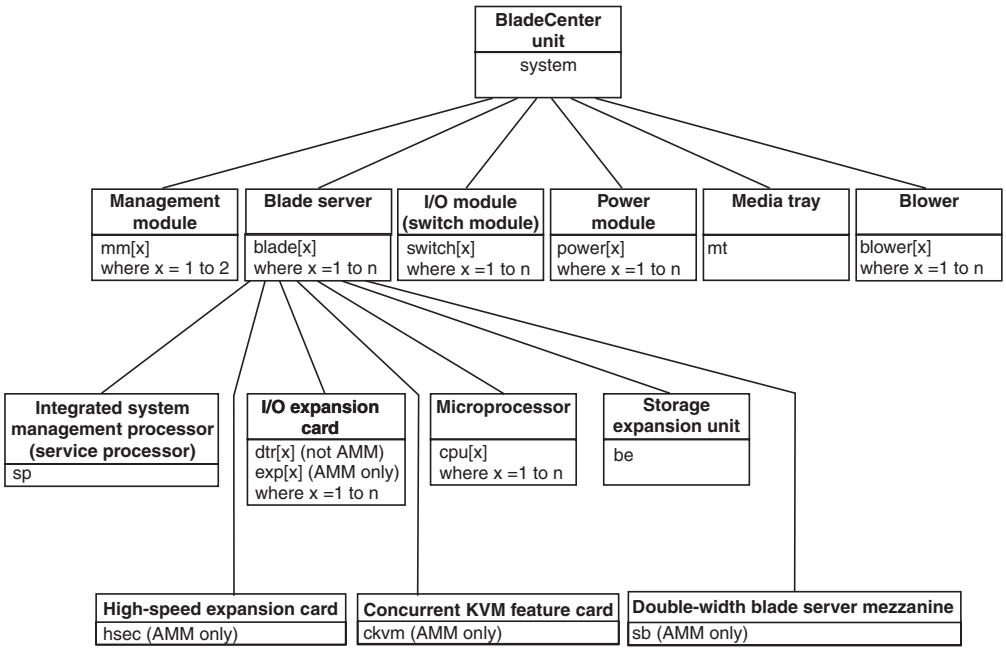
  Note: If you receive a `Command not found` error, make sure that you are typing the commands in the correct case; they are case sensitive. For a list of valid commands, type `help` or `?`.

- Data types

  The ip_address data type uses a predefined formatted string of *xxx.xxx.xxx.xxx*, where *xxx* is a number from 0 to 255
- Delimiters
  - Options are delimited with a minus sign.
  - In a command that requires parameters, a single space is expected between the option and the parameter. Any additional spaces are ignored.
- Output format
  - Failed commands generate failure messages.
  - Successful commands are indicated by the message `OK`, or by the display of command results.
- Strings
  - Strings containing spaces should be enclosed in quotation marks, such as in `snmp -cn "John B. Doe"`.
  - String parameters can be mixed case.
- The `help` command lists all commands and a brief description of each command. You can also issue the help command by typing `?`. Adding the `-h` parameter to any command displays its syntax.
- You can use the up arrow and down arrow keys in the command-line interface to access the last eight commands that were entered.

Selecting the command target

You can use the command-line interface to target commands to the management module or to other devices installed in the BladeCenter unit. The command-line prompt indicates the persistent command environment: the environment where commands are entered unless otherwise redirected. When a command-line interface session is started, the persistent command environment is “system”; this indicates that commands are being directed to the BladeCenter unit. Command targets are specified hierarchically, as shown in the following illustration.



You can change the persistent command environment for the remainder of a command-line interface session by using the `env` command (see “env (environment) command” on page 18). When you list the target as a command attribute using the `-T` option, you change the target environment for the command that you are entering, temporarily overriding the persistent command environment. Target environments can be specified using the full path name, or using a partial path name based on the persistent command environment. Full path names always begin with “system”. The levels in a path name are divided using a colon “:”.

For example:

- Use the `-T system:mm[1]` option to redirect a command to the management module in bay 1.
- Use the `-T system:switch[1]` option to redirect a command to the I/O (switch) module in I/O (switch) module bay 1.
- Use the `-T sp` option to redirect a command to the integrated system management processor (service processor) of the blade server in blade bay 3, when the persistent command environment is set to the blade server in blade bay 3.

Most management-module commands must be directed to the primary management module. If only one management module is installed in the BladeCenter unit, it will always act as the primary management module. Either management module can function as the primary management module; however, only one management module can be primary at one time. You can determine which management module is acting as the primary management module using the `list` command (see “list (system physical configuration) command” on page 24).

Commands and user authority

Some commands in the command-line interface can only be successfully executed by users who are assigned a required level of authority. Users with “Supervisor” command authority can successfully execute all commands. Commands that display information do not require any special command authority; however, users can be assigned restricted read-only access, as follows:

- Users with “Operator” command authority can successfully execute all commands that display information.
- Users with “Chassis Operator” custom command authority can successfully execute commands that display information about the common BladeCenter unit components.
- Users with “Blade Operator” custom command authority can successfully execute commands that display information about the blade servers.
- Users with “Switch Operator” custom command authority can successfully execute commands that display information about the I/O modules.

Table 1 on page 6 shows the command-line interface commands and their required authority levels. To use the table, observe the following guidelines:

- The commands listed in this table only apply to the command variants that set values or cause an action: display variants of the commands do not require any special command authority.
- When only one command authority at a time is required to execute a command, this is indicated by a “•” entry in a table row.
- When a command has several rows associated with it, each row indicates one of the valid user command authorities needed to successfully execute the

command. For example, the `clearlog` command is available to users with the "Supervisor" command authority or to users with the "Chassis Log Administration" command authority.

- When a combination of two or more command authorities at a time is required to execute a command, this is indicated by multiple "◇" entries in a table row. The user must be assigned both of these command authorities to successfully execute the command. For example, one available authority combination for the `power -on -c` command is the "Blade Server Remote Presence" command authority and the "Blade Administration" command authority.

Important: Command authority definitions might change between firmware versions. Make sure that the command authority level set for each user is correct after updating management-module firmware.

Notes:

1. LDAP authority levels are not supported by the management-module Web interface.
2. To use the LDAP authority levels, you must make sure that the version of LDAP security used by the management module is set to v2 (enhanced role-based security model). See "ldapcfg command (advanced management module only)" on page 54 for information.

Table 1. Command authority relationships

	Authority											LDAP Authority				
Command	**Supervisor**	**Chassis User**	**Account Management Blade Server Remote Presence**	**Chassis Administration**	**Blade Administration**	**Blade Remote Presence**	**I/O Module Administration**	**Chassis Log Administration**	**Chassis Configuration**	**Blade Configuration**	**I/O Module Configuration**	**Blade Remote Presence View Video**	**Blade Remote Presence KVM**	**Blade Remote Presence Remote Drive Read**	**Blade Remote Presence Remote Drive Read or Write**	**Remote Presence Supervisor**
alarm -c, -r, -s	•															
									•							
										•						
											•					
alarm -q -g	•															
			•													
					•											

Table 1. Command authority relationships (continued)

Command	Authority											LDAP Authority				
	Supervisor	Chassis User	Account Management Blade Server Remote Presence	Chassis Administration	Blade Administration	Blade Remote Presence	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration	Blade Remote Presence View Video	Blade Remote Presence KVM	Blade Remote Presence Remote Drive Read	Blade Remote Presence Remote Drive Read or Write	Remote Presence Supervisor
alertentries	•															
									•							
boot	•															
					•											
boot -c	•															
			◇		◇											
boot -p	•															
					•											
clear	•															
				◇					◇							
							◇				◇					
clearlog	•															
								•								
console	•															
			•													
dns	•															
									•							
fuelg	•															
									•							
identify	•															
									•							
										•						

Table 1. Command authority relationships (continued)

Command	Authority											LDAP Authority				
	Supervisor	Chassis User	Account Management Blade Server Remote Presence	Chassis Administration	Blade Administration	Blade Remote Presence	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration	Blade Remote Presence View Video	Blade Remote Presence KVM	Blade Remote Presence Remote Drive Read	Blade Remote Presence Remote Drive Read or Write	Remote Presence Supervisor
ifconfig	•															
									•							
										•						
											•					
kvm	•															
						•										
ldapcfg	•															
									•							
mt	•															
						•										
nat	•															
											•					
portcfg	•															
									•							
ports	•															
									•							
power -on, -off, -cycle	•															
					•											
							•									
power -on -c, -cycle -c	•															
			◇		◇											
read	•															
									•							

Table 1. Command authority relationships (continued)

Command	Authority											LDAP Authority				
	Supervisor	Chassis User	Account Management Blade Server Remote Presence	Chassis Administration	Blade Administration	Blade Remote Presence	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration	Blade Remote Presence View Video	Blade Remote Presence KVM	Blade Remote Presence Remote Drive Read	Blade Remote Presence Remote Drive Read or Write	Remote Presence Supervisor
reset (blade server or ISMP)	•															
					•											
reset (I/O module)	•															
							•									
reset (management module)	•															
				•												
reset -c (blade server or ISMP)	•															
			◇		◇											
reset -clr, -dg, -ddg, -sft (blade server)	•															
					•											
reset -exd, -full, -std (I/O module)	•															
							•									
reset -f (management module)	•															
				•												
service	•															
									•							
slp	•															
									•							
smtp	•															
									•							
snmp	•															
									•							

Table 1. Command authority relationships (continued)

Command	Authority											LDAP Authority				
	Supervisor	Chassis User	Account Management Blade Server Remote Presence	Chassis Administration	Blade Administration	Blade Remote Presence	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration	Blade Remote Presence View Video	Blade Remote Presence KVM	Blade Remote Presence Remote Drive Read	Blade Remote Presence Remote Drive Read or Write	Remote Presence Supervisor
sol	•															
									•							
										•						
sshcfg	•															
									•							
tcpcmdmode	•															
									•							
telnetcfg	•															
									•							
update	•															
				•												
					•											
							•									
uplink	•															
									•							
users	•															
		•														
write	•															
									•							

Cabling the management module

You must connect a client computer to the management module to configure and manage operation of the BladeCenter unit. All management modules support a remote management and console (Ethernet) connection. The advanced management module also supports connection through the serial management port.

You can manage the BladeCenter unit by using by using the command-line interface that you access through Telnet or through the serial management port (advanced management module only). You can also use the graphical user interface that is provided by the management-module Web interface to manage the BladeCenter unit and blade servers that support KVM. Management connections to blade servers that do not support KVM are made using an SOL session through the management-module command-line interface. To connect to the management-module command-line interface, you need the following equipment and information:

- A computer with Ethernet or serial connection capability. To facilitate connections at multiple locations, you can use a notebook computer.
- The management-module MAC address (listed on the label on the management module).
- For networked connection to the management module, you need the following equipment:
  - A standard Ethernet cable
  - A local Ethernet network port (facility connection)
- For direct connection of a computer to the management-module remote management and console (Ethernet) connector, an Ethernet crossover cable. The advanced management module can use either a standard Ethernet cable or an Ethernet crossover cable to make this connection.
- For serial connection of a computer to the advanced management-module serial connector, you need a serial cable. See the *Installation Guide* for your management module for cabling information and instructions.

For information about accessing the management-module Web interface, see the *BladeCenter Management Module User's Guide*.

The following sections describe how to cable to the management module to perform initial configuration of the BladeCenter unit. See the *Installation Guide* for your management module for specific cabling instructions.

Networked connection

Connect one end of a Category 5 or higher Ethernet cable to the remote management and console (Ethernet) connector on the management module. Connect the other end of the Ethernet cable to the facility network.

Direct connection

Connect one end of a Category 5 or higher Ethernet cable (advanced management module only) or a Category 5 or higher Ethernet crossover cable (management module and advanced management module) to the remote management and console (Ethernet) connector on the management module. Connect the other end of the cable to the Ethernet connector on the client computer.

Note: The advanced management module can perform an automatic media dependent interface (MDI) crossover, eliminating the need for crossover cables or

cross-wired (MDIX) ports. You might need to use a crossover cable to connect to the advanced management module if the network interface card in the client computer is very old.

Serial connection (advanced management module only)

Connect one end of a serial cable to the serial connector on the management module. Connect the other end of the serial cable to the serial connector on the client computer. See the *Installation Guide* for your management module for cabling information and instructions.

Starting the command-line interface

Access the management-module command-line interface from a client computer by establishing a Telnet connection to the IP address of the management module or by establishing a Secure Shell (SSH) connection. For the advanced management module, you can also access the command-line interface using a serial connection. You can establish up to 20 separate Telnet, serial, or SSH sessions to the BladeCenter management module, giving you the ability to have 20 command-line interface sessions active at the same time.

Although a remote network administrator can access the management-module command-line interface through Telnet, this method does not provide a secure connection. As a secure alternative to using Telnet to access the command-line interface, use a serial or SSH connection. SSH ensures that all data that is sent over the network is encrypted and secure.

The following SSH clients are available. While some SSH clients have been tested, support or non-support of any particular SSH client is not implied.

- The SSH clients distributed with operating systems such as Linux®, AIX®, and UNIX® (see your operating-system documentation for information). The SSH client of Red Hat Linux 8.0 Professional was used to test the command-line interface.
- The SSH client of cygwin (see http://www.cygwin.com for information)
- Putty (see http://www.chiark.greenend.org.uk/~sgtatham/putty for information)

The following table shows the types of encryption algorithms that are supported, based on the client software version that is being used.

Algorithm	SSH version 1.5 clients	SSH version 2.0 clients
Public key exchange	SSH 1-key exchange algorithm	Diffie-Hellman-group 1-sha-1
Host key type	RSA (1024-bit)	DSA (1024-bit)
Bulk cipher algorithms	3-des	3-des-cbc or blowfish-cbc
MAC algorithms	32-bit crc	Hmac-sha1

The following sections describe how to connect to the management module to perform initial configuration of the BladeCenter unit. The management module has the following default settings:

- IP address: 192.168.70.125
- Subnet: 255.255.255.0
- User ID: USERID (all capital letters)
- Password: PASSW0RD (note the number zero, not the letter O, in PASSW0RD)

The computer that you are connecting to the management module must be configured to operate on the same subnet as the BladeCenter management module. If the IP address of the management module is outside of your local domain, you must change the Internet protocol properties on the computer that you are connecting.

Telnet connection

To log on to the management module using Telnet, complete the following steps:

1. From a command-line prompt on the network-management workstation, type `telnet 192.168.70.125`, and press Enter. The IP address 192.168.70.125 is the default IP address of the management module; if a new IP address has been assigned to the management module, use that one instead.
2. At the login prompt, type the management-module user ID. At the password prompt, type the management-module password. The user ID and password are case sensitive and are the same as those that are used for management-module Web access. The default management-module user name is USERID and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

   The CLI command prompt is displayed. You can now enter commands for the management module.

Serial connection

After connecting a serial cable from the management module to the client computer, complete the following steps:

1. Open a terminal session on the client computer, and make sure that the serial port settings for the client computer match the settings for the serial port on the management module. The default management-module serial port settings are as follows:
   - Baud rate: 57600
   - Parity: no parity
   - Stop bits: 1
2. Remove the management module from the BladeCenter unit; then, reinsert it.
3. At the login prompt, type the management-module user ID. At the password prompt, type the management-module password. The user ID and password are case sensitive and are the same as those that are used for management-module Web access. The default management-module user name is USERID and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

   The CLI command prompt is displayed. You can now enter commands for the management module.

Secure Shell (SSH) connection

To log on to the management module using SSH, complete the following steps:

1. Make sure that the SSH service on the network-management workstation is enabled. See your operating-system documentation for instructions.
2. Make sure that the SSH server on the BladeCenter management module is enabled. See the *BladeCenter Management Module User's Guide* for instructions.
3. Start an SSH session to the management module using the SSH client of your choice. For example, if you are using the cygwin client, from a command-line prompt on the network-management workstation, type `ssh 192.168.70.125`, and

press Enter. The IP address 192.168.70.125 is the default IP address of the management module; if a new IP address has been assigned to the management module, use that one instead.

4. Type the management-module user ID when prompted. At the password prompt, type the management-module password. The user ID and password are case sensitive and are the same as those that are used for management-module Web access. The default management-module user name is USERID and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

   The CLI command prompt is displayed. You can now enter commands for the management module.

BladeCenter unit configuration

The BladeCenter unit automatically detects the modules and blade servers that are installed and stores the vital product data (VPD). When the BladeCenter unit is started, the management module automatically configures the remote management port of the management module, so that you can configure and manage BladeCenter components. You configure and manage BladeCenter components remotely using the management-module command-line interface (CLI) or the management-module Web interface.

To communicate with network resources and with the I/O modules in the BladeCenter unit, you must configure IP addresses for the management module and I/O modules. Management-module IP addresses can be configured using the Web interface or command-line interface. There are several ways to configure the I/O modules: through the management-module Web interface, or through an external I/O-module port enabled through the management module, using a Telnet interface, serial connection (advanced management module only), or a Web browser. See the documentation that comes with each I/O module for information and instructions.

To communicate with the blade servers for functions such as deploying an operating system or application program over a network, you must also configure at least one external (in-band) port on an Ethernet switch module in I/O-module bay 1 or 2.

Note: If a pass-thru module is installed in I/O-module bay 1 or 2 (instead of an Ethernet I/O module), you will need to configure the network switch that the pass-thru module is connected to; see the documentation that comes with the network switch for instructions.

Configuring the management module

You configure only the primary (active) management module. The redundant management module, if present, receives the configuration and status information automatically from the primary management module when necessary. The configuration information in this section applies to the primary management module, which might be the only management module in the BladeCenter unit.

If the management module that you installed is a replacement for the only management module in the BladeCenter unit, and you saved the configuration file before replacing the management module, you can apply the saved configuration file to the replacement management module. See “read command (advanced management module only)” on page 66 for information about applying a saved configuration file. Other management modules must have their configurations

restored using the management-module Web interface (see the *BladeCenter Management Module User's Guide* for information).

For the primary management module to communicate, you must configure the IP addresses for the following internal and external ports:

- The external Ethernet (remote management) port (eth0) of the management module. The initial automatic management module configuration enables a remote console to connect to the management module to configure the port completely and to configure the rest of the BladeCenter unit.
- The internal Ethernet port (eth1) on the management module for communication with the I/O modules. Internal Ethernet ports for the advanced management module cannot be configured.

After you connect the primary management module to the network, the Ethernet port connection is configured in one of the following ways. Either of these actions enables the Ethernet connection on the primary management module.

- If you have an accessible, active, and configured dynamic host configuration protocol (DHCP) server on the network, IP address, gateway address, subnet mask, and DNS server IP address are set automatically. The host name is set to the management-module MAC address by default, and the domain server cannot change it.
- If the DHCP server does not respond within 3 minutes after the port is connected, the management module uses the factory-defined static IP address and default subnet address.

Important: You can not connect to the management module using the factory-defined static IP address and default subnet address until after this 3-minute period passes.

Note: If the IP configuration is assigned by the DHCP server, the network administrator can use the MAC address of the management-module network interface to find out what IP address is assigned.

To configure the management-module internal and external Ethernet ports, complete the following steps:

1. Connect to the management-module command-line interface (see "Starting the command-line interface" on page 12 for more information).
2. Configure the external Ethernet interface (eth0), using the ifconfig command (see "ifconfig command (advanced management module only)" on page 49 for instructions).
3. For management modules other than the advanced management module, configure the internal Ethernet interface (eth1), using the ifconfig command (see "ifconfig command (advanced management module only)" on page 49 for instructions).

   Notes:

   a. The internal Ethernet management port on each I/O module provides for communication with the management module. You configure this port by configuring the IP address for the I/O module (see the *BladeCenter Management Module User's Guide* and the *User's Guide* for your I/O module type for information and instructions). Some types of I/O modules, such as the pass-thru module, have no management port. See the documentation that comes with each I/O module to determine what else you must configure in the I/O module.

b. For I/O module communication with a remote management station, such as the IBM Director server, through the management-module external Ethernet port, the I/O module internal network interface and the management-module internal and external interfaces must be on the same subnet.
c. To communicate with the blade servers for functions such as deploying an operating system or application program, you also will need to configure at least one external (in-band) port on an Ethernet I/O module.

Starting an SOL session

Note: Serial over LAN (SOL) must be enabled for both the BladeCenter unit and the blade server before you can start an SOL session with the blade server. See “sol (serial over LAN) command” on page 75 and the *BladeCenter Serial over LAN Setup Guide* for information about setting up and enabling SOL.

After you start a Telnet or SSH session to the BladeCenter management module, you can start an SOL session to any individual blade server that supports SOL. Since you can start up to 20 separate Web interface, Telnet, serial (advanced management module only), or SSH sessions to the BladeCenter management module, this gives you the ability to have simultaneous SOL sessions active for each blade server installed in the BladeCenter unit.

Start an SOL session using the `console` command, from the command line, indicating the target blade server. For example, to start an SOL connection to the blade server in blade bay 6, type

```
console -T system:blade[6]
```

Note: A blade server assembly that occupies more than one blade bay is identified by the lowest bay number that it occupies.

Once an SOL session is started, all commands are sent to the blade server specified by the `console` command until the SOL session is ended, regardless of the persistent command target that was in effect before the SOL session.

See “sol (serial over LAN) command” on page 75 and the *IBM BladeCenter Serial over LAN Setup Guide* for information about configuring a blade server for SOL. See your operating-system documentation for information about SOL commands that you can enter using the command-line interface.

Ending an SOL session

To end an SOL session, press Esc followed by an open parenthesis:

Esc (

When the SOL session ends, the command-line interface will return to the persistent command target that was in effect before the SOL session. If you want to end the Telnet or SSH command-line session, type `exit`.

Note: Exiting an SOL session does not stop the flow of serial data.

Chapter 3. Command reference

This section contains command function, usage information, and examples. It is divided into the following subsections:

- "Built-in commands" on page 18
  - env (environment) command
  - help command
  - history command
  - list (system physical configuration) command
- "Common commands" on page 25
  - health command
  - identify (location LED) command
  - info (configuration information) command
  - update (update firmware) command
- "Configuration commands" on page 33
  - alertentries command
  - clear command (management modules other than the advanced management module)
  - clear command (advanced management module only)
  - dhcpinfo command
  - displaysd command (advanced management module only)
  - dns command
  - ifconfig command (management modules other than the advanced management module)
  - ifconfig command (advanced management module only)
  - ldapcfg command (advanced management module only)
  - nat command (advanced management module only)
  - portcfg command (advanced management module only)
  - ports command (advanced management module only)
  - read command (advanced management module only)
  - service command (advanced management module only)
  - slp command (advanced management module only)
  - smtp command
  - snmp command
  - sol (serial over LAN) command
  - sshcfg command (advanced management module only)
  - tcpcmdmode command (management modules other than the advanced management module)
  - tcpcmdmode command (advanced management module only)
  - telnetcfg (Telnet configuration) command
  - uplink (management module failover) command
  - users command (management modules other than the advanced management module)
  - users command (advanced management module only)
  - write command (advanced management module only)
- "Event-log commands" on page 104
  - clearlog command
  - displaylog command
- "Power-control commands" on page 106
  - boot command
  - fuelg command (management modules other than the advanced management module)
  - fuelg command (advanced management module only)
  - power command
  - reset command

- "Session commands" on page 118
  - console command
  - exit command
  - kvm (keyboard, video, mouse) command (advanced management module only)
  - mt (media tray) command (advanced management module only)
- "System management commands (for BladeCenter T only)" on page 122
  - alarm command

Adding a `-h`, `-help`, or `?` option to a command displays syntax help for that command. For example, to display help for the environment command, type one of the following commands:

- `env -h`
- `env -help`
- `env ?`

You can target a command to a device other than the one that is set as the default by adding a `-T` option to a command. See "Selecting the command target" on page 4 for information.

Built-in commands

Use these commands to perform top-level functions within the command-line interface:

- env (environment) command
- help command
- history command
- list (system physical configuration) command

env (environment) command

This command sets the persistent environment for commands that are entered during the remainder of the current session. The persistent command environment is indicated by the command prompt. When you start the command-line interface, the persistent command environment is the BladeCenter unit, denoted as "system" by the command prompt. You can target a single command to an environment other than the one that is set as the default by adding a `-T` option to the command that includes a valid target destination (see "Selecting the command target" on page 4 for information). Target environments can be specified using the full path name, or using a partial path name based on the persistent command environment. Full path names always begin with "system". The levels in a path name are divided using a colon ":".

The following table lists BladeCenter components and the command paths that are supported as targets by the env command.

Component	Target path
BladeCenter unit	system
Management module	system:mm[*x*]
Blade server	system:blade[*x*]
Blade server integrated system management processor (BMC or service processor)	system:blade[*x*]:sp

Component	Target path
Blade server I/O-expansion card	system:blade[*x*]:exp[*x*] (advanced management module only) system:blade[*x*]:dtr[*x*] (management modules other than the advanced management module)
Blade server microprocessor	system:blade[*x*]:cpu[*x*]
Blade server storage expansion unit	system:blade[*x*]:be[*x*]
Blade server high-speed expansion card (advanced management module only)	system:blade[*x*]:hsec
Blade server mezzanine for double-width form factor (advanced management module only)	system:blade[*x*]:sb
Blade server concurrent KVM feature card (advanced management module only)	system:blade[*x*]:ckvm
I/O module	system:switch[*x*]
Power module	system:power[*x*]
Blower	system:blower[*x*]
Media tray	system:mt

Table 2. env (environment) command

Function	What it does	Command	Valid targets
Set BladeCenter unit as command target	Sets the BladeCenter unit as the persistent target for commands during the current session. This is the persistent command environment you are in at the beginning of each command-line interface session, indicated by the `system>` prompt.	env env -T system	The env command can be directed to any installed device.
Set management module as command target	Sets the management module as the persistent target for commands during the current session.	env -T system:mm[*x*] where *x* is the bay (1 or 2) that identifies the management module.	The env command can be directed to any installed device, in this case `-T system:mm[x]` where *x* is the management-module bay number.
Set blade server as command target	Sets the specified blade server as the persistent target for commands during the current session.	env -T system:blade[*x*] where *x* is the blade bay that identifies the blade server. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies.	The env command can be directed to any installed device, in this case `-T system:blade[x]` where *x* is the blade bay that identifies the blade server.

Table 2. env (environment) command (continued)

Function	What it does	Command	Valid targets
Set blade server sub-component as command target	Sets the specified sub-component on the specified blade server as the persistent target for commands during the current session. Valid sub-components are: • Integrated system management processor (BMC or service processor) • I/O-expansion card • Microprocessor • Storage expansion unit • Concurrent KVM feature card (advanced management module only) • High-speed expansion card (advanced management module only) • Mezzanine assembly for double-width form factor blade servers (advanced management module only)	env -T system:blade[*x*]:*comp* where *x* is the blade bay that identifies the blade server on which the sub-component is installed. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies. where *comp* is the sub-component: • "sp" for BMC or service processor • "exp[*x*]" for I/O-expansion card (where *x* identifies the expansion card) (advanced management module only) • "dtr[*x*]" for I/O-expansion card (where *x* identifies the expansion card) (management modules other than the advanced management module) • "cpu[*x*]" for microprocessor (where *x* identifies the microprocessor) • "be[*x*]" for storage expansion unit (where *x* identifies the expansion unit) • "ckvm" for concurrent KVM feature card (advanced management module only) • "hsec" for high-speed expansion card (advanced management module only) • "sb" for mezzanine assembly for double-width form factor blade servers (advanced management module only)	The env command can be directed to any installed device, in this case `-T system:blade[x]:sp` where *x* is the blade bay that identifies the blade server on which the integrated system management processor is installed.

Table 2. env (environment) command (continued)

Function	What it does	Command	Valid targets
Set I/O (switch) module as command target	Sets the specified I/O (switch) module as the persistent target for commands during the current session.	env -T system:switch[*x*] where *x* is the I/O (switch) module bay where the I/O (switch) module is installed.	The env command can be directed to any installed device, in this case `-T system:switch[x]` where *x* is the I/O (switch) module bay where the I/O (switch) module is installed.
Set power module as command target	Sets the specified power module as the persistent target for commands during the current session.	env -T system:power[*x*] where *x* is the power module bay where the power module is installed.	The env command can be directed to any installed device, in this case `-T system:power[x]` where *x* is the power module bay where the power module is installed.
Set blower as command target	Sets the specified blower as the persistent target for commands during the current session.	env -T system:blower[*x*] where *x* is the blower bay where the blower is installed.	The env command can be directed to any installed device, in this case `-T system:blower[x]` where *x* is the blower bay where the blower is installed.
Set media tray as command target	Sets the media tray as the persistent target for commands during the current session.	env -T system:mt	The env command can be directed to any installed device, in this case `-T system:mt`

Example:
To set the persistent target of commands to the service processor on the blade server in blade bay 5, while the BladeCenter unit is set as the default command target, at the `system>` prompt, type

```
env -T system:blade[5]:sp
```

The following example shows the information that is returned:

```
system> env -T system:blade[5]:sp
OK
system:blade[5]:sp>
```

To set the persistent target of commands to the service processor on the blade server in blade bay 5, while the BladeCenter unit is set as the default command target, at the `system>` prompt, you can also type

```
env -T blade[5]:sp
```

The following example shows the information that is returned:

```
system> env -T blade[5]:sp
```

```
OK
system:blade[5]:sp>
```

To issue the reset command on the blade server in blade bay 5, while the management module is set as the default command target, at the `system:mm[x]>` prompt, type

```
reset -T system:blade[5]
```

help command

This command displays a list of all commands that are available in the command-line interface with a brief description of each command. You can also issue the help command by typing `?`. Adding a `-h`, `-help`, or `?` option to a command displays syntax help for the command.

Table 3. help command

Function	What it does	Command	Valid targets
Help	Displays a list of commands and a brief description of each command.	help	Any installed device.
		?	Any installed device.

Example:
To display a list of commands, while management module 1 is set as the default command target, at the `system:mm[1]>` prompt, type

```
help
```

The following example shows the information that is returned:

```
system:mm[1]> help
           ?- Display commands
alertentries- View/edit remote alert recipients
        boot- Boot target
       clear- Clear the config
    clearlog- Clear the event log
     console- Start SOL session to a blade
    dhcpinfo- View DHCP server assigned settings
  displaylog- Display event log entries
   displaysd- Display service data
         dns- View/edit DNS config
         env- Set persistent command target
        exit- Log off
      health- View system health status
        help- Display command list
     history- Display command history
    identify- Control target location LED
    ifconfig- View/edit network interface config
        info- Display identity and config of target
         kvm- Controls the kvm owner
     ldapcfg- View/edit LDAP config
        list- Display installed targets
          mt- Controls the media tray owner
         nat- Display and configure NAT
     portcfg- Serial port configuration
       ports- Port configuration
       power- Control target power
        read- Restore configuration from chassis
       reset- Reset target
```

```
   service- Enable debugging by service personnel
  shutdown- Shutdown target
       slp- View/edit SLP parameters
      smtp- View/edit SMTP config
      snmp- View/edit SNMP config
       sol- View SOL status and view/edit SOL config
    sshcfg- View/edit SSH config
tcpcmdmode- View/edit TCP command mode config
 telnetcfg- View/edit telnet config
    update- Update firmware from TFTP server
     users- View/edit user login profiles
     alarm- Manage Telco System Management alarm(s)
     write- Save configuration to chassis

Type "<command> -h" for individual command syntax help.
       [ ] is used for indexing (by bay number)
       < > denotes a variable
       { } denotes optional arguments
        |  denotes choice
system:mm[1]>
```

To obtain help about the `env` command, type one of the following commands:

- `env -h`
- `env -help`
- `env ?`

history command

This command displays the last eight commands that were entered, allowing the user to choose and re-enter one of these commands. You choose the command to re-enter from the displayed list by typing an exclamation point (!) followed immediately by the numeric designation the command is assigned in the list. You can also recall one of the past eight previously entered commands using the up-arrow and down-arrow keys.

Table 4. history command

Function	What it does	Command	Valid targets
Command history	Displays the last eight commands that were entered.	history	Any installed device.
Re-enter previous command using numeric designation	Re-enters a numerically-specified command from the command history.	!*x* where *x* is the number of the command (0 - 7) to re-enter from the command history list.	Any installed device.

Example:

To display a list of the last eight commands entered, while management module 1 is set as the default command target, at the `system:mm[1]>` prompt, type

```
history
```

To re-enter the command designated by “2” in the command history, type

```
!2
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> history
 0 dns
 1 dns -on
 2 dns
 3 dns -i1 192.168.70.29
 4 dns
 5 dns -i1 192.168.70.29 -on
 6 dns
 7 history
system:mm[1]> !2
Enabled
-i1 192.168.70.29
-i2 0.0.0.0
-i3 0.0.0.0
system:mm[1]>
```

list (system physical configuration) command

This command displays a list of devices present within the command target. It can be used to determine how many management modules are installed in the BladeCenter unit and which management module is set as primary.

Table 5. list (system physical configuration) command

Function	What it does	Command	Valid targets
View command target	Displays the current command target. If a management-module bay is the current command target, it will be identified as primary or redundant.	list	Any installed device.
View system configuration tree	Displays the tree structure of devices present in the BladeCenter unit, starting at the command target level. If management-module bays are part of the tree, they will be identified as primary or redundant.	list -l *depth* where *depth* is “all” or “a” for full tree display, starting at the command target level. Specifying a *depth* of “1” displays the current command target. Specifying a *depth* of “2” displays the content of the current command target plus one level below it.	Any installed device.

Example:

To display a list of devices installed in the BladeCenter unit, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
list -l a
```

(This is the command syntax that can be used to determine the primary management module.)

The following example shows the information that is returned when the command is run on an advanced management module:

```
system> list -l a
```

```
system
        mm[1]    primary
        power[4]
        blower[1]
        blower[2]
        blade[1]
                sp
                exp[1]
        blade[5]
                sp
        blade[6]
                sp
        blade[7]
                sp
        blade[8]
                sp
        mt
system>
```

Common commands

Use these commands to monitor and control operation of BladeCenter components using the command-line interface:

- health command
- identify (location LED) command
- info (configuration information) command
- update (update firmware) command

health command

This command displays the current health status of the command target. It can also be used to display the alerts that are active for the command target. You can only specify one command target each time you run the health command.

Table 6. health command

Function	What it does	Command	Valid targets

Display health status	Displays the current health status of the command target. Return values are different for the BladeCenter and BladeCenter T configurations.
	• Possible return values for the BladeCenter configuration are:
	– ok
	– warning
	– critical
	• Possible return values for the BladeCenter T configurations are:
	– ok
	– minor
	– major
	– critical
		health	`-T system`
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:power[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Table 6. health command (continued)

Function	What it does	Command	Valid targets

Display health status for tree	Displays the current health status of the tree structure of devices present in the BladeCenter unit, starting at the command target level. If management-module bays are part of the tree, they will be identified as primary or redundant. Return values are different for the BladeCenter and BladeCenter T configurations.
	• Possible return values for the BladeCenter configuration are:
	– ok
	– warning
	– critical
	• Possible return values for the BladeCenter T configurations are:
	– ok
	– minor
	– major
	– critical
		health -l *depth*
		
		where *depth* is “2”, “all”, or “a” for full tree display, starting at the command target level.
		
		Specifying a *depth* of “1” displays health status of the current command target.
			`-T system`
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Display health status and alerts	Displays the current health status and active alerts for the command target. Return values are different for the BladeCenter and BladeCenter T configurations.
	• Possible return values for the health status of the BladeCenter configuration are:
	– ok
	– warning
	– critical
	• Possible return values for the health status of the BladeCenter T configurations are:
	– ok
	– minor
	– major
	– critical
	• Active alert information provides short text descriptions of alerts that are active for each monitored component.
	
	The total amount of information returned from the `health -f` command is limited to 1024 bytes.
		health -f	`-T system`
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Example:
To display the overall health status of the BladeCenter T unit, while the BladeCenter T unit is set as the default command target, at the `system>` prompt, type

```
health
```

To display the health status of all components installed in the BladeCenter T unit, that are valid command targets, while the BladeCenter T unit is set as the default command target, at the system> prompt, type

```
health -l a
```

To display the health status of the blade server installed in blade bay 5, while the BladeCenter T unit is set as the default command target, at the system> prompt, type

```
health -T system:blade[5]
```

To display the health status and alerts for all components installed in the BladeCenter T unit, that are valid command targets, while the BladeCenter T unit is set as the default command target, at the system> prompt, type

```
health -l a -f
```

The following example shows the information that is returned from these commands:

```
system> health
system:major
system> health -l a
system:major
   mm[1]:ok
   blade[1]:ok
   blade[3]:ok
   blade[5]:minor
   power[1]:ok
   power[2]:minor
   blower[1]:ok
   blower[2]:ok
   blower[3]:ok
   blower[4]:ok
   switch[1]:major
system> health -T system:blade[5]
blade[5]:minor
health -l a -f
system:major
   blade[5]:minor
      5V over voltage
      CPU1 temperature warning
   power[2]:minor
      5V over voltage
   switch[1]:major
      temperature fault
system>
```

identify (location LED) command

This command controls operation of the location LED in a blade server or in the BladeCenter unit. It can also be used to display the state of a location LED.

Table 7. identify (location LED) command

Function	What it does	Command	Valid targets

Display location LED state	Displays the current state of the location LED in the command target.
	
	Possible LED states are:
	• off
	• on
	• blink
		identify	`-T system`
			`-T system:blade[x]`
			
			where *x* is the blade bay number.

Set location LED state	Sets the state of the location LED in the command target.	identify -s *state*
		
		where *state* is “on”, “off”, or “blink”.
		
		Command use restricted (see “Commands and user authority” on page 5).
			`-T system`
			`-T system:blade[x]`
			
			where *x* is the blade bay number.

Turn on BladeCenter unit location LED for specified period of time	Turns on the location LED in the BladeCenter unit for a specified period of time before turning it off automatically.	identify -s on -d *time* where *time* is the number of seconds the location LED will remain lit. Command use restricted (see “Commands and user authority” on page 5).	`-T system`

Example:
To display the status of the location LED in the blade server in blade bay 4, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
identify -T system:blade[4]
```

To light the location LED in the blade server in blade bay 4, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
identify -s on -T system:blade[4]
```

The following example shows the information that is returned from a series of identify commands:

```
system> identify -T system:blade[4]
-s off
system> identify -s on -T system:blade[4]
OK
system> identify -T system:blade[4]
-s on
system>
```

info (configuration information) command

This command displays information about BladeCenter components and their configuration.

Table 8. info (configuration information) command

Function	What it does	Command	Valid targets

Display component information	Displays identification and configuration information for the command target.	info
		
		Note: Only one target at a time can be viewed with the info command.
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:blade[x] :exp[x]` (for advanced management modules)
			`-T system:blade[x] :dtr[x]` (for management modules other than the advanced management module)
			`-T system:blade[x]:sp`
			`-T system:blade[x]:be`
			`-T system:blade[x]:sb` (for advanced management modules)
			`-T system:blade[x]: cpu[x]`
			`-T system:blade[x]:hsec` (for advanced management modules)
			`-T system:blade[x]:ckvm` (for advanced management modules)
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:mt`
			
			where *x* is the management-module bay number, blade server bay number, I/O (switch) module bay number, microprocessor number, power module bay number, or daughter-card number.

Notes:

1. The command targets `-T system:blade[x]:exp[x]` and `-T system:blade[x]:dtr[x]` are shown with a line break before the `:exp[x]` or `:dtr[x]`. When these command targets are entered, the entire entry must all be on one line.

2. This command returns vital product data (VPD) information for the command target. For some targets, additional VPD information is available when using the advanced management module.

Example:
To view the information about the management module in management-module bay 1, while this management module is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
info
```

The following example shows the information that is returned from the info command:

```
system:mm[1]> info
UUID: 0000 0000 0000 0000 0000 0000 0000 0000
Manuf ID: SLRM
Mach type/model: Management Module
Mach serial number: n/a
Manuf date: 4102
Part no.: 02R1606
FRU no.: 59P6622
FRU serial no.: J1P702A511F
Main application
   Build ID:       DVETXX-
   File name:      CNETMNUS.PKT
   Rel date:       05-27-04
   Rev:            16
Boot ROM
   Build ID:       BRBR14-
   File name:      CNETBRUS.PKT
   Rel date:       09-12-02
   Rev:            16
Remote control
   Build ID:       BRRG14-
   File name:      CNETRGUS.PKT
   Rel date:       09-12-02
   Rev:            16
system:mm[1]>
```

update (update firmware) command

This command updates firmware using a Trivial File Transfer Protocol (TFTP) server and displays information about firmware installed in BladeCenter components.

Table 9. update (update firmware) command

Function	What it does	Command	Valid targets

Display update command help	Displays information about using the update command.	update	`-T system:mm[x]`
			`-T system:blade[x]:sp`
			`-T system:switch[x]`
			where *x* is the primary management-module, blade server bay number, or I/O (switch) module bay number.

Table 9. update (update firmware) command (continued)

Function	What it does	Command	Valid targets

Display firmware attributes	Displays attributes of the firmware installed in the command target. Return values are:
	• Firmware type
	• Build ID
	• Filename
	• Release date
	• Revision level
		update -a	`-T system:mm[x]`
			`-T system:blade[x]:sp`
			`-T system:switch[x]`
			where *x* is the primary management-module, blade server bay number, or I/O (switch) module bay number.

Update firmware	Update firmware for the command target.
	Important: Command authority definitions might change between firmware versions. Make sure that the command authority level set for each user is correct after updating management-module firmware.
		update -i *ip_address* -l *filelocation*
		where:
		• *ip_address* is the IP address of TFTP server.
		• *filelocation* is the location of the firmware update file.
		Command use restricted (see "Commands and user authority" on page 5).
			`-T system:mm[x]`
			`-T system:blade[x]:sp`
			`-T system:switch[x]`
			where *x* is the primary management-module, blade server bay number, or I/O (switch) module bay number.

Update firmware (verbose)	Update firmware for the command target, showing details of the firmware download and flash operations. The detailed information is not shown until the update is complete, which might take several minutes.
	Important: Command authority definitions might change between firmware versions. Make sure that the command authority level set for each user is correct after updating management-module firmware.
		update -i *ip_address* -l *filelocation* -v
		where:
		• *ip_address* is the IP address of TFTP server.
		• *filelocation* is the location of the firmware update file.
		Command use restricted (see "Commands and user authority" on page 5).
			`-T system:mm[x]`
			`-T system:blade[x]:sp`
			`-T system:switch[x]`
			where *x* is the primary management-module, blade server bay number, or I/O (switch) module bay number.

Example:
To update the firmware and display update details for the management module in management-module bay 1, while this management module is set as the persistent command environment, type the following command at the `system:mm[1]>` prompt. For this example, the IP address of the TFTP server is 192.168.70.120 and the firmware file containing the update is named dev_mm.pkt.

```
update -v -i 192.168.70.120 -l dev_mm.pkt
```

To display information about firmware installed in the management module in management-module bay 1, while this management module is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
update -a
```

To update the service-processor firmware in the blade server in blade bay 8 (not using verbose mode), while the management module in management-module bay 1 is set as the persistent command environment, type the following command at the

system:mm[1]> prompt. For this example, the IP address of the TFTP server is 192.168.70.120 and the firmware file containing the update is named h8.pkt.

```
update -i 192.168.70.120 -l h8.pkt -T system:blade[8]:sp
```

The following example shows the information that is returned from these three update commands:

```
system:mm[1]> update -v -i 192.168.70.120 -l dev_mm.pkt
TFTP file upload successful 1517829.
Starting flash packet preparation.
Flash preparation - packet percent complete 24.
Flash preparation - packet percent complete 48.
Flash preparation - packet percent complete 72.
Flash preparation - packet percent complete 96.
Flash preparation - packet percent complete 100.
Flash operation phase starting.
Flashing - packet percent complete 34.
Flashing - packet percent complete 38.
Flashing - packet percent complete 50.
Flashing - packet percent complete 55.
Flashing - packet percent complete 80.
Flashing - packet percent complete 90.
Flash operation complete. The new firmware will become active after the next
reset of the MM.
OK
system:mm[1]> update -a
Bay 1 Name 1
Firmware type: Main application
Build ID: BRETKD+
Filename: CNETMNUS.PKT
Released: 11-17-03
Revision: 16
Firmware type: Boot ROM
Build ID: BRBR1B+
Filename: CNETBRUS.PKT
Released: 10-27-03
Revision: 16
Firmware type: Remote control
Build ID: BRRG1B+
Filename: CNETRGUS.PKT
Released: 10-27-03
Revision: 16
OK
system:mm[1]> update -i 192.168.70.120 -l h8.pkt -T system:blade[8]:sp
OK
system:mm[1]>
```

Configuration commands

Use these commands to view and configure network settings and Ethernet interfaces:

- alertentries command
- clear command (management modules other than the advanced management module)
- clear command (advanced management module only)
- dhcpinfo command
- displaysd command (advanced management module only)
- dns command
- ifconfig command (management modules other than the advanced management module)
- ifconfig command (advanced management module only)
- ldapcfg command (advanced management module only)
- nat command (advanced management module only)
- portcfg command (advanced management module only)
- ports command (advanced management module only)
- service command (advanced management module only)
- slp command (advanced management module only)
- smtp command
- snmp command
- sol (serial over LAN) command
- sshcfg command (advanced management module only)
- tcpcmdmode command (management modules other than the advanced management module)
- tcpcmdmode command (advanced management module only)
- telnetcfg (Telnet configuration) command
- uplink (management module failover) command
- users command (management modules other than the advanced management module)
- users command (advanced management module only)

alertentries command

This command manages the recipients of alerts generated by the primary management module.

Table 10. alertentries command

Function	What it does	Command	Valid targets
Display alert properties for all recipients	Displays alert properties for all management-module alert recipients. Returned values for each alert recipient are: • recipient name • notification method (E-Mail over LAN/Director comp./SNMP over LAN) • type of alerts received (Receives critical alerts only/Receives all alerts/Disabled)	alertentries	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display alert properties for alert recipients	Displays alert properties for the specified management-module alert recipient profile. Returned values are: • -status *alert_recipient_status* (on/off) • -n *alert_recipient_name* • -f *alert_type* (critical/none) • -t *notification_method* (email/director/snmp) • -e *email_address* (used for e-mail notifications) • -i *static_IP_addr/hostname* (used for IBM Director notifications)	alertentries -*recip_number* where *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the “Display alert properties for all recipients” list.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Delete alert recipient	Delete the specified alert recipient.	alertentries -*recip_number* -del where *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the “Display alert properties for all recipients” list. It is possible to delete an empty alert recipient. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 10. alertentries command (continued)

Function	What it does	Command	Valid targets
Create alert recipient	Create the specified alert recipient. All fields must be specified when creating an alert recipient.	alertentries -*recip_number* -n *recip_name* -status *alert_status* -f *filter_type* -t *notification_method* -e *email_addr* -i *ip_addr/hostname* where: • *recip_number* is a number from 1 to 12 that corresponds to an unused recipient number in the “Display alert properties for all recipients” list. • *recip_name* is a alphanumeric string up to 31 characters in length containing any character, including spaces, except for angle brackets (< and >). If the string includes spaces it must be enclosed in double-quotes. • *alert_status* is on or off for receipt of alerts. • *filter_type* filters the alert types received: critical (receive critical alerts only) or none (receive all alerts). • *notification_method* is email, director (IBM Director) or snmp. – For e-mail, you must specify an e-mail address (-e argument). – For director, you must specify an IP address (-i argument). – If snmp is selected, the -e and -i arguments are not needed. • *email_addr* is a valid e-mail address string up to 63 characters in length. *(continued on next page)*	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 10. alertentries command (continued)

Function	What it does	Command	Valid targets
Create alert recipient *(continued)*		• *ip_addr/hostname* is a valid static IP address or an alphanumeric hostname string for the recipient that is up to 49 characters in length that can include periods (.), hyphens (-), and underscores (_). Command use restricted (see "Commands and user authority" on page 5).	
Set alert recipient name	Sets a name for the specified alert recipient.	alertentries -*recip_number* -n *recip_name* where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *recip_name* is a alphanumeric string up to 31 characters in length that can include any character, including spaces, except for angle brackets (< and >). If the name includes spaces it must be enclosed in double-quotes. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set alert recipient status	Sets status for the specified alert recipient. The status determines if a recipient will receive alarm notifications.	alertentries -*recip_number* -status *alert_status* where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *alert_status* is on or off. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 10. alertentries command (continued)

Function	What it does	Command	Valid targets
Set alert types received	Filters the types of alert that are received by the specified alert recipient.	alertentries -*recip_number* -f *filter_type* where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *alert_type* filters the alert types received: critical (receive critical alerts only) or none (receive all alerts). Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Set alert notification method	Sets the alert notification method for the specified alert recipient.	alertentries -*recip_number* -t *notification_method* where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *notification_method* is email, director (IBM Director) or snmp. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Set alert recipient e-mail address	Sets the e-mail address for the specified alert recipient. This e-mail address is used to send alerts to the recipient via e-mail. The e-mail address can be set only if the alert notification method (-t option) is set to email. The -t and -e options can be combined within the same command.	alertentries -*recip_number* -e *email_addr* where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *email_addr* is a valid e-mail address string up to 63 characters in length. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Table 10. alertentries command (continued)

Function	What it does	Command	Valid targets
Set alert recipient IP address or hostname	Sets the IP address or hostname used to send alert notifications to the specified alert recipient using IBM Director. The IP address or hostname used to send alert notifications can be set only if the alert notification method (-t option) is set to director (IBM Director). The -t and -i options can be combined within the same command.	alertentries -*recip_number* -i *ip_addr/hostname* where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *ip_addr/hostname* is a valid static IP address or an alphanumeric hostname string up to 49 characters in length that can include periods (.), hyphens (-), and underscores (_). Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:
To view the configuration for alert recipient 1, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
alertentries -1
```

To configure alert recipient 2 to receive only critical alert notifications by e-mail, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
alertentries -2 -n test2 -status on -f critical -t email -e test2@us.ibm.com
```

To configure alert recipient 3 to receive all alert notifications through IBM Director, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
alertentries -3 -n test3 -status on -f none -t director -i 192.168.70.140
```

To configure alert recipient 4 to receive all alert notifications through SNMP, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
alertentries -4 -n test4 -status on -f none -t snmp
```

The following example shows the information that is returned from these commands:

```
system:mm[1]> alertentries -1
-status on
-n test1
-f critical
-t email
-e test1@us.ibm.com
system:mm[1]> alertentries -2 -n test2 -status on -f critical -t email
-e test2@us.ibm.com
```

```
OK
system:mm[1]> alertentries -3 -n test3 -status on -f none -t director
-i 192.168.70.140
OK
system:mm[1]> alertentries -4 -n test4 -status on -f none -t snmp
OK
system:mm[1]>
```

clear command (management modules other than the advanced management module)

Note: The clear command operates differently for the advanced management module and for other management module types. The following command description is for management modules other than the advanced management module. See “clear command (advanced management module only)” on page 40 for command syntax for the advanced management module.

This command restores the primary management module configuration or an I/O (switch) module configuration to the default settings. The command must always include the `-config` option.

Table 11. clear command (management modules other than the advanced management module)

Function	What it does	Command	Valid targets
Restore default configuration of primary management module	Restores the default configuration of the primary management module; then, resets the management module. No results are returned from this command because it resets the management module. When you restore the management-module configuration, the Ethernet configuration method is set to a value of dthens. After the management module resets, this causes the management module to try dhcp configuration and then default to the static IP configuration, which might cause the management module to remain offline for longer than normal. See the “ifconfig command (advanced management module only)” on page 49 for information.	clear -config Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Restore default configuration of I/O (switch) module	Restores the configuration of the specified I/O (switch) module to the default settings.	clear -config Command use restricted (see “Commands and user authority” on page 5).	`-T system:switch[`*x*`]` where *x* is the I/O (switch) module bay number.

Example:
To restore the primary management-module configuration to default settings, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
clear -config
```

No results are returned from this command. After the management module resets, you will need to start a new command-line session.

clear command (advanced management module only)

Note: The clear command operates differently for the advanced management module and for other management module types. The following command description is for the advanced management module. See “clear command (management modules other than the advanced management module)” on page 39 for command syntax for management modules other than the advanced management module.

This command restores the primary management module configuration or an I/O (switch) module configuration to the default settings. The command must always include the `-cnfg` or `-config` option.

Table 12. clear command (advanced management module only)

Function	What it does	Command	Valid targets
Restore default configuration of primary management module and keep logs	Restores the default configuration of the primary management module, retaining log information; then, resets the management module. No results are returned from this command because it resets the management module. When you restore the management-module configuration, the Ethernet configuration method is set to a value of dthens. After the management module resets, this causes the management module to try dhcp configuration and then default to the static IP configuration, which might cause the management module to remain offline for longer than normal. See the “ifconfig command (advanced management module only)” on page 49 for information.	clear -cnfg Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 12. clear command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Restore default configuration of primary management module and delete logs (This command option should be used only for backward compatibility with scripts.)	Restores the default configuration of the primary management module, deleting log information; then, resets the management module. No results are returned from this command because it resets the management module. When you restore the management-module configuration, the Ethernet configuration method is set to a value of dthens. After the management module resets, this causes the management module to try dhcp configuration and then default to the static IP configuration, which might cause the management module to remain offline for longer than normal. See the "ifconfig command (advanced management module only)" on page 49 for information.	clear -cnfg Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Restore default configuration of I/O (switch) module	Restores the configuration of the specified I/O (switch) module to the default settings.	clear -cnfg Command use restricted (see "Commands and user authority" on page 5).	`-T system:switch[x]` where *x* is the I/O (switch) module bay number.
Restore default configuration of I/O (switch) module (This command option should be used only for backward compatibility with scripts.)	Restores the configuration of the specified I/O (switch) module to the default settings.	clear -config Command use restricted (see "Commands and user authority" on page 5).	`-T system:switch[x]` where *x* is the I/O (switch) module bay number.

Example:
To restore the primary management-module configuration to default settings and retain log information, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
clear -cnfg
```

No results are returned from this command. After the management module resets, you will need to start a new command-line session.

dhcpinfo command

This command displays the IP configuration that is assigned to the primary management module by the DHCP server.

Note: The `dhcpinfo` command does not apply to eth1, which always uses a static IP configuration.

Table 13. dhcpinfo command

Function	What it does	Command	Valid targets
Display Ethernet channel 0 DHCP configuration	If the IP configuration for eth0 is assigned by a DHCP server, the configuration that is assigned by the DHCP server and DHCP server information is displayed. If the IP configuration for eth0 is *not* assigned by a DHCP server, an error message is displayed. Possible configuration values returned are: • -server *dhcp_ip_address* • -n *hostname* • -i ip_address • -g *gateway_address* • -s *subnet_mask* • -d *domainname* • -dns1 *primary _dns_ip_address* • -dns2 *secondary _dns_ip_address* • -dns3 *tertiary _dns_ip_1address*	dhcpinfo -eth0	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:
To display the DHCP server assigned network settings for Ethernet channel 0, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
dhcpinfo -eth0
```

The following example shows the information that is returned:

```
system:mm[1]> dhcpinfo -eth0
-server 192.168.70.29
-n MM00096BCA0C80
-i 192.168.70.183
-g 192.168.70.29
-s 255.255.255.0
-d linux-sp.raleigh.ibm.com
-dns1 192.168.70.29
-dns2 0.0.0.0
-dns3 0.0.0.0
system:mm[1]>
```

displaysd command (advanced management module only)

This command captures and displays service information. Service information includes BladeCenter VPD, the management-module event log, and connection status and self-test results from the primary management module. If multiple user interface sessions issue the displaysd command, the commands will be processed in the order that they are received.

Table 14. displaysd command

Function	What it does	Command	Valid targets
Capture and display service information	Capture and display service information on screen.	displaysd	`-T system`
Display management module connection and self-test status	Displays connection status and latest self-test results for all installed management modules.	displaysd -mmstat	`-T system`

Example:
To capture and display service information, while the chassis is set as the persistent command environment, at the `system>` prompt, type

```
displaysd
```

The following example shows the information that is returned:

```
system> displaysd
SPAPP Capture Available
Time: 10/04/2005 21:47:43
UUID: Not Available
•
•
•
system>
```

Note: If a large amount of service information is available, display could exceed the capacity of your command-prompt window, resulting in loss of information displayed at the start of the data set. If this happens, you will need to clear the management-module event log to reduce the amount of information being captured.

dns command

This command configures and displays the management-module DNS settings.

Table 15. dns command

Function	What it does	Command	Valid targets
Display DNS configuration of management module	Displays the current DNS configuration of the management module. Possible return values are: • enabled • disabled • -i1 *first ip_address* • -i2 *second ip_address* • -i3 *third ip_address*	dns	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
DNS - enable	Enables the management-module DNS configuration.	dns -on Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 15. dns command (continued)

Function	What it does	Command	Valid targets
DNS - disable	Disables the management-module DNS configuration.	dns -off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
DNS first IP address - set	Checks syntax and sets the first IP address.	dns -i1 *ip_address* where *ip_address* is the first IP address. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
DNS second IP address - set	Checks syntax and sets the second IP address.	dns -i2 *ip_address* where *ip_address* is the second IP address. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
DNS third IP address - set	Checks syntax and sets the third IP address.	dns -i3 *ip_address* where *ip_address* is the third IP address. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Example:
To set the first IP address of the management-module DNS server to 192.168.70.29 and enable DNS on the primary management module, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
dns -i1 192.168.70.29 -on
```

To display the DNS status of the primary management module, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
dns
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> dns -i1 192.168.70.29 -on
Changes to the network settings will take effect after the next reset of the MM.
system:mm[1]> dns
Enabled
-i1 192.168.70.29
-i2 0.0.0.0
-i3 0.0.0.0
system:mm[1]>
```

ifconfig command (management modules other than the advanced management module)

Note: The ifconfig command operates differently for the advanced management module and for other management module types. The following command description is for management modules other than the advanced management module. See “ifconfig command (advanced management module only)” on page 49 for command syntax for the advanced management module.

This command configures and displays the network interface settings for the management-module Ethernet interface and the blade server integrated system management processors.

Table 16. ifconfig command (management modules other than the advanced management module)

Function	What it does	Command	Valid targets
Display Ethernet channel 0 configuration	Displays the current configuration of Ethernet channel 0. Possible return values are: • enabled • disabled • -i *static_ip_address* • -g *gateway_address* • -s *subnet_mask* • -n *hostname* • -c *config_method* • -r *data_rate* • -d *duplex_mode* • -m *mtu* • -l *locally_administered_mac_addr* • -b *burnedin_mac_address*	ifconfig -eth0	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 static IP address	Checks syntax and sets the static IP address for Ethernet channel 0.	ifconfig -eth0 -i *ip_address* where *ip_address* is the static IP address for Ethernet channel 0. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 gateway IP address	Checks syntax and sets the gateway IP address for Ethernet channel 0.	ifconfig -eth0 -g *ip_address* where *ip_address* is the gateway IP address for Ethernet channel 0. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 subnet mask	Checks syntax and sets the subnet mask for Ethernet channel 0.	ifconfig -eth0 -s *sub_mask* where *sub_mask* is the subnet mask for Ethernet channel 0. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 16. ifconfig command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Set Ethernet channel 0 hostname	Checks syntax and sets the host name for Ethernet channel 0.	ifconfig -eth0 -n *hostname* where *hostname* is the host name for Ethernet channel 0. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 configuration method	Checks syntax and sets the configuration method for Ethernet channel 0. A value of dthens will try the dhcp configuration and default to the static IP configuration if dhcp is unsuccessful.	ifconfig -eth0 -c *config_method* where *config_method* is dhcp, static, or dthens. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 data rate	Checks syntax and sets the data rate for Ethernet channel 0.	ifconfig -eth0 -r *data_rate* where *data_rate* is auto, 10, or 100. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 duplex mode	Checks syntax and sets the duplex mode for Ethernet channel 0.	ifconfig -eth0 -d *duplex_mode* where *duplex_mode* is auto, half, or full. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 MTU	Checks syntax and sets the MTU (maximum transmission unit) for Ethernet channel 0.	ifconfig -eth0 -m *mtu* where *mtu* is between 60 and 1500, inclusive. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 static MAC address (locally administered)	Checks syntax and sets the locally administered MAC address to the specified MAC address for Ethernet channel 0.	ifconfig -eth0 -l *address* where *address* is the locally administered MAC address for Ethernet channel 0. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 16. ifconfig command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Display Ethernet channel 1 configuration	Displays the current configuration of Ethernet channel 1. Possible return values are: • enabled • disabled • -i *static_ip_address* • -g *gateway_address* • -s *subnet_mask* • -r *data_rate* • -d *duplex_mode* • -m *mtu* • -l *locally_administered_mac_addr* • -b *burnedin_mac_address*	ifconfig -eth1	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 1 static IP address	Checks syntax and sets the static IP address for Ethernet channel 1.	ifconfig -eth1 -i *ip_address* where *ip_address* is the static IP address for Ethernet channel 1. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 1 gateway IP address	Checks syntax and sets the gateway IP address for Ethernet channel 1.	ifconfig -eth1 -g *ip_address* where *ip_address* is the gateway IP address for Ethernet channel 1. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 1 subnet mask	Checks syntax and sets the subnet mask for Ethernet channel 1.	ifconfig -eth1 -s *sub_mask* where *sub_mask* is the subnet mask for Ethernet channel 1. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 1 static MAC address (locally administered)	Checks syntax and sets the locally administered MAC address to the specified MAC address for Ethernet channel 1.	ifconfig -eth1 -l *address* where *address* is the locally administered MAC address for Ethernet channel 1. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable Ethernet channel 1	Enables Ethernet channel 1.	ifconfig -eth1 -up Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 16. ifconfig command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Disable Ethernet channel 1	Disables Ethernet channel 1.	ifconfig -eth1 -down Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set starting IP address for blade server integrated system management processor	Sets the starting point of the integrated system management processor IP addresses for blade servers that are installed in the BladeCenter unit.	ifconfig -i *ip_address* where *ip_address* is the starting IP address for all blade servers that are installed in the BladeCenter unit. Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[1]:sp`

Example:

To display the configuration for Ethernet channel 0, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
ifconfig -eth0
```

To set the static IP address for Ethernet channel 0 to 192.168.70.133, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
ifconfig -eth0 -i 192.168.70.133 -c static
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> ifconfig -eth0
Enabled
-i 10.10.10.10
-g 0.0.0.0
-s 255.255.255.0
-n MM00096BCA0C80
-c Try DHCP server.  If it fails, use static IP config.
-r Auto
-d Auto
-m 1500
-l 00:00:00:00:00:00
-b 00:09:6B:CA:0C:80
system:mm[1]> ifconfig -eth0 -i 192.168.70.133 -c static
Changes to the network settings will take effect after the next reset of the MM.
system:mm[1]>
```

ifconfig command (advanced management module only)

Note: The ifconfig command operates differently for the advanced management module and for other management module types. The following command description is for the advanced management module. See “ifconfig command (management modules other than the advanced management module)” on page 45 for command syntax for management modules other than the advanced management module.

This command configures and displays the network interface settings for the management-module Ethernet interface, I/O-module Ethernet interface, and the blade server integrated system management processors and installed options.

Table 17. ifconfig command (advanced management module only)

Function	What it does	Command	Valid targets
Display management module Ethernet channel 0 configuration	Displays the current configuration of Ethernet channel 0 for the management module. Possible return values are: • enabled • disabled • -i *static_ip_address* • -g *gateway_address* • -s *subnet_mask* • -n *hostname* • -c *config_method* • -r *data_rate* • -d *duplex_mode* • -m *mtu* • -l *locally_administered_mac_addr* • -b *burnedin_mac_address*	ifconfig -eth0	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 static IP address	Checks syntax and sets the static IP address for Ethernet channel 0 for the management module.	ifconfig -eth0 -i *ip_address* where *ip_address* is the static IP address for Ethernet channel 0. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 gateway IP address	Checks syntax and sets the gateway IP address for Ethernet channel 0 for the management module.	ifconfig -eth0 -g *ip_address* where *ip_address* is the gateway IP address for Ethernet channel 0. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 17. ifconfig command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Set management module Ethernet channel 0 subnet mask	Checks syntax and sets the subnet mask for Ethernet channel 0 for the management module.	ifconfig -eth0 -s *sub_mask* where *sub_mask* is the subnet mask for Ethernet channel 0. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 hostname	Checks syntax and sets the host name for Ethernet channel 0 for the management module.	ifconfig -eth0 -n *hostname* where *hostname* is the host name for Ethernet channel 0. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 configuration method	Checks syntax and sets the configuration method for Ethernet channel 0 for the management module. A value of dthens will try the dhcp configuration and default to the static IP configuration if dhcp is unsuccessful.	ifconfig -eth0 -c *config_method* where *config_method* is dhcp, static, or dthens. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 data rate	Checks syntax and sets the data rate for Ethernet channel 0 for the management module.	ifconfig -eth0 -r *data_rate* where *data_rate* is auto, 10, or 100. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 duplex mode	Checks syntax and sets the duplex mode for Ethernet channel 0 for the management module.	ifconfig -eth0 -d *duplex_mode* where *duplex_mode* is auto, half, or full. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 MTU	Checks syntax and sets the MTU (maximum transmission unit) for Ethernet channel 0 for the management module.	ifconfig -eth0 -m *mtu* where *mtu* is between 60 and 1500, inclusive. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 17. ifconfig command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Set management module Ethernet channel 0 static MAC address (locally administered)	Checks syntax and sets the locally administered MAC address to the specified MAC address for Ethernet channel 0 for the management module.	ifconfig -eth0 -l *address* where *address* is the locally administered MAC address for Ethernet channel 0. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable management module Ethernet channel 0	Enables the Ethernet channel 0 interface for the management module.	ifconfig -eth0 -up Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Disable management module Ethernet channel 0	Disables the Ethernet channel 0 interface for the management module.	ifconfig -eth0 -down Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set starting IP address for blade server integrated system management processor	Sets the starting point of the integrated system management processor IP addresses for blade servers that are installed in the BladeCenter unit. **Note:** This command has similar function to the ifconfig -bsmp *ip_address* command.	ifconfig -i *ip_address* where *ip_address* is the IP address of the specified blade server. The IP addresses for all other blade servers that are installed in the BladeCenter unit will be calculated based on this address. Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[x]:sp` where *x* is the blade server bay number.
Set starting IP address for blade server integrated system management processor	Sets the starting point of the integrated system management processor IP addresses for blade servers that are installed in the BladeCenter unit. **Note:** This command has similar function to the ifconfig -i *ip_address* command.	ifconfig -bsmp *ip_address* where *ip_address* is the starting IP address for all blade servers installed in the BladeCenter unit. Command use restricted (see "Commands and user authority" on page 5).	`-T system`
Enable cKVM feature for blade server	Enable cKVM feature for the specified blade server. **Note:** The cKVM feature requires special hardware and is not available for all blade servers.	ifconfig -ckvm enabled Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.
Disable cKVM feature for blade server	Disable cKVM feature for the specified blade server.	ifconfig -ckvm disabled Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.

Table 17. ifconfig command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Display network settings for BladeCenter unit	Displays network settings for the BladeCenter unit. Valid return values are: • -bsmp *base_bsmp_ip_address* • -v *VLAN-id*	ifconfig	`-T system`
VLAN ID for BladeCenter unit	Checks syntax and sets the VLAN ID for the BladeCenter unit.	ifconfig -v *VLAN-id* where *VLAN-id* is from 1 to 4095, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system`
Enable global cKVM feature for BladeCenter unit	Enable cKVM feature globally for the BladeCenter unit. (This is the same as running the ifconfig -ckvm enable command directed to each blade server.)	ifconfig -ckvm enable Command use restricted (see "Commands and user authority" on page 5).	`-T system`
Disable global cKVM feature for BladeCenter unit	Disable cKVM feature globally for the BladeCenter unit. (This is the same as running the ifconfig -ckvm disable command directed to each blade server.)	ifconfig -ckvm disable Command use restricted (see "Commands and user authority" on page 5).	`-T system`
Display network settings for I/O module	Displays network settings for the specified I/O module. Valid return values are: • I/O-module type • -i *ip_address* • -s *subnet_mask* • -g *gateway_address* • -em *ext_mgt_status* • -ep *ext_port_status*	ifconfig	`-T system:switch[x]` where *x* is the I/O-module bay number.
Set I/O-module gateway IP address	Checks syntax and sets the gateway IP address for the specified I/O module.	ifconfig -intf -g *ip_address* where *ip_address* is the gateway IP address for the I/O module. Command use restricted (see "Commands and user authority" on page 5).	`-T system:switch[x]` where *x* is the I/O-module bay number.
Set I/O-module subnet mask	Checks syntax and sets the subnet mask for the specified I/O module.	ifconfig -intf -s *sub_mask* where *sub_mask* is the subnet mask for the I/O module. Command use restricted (see "Commands and user authority" on page 5).	`-T system:switch[x]` where *x* is the I/O-module bay number.

Table 17. ifconfig command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Enable external management for I/O module	Enables external management on all ports for the specified I/O module.	ifconfig -intf -em enabled Command use restricted (see "Commands and user authority" on page 5).	-T system:switch[*x*] where *x* is the I/O-module bay number.
Disable external management for I/O module	Disables external management on all ports for the specified I/O module.	ifconfig -intf -em disabled Command use restricted (see "Commands and user authority" on page 5).	-T system:switch[*x*] where *x* is the I/O-module bay number.
Enable external ports for I/O module	Enables external ports for the specified I/O module.	ifconfig -intf -ep enabled Command use restricted (see "Commands and user authority" on page 5).	-T system:switch[*x*] where *x* is the I/O-module bay number.
Disable external ports for I/O module	Disables external ports for the specified I/O module.	ifconfig -intf -ep disabled Command use restricted (see "Commands and user authority" on page 5).	-T system:switch[*x*] where *x* is the I/O-module bay number.

Example:

To display the configuration for Ethernet channel 0, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
ifconfig -eth0
```

To set the static IP address for Ethernet channel 0 to 192.168.70.133, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
ifconfig -eth0 -i 192.168.70.133 -c static
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> ifconfig -eth0
Enabled
-i 10.10.10.10
-g 0.0.0.0
-s 255.255.255.0
-n MM00096BCA0C80
-c Try DHCP server.  If it fails, use static IP config.
-r Auto
-d Auto
-m 1500
-l 00:00:00:00:00:00
-b 00:09:6B:CA:0C:80
system:mm[1]> ifconfig -eth0 -i 192.168.70.133 -c static
Changes to the network settings will take effect after the next reset of the MM.
system:mm[1]>
```

ldapcfg command (advanced management module only)

This command sets and displays the LDAP configuration settings for the advanced management module.

Table 18. ldapcfg command

Function	What it does	Command	Valid targets
Display LDAP settings	Displays the LDAP settings for the management module. Returned values are: • -v *version* • -t *name*	ldapcfg	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set LDAP security version	Sets version of LDAP security used by the management module.	ldapcfg -v *version* where *version* is: • v1 for old user permission model • v2 for the enhanced role-based security model Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set LDAP name	Sets the LDAP name for the management module.	ldapcfg -t *name* where *name* is an alphanumeric string up to 63 characters in length containing any character except for angle brackets (< and >) and spaces. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

To set the management module LDAP security version to v1, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
ldapcfg -v v1
```

To display the management module LDAP settings, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
ldapcfg
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> ldapcfg -v v1
OK
system:mm[1]> ldapcfg
-v v1
-t AMM_one
system:mm[1]>
```

nat command (advanced management module only)

This command sets and displays the network protocol settings for the specified I/O module.

Notes:

1. If the nat command is directed to an I/O module that does not support the network address table (NAT), the “NAT configuration is not supported on this IO module” message is returned.
2. When setting values for an empty row in the network address table, all options must be specified together using a single command.

Table 19. nat command

Function	What it does	Command	Valid targets
Display I/O-module network protocol settings	Displays the network port settings for the specified I/O module. Returned values include those in Table 20 on page 57.	nat	`-T system:switch[x]` where *x* is the I/O-module bay number.
Reset I/O-module network protocol settings	Resets all network port settings for the specified I/O module to the default values. Default values are in Table 20 on page 57. You must activate any changes to the network protocol settings before they take effect.	nat -reset Command use restricted (see “Commands and user authority” on page 5).	`-T system:switch[x]` where *x* is the I/O-module bay number.
Activate I/O-module network protocol settings	Activates all network port settings for the specified I/O module, putting them into effect.	nat -activate Command use restricted (see “Commands and user authority” on page 5).	`-T system:switch[x]` where *x* is the I/O-module bay number.
Set protocol name for row in I/O-module NAT table	Sets a protocol name for the specified row in the NAT table for the specified I/O module.	nat -*index* -pn *protocol_name* where: • *index* is a number from 1 to 10 that corresponds to a row in the NAT table. • *protocol_name* is FTP, HTTP, HTTPS, NTP, Radius, SSH, SNMP, SNMP-Trap, SYSLOGD, TACACS+, TELNET, or TFTP. Command use restricted (see “Commands and user authority” on page 5).	`-T system:switch[x]` where *x* is the I/O-module bay number.

Table 19. nat command (continued)

Function	What it does	Command	Valid targets
Set protocol ID for row in NAT table	Sets a protocol ID for the specified row in the NAT table for the specified I/O module.	nat -*index* -pi *protocol_id* where: • *index* is a number from 1 to 10 that corresponds to a row in the NAT table. • *protocol_id* is tcp or udp. Command use restricted (see "Commands and user authority" on page 5).	`-T system:switch[x]` where *x* is the I/O-module bay number.
Set internal port number for row in NAT table	Sets the internal port number for the specified row in the NAT table for the specified I/O module.	nat -*index* -ip *port_number* where: • *index* is a number from 1 to 10 that corresponds to a row in the NAT table. • *port_number* is between 1 and 65534, inclusive. Command use restricted (see "Commands and user authority" on page 5).	`-T system:switch[x]` where *x* is the I/O-module bay number.
Set external port number for row in NAT table	Sets the external port number for the specified row in the NAT table for the specified I/O module.	nat -*index* -ep *port_number* where: • *index* is a number from 1 to 10 that corresponds to a row in the NAT table. • *port_number* is between 1000 and 65534, inclusive. Command use restricted (see "Commands and user authority" on page 5).	`-T system:switch[x]` where *x* is the I/O-module bay number.
Set state for row in NAT table	Enables or disables the specified row in the NAT table for the specified I/O module.	nat -*index* -en *state* where: • *index* is a number from 1 to 10 that corresponds to a row in the NAT table. • *state* is enabled or disabled. Command use restricted (see "Commands and user authority" on page 5).	`-T system:switch[x]` where *x* is the I/O-module bay number.

Table 20. Default NAT table values for nat command

Index	Protocol Name	Protocol ID	Internal Port	External Port	State
1	http	tcp	80	1080	enabled
2	telnet	tcp	23	1023	enabled
3	https	tcp	43	1043	enabled
4	ssh	tcp	22	1022	enabled
5	snmp	udp	161	1161	enabled
6 through 10	unset				

Example:

To display network protocol settings for the I/O module in I/O-module bay 3, while I/O-module bay 3 is set as the persistent command environment, at the `system:switch[3]>` prompt, type

```
nat
```

The following example shows the information that is returned from this command:

```
system:switch[3]> nat
Index   Protocol Name   Protocol ID   Internal Port   External Port   Enabled
1       http            tcp           80              1080            enabled
2       telnet          tcp           23              1023            enabled
3       https           tcp           43              1043            enabled
4       ssh             tcp           22              1022            enabled
5       snmp            udp           161             1161            enabled
system:switch[3]>
```

portcfg command (advanced management module only)

This command configures and displays the settings for the advanced management-module serial port.

Table 21. portcfg command

Function	What it does	Command	Valid targets
Display management-module serial port configuration	Displays the current configuration of the management-module serial port. Possible return values are: • -b *baud_rate* • -p *parity* • -s *stop_bits*	portcfg -com1	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management-module serial port baud rate	Checks syntax and sets the baud (communications) rate of the management-module serial port.	portcfg -com1 -b *baud_rate* where *baud_rate* is 2400, 4800, 9600, 19200, 38400, or 57600. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 21. portcfg command (continued)

Function	What it does	Command	Valid targets
Set management-module serial port parity	Checks syntax and sets the parity of the management-module serial port.	portcfg -com1 -p *parity* where *parity* is none, odd, even, mark, or space. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management-module serial port stop bits	Checks syntax and sets the number of stop bits for the management-module serial port.	portcfg -com1 -s *stop_bits* where *stop_bits* is 1 or 2. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

To display the configuration for the management-module serial port, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
portcfg -com1
```

To set the baud rate for the management-module serial port to 9600, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
portcfg -com1 -b 9600
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> portcfg -com1
-b 2400
-p odd
-s 1
system:mm[1]> portcfg -com1 -b 9600
OK
system:mm[1]>
```

ports command (advanced management module only)

This command sets and displays the network port configuration settings for the advanced management module.

Table 22. ports command

Function	What it does	Command	Valid targets
Display network port settings	Displays the network port settings for the management module. Returned values are: • -ftpp *FTP_port_num* • -ftpdp *FTP_data_port_num* • -httpp *HTTP_port_num* • -httpsp *HTTPS_port_num* • -kvmp *KVM_port_num* • -rdp *rem_dsk_port_num* • -rdocp *rem_dsk_on_chp_port_num* • -snmpap *SNMP_agent_port_num* • -snmptp *SNMP_traps_port_num* • -sshp *SSH_port_num* • -telnetp *Telnet_port_num* • -tftpp *TFTP_port_num* • -sftpp *secure_TFTP_port_num* • -ftpe *FTP_state* • -httpse *HTTPS_port_state* • -ntpe *NTP_state* • -snmp1ae *SNMPv1_agent_state* • -snmp3ae *SNMPv3_agent_state* • -snmpte *SNMP_traps_state* • -sshe *SSH_port_state* • -tcme *TCP_cmd_mode_state* • -telnete *Telnet_port_state*- • -sftpe *secure_TFTP_state* • -tftpe *TFTP_state* • -tcmt *TCP_cmd_mode_timeout* • -telnett *Telnet_port_timeout*	ports	`-T system:mm[x]` where *x* is the primary management-module bay number.
Reset network port settings	Resets all network port settings for the management module to the default values. Default values are: • -ftpp: 21 • -ftpdp: 20 • -httpp: 80 • -httpsp: 443 • -kvmp: 3900 • -rdp: 1044 • -rdocp: 1045 • -snmpap: 161 • -snmptp: 162 • -sshp: 22 • -telnetp: 23 • -tftpp: 69 • -sftpp: 5222	ports -reset Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 22. ports command (continued)

Function	What it does	Command	Valid targets
Set FTP port number	Sets the port number for the management module FTP port.	ports -ftpp *FTP_port_num* where *FTP_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set FTP data port number	Sets the port number for the management module FTP data port.	ports -ftpdp *FTP_data_port_num* where *FTP_data_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set HTTP port number	Sets the port number for the management module HTTP port.	ports -httpp *HTTP_port_num* where *HTTP_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set HTTPS port number	Sets the port number for the management module HTTPS port.	ports -httpsp *HTTPS_port_num* where *HTTPS_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 22. ports command (continued)

Function	What it does	Command	Valid targets
Set KVM port number	Sets the port number for the management module KVM port.	ports -kvmp *KVM_port_num* where *KVM_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set remote disk port number	Sets the port number for the management module remote disk port.	ports -rdp *rem_dsk_port_num* where *rem_dsk_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set remote disk on chip port number	Sets the port number for the management module remote disk on chip port.	ports -rdocp *rem_dsk_on_chp_port_num* where *rem_dsk_on_chp_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set SNMP agent port number	Sets the port number for the management module SNMP agent port.	ports -snmpap *SNMP_agent_port_num* where *SNMP_agent_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 22. ports command (continued)

Function	What it does	Command	Valid targets
Set SNMP traps port number	Sets the port number for the management module SNMP traps port.	ports -snmptp *SNMP_traps_port_num* where *SNMP_traps_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set SSH port number	Sets the port number for the management module SSH port.	ports -sshp *SSH_port_num* where *SSH_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Telnet port number	Sets the port number for the management module Telnet port.	ports -telnetp *Telnet_port_num* where *Telnet_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set TFTP port number	Sets the port number for the management module TFTP port.	ports -tftpp *TFTP_port_num* where *TFTP_port_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable FTP	Enables FTP for the management module.	ports -ftpe on Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 22. ports command (continued)

Function	What it does	Command	Valid targets
Disable FTP	Disables FTP for the management module.	ports -ftpe off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Enable HTTPS port	Enables the management module HTTPS port.	ports -httpse on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable HTTPS port	Disables the management module HTTPS port.	ports -httpse off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Enable NTP	Enables NTP for the management module.	ports -ntpe on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable NTP	Disables NTP for the management module.	ports -ntpe off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Enable SNMPv1 agent	Enables the SNMPv1 agent for the management module.	ports -snmp1ae on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable SNMPv1 agent	Disables the SNMPv1 agent for the management module.	ports -snmp1ae off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Enable SNMPv3 agent	Enables the SNMPv3 agent for the management module.	ports -snmp3ae on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable SNMPv3 agent	Disables the SNMPv3 agent for the management module.	ports -snmp3ae off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Enable SNMP traps	Enables the SNMP traps for the management module.	ports -snmpte on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable SNMP traps	Disables the SNMP traps for the management module.	ports -snmpte off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Table 22. ports command (continued)

Function	What it does	Command	Valid targets
Enable SSH port	Enables the management module SSH port.	ports -sshe on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable SSH port	Disables the management module SSH port.	ports -sshe off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Enable TCP command mode	Enables the TCP command mode for the management module.	ports -tcme on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable TCP command mode	Disables the TCP command mode for the management module.	ports -tcme off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Enable Telnet port	Enables the management module Telnet port.	ports -telnete on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable Telnet port	Disables the management module Telnet port.	ports -telnete off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Enable TFTP	Enables TFTP for the management module.	ports -tftpe on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable TFTP	Disables TFTP for the management module.	ports -tftpe off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Set TCP command-mode timeout	Sets the TCP command-mode timeout value for the management module.	ports -tcmt *timeout* where *timeout* is from 0 seconds (no timeout) to 4294295967 seconds, inclusive. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Table 22. ports command (continued)

Function	What it does	Command	Valid targets
Set Telnet port timeout	Sets the Telnet port timeout value for the management module.	ports -telnett *timeout* where *timeout* is from 0 seconds (no timeout) to 4294295967 seconds, inclusive. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

To disable FTP for the management module, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
ports -ftpe off
```

To display the management module network port settings, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
ports
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> ports -ftpe off
These configuration changes will become active after the next reset of the MM.
system:mm[1]> ports
-ftpp 21
-ftpdp 20
-httpp 80
-httpsp 443
-kvmp 3900
-rdp 1044
-rdocp 1045
-snmpap 161
-snmptp 162
-sshp 22
-telnetp 23
-tftpp 69
-sftpp n/a
-ftpe off
-httpse off
-ntpe off
-ftpp 21
-snmp1ae on
-snmp3ae on
-snmpte on
-sshe off
-tcme on
-telnete on
-sftpe ---
-tftpe off
-tcmt 0
```

```
-telnett 10000
system:mm[1]>
```

read command (advanced management module only)

This command restores the management-module configuration that was previously saved to the BladeCenter unit chassis using the write command (advanced management module only).

Table 23. read command

Function	What it does	Command	Valid targets
Restore management-module configuration	Restores the management-module configuration from an image that was previously saved to the BladeCenter unit chassis.	read -config chassis Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable automatic management-module configuration	Enables automatic configuration of the management module, based on settings stored in the BladeCenter unit chassis, when the management module is installed.	read -auto on Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Disable automatic management-module configuration	Disables automatic configuration of the management module, based on settings stored in the BladeCenter unit chassis, when the management module is installed.	read -auto off Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

To restore the management-module configuration from an image previously saved to the BladeCenter unit chassis, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
read -config chassis
```

The following example shows the information that is returned from this command:

```
system:mm[1]> read -config chassis
OK
Configuration restore from the chassis was successful
Restart the MM for the new settings to take effect
system:mm[1]>
```

service command (advanced management module only)

This command configures and displays the management-module service setting.

Table 24. service command

Function	What it does	Command	Valid targets
Display service setting	Displays the service setting for technician debug (enable or disable).	service	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 24. service command (continued)

Function	What it does	Command	Valid targets
Enable technician debug	Configure service setting to enable technician debug of the advanced management module.	service -enable Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable technician debug	Configure service setting to disable (default setting) technician debug of the advanced management module.	service -disable Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Example:

To enable technician debug of the advanced management module, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
service -enable
```

To display the service setting of the advanced management module, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
service
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> service -enable
OK
system:mm[1]> service
Service by support personnel: Enabled
system:mm[1]>
```

slp command (advanced management module only)

This command sets and displays the service location protocol (SLP) settings for the management module.

Table 25. slp command

Function	What it does	Command	Valid targets
Display management-module SLP settings	Displays the SLP settings for the primary management module. Returned values are: • -t *address_type* • -i *multicast_addr*	slp	-T system:mm[*x*] where *x* is the primary management-module bay number.
Set management-module SLP address type	Sets the SLP address type for the primary management module.	slp -t *address_type* where *address_type* is multicast or broadcast. Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Table 25. slp command (continued)

Function	What it does	Command	Valid targets
Set management-module SLP multicast address	Sets the SLP multicast address for the primary management module.	slp -i *multicast_addr* where *multicast_addr* is the multicast IP address. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Example:

To set the SLP address type of the advanced management module to multicast, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
slp -t multicast
```

To display the SLP settings of the advanced management module, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
slp
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> slp -t multicast
OK
system:mm[1]> slp
-t multicast
-i 255.255.255.255
system:mm[1]>
```

smtp command

This command configures and displays the management-module SMTP settings.

Table 26. smtp command

Function	What it does	Command	Valid targets
Display SMTP server host name or IP address	Displays the SMTP server host name or IP address.	smtp	-T system:mm[*x*] where *x* is the primary management-module bay number.
Server host name or IP address - set	Checks syntax and sets the server host name or IP address.	smtp -s *hostname/ip_address* where *hostname/ip_address* is the host name or IP address of the server. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Example:

To set the SMTP server host name to us.ibm.com, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
smtp -s us.ibm.com
```

To display the SMTP configuration, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
smtp
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> smtp -s us.ibm.com
OK
system:mm[1]> smtp
-s us.ibm.com
system:mm[1]>
```

snmp command

This command configures and displays the management-module SNMP settings.

Table 27. snmp command

Function	What it does	Command	Valid targets
Display SNMP configuration of management module	Displays the current SNMP configuration of the management module. Possible return values are: • -a enabled/disabled • -t enabled/disabled • -c1 *community1_name* • -c1i1 *community1_ipaddr1_or_hstname* • -c1i2 *community1_ipaddr2_or_hstname* • -c1i3 *community1_ipaddr3_or_hstname* • -c2 *community2_name* • -c2i1 *community2_ipaddr1_or_hstname* • -c2i2 *community2_ipaddr2_or_hstname* • -c2i3 *community2_ipaddr3_or_hstname* • -c3 *community3_name* • -c3i1 *community3_ipaddr1_or_hstname* • -c3i2 *community3_ipaddr2_or_hstname* • -c3i3 *community3_ipaddr3_or_hstname* • -cn *contact_name* • -l *location*	snmp	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMPv1 agent - enable	Enables the management-module SNMPv1 agent. **Note:** SNMPv1 community setup required (see the `snmp -cx` commands, starting on page 70, for information).	snmp -a -on Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 27. snmp command (continued)

Function	What it does	Command	Valid targets
SNMPv1 agent - disable	Disables the management-module SNMPv1 agent.	snmp -a -off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
SNMPv3 agent - enable	Enables the management-module SNMPv3 agent. **Note:** SNMPv3 user setup required (see the users command, on page 86, for information).	snmp -a3 -on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
SNMPv3 agent - disable	Disables the management-module SNMPv3 agent.	snmp -a3 -off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
SNMP traps - enable	Enables the management-module SNMP traps.	snmp -t -on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
SNMP traps - disable	Disables the management-module SNMP traps.	snmp -t -off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
SNMP community 1 name - set	Sets the name of community 1.	snmp -c1 *name* where *name* is a descriptive name of community 1. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
SNMP community 1 first host name or IP address - set	Checks syntax and sets the first host name or IP address of community 1.	snmp -c1i1 *hostname/ip_address* where *hostname/ip_address* is the first host name or IP address of community 1. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Table 27. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 1 second host name or IP address - set	Checks syntax and sets the second host name or IP address of community 1.	snmp -c1i2 *hostname/ip_address* where *hostname/ip_address* is the second host name or IP address of community 1. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMP community 1 third host name or IP address - set	Checks syntax and sets the third host name or IP address of community 1.	snmp -c1i3 *hostname/ip_address* where *hostname/ip_address* is the third host name or IP address of community 1. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMPv3 community 1 view type - set	Sets the SNMPv3 view type for community 1.	snmp -ca1 *type* where *type* is get, set, or trap. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMP community 2 name - set	Sets the name of community 2.	snmp -c2 *name* where *name* is a descriptive name of community 2. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMP community 2 first host name or IP address - set	Checks syntax and sets the first host name or IP address of community 2.	snmp -c2i1 *hostname/ip_address* where *hostname/ip_address* is the first host name or IP address of community 2. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 27. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 2 second host name or IP address - set	Checks syntax and sets the second host name or IP address of community 2.	snmp -c2i2 *hostname/ip_address* where *hostname/ip_address* is the second host name or IP address of community 2. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMP community 2 third host name or IP address - set	Checks syntax and sets the third host name or IP address of community 2.	snmp -c2i3 *hostname/ip_address* where *hostname/ip_address* is the third host name or IP address of community 2. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMPv3 community 2 view type - set	Sets the SNMPv3 view type for community 2.	snmp -ca2 *type* where *type* is get, set, or trap. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMP community 3 name - set	Sets the name of community 3.	snmp -c3 *name* where *name* is a descriptive name of community 3. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMP community 3 first host name or IP address - set	Checks syntax and sets the first host name or IP address of community 3.	snmp -c3i1 *hostname/ip_address* where *hostname/ip_address* is the first host name or IP address of community 3. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 27. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 3 second host name or IP address - set	Checks syntax and sets the second host name or IP address of community 3.	snmp -c3i2 *hostname/ip_address* where *hostname/ip_address* is the second host name or IP address of community 3. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
SNMP community 3 third host name or IP address - set	Checks syntax and sets the third host name or IP address of community 3.	snmp -c3i3 *hostname/ip_address* where *hostname/ip_address* is the third host name or IP address of community 3. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
SNMPv3 community 3 view type - set	Sets the SNMPv3 view type for community 3.	snmp -ca3 *type* where *type* is get, set, or trap. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
SNMP contact name - set	Sets the contact name.	snmp -cn *contact_name* Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
SNMP location - set	Sets the location.	snmp -l *hostname/ip_address* Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Example:
To view the SNMP configuration, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
snmp
```

To enable the SNMP agent and SNMP traps, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
snmp -a -on -t -on
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> snmp
```

```
-a Disabled
-t Disabled
-l No Location Configured
-cn No Contact Configured
-c1 com1
-c1i1 1.2.3.4
-c1i2
-c1i3
-c2 com2
-c2i1 1.2.3.4
-c2i2
-c2i3
-c3
-c3i1
-c3i2
-c3i3
system:mm[1]> snmp -a -on -t -on
Changes to the network settings will take effect after the next reset of the MM.
system:mm[1]>
```

sol (serial over LAN) command

This command configures SOL functions and indicates SOL status.

Table 28. sol (serial over LAN) command

Function	What it does	Command	Valid targets

Display SOL status	Displays the SOL status for the targeted device:
	• When the command target is the primary management module, it displays the following values:
	– -status *on/off* (global SOL status)
	– -c *retry_count*
	– -e *CLI_key_sequence*
	– -i *retry_interval*
	– -r *reset_blade_key_seq*
	– -s *send_threshold*
	– -t *accumulate_timeout*
	– -v *VLAN_id*
	Note: For the advanced management module, the *VLAN_id* is identified as "VLAN ID". For management modules other than the advanced management module, the *VLAN_id* is identified by the "-v" value that is returned.
	• When the command target is a blade server, it displays the following:
	– -status *on/off* (SOL status for the blade server)
	– Status of any SOL sessions for that blade server:
	- There is no SOL session opening for that blade.
	- There is an SOL session opening for that blade.
	- There is an SOL session opening and it is connected to a telnet session.
		sol	`-T system:mm[x]`
			`-T system:blade[x]`
			where *x* is the primary management-module or blade server bay number.

SOL retry interval - set	Sets the SOL retry interval to the input value.	sol -i *value* where *value* is from 10 ms to 2550 ms, inclusive, in 10 ms increments. If you enter a value less than 10 ms, the retry interval will be set to 10 ms. If you enter a value greater than 2550 ms, the retry interval will be set to 2550 ms. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 28. sol (serial over LAN) command (continued)

Function	What it does	Command	Valid targets
SOL retry count - set	Sets the SOL retry count to the input value.	sol -c *value* where *value* is from 0 to 7, inclusive. If you enter a value of 0, no retries will be attempted. If you enter a value greater than 7, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SOL send threshold - set	Sets the SOL send threshold to the input value. Setting the threshold value to 1 causes the blade server integrated system management processor to send an SOL packet as soon as the first character is received.	sol -s *value* where *value* is from 1 to 251, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SOL accumulate timeout - set	Sets the SOL accumulate timeout to the input value.	sol -t *value* where *value* is from 5 ms to 1275 ms, inclusive. If you enter a value less than 5 ms, the accumulate timeout will be set to 5 ms. If you enter a value greater than 1275 ms, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SOL enable - global	Enables SOL globally for the BladeCenter unit. The global SOL enable command does not affect the SOL session status for each blade server.	sol -status on Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SOL enable - blade server	Enables SOL for the specified blade server.	sol -status on Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.
SOL disable - global	Disables SOL globally for the BladeCenter unit. The global SOL disable command does not affect the SOL session status for each blade server.	sol -status off Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SOL disable - blade server	Disables SOL for the specified blade server.	sol -status off Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.

Table 28. sol (serial over LAN) command (continued)

Function	What it does	Command	Valid targets
SOL VLAN ID - set *(This command is not available for the advanced management module. For the advanced management module, the SOL VLAN ID is set using the "ifconfig command (advanced management module only)" on page 49.)*	Sets the SOL VLAN ID to the input value.	sol -v *value* where *value* is from 1 to 4095, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
CLI key sequence - set	Sets the key sequence that is used to enter the CLI while a Telnet session in SOL mode.	sol -e *value* where *value* is the key sequence. In this sequence, a ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example: • ^[(the carat symbol followed by a left bracket) means Esc • ^M (the carat symbol followed by a capitol M) means carriage return. Refer to an ASCII-to-key conversion table for a complete listing of control-key sequences. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 28. sol (serial over LAN) command (continued)

Function	What it does	Command	Valid targets
Reset blade server key sequence - set	Sets the key sequence that will reset a blade server while a Telnet session in SOL mode.	sol -r *value* where *value* is the key sequence. In this sequence, a ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example: • ^[(the carat symbol followed by a left bracket) means Esc • ^M (the carat symbol followed by a capitol M) means carriage return. Refer to an ASCII-to-key conversion table for a complete listing of control-key sequences. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

To set the SOL accumulate timeout to 25 ms, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
sol -t 25
```

To set the reset blade server key sequence to Esc R Esc r Esc R, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
sol -r ^[R^[r^[R
```

To display the SOL settings, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
sol
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> sol -t 25
OK
system:mm[1]> sol
-status on
-c 0
-e ^[(
-i 250
-r ^[R^[r^[R
-s 250
-t 25
-v 4095
system:mm[1]>
```

sshcfg command (advanced management module only)

This command sets and displays the SSH v1 status of the management module. (SSH v2 is always enabled.)

Table 29. sshcfg command

Function	What it does	Command	Valid targets
Display SSH v1 status	Displays the SSH v1 status of the management module.	sshcfg	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable SSH v1	Enables SSH v1 for the management module.	sshcfg -v1 on Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Disable SSH v1	Disables SSH v1 for the management module.	sshcfg -v1 off Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

To enable SSH v1, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
sshcfg -v1 on
```

To display SSH v1 status, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
sshcfg
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> sshcfg -v1 on
OK
system:mm[1]> sshcfg
-v1 on
system:mm[1]>
```

tcpcmdmode command (management modules other than the advanced management module)

Note: The tcpcmdmode command operates differently for the advanced management module and for other management module types. The following command description is for management modules other than the advanced management module. See "tcpcmdmode command (advanced management module only)" on page 81 for command syntax for the advanced management module.

This command displays and changes the timeout of the TCP command-mode sessions that are used by *IBM Director* software for out-of-band communication with the management module. This command is also used to enable or disable the TCP command-mode sessions.

Table 30. tcpcmdmode command (management modules other than the advanced management module)

Function	What it does	Command	Valid targets
Display TCP command-mode session status and timeout	Displays the TCP command-mode session status (on or off) and timeout.	tcpcmdmode	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set TCP command-mode session timeout	Sets the TCP command-mode session timeout value.	tcpcmdmode -t *timeout* where *timeout* is from 0 seconds (no timeout) to 4294967295 seconds, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable TCP command-mode sessions	Enables TCP command-mode sessions that are used by *IBM Director* software for out-of-band communication with the management module.	tcpcmdmode -status on Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Disable TCP command-mode sessions	Disables TCP command-mode sessions that are used by *IBM Director* software for out-of-band communication with the management module.	tcpcmdmode -status off Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:
To enable a TCP command-mode session for the primary management module, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
tcpcmdmode -status on
```

To set the TCP command-mode session timeout for the primary management module to 6 minutes, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
tcpcmdmode -t 360
```

To display the TCP command-mode session status and timeout for the primary management module, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
tcpcmdmode
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> tcpcmdmode -status on
OK
system:mm[1]> tcpcmdmode -t 360
OK
system:mm[1]> tcpcmdmode
-status on
-t 360
```

```
system:mm[1]>
```

tcpcmdmode command (advanced management module only)

Note: The tcpcmdmode command operates differently for the advanced management module and for other management module types. The following command description is for the advanced management module. See “tcpcmdmode command (management modules other than the advanced management module)” on page 79 for command syntax for management modules other than the advanced management module.

This command displays and changes the timeout of the TCP command-mode sessions that are used by *IBM Director* software for out-of-band communication with the management module. This command is also used to enable or disable the TCP command-mode sessions.

Table 31. tcpcmdmode command (advanced management module only)

Function	What it does	Command	Valid targets
Display TCP command-mode session status and timeout	Displays the TCP command-mode session status (maximum number of sessions) and timeout.	tcpcmdmode	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set TCP command-mode session timeout	Sets the TCP command-mode session timeout value.	tcpcmdmode -t *timeout* where *timeout* is from 0 seconds (no timeout) to 4294967295 seconds, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Disable TCP command-mode sessions	Disables TCP command-mode sessions that are used by *IBM Director* software for out-of-band communication with the management module.	tcpcmdmode -status 0 Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable and set number of TCP command-mode sessions	Enables TCP command-mode and sets the maximum number of sessions that can be used by *IBM Director* software for out-of-band communication with the management module.	tcpcmdmode -status *number_sessions* where *number_sessions* is from 0 (disabled) to 5, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:
To enable a maximum of three TCP command-mode sessions for the primary management module, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
tcpcmdmode -status 3
```

To set the TCP command-mode session timeout for the primary management module to 6 minutes, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
tcpcmdmode -t 360
```

To display the TCP command-mode session status and timeout for the primary management module, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
tcpcmdmode
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> tcpcmdmode -status 3
OK
system:mm[1]> tcpcmdmode -t 360
OK
system:mm[1]> tcpcmdmode
-status 3 connection
-t 360
system:mm[1]>
```

telnetcfg (Telnet configuration) command

This command displays and configures the command-line session parameters of the primary management module.

Table 32. telnetcfg (Telnet configuration) command

Function	What it does	Command	Valid targets
Display command-line session configuration	Displays the command-line session configuration of the primary management module.	telnetcfg	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display command-line session timeout (management modules other than the advanced management module)	Displays the command-line session timeout value, in seconds, of the primary management module.	telnetcfg -t	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set command-line session timeout for primary management module	Sets the command-line session timeout value for the primary management module.	telnetcfg -t *timeout* where *timeout* is from 0 seconds (no timeout) to 4294967295 seconds, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:
To set the command-line session timeout for the primary management module to 6

minutes, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
telnetcfg -t 360
```

To display the command-line session configuration for the primary management module, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
telnetcfg
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> telnetcfg -t 360
OK
system:mm[1]> telnetcfg
-t 360
system:mm[1]>
```

uplink (management module failover) command

This command displays and configures the management-module uplink failover feature. If the external network interface of the primary management module fails, this feature forces a failover to the redundant management module, if one is installed.

Table 33. uplink command

Function	What it does	Command	Valid targets
Display uplink failover status	Displays the management-module uplink failover status (enabled or disabled) and the failover delay.	uplink	-T system:mm[*x*] where *x* is the primary management-module bay number.
Set network uplink failover delay	Sets the amount of time between detection of a management-module uplink failure and failover to the redundant management module.	uplink -del *delay* where *delay* is from 1 to 255 minutes, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Enable uplink failover	Enables failover to the redundant management module if the external network interface of the primary management module fails.	uplink -on Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Disable uplink failover	Disables failover to the redundant management module if the external network interface of the primary management module fails.	uplink -off Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Example:
To enable failover to the redundant management module if the external network interface of the primary management module fails, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
uplink -on
```

To set the uplink failover delay to 3 minutes, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
uplink -del 3
```

To display the uplink failover configuration, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
uplink
```

The following example shows the information that is returned from these three commands:

```
system:mm[1]> uplink -on
OK
system:mm[1]> uplink -del 3
Uplink delay set to 3 minute(s).
OK
system:mm[1]> uplink
Failover on network uplink loss is enabled.
Uplink delay: 3 minute(s)
system:mm[1]>
```

users command (management modules other than the advanced management module)

Note: The users command operates differently for the advanced management module and for other management module types. The following command description is for management modules other than the advanced management module. See “users command (advanced management module only)” on page 95 for command syntax for the advanced management module.

This command displays and configures user accounts, also called user profiles, of the primary management module.

Important: Command authority definitions might change between firmware versions. Make sure that the command authority level set for each user is correct after updating management-module firmware.

Table 34. users (management-module users) command (management modules other than the advanced management module)

Function	What it does	Command	Valid targets
Display all user profiles	Displays all 12 management-module user profiles. Returned values are: • User name • Authority level	users	-T system:mm[*x*] where *x* is the primary management-module bay number.

Table 34. users (management-module users) command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Display single user profile	Displays the specified management-module user profile. Returned values are: • User name • Authority level • Context name • Authentication protocol • Privacy protocol • Access type • Hostname/IP address	users -*user_number* where *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Delete user profile	Delete the specified management-module user profile.	users -*user_number* -clear where *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. It is possible to delete an empty user profile. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 34. users (management-module users) command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Create user profile	Create the specified management-module user profile. All fields must be specified when creating a user profile for the BladeCenter T management module. For management modules other than those installed in a BladeCenter T unit, only the following user-profile fields are required: • *-user_number* • -n *user_name* • -a *user_authority* • -p *user_password*	users -*user_number* -n *user_name* -p *user_password* -a *user_authority* -cn *context_name* -ap *auth_protocol* -pp *privacy_protocol* -ppw *privacy_pwd* -at *access_type* -i *ip_addr/hostname* where: • *user_number* is a number from 1 to 12 that corresponds to an unused user number in the “Display all user profiles” list. • *user_name* is a alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_). Each of the 12 user names must be unique. • *user_password* can be blank or an alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_), and must include at least one alphabetic and one non-alphabetic character. • *user_authority* is one of the following: – operator (read-only) – rbs (see “Set user authority level” on page 91 for more information) for scripting on management modules other than the advanced management module, *user_authority* is one of the following: – super (Supervisor) – custom (see “Set user authority level” on page 89 for more information) – ro (read-only) *(continued on next page)*	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 34. users (management-module users) command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Create user profile *(continued)*		• *context_name* is a string for SNMPv3 context that is up to 31 characters in length. Each of the 12 context names must be unique. • *auth_protocol* is an SNMPv3 authentication protocol of sha, md5, or blank (no entry) for none. • *privacy_protocol* is an SNMPv3 privacy protocol of des or blank (no entry) for none. If the privacy protocol is set to none, no -ppw command option (privacy password) is required. • *privacy_pwd* is an SNMPv3 privacy password string of up to 31 characters in length. If the privacy protocol is set to none, the -ppw command option does not need to be used unless a privacy password is required. • *access_type* is an SNMPv3 access type of read, write, or traps. • *ip_addr/hostname* is a valid SNMPv3 static IP address or an alphanumeric hostname string up to 63 characters in length. Command use restricted (see “Commands and user authority” on page 5).	

Table 34. users (management-module users) command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Set user name	Sets a user name in the specified management-module user profile.	users -*user_number* -n *user_name* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *user_name* is a alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_). Each of the 12 user names must be unique. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set user password	Sets a user password in the specified management-module user profile.	users -*user_number* -p *user_password* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *user_password* can be blank or an alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_), and must include at least one alphabetic and one non-alphabetic character. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 34. users (management-module users) command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Set user authority level	Sets a user authority level in the specified management-module user profile.	users -*user_number* -a *user_authority* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *user_authority* is one of the following: – operator (read-only) – rbs (custom) The custom authority level parameter is specified using the following syntax: `rbs:levels:devices` where the *levels* are one or more of the following authority levels, separated by a vertical bar (|): • super (Supervisor) • cam (Chassis User Account Management) • clm (Chassis Log Management) • co (Chassis Operator) • cc (Chassis Configuration) • ca (Chassis Administration) • bo (Blade Operator) • brp (Blade Remote Present) • bc (Blade Configuration) • ba (Blade Administration) • so (I/O Module Operator) • sc (I/O Module Configuration) • sa (I/O Module Administration) *(continued on next page)*	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 34. users (management-module users) command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Set user authority level *(continued)*		where the *devices* are one or more of the following devices, separated by a vertical bar (|). Ranges of devices are separated by a dash (-). • c*n* (Chassis *n*, where *n* is a valid chassis number. Use c1 for single-chassis environments.) • b*n* (Blade *n*, where *n* is a valid blade bay number in the chassis) • s*n* (I/O module *n*, where *n* is a valid I/O module bay number in the chassis) Command use restricted (see “Commands and user authority” on page 5).	

Table 34. users (management-module users) command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Set user authority level (These are the previous version of authority levels that are used only for backward compatibility with scripts.)	Sets a user authority level in the specified management-module user profile.	users -*user_number* -a *user_authority* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *user_authority* is one of the following: – ro (read-only) – super (Supervisor) – custom The custom authority level parameter is specified using the following syntax: `custom:level1|level2` where the *levels* are one or more of the following authority levels, separated by a vertical bar (|): • am (User Account Management Access) • rca (Blade Server Remote Console Access) • rcvma (Remote Console and Virtual Media Access) • pr (Blade and I/O Power Restart Access) • cel (Ability to Clear Event Logs) • bc (Basic Configuration Permission) • nsc (Network and Security Configuration Permission) • ac (Advanced Configuration) Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 34. users (management-module users) command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Set SNMPv3 user context name	Sets an SNMPv3 context name in the specified management-module user profile. The context name defines the context the SNMPv3 user is working in. A context name can be shared by multiple users.	users -*user_number* -cn *context_name* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • *context_name* is a string up to 31 characters in length. Each of the 12 context names must be unique. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set SNMPv3 user authentication protocol	Sets the SNMPv3 authentication protocol to be used for the specified management-module user profile.	users -*user_number* -ap *auth_protocol* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • *auth_protocol* is sha, md5, or blank (no entry) for none. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set SNMPv3 user privacy protocol	Sets the SNMPv3 privacy protocol to be used for the specified management-module user profile. If the privacy protocol is set to none, no -ppw command option (privacy password) is required.	users -*user_number* -pp *privacy_protocol* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • *privacy_protocol* is des or blank (no entry) for none. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 34. users (management-module users) command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Set privacy password for SNMPv3 user	Sets an SNMPv3 privacy password in the specified management-module user profile.	users -*user_number* -ppw *privacy_pwd* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *privacy_pwd* is a string up to 31 characters in length. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Set access type for SNMPv3 user	Sets an SNMPv3 access type for the specified management-module user profile. This command supports the following access types: • read: the user can query Management Information Base (MIB) objects and receive traps. • write: the user can query and set MIB objects and receive traps. • traps: the user can only receive traps.	users -*user_number* -at *access_type* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *access_type* is read, write, or traps. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Set IP address or hostname for SNMPv3 trap receiver	Sets the IP address or hostname that will receive SNMPv3 traps for the specified management-module user profile.	users -*user_number* -i *ip_addr/hostname* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *ip_addr/hostname* is a valid static IP address or an alphanumeric hostname string up to 63 characters in length. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.

Example:
To create user number 3 with a user name of user3 who has supervisor rights to all BladeCenter components, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
users -3 -n user3 -p passw0rd -a rbs:super:c1|b1-b14|s1-s4 -cn joe -ap md5 -pp des
-ppw passw0rd -at read -I 192.168.70.129
```

Note: The entry beginning with users -3 -n... is shown with a line break after -pp des. When this command is entered, the entire entry must all be on one line.

To set the command authority for an existing user number 4 to Blade Operator for blade 1, blade 2, and blade 3 and Chassis Log Management, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
users -4 -rbs:bo|clm:b1-b3|c1
```

To display all users, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
users
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> users -3 -n user3 -p passw0rd -a rbs:super:c1|b1-b14|s1-s4
-cn joe -ap md5 -pp des -ppw passw0rd -at read -I 192.168.70.129
OK
system:mm[1]> users -4 -rbs:bo|clm:b1-b3|c1
OK
system:mm[1]> users
1. USERID
   Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Switches:1|2|3|4
2. <not used>
3. user3
   Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Switches:1|2|3|4
4. user4
   Role:blade operator|chassis log management
   Blades:1|2|3
   Chassis:1
   Switches:N/A
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system:mm[1]>
```

Note: The entry beginning with `users -3 -n...` is shown with a line break after `-a rbs:super:c1|b1-b14|s1-s4`. When this command is entered, the entire entry must all be on one line.

users command (advanced management module only)

Note: The users command operates differently for the advanced management module and for other management module types. The following command description is for the advanced management module. See “users command (management modules other than the advanced management module)” on page 84 for command syntax for management modules other than the advanced management module.

This command displays and configures user accounts, also called user profiles, of the primary management module.

Important: Command authority definitions might change between firmware versions. Make sure that the command authority level set for each user is correct after updating management-module firmware.

Table 35. users (management-module users) command (advanced management module only)

Function	What it does	Command	Valid targets
Display all user profiles	Displays all 12 management-module user profiles. Returned values are: • User name • Authority level	users	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display active users	Displays all users that are currently logged in to the management module. Returned values are: • User name • User IP address • Connection type (SNMPv1, SNMPv3, SSH, TCP command mode, Telnet, Web)	users -curr	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display single user profile	Displays the specified management-module user profile. Returned values are: • User name • Authority level • Context name • Authentication protocol • Privacy protocol • Access type • Hostname/IP address	users -*user_number* where *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 35. users (management-module users) command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Delete user profile	Delete the specified management-module user profile.	users -*user_number* -clear where *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. It is possible to delete an empty user profile. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 35. users (management-module users) command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Create user profile	Create the specified management-module user profile. All fields must be specified when creating a user profile for the BladeCenter T management module. For management modules other than those installed in a BladeCenter T unit, only the following user-profile fields are required: • -*user_number* • -n *user_name* • -a *user_authority* • -p *user_password*	users -*user_number* -n *user_name* -p *user_password* -a *user_authority* -cn *context_name* -ap *auth_protocol* -pp *privacy_protocol* -ppw *privacy_pwd* -at *access_type* -i *ip_addr/hostname* where: • *user_number* is a number from 1 to 12 that corresponds to an unused user number in the “Display all user profiles” list. • *user_name* is a alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_). Each of the 12 user names must be unique. • *user_password* can be blank or an alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_), and must include at least one alphabetic and one non-alphabetic character. • *user_authority* is one of the following: – operator (read-only) – rbs (see “Set user authority level” on page 99 for more information) Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 35. users (management-module users) command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Set user name	Sets a user name in the specified management-module user profile.	users -*user_number* -n *user_name* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • *user_name* is a alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_). Each of the 12 user names must be unique. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set user password	Sets a user password in the specified management-module user profile.	users -*user_number* -p *user_password* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • *user_password* can be blank or an alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_), and must include at least one alphabetic and one non-alphabetic character. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 35. users (management-module users) command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Set user authority level	Sets a user authority level in the specified management-module user profile.	users -*user_number* -a *user_authority* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *user_authority* is one of the following: – operator (read-only) – rbs (custom) The custom authority level parameter is specified using the following syntax: `rbs:levels:devices` where the *levels* are one or more of the following authority levels, separated by a vertical bar (|): • super (Supervisor) • cam (Chassis User Account Management) • clm (Chassis Log Management) • co (Chassis Operator) • cc (Chassis Configuration) • ca (Chassis Administration) • bo (Blade Operator) • brp (Blade Remote Present) • bc (Blade Configuration) • ba (Blade Administration) • so (I/O Module Operator) • sc (I/O Module Configuration) • sa (I/O Module Administration) *(continued on next page)*	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 35. users (management-module users) command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Set user authority level *(continued)*		the *levels* can also include one or more of the following authority levels when using LDAP. **Notes:** 1. The LDAP authority levels are not supported by the management-module Web interface. 2. To use the LDAP authority levels, make sure that the version of LDAP security used by the management module is set to v2 (enhanced role-based security model). See "ldapcfg command (advanced management module only)" on page 54 for information. • brpv (Blade Remote Presence View Video) • brpk (Blade Remote Presence KVM) • brpr (Blade Remote Presence Remote Drive Read) • crpru (Blade Remote Presence Remote Drive Read or Write) • rps (Remote Presence Supervisor) where the *devices* are one or more of the following devices, separated by a vertical bar (|). Ranges of devices are separated by a dash (-). • c*n* (Chassis *n*, where *n* is a valid chassis number. Use c1 for single-chassis environments.) • b*n* (Blade *n*, where *n* is a valid blade bay number in the chassis) • s*n* (I/O module *n*, where *n* is a valid I/O module bay number in the chassis) Command use restricted (see "Commands and user authority" on page 5).	

Table 35. users (management-module users) command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Set SNMPv3 user context name	Sets an SNMPv3 context name in the specified management-module user profile. The context name defines the context the SNMPv3 user is working in. A context name can be shared by multiple users.	users -*user_number* -cn *context_name* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *context_name* is a string up to 31 characters in length. Each of the 12 context names must be unique. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set SNMPv3 user authentication protocol	Sets the SNMPv3 authentication protocol to be used for the specified management-module user profile.	users -*user_number* -ap *auth_protocol* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *auth_protocol* is sha, md5, or blank (no entry) for none. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set SNMPv3 user privacy protocol	Sets the SNMPv3 privacy protocol to be used for the specified management-module user profile. If the privacy protocol is set to none, no -ppw command option (privacy password) is required.	users -*user_number* -pp *privacy_protocol* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *privacy_protocol* is des or blank (no entry) for none. Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 35. users (management-module users) command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Set privacy password for SNMPv3 user	Sets an SNMPv3 privacy password in the specified management-module user profile.	users -*user_number* -ppw *privacy_pwd* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • *privacy_pwd* is a string up to 31 characters in length. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set access type for SNMPv3 user	Sets an SNMPv3 access type for the specified management-module user profile. This command supports the following access types: • get: the user can query Management Information Base (MIB) objects and receive traps. • set: the user can query and set MIB objects and receive traps. • trap: the user can only receive traps.	users -*user_number* -at *access_type* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • *access_type* is get, set, or trap. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set IP address or hostname for SNMPv3 trap receiver	Sets the IP address or hostname that will receive SNMPv3 traps for the specified management-module user profile.	users -*user_number* -i *ip_addr/hostname* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • *ip_addr/hostname* is a valid static IP address or an alphanumeric hostname string up to 63 characters in length. Command use restricted (see “Commands and user authority” on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:
To create user number 3 with a user name of user3 who has supervisor rights to all BladeCenter components, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
users -3 -n user3 -p passw0rd -a rbs:super:c1|b1-b14|s1-s4 -cn joe -ap md5 -pp des
-ppw passw0rd -at get -I 192.168.70.129
```

Note: The entry beginning with users -3 -n... is shown with a line break after -pp des. When this command is entered, the entire entry must all be on one line.

To set the command authority for an existing user number 4 to Blade Operator for blade 1, blade 2, and blade 3 and Chassis Log Management, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
users -4 -rbs:bo|clm:b1-b3|c1
```

To display all users, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
users
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> users -3 -n user3 -p passw0rd -a rbs:super:c1|b1-b14|s1-s4
-cn joe -ap md5 -pp des -ppw passw0rd -at get -I 192.168.70.129
OK
system:mm[1]> users -4 -rbs:bo|clm:b1-b3|c1
OK
system:mm[1]> users
1. USERID
   Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Switches:1|2|3|4
2. <not used>
3. user3
   Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Switches:1|2|3|4
4. user4
   Role:blade operator|chassis log management
   Blades:1|2|3
   Chassis:1
   Switches:N/A
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system:mm[1]>
```

Note: The entry beginning with `users -3 -n...` is shown with a line break after `-a rbs:super:c1|b1-b14|s1-s4`. When this command is entered, the entire entry must all be on one line.

write command (advanced management module only)

This command saves the management-module configuration to the chassis of the BladeCenter unit.

Table 36. write command

Function	What it does	Command	Valid targets
Save management-module configuration	Saves an image of the management-module configuration to the BladeCenter unit chassis.	write -config chassis Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

To save the management-module configuration to an image on the BladeCenter chassis, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
write -config chassis
```

The following example shows the information that is returned from this command:

```
system:mm[1]> write -config chassis
OK
Configuration settings were successfully saved to the chassis
system:mm[1]>
```

Event-log commands

Use these commands to view and clear primary management-module event log entries:

- clearlog command
- displaylog command

clearlog command

This command clears the management-module event log.

Table 37. clearlog (clear management-module event log) command

Function	What it does	Command	Valid targets
Clear management-module event log	Clears the management-module event log and displays a message confirming that the event log was cleared.	clearlog Command use restricted (see "Commands and user authority" on page 5).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:
To clear the management-module event log, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
clearlog
```

The following example shows the information that is returned:

```
system:mm[1]> clearlog
OK
system:mm[1]>
```

displaylog command

This command displays management-module event log entries.

Table 38. displaylog (display management-module event log) command

Function	What it does	Command	Valid targets
Display management-module event log entries	Displays five entries from the management-module event log. The first time the command is executed, the five most recent log entries are displayed. Each subsequent time the command is issued, the next five entries in the log display.	displaylog	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display management-module event log entries (reset counter)	Resets the counter and displays the first five entries in the management-module event log.	displaylog -f	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display all management-module event log entries (advanced management module only)	Displays all entries in the advanced management module event log.	displaylog -a	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

To display the first five primary management-module event log entries, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
displaylog -f
```

To display the next five management-module event log entries, type (a second time)

```
displaylog
```

To display the next five management-module event log entries, type

```
displaylog
```

The following example shows the information that is returned from these three commands:

```
system:mm[1]> displaylog -f
1       I       SERVPROC        10/27/03        19:45:57        Remote
Login Successful. Login ID:''USERID' CLI authenticated from
192.168.70.231 (Telnet).'
2       E       SERVPROC        10/27/03        19:42:58        Failure
reading I2C device. Check devices on bus 4.
3       E       SERVPROC        10/27/03        19:42:58        Failure
reading I2C device. Check devices on bus 3.
4       E       SERVPROC        10/27/03        19:42:58        Failure
reading I2C device. Check devices on bus 2.
```

```
5       I       SERVPROC        10/27/03        19:41:54        Remote
Login Successful. Login ID:''USERID' from WEB browser at
IP@=192.168.70.231'
system:mm[1]> displaylog
6       E       SERVPROC        10/27/03        19:41:53        Blower 2
Fault Multiple blower failures
7       E       SERVPROC        10/27/03        19:41:53        Blower 1
Fault Single blower failure
8       I       SERVPROC        10/27/03        19:41:48
Ethernet[1] Link Established at 100Mb, Full Duplex.
9       I       SERVPROC        10/27/03        19:41:48
Ethernet[1] configured to do 100Mb/Full Duplex.
10      I       SERVPROC        10/27/03        19:41:48
Ethernet[1] MAC Address currently being used: 0x00-09-6B-CA-0C-81
system:mm[1]> displaylog
11      I       SERVPROC        10/27/03        19:41:48
Ethernet[0] Link Established at 100Mb, Full Duplex.
12      I       SERVPROC        10/27/03        19:41:48
Ethernet[0] configured to do Auto Speed/Auto Duplex.
13      I       SERVPROC        10/27/03        19:41:48
Ethernet[0] MAC Address currently being used: 0x00-09-6B-CA-0C-80
14      I       SERVPROC        10/27/03        19:41:48
Management Module Network Initialization Complete.
15      I       SERVPROC        10/27/03        19:41:46        ENET[1]
IP-Cfg:HstName=MM00096BCA0C81, IP@=192.168.70.126 ,GW@=0.0.0.0,
NetMsk=255.255.255.0
system:mm[1]>
```

The following example shows the information that is returned if the displaylog command is run after the event log is cleared:

```
system:mm[1]> displaylog -f
1       I       SERVPROC        10/27/03        19:53:02        System
log cleared.
(There are no more entries in the event log.)
system:mm[1]>
```

Power-control commands

Use these commands to control operation of the BladeCenter unit, blade servers, and I/O (switch) modules:

- boot command
- fuelg command (management modules other than the advanced management module)
- fuelg command (advanced management module only)
- power command
- reset command

boot command

This command resets blade servers with several different restart options.

Table 39. boot command

Function	What it does	Command	Valid targets
Reset blade server	Performs an immediate reset and restart of the specified blade server. This command will start a blade server that is turned off.	boot Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[`*x*`]` where *x* is the blade server bay number.
Reset blade server to command console	Resets the specified blade server, causing it to open a command console with an SOL session when it restarts. This command will start a blade server that is turned off.	boot -c Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[`*x*`]` where *x* is the blade server bay number.
Power cycle	Cycles power for the specified blade server. If the blade server is off, it will turn on. If the blade server is on, it will turn off and then turn on.	boot -p powercycle Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[`*x*`]` where *x* is the blade server bay number.
Reset blade server	Performs an immediate reset and restart of the specified blade server. This command will start a blade server that is turned off.	boot -p reset Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[`*x*`]` where *x* is the blade server bay number.

Example:
To boot the blade server in blade bay 3, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
boot -T system:blade[3]
```

The following example shows the information that is returned:

```
system:mm[1]>  boot -T system:blade[3]
OK
system:mm[1]>
```

fuelg command (management modules other than the advanced management module)

Note: The fuelg command operates differently for the advanced management module and for other management module types. The following command description is for management modules other than the advanced management module. See "fuelg command (advanced management module only)" on page 110 for command syntax for the advanced management module.

This command displays power domain information, listing the power modules that are installed in the BladeCenter unit and information about how the power in each domain is used. This command also configures the power domain policies for oversubscription and quiet mode.

Table 40. fuelg command (management modules other than the advanced management module)

Function	What it does	Command	Valid targets
Display power domain status overview	Displays health status and total power usage information for all power domains	fuelg	`-T system`
Display detailed power domain status	Displays detailed status and usage information for the specified power domains	fuelg *domain* where *domain* is “pd1” for power domain 1 and “pd2” for power domain 2. If no *domain* is specified, a status overview for all power domains displays.	`-T system`
Set power domain redundancy loss policy	Sets how the BladeCenter unit responds to a condition that could cause a loss of redundant power.	fuelg *domain* -os *policy* where: • *domain* is “pd1” for power domain 1 and “pd2” for power domain 2. If no *domain* is specified, the *policy* is applied to all power domains. • *policy* of: – “none” (default) allows loss of redundancy. – “nonrecov” prevents components from turning on that will cause loss of power redundancy. – “recov” power throttles components to maintain power redundancy and prevents components from turning on that will cause loss of power redundancy. Command use restricted (see “Commands and user authority” on page 5).	`-T system`

Table 40. fuelg command (management modules other than the advanced management module) (continued)

Function	What it does	Command	Valid targets
Thermal event response (quiet mode)	Sets how the BladeCenter unit blowers respond to thermal events.	fuelg -qm *setting* where the quiet-mode *setting* of: • "off" (default) allows blowers to increase speed to provide additional cooling. • "on" keeps blowers at a fixed speed and power throttles BladeCenter components to reduce power consumption (only for BladeCenter components that support power throttling). Command use restricted (see "Commands and user authority" on page 5).	`-T system`

Example:
To view a power domain status overview, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
fuelg
```

To reduce fan noise during thermal events for all power domains, while the BladeCenter unit is set as the persistent command environment with a management module other than an advanced management module, at the `system>` prompt, type

```
fuelg -qm on
```

To view the detailed power domain status for power domain 1, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
fuelg pd1
```

The following example shows the information that is returned when the fuelg command is run on a management module other than an advanced management module.

```
system>  fuelg
Note: All power values are displayed in Watts.

Power Domain 1
--------------
Status: Power domain status is good.
Modules:
 Bay 1:   2000
 Bay 2:   2000
Power Budget:  3200
Reserved Power:  400
Remaining Power:  2800
Power in Use:  400
```

```
Power Domain 2
--------------
Status: Power domain status is good.
Modules:
 Bay 3: 1800
 Bay 4: 1800
Power Budget:  2880
Reserved Power:  0
Remaining Power:  2880
Power in Use:  0

-qm off
system>  fuelg -qm on
OK
system>  fuelg pd1
                            Power  -- Allocated Power --
Bay(s)  Module              State  Current   Max    Min
======  ==================  =====  =======  =====  =====
Chassis Components
        Midplane             On         10     10     10
no media tray
Blowers
     1  Blower 1 (NP)        On        120    120    120
     2  Blower 2 (NP)        On        120    120    120
Management Modules
     1  WMN315619689         On         25     25     25
     2  Backup MM (NP)                  25     25     25
I/O Modules
     1  I/O Module 2 (NP)               45     45     45
     2  I/O Module 2 (NP)               45     45     45

Domain totals:
  Allocated Power                      390    390    390

Note: (T) means "throttled", (U) means "unable to power up",
      * means "the blade may throttle", (NP) means "the module is not
      present", (D) means "discovering", (C) means "comm error", SB
      means "Standby"

-os none
system>
```

fuelg command (advanced management module only)

Notes:

1. The fuelg command operates differently for the advanced management module and for other management module types. The following command description is for the advanced management module. See “fuelg command (management modules other than the advanced management module)” on page 107 for command syntax for management modules other than the advanced management module.
2. For scripting purposes, the -wm and -os fuelg options for management modules other than the advanced management module are supported by the advanced management module.

This command displays power domain information, listing the power modules that are installed in the BladeCenter unit and information about how the power in each domain is used. This command also configures the power domain policies for power redundancy loss and limiting fan noise during thermal events.

Table 41. fuelg command (advanced management module only)

Function	What it does	Command	Valid targets
Display power domain status overview	Displays health status and total power usage information for all power domains	fuelg	`-T system`
Display detailed power domain status	Displays detailed status and usage information for the specified power domains	fuelg *domain* where *domain* is “pd1” for power domain 1 and “pd2” for power domain 2. If no *domain* is specified, a status overview for all power domains displays.	`-T system`
Set power domain redundancy loss policy	Sets how the BladeCenter unit responds to a condition that could cause a loss of redundant power.	fuelg *domain* -pm *policy* where: • *domain* is “pd1” for power domain 1 and “pd2” for power domain 2. If no *domain* is specified, the *policy* is applied to all power domains. • *policy* of: – “nonred” (default) allows loss of redundancy. – “redwoperf” prevents components from turning on that will cause loss of power redundancy. – “redwperf” power throttles components to maintain power redundancy and prevents components from turning on that will cause loss of power redundancy. Command use restricted (see “Commands and user authority” on page 5).	`-T system`

Table 41. fuelg command (advanced management module only) (continued)

Function	What it does	Command	Valid targets
Thermal event response (acoustic mode)	Sets how the BladeCenter unit blowers respond to thermal events.	fuelg -am *setting* where the acoustic-mode *setting* of: • "off" (default) allows blowers to increase speed to provide additional cooling. • "on" keeps blowers at a fixed speed and power throttles BladeCenter components to reduce power consumption (only for BladeCenter components that support power throttling). Command use restricted (see "Commands and user authority" on page 5).	`-T system`

Example:
To view a power domain status overview, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
fuelg
```

To reduce fan noise during thermal events for all power domains, while the BladeCenter unit is set as the persistent command environment with an advanced management module, at the `system>` prompt, type

```
fuelg -am on
```

To view the detailed power domain status for power domain 1, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
fuelg pd1
```

The following example shows the information that is returned when the fuelg command is run on an advanced management module.

```
system>  fuelg
Note: All power values are displayed in Watts.

Power Domain 1
--------------
Status: Power domain status is good.
Modules:
 Bay 1:   2880
 Bay 2:   2880
Power Management Policy: Non-redundant
Power in Use:  920
Total Power:  3520
Allocated Power (Max):  1280
Remaining Power:  2240
```

```
Power Domain 2
--------------
Status: Power domain status is good.
Modules:
 Bay 3:   2880
 Bay 4:   2880
Power Management Policy: Non-redundant
Power in Use:  920
Total Power:  3520
Allocated Power (Max):  1280
Remaining Power:  2240

-am off
system>  fuelg -am on
OK
system>  fuelg pd1
                             Power  -- Allocated Power --
Bay(s)  Module               State  Current   Max    Min
======  ===================  =====  =======  =====  =====
Chassis Components
        Midplane              On         10     10     10
        Media Tray            On         10     10     10
Fan Packs
     1  Fan Pack 1            On         30     30     30
     2  Fan Pack 2            On         30     30     30
     3  Fan Pack 3            On         30     30     30
     4  Fan Pack 4            On         30     30     30
Management Modules
     1  WMN315619689          On         25     25     25
     2  Standby MM (NP)                  25     25     25
I/O Modules
     1  I/O Module 2 (NP)                45     45     45
     2  I/O Module 2 (NP)                45     45     45
Blade Servers
     1  Blade_one             SB         30    110     80
           (0%,0%)
     2  Blade_two             SB         30    215    122
           (0%,0%,0%,0%)

Domain totals:
  Allocated Power                      390    390    390

Note: (T) means "throttled", (U) means "unable to power up",
      * means "the blade may throttle", (NP) means "the module is not
      present", (D) means "discovering", (C) means "comm error", (SB)
      means "Standby"

-pm none
system>
```

power command

This command turns on and turns off blade servers and I/O (switch) modules.

Table 42. power command

Function	What it does	Command	Valid targets

Power on	Turns on the specified blade server or I/O (switch) module.	power -on
		
		Command use restricted (see “Commands and user authority” on page 5).
			`-T system:blade[x]`
			`-T system:switch[x]`
			
			where *x* is the blade server or I/O (switch) module bay number.

Power on to command console	Opens a command console with an SOL session when the specified blade server is turned on.	power -on -c Command use restricted (see “Commands and user authority” on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.

Power off	Turns off the specified blade server or I/O (switch) module.	power -off
		
		Command use restricted (see “Commands and user authority” on page 5).
			`-T system:blade[x]`
			`-T system:switch[x]`
			
			where *x* is the blade server or I/O (switch) module bay number.

Power cycle	Cycles power for the specified blade server or I/O (switch) module. If the blade server or I/O (switch) module is off, it will turn on. If the blade server or I/O (switch) module is on, it will turn off and then turn on.	power -cycle
		
		Command use restricted (see “Commands and user authority” on page 5).
			`-T system:blade[x]`
			`-T system:switch[x]`
			
			where *x* is the blade server or I/O (switch) module bay number.

Power cycle to command console	Cycles power for the specified blade server. If the blade server is off, it opens a command console with an SOL session when it is turned on. If the blade server is on, it will turn off and then turn on.	power -cycle -c Command use restricted (see “Commands and user authority” on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.

Display power state	Displays the current power state for the specified blade server or I/O (switch) module. Possible return values are on and off.	power -state	`-T system:blade[x]`
			`-T system:switch[x]`
			
			where *x* is the blade server or I/O (switch) module bay number.

Table 42. power command (continued)

Function	What it does	Command	Valid targets
Display POST status for I/O (switch) module	Displays the POST status for the specified I/O (switch) module. If the command is run while POST is in progress, it returns the level of POST that is currently in process. If the command is run after POST is complete, it displays one of the following return values: • The `POST results could not be read.` message displays if there was an internal error during POST. • The `POST results not complete: hex_code` message displays if POST results are not available after POST completes. • If POST returns valid results, one of the following messages displays: – *hex_code*`: Base internal function failure detected.` – *hex_code*`: Internal interface failure detected.` – *hex_code*`: External interface failure detected.` – *hex_code*`: Module completed POST successfully.` – *hex_code*`: Cannot decode POST result code.` • The `Invalid POST results.` message displays if none of the above conditions is true. Where *hex_code* is a hexadecimal code. See the documentation that comes with your I/O module for information. **Note:** This command option is not supported for serial concentrator I/O (switch) modules.	power -state -post	`-T system:switch[`*x*`]` where *x* is the I/O (switch) module bay number.

Example:

To display the power state for the blade server in blade bay 5, while this blade server is set as the persistent command environment, at the `system:blade[5]>` prompt, type

```
power -state
```

To turn on the blade server in blade bay 5, while this blade server is set as the persistent command environment, at the `system:blade[5]>` prompt, type

```
power -on
```

To display the power state for the blade server in blade bay 5 again, while this blade server is set as the persistent command environment, at the system:blade[5]> prompt, type

```
power -state
```

The following example shows the information that is returned from these three commands:

```
system:blade[5]> power -state
Off
system:blade[5]> power -on
OK
system:blade[5]> power -state
On
system:blade[5]>
```

reset command

This command resets blade servers, blade server integrated system management processors (service processors), I/O (switch) modules, or the primary management module.

Table 43. reset command

Function	What it does	Command	Valid targets
Reset	Performs an immediate reset and restart of the specified device.	reset Command use restricted (see "Commands and user authority" on page 5).	-T system:blade[*x*] -T system:switch[*x*] -T system:blade[*x*]:sp -T system:mm[*x*] where *x* is the blade server, I/O (switch) module, or primary management-module bay number.
Reset blade server to command console	Opens a command console with an SOL session when the specified blade server is reset.	reset -c Command use restricted (see "Commands and user authority" on page 5).	-T system:blade[*x*] -T system:blade[*x*]:sp where *x* is the blade server bay number.
Reset management module with failover	Resets the primary management module, enabling failover if a redundant management module is present. An error message is displayed if you try to enable failover when a redundant management module is not installed.	reset -f Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] where *x* is the primary management-module bay number.
Reset I/O (switch) module with standard diagnostics	Performs an immediate reset and restart of the specified device, running standard diagnostics on the I/O (switch) module after it restarts. Running the reset -std command gives the same result as running the reset command on a I/O (switch) module.	reset -std Command use restricted (see "Commands and user authority" on page 5).	-T system:switch[*x*] where *x* is the I/O (switch) module bay number.

Table 43. reset command (continued)

Function	What it does	Command	Valid targets
Reset I/O (switch) module with extended diagnostics	Performs an immediate reset and restart of the specified device, running extended diagnostics on the I/O (switch) module after it restarts.	reset -exd Command use restricted (see "Commands and user authority" on page 5).	`-T system:switch[x]` where *x* is the I/O (switch) module bay number.
Reset I/O (switch) module with full diagnostics	Performs an immediate reset and restart of the specified device, running full diagnostics on the I/O (switch) module after it restarts.	reset -full Command use restricted (see "Commands and user authority" on page 5).	`-T system:switch[x]` where *x* is the I/O (switch) module bay number.
Restart blade server with NMI	Command results depend on the blade server model that is specified: • For a JS20 blade server, the command performs an immediate reset and restart of the specified blade server with non-maskable interrupt (NMI). • For all other blade servers, the command performs an immediate reset and restart of the specified blade server.	reset -sft Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.
Restart blade server and clear NVRAM	Command results depend on the blade server model that is specified: • For a JS20 blade server, the command performs an immediate reset and restart of the specified JS20 blade server and clears all settings stored in non-volatile memory (NVRAM). • For all other blade servers, the command performs an immediate reset and restart of the specified blade server.	reset -clr Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.
Restart blade server and run diagnostics	Command results depend on the blade server model that is specified: • For a JS20 blade server, the command performs an immediate reset and restart of the specified JS20 blade server and runs diagnostics. • For all other blade servers, the command performs an immediate reset and restart of the specified blade server.	reset -dg Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.

Table 43. reset command (continued)

Function	What it does	Command	Valid targets
Restart blade server and run diagnostics using default boot sequence	Command results depend on the blade server model that is specified: • For a JS20 blade server, the command performs an immediate reset and restart of the specified JS20 blade server and runs diagnostics using the default boot sequence configured for the blade server. • For all other blade servers, the command performs an immediate reset and restart of the specified blade server.	reset -ddg Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.

Example:
To reset the service processor on the blade server in blade bay 5, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
reset
```

The following example shows the information that is returned:

```
system> reset -T blade[5]:sp
OK
system>
```

Session commands

Use these commands to start an SOL connection to the command console of a specific blade server or to end a command console session:

- console command
- exit command
- kvm (keyboard, video, mouse) command (advanced management module only)
- mt (media tray) command (advanced management module only)

console command

This command sets up a serial over LAN connection to the command console of a blade server.

To end an SOL session, press Esc followed by an open parenthesis:

Esc (

Table 44. console command

Function	What it does	Command	Valid targets
Create SOL session with blade server	Creates an SOL connection to the specified blade server.	console Command use restricted (see "Commands and user authority" on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.

Table 44. console command (continued)

Function	What it does	Command	Valid targets
Create override SOL session with blade server	Creates an SOL connection to the specified blade server, with the override option enabled. This enables you to end an existing SOL session to that blade server and start a new one.	console -o Command use restricted (see “Commands and user authority” on page 5).	`-T system:blade[x]` where *x* is the blade server bay number.

Example:
To start an SOL connection to the blade server in blade bay 14, while this blade server is set as the persistent command environment, at the `system:mm[x]>` prompt, type

```
sol -T system:blade[14]
```

exit command

This command exits the command-line interface, terminating the current session.

Table 45. exit command

Function	What it does	Command	Valid targets
Exit	Terminates the current command-line interface session.	exit	Any installed device.

Example:
To terminate the current command-line interface session, type

```
exit
```

kvm (keyboard, video, mouse) command (advanced management module only)

This command sets and displays the blade server that is in control of the BladeCenter unit shared KVM.

Table 46. kvm command

Function	What it does	Command	Valid targets
Display KVM owner	Displays the number of the blade server that has KVM ownership. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies. A return value of 0 indicates that no owner is set.	kvm Command use restricted (see “Commands and user authority” on page 5).	`-T system`

Table 46. kvm command (continued)

Function	What it does	Command	Valid targets
Set KVM owner	Sets a blade server as the KVM owner.	kvm -b *blade_server* where *blade_server* is the blade bay that identifies the blade server. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies. A setting of “0” sets no owner. Command use restricted (see “Commands and user authority” on page 5).	`-T system`

Example:

To set the KVM owner to the blade server in blade bay 1, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
kvm -T system -b 1
```

To display the KVM owner, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
kvm -T system
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> kvm -T system -b 1
OK
system:mm[1]> kvm -T system
-b 1
system:mm[1]>
```

mt (media tray) command (advanced management module only)

This command sets and displays the blade server that is in control of the BladeCenter unit shared media tray.

Table 47. mt command

Function	What it does	Command	Valid targets
Display media tray owner	Displays the number of the blade server that has media tray ownership. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies. A return value of 0 indicates that no owner is set.	mt	`-T system`

Table 47. mt command (continued)

Function	What it does	Command	Valid targets
Set media tray owner	Sets a blade server as the media tray owner.	mt -b *blade_server* where *blade_server* is the blade bay that identifies the blade server. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies. A setting of “0” sets no owner. Command use restricted (see “Commands and user authority” on page 5).	`-T system`

Example:

To set the media tray owner to the blade server in blade bay 1, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
mt -T system -b 1
```

To display the media tray owner, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
mt -T system
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> mt -T system -b 1
OK
system:mm[1]> mt -T system
-b 1
system:mm[1]>
```

System management commands (for BladeCenter T only)

Use these commands to manage alarms for monitored parameters of the BladeCenter T unit:

- alarm command

alarm command

This command displays alarm information, acknowledges alarms, and clears alarms for the specified command target.

Table 48. alarm command

Function	What it does	Command	Valid targets

Display all alarms	Display all alerts generated by the target component. When directed to the BladeCenter unit, the command returns a summary of alarms for all BladeCenter components. When directed to a component installed in the BladeCenter unit, the command returns a detailed alarm listing for that component.
	
	Detailed alarm listings include an alarm key that can be used to acknowledge or clear an alarm.
		alarm	`-T system`
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Display power alarms	Display all power related alerts generated by the target component. When directed to the BladeCenter unit, the command returns a summary of alarms for all BladeCenter components. When directed to a component installed in the BladeCenter unit, the command returns a detailed alarm listing for that component.
	
	Detailed alarm listings include an alarm key that can be used to acknowledge or clear an alarm.
		alarm -p	`-T system`
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Display alarm information (specified by alarm generator ID)	Display information for alarm specified by the generator ID.	alarm -q -g *value*
		
		where *value* is the generator ID.
		
		Command use restricted (see “Commands and user authority” on page 5).
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Table 48. alarm command (continued)

Function	What it does	Command	Valid targets

Display alarm information (specified by alarm ID)	Display information for alarm specified by the alarm ID.	alarm -q -a *value*
		
		where *value* is the alarm ID.
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Display detailed alarm information (specified by generator information)	Display detailed information for alarm specified by the alarm generator information. Information returned includes the alarm description that is shown by the management-module Web interface and other information such as the alarm severity, power source, software indicator, and an alarm key.	alarm -q -o *value*
		
		where *value* is the generator information.
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Display alarm information (specified by complete alarm key)	Display information for alarm specified by the complete alarm key.	alarm -q -k *m:g:o:a*
		
		where *m:g:o:a* is the complete alarm key:
		• *m* is the module ID
		• *g* is the generator ID
		• *o* is the generator information
		• *a* is the alarm ID
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Acknowledge alarm (specified by alarm generator ID)	Acknowledge the alarm specified by the generator ID.	alarm -r -g *value*
		
		where *value* is the generator ID.
		
		Command use restricted (see “Commands and user authority” on page 5).
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Table 48. alarm command (continued)

Function	What it does	Command	Valid targets
Acknowledge alarm (specified by generator information)	Acknowledge the alarm specified by the generator information.	alarm -r -o *value* where *value* is the generator information. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] -T system:blade[*x*] -T system:switch[*x*] -T system:power[*x*] -T system:blower[*x*] where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.
Acknowledge alarm (specified by alarm ID)	Acknowledge the alarm specified by the alarm ID.	alarm -r -a *value* where *value* is the alarm ID. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] -T system:blade[*x*] -T system:switch[*x*] -T system:power[*x*] -T system:blower[*x*] where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.
Acknowledge alarm (specified by complete alarm key)	Acknowledge the alarm specified by the complete alarm key.	alarm -r -k *m:g:o:a* where *m:g:o:a* is the complete alarm key: • *m* is the module ID • *g* is the generator ID • *o* is the generator information • *a* is the alarm ID Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] -T system:blade[*x*] -T system:switch[*x*] -T system:power[*x*] -T system:blower[*x*] where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.
Clear alarm (specified by alarm generator ID)	Clear the alarm specified by the generator ID.	alarm -c -g *value* where *value* is the generator ID. Command use restricted (see "Commands and user authority" on page 5).	-T system:mm[*x*] -T system:blade[*x*] -T system:switch[*x*] -T system:power[*x*] -T system:blower[*x*] where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Table 48. alarm command (continued)

Function	What it does	Command	Valid targets

Clear alarm (specified by generator information)	Clear the alarm specified by the generator information.	alarm -c -o *value*
		
		where *value* is the generator information.
		
		Command use restricted (see "Commands and user authority" on page 5).
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Clear alarm (specified by alarm ID)	Clear the alarm specified by the alarm ID.	alarm -c -a *value*
		
		where *value* is the alarm ID.
		
		Command use restricted (see "Commands and user authority" on page 5).
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Clear alarm (specified by complete alarm key)	Clear the alarm specified by the complete alarm key.	alarm -c -k *m:g:o:a*
		
		where *m:g:o:a* is the complete alarm key:
		• *m* is the module ID
		• *g* is the generator ID
		• *o* is the generator information
		• *a* is the alarm ID
		
		Command use restricted (see "Commands and user authority" on page 5).
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Set alarm	Set an alarm for the specified target, including severity level and description.	alarm -s -l *level desc*
		
		where
		• *level* is the severity level:
		– CRT (critical)
		– MJR (major)
		– MNR (minor)
		• *desc* is a short text description of the alarm
		
		Command use restricted (see "Commands and user authority" on page 5).
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:blower[x]`
			
			where *x* is the primary management-module, blade server, I/O (switch) module, power module, or blower bay number.

Example:
To display the alarm status for the BladeCenter T unit, while the BladeCenter T unit is set as the persistent command environment, at the system> prompt, type

```
alarm
```

To display the power alarm status for the BladeCenter T unit, while the BladeCenter T unit is set as the persistent command environment, at the system> prompt, type

```
alarm -p
```

To display detailed power alarm status for the power module in power bay 2, while the BladeCenter T unit is set as the persistent command environment, at the system> prompt, type

```
alarm -T system:power[2]
```

The following example shows the information that is returned from a series of alarm commands. This example assumes that the blade server in blade bay 3 has a major over-temperature fault and that the power module in power bay 2 has a critical fault.

```
system> alarm
Alarms Summary List
Module    Severity    Power    S/W
power[2]  CRT         Yes      No
blade[3]  MJR         No       No
system> alarm -p
Alarms Summary List
Module    Severity    Power    S/W
power[2]  CRT         Yes      No
system> alarm -T system:power[2]
Alarms Detailed List
Severity    Power    S/W    Description        Key
CRT         Yes      No     Under Voltage      2:1:3:2
system> alarm -c -k 2:1:3:2 -T system:power[2]
Alarm Cleared
system> alarm -T system:power[2]
No Active Alarms
system> alarm
Alarms Summary List
Module    Severity    Power    S/W
blade[3]  MJR         No       No
system> alarm -T system:blade[3]
Alarms Detailed List
Severity    Power    S/W    Description        Key
MJR         No       No     Over temperature   3:3:1:3
system> alarm -s -l CRT
OK
system> alarm -s -l MNR -p Investigate Watts -T system:blade[2]
OK
system> alarm -s -l CRT -p Under Voltage -T system:blade[2]
Failed. AlarmID is being used
system>
```

Chapter 4. Error messages

The command-line interface provides error messages specific to each command. The following topics list the common error messages that apply to all commands and command-specific error messages, along with their definitions.

- "Common errors" on page 128
- "alarm command errors" on page 129
- "alertentries command errors" on page 130
- "boot command errors" on page 130
- "clear command errors" on page 130
- "clearlog command errors" on page 131
- "console command errors" on page 131
- "dhcpinfo command errors" on page 131
- "displaylog command errors" on page 131
- "displaysd command errors" on page 132
- "dns command errors" on page 132
- "fuelg command errors" on page 132
- "health command errors" on page 133
- "identify command errors" on page 133
- "ifconfig command errors" on page 133
- "info command errors" on page 135
- "kvm command errors" on page 136
- "ldapcfg command errors" on page 136
- "list command errors" on page 136
- "mt command errors" on page 136
- "nat command errors" on page 136
- "portcfg command errors" on page 137
- "ports command errors" on page 137
- "power command errors" on page 137
- "read command errors" on page 138
- "reset command errors" on page 138
- "service command errors" on page 138
- "slp command errors" on page 138
- "smtp command errors" on page 139
- "snmp command errors" on page 139
- "sol command errors" on page 139
- "sshcfg command errors" on page 140
- "tcpcmdmode command errors" on page 141
- "telnetcfg command errors" on page 141
- "update command errors" on page 141
- "uplink command errors" on page 143
- "users command errors" on page 143
- "write command errors" on page 146

Common errors

The following table lists error messages that apply to all commands. Each command that has unique errors will also have a list of command-specific error messages.

Table 49. Common errors

Error message	Definition
Command line contains extraneous arguments	Displays when extra command arguments are entered.
Duplicate option: *option* where *option* identifies the command option that was entered more than once.	Displays when a user tries to enter the same command option in a single command multiple times. For example, `dns -i 192.168.70.29 -i`
Each option can only be used once per command.	Displays when a user tries to enter the same command option in a single command multiple times. For example, `env -T system:blade[4] -T system:blade[5]`.
Error writing data for option *option* where *option* identifies the command option that is returning an error.	Displays when an internal error occurs while writing a command option value.
Illegal option: *option* where *option* identifies the illegal short command option that was entered.	Displays when an illegal short command option is entered.
Integer argument out of range (*range* - *range*) for *option*: *argument* where: • *range* identifies the range limits • *option* identifies the command option • *argument* identifies the integer that is out of range	Displays when an integer is entered that is out of range.
Invalid integer argument for *option*: *argument* where: • *option* identifies the command option • *argument* identifies the invalid argument	Displays when an invalid integer is entered.
Invalid option	Displays when an invalid command option is entered.
Invalid option argument for *option*: *argument* where: • *option* identifies the command option • *argument* identifies the invalid argument	Displays when an invalid argument for a command option is entered.
Invalid target path	Displays when a user tries to issue a command to a target that is not valid.
Long option *option* requires an argument where *option* identifies the long command option that is missing an argument.	Displays when a long command option is entered without a required argument.
Missing option name	Displays when a dash (-) is entered with out a command option name.
Read/write command error	Displays when an internal error occurs while executing the command.

Table 49. Common errors (continued)

Error message	Definition
Short option *option* requires an argument where *option* identifies the short command option that is missing an argument.	Displays when a short command option is entered without a required argument.
The target bay is empty.	Displays when the user tries to issue a command to an empty blade bay, blower bay, I/O-module bay, management-module bay, or power bay.
The target bay is out of range.	Displays when a user tries to issue a command to a target that is out of range for that target. For example, the `env -T system:blade[15]` command is out of range because the BladeCenter unit has only 14 blade bays.
Unrecognized long option: *option* where *option* identifies the illegal long command option that was entered.	Displays when an illegal long command option is entered.
User does not have the authority to issue this command	Displays when a user lacks the authority level necessary to execute a command.

alarm command errors

The following table lists error messages for the alarm command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 50. alarm command errors

Error message	Definition
Alarm Description must be provided for setting an alarm.	Displays when the user tries to set an alarm without providing an alarm description.
Alarm ID must be from 1 to 255.	Displays when an invalid alarm ID is entered.
Generator ID must be from 1 to 255.	Displays when an invalid generator ID is entered.
Generator ID must be provided.	Displays when a generator information ID is provided without a generator ID.
Module ID must be from 1 to 255.	Displays when an invalid module ID is entered.
No active alarm.	Displays when no active alarm is found for the command target.
No matching alarm.	Displays when no matching alarm is found for the command target.
Severity level must be provided for setting an alarm.	Displays when the user tries to set an alarm without specifying the severity level.
Software Generator ID must be from 1 to 255.	Displays when an invalid generator information is entered.
The entered Alarm Key is not in proper format.	Displays when an invalid alarm key is entered.
Unable to acknowledge the requested alarm.	Displays when an internal error occurs while acknowledging an alarm.
Unable to clear the requested alarm.	Displays when an internal error occurs while clearing an alarm.
Unable to set the requested alarm.	Displays when an internal error occurs while setting an alarm.

alertentries command errors

The following table lists error messages for the alertentries command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 51. alertentries command errors

Error message	Definition
An entry cannot be modified and deleted in the same command.	Displays when a user tries to modify an entry and delete it in the same command.
Arguments containing spaces must be enclosed in quotation marks.	Displays when a user tries to enter a string containing spaces that has an opening quotation mark without a closing quotation mark.
Invalid input. Angle brackets are not allowed in the name field.	Displays when a user tries to enter a string parameter containing < or > for the -n (name) command option.
Invalid option	Displays when an invalid command option is entered. This includes numeric options for the alert recipient that are not from 1 through 12.
Invalid parameter. Input must be numeric.	Displays when a user tries to enter a parameter value containing non-numeric characters for a command option requiring numeric input.
Syntax error. -e can only be used in conjunction with the email argument.	Displays when a user tries to enter an invalid e-mail address for the -e command option.
Syntax error. -i can only be used in conjunction with the director argument.	Displays when a user tries to enter an invalid IP address for the -i command option.
Syntax error. Type alertentries -h for help.	Displays when an alert entry number is entered without the leading dash (-).
The name must be less than 32 characters long.	Displays when a user tries to enter too many characters in an input field.
When creating a new entry, all options are required.	Displays when a required command option is missing when creating a user.

boot command errors

There are no unique errors for the boot command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

clear command errors

The following table lists error messages for the clear command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 52. clear command errors

Error message	Definition
Firmware update is in progress. Try again later.	Displays when the user tries to reset the management module to its default configuration during a firmware update. The error message displays and the management-module configuration does not reset.
Internal error resetting to defaults.	Displays when an internal error occurs while resetting the management module to its default configuration. The error message displays and the management-module configuration does not reset.

clearlog command errors

The following table lists error messages for the clearlog command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 53. clearlog command errors

Error message	Definition
Error clearing the event log.	Displays when an internal error occurs while clearing the event log.

console command errors

The following table lists error messages for the console command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 54. console command errors

Error message	Definition
Error entering console mode.	Displays when an internal error occurs while trying to establish an SOL connection.
Global SOL is not enabled	Displays when SOL is not enabled globally.
Internal Error	Displays when an internal error occurs while processing the command.
SOL is not ready	Displays when the blade server is not available, or when a socket needed to establish a connection to the blade server is not available.
SOL on blade is not enabled	Displays when SOL is not enabled on the blade server where the user is trying to start an SOL session.
SOL session is already active	Displays when the user cannot start an SOL session with a blade server because an SOL session with that blade server is already in progress.

dhcpinfo command errors

There are no unique errors for the dhcpinfo command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

displaylog command errors

The following table lists error messages for the displaylog command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 55. displaylog command errors

Error message	Definition
(There are no more entries in the event log.)	Displays when there are no more event log entries to display.

displaysd command errors

There are no unique errors for the displaysd command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

dns command errors

The following table lists error messages for the dns command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 56. dns command errors

Error message	Definition
At least one address is required to enable DNS.	Displays when a user tries to enable DNS without configuring at least one address.
Invalid ip address	Displays when a user tries to set an invalid IP address.
-on and -off cannot both be used in the same command.	Displays when a user tries to enable and disable DNS in the same command.

fuelg command errors

The following table lists error messages for the fuelg command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 57. fuelg command errors

Error message	Definition
A power module failure in domain *domain_number* can result in an immediate shutdown. where *domain_number* identifies the power domain.	Displays when a power module fails and the domain in which it is installed loses redundancy. The BladeCenter unit might turn itself off, based on the power management configuration.
Blade *blade_number* is not allowed to power on because of insufficient power. where *blade_number* identifies the blade server.	Displays when there is insufficient power available in the power domain to turn on this blade server.
Blade *blade_number* is throttled. where *blade_number* identifies the blade server.	Displays when the specified blade server has reduced power (power throttling) in response to a thermal event or oversubscription condition.
Blade *blade_number* was instructed to power off due to power budget restrictions. where *blade_number* identifies the blade server.	Displays when BladeCenter power management turns off a blade server that is already on in response to a oversubscription condition.
Demand exceeds a single power module. Throttling can occur in power domain *domain_number*. where *domain_number* identifies the power domain.	Displays when the power requirements of components installed in a power domain exceed the level required for redundant operation. Power throttling of BladeCenter components might be able to correct the problem.
There are mismatched power modules in power domain *domain_number*. where *domain_number* identifies the power domain.	Displays when the power modules installed in a power domain have different ratings.

health command errors

There are no unique errors for the health command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

identify command errors

The following table lists error messages for the identify command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 58. identify command errors

Error message	Definition
Delay value must be less than 60	Displays when a user tries to enter a -d value that is greater than 60 seconds.
Identify: Error accessing remote LED	Displays when an internal error occurs while processing the command.
Identify: error getting LED status	Displays when an internal error occurs while processing the command.
Identify: error setting Management Module LED	Displays when an internal error occurs while processing the command.
Identify: Error unknown command	Displays when an internal error occurs while processing the command.
Identify: LED status not supported	Displays when the user tries to get the status of an LED that is not supported by a blade server.
Identify: unknown LED state *state* where *state* identifies the LED state that was returned.	Displays when an LED state other than on, off, or blinking is returned.
Identify: Unknown return status *status* where the *status* value varies based on the problem that was encountered.	Displays when an internal error occurs while processing the command.
Syntax error.	Displays when the user tries to enter an invalid command option. Type `identify -h` for command help.

ifconfig command errors

The following table lists error messages for the ifconfig command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 59. ifconfig command errors

Error message	Definition
Error reading gateway address.	Displays when an internal error occurs while reading the gateway address of a network interface (eth0 or eth1).
Error reading IP Address.	Displays when an internal error occurred while reading the IP address of the integrated system management processor on a blade server, or while reading the IP address of a network interface (eth0 or eth1).
Error reading the burned-in MAC address.	Displays when an internal error occurs while reading the burned-in MAC address of a network interface (eth0 or eth1).
Error reading the data rate.	Displays when an internal error occurs while reading the data rate setting of a network interface (eth0 or eth1).

Table 59. ifconfig command errors (continued)

Error message	Definition
Error reading the DHCP configuration.	Displays when an internal error occurs while reading the DHCP setting of a network interface (eth0).
Error reading the duplex setting.	Displays when an internal error occurs while reading the duplex setting of a network interface (eth0 or eth1).
Error reading the hostname.	Displays when an internal error occurs while reading the host name of a network interface (eth0).
Error reading the locally administered MAC address.	Displays when an internal error occurs while reading the locally administered MAC address of a network interface (eth0 or eth1).
Error reading the maximum transmission unit.	Displays when an internal error occurs while reading the maximum transmission unit (MTU) setting of a network interface (eth0 or eth1).
Error reading the subnet mask.	Displays when an internal error occurs while reading the subnet mask of a network interface (eth0 or eth1).
Error writing IP Address.	Displays when an internal error occurs while setting the IP address of the integrated system management processor on a blade server.
Invalid IP arg for *option*: *ip_address*. Each byte has to be in the range (0-255) where: • *option* identifies the command option • *ip_address* identifies the invalid IP address argument	Displays when the user tries to enter an IP address that is out of range. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255.
Invalid IP arg for *option*: *ip_address*. Enter 4 bytes separated by 3 dots where: • *option* identifies the command option • *ip_address* identifies the invalid IP address argument	Displays when the user tries to enter an IP address that is too long. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255.
Invalid IP arg for *option*: *ip_address*. Too few bytes where: • *option* identifies the command option • *ip_address* identifies the invalid IP address argument	Displays when the user tries to enter an IP address with too few bytes. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255.
Invalid IP arg for *option*: *ip_address*. Too many bytes where: • *option* identifies the command option • *ip_address* identifies the invalid IP address argument	Displays when the user tries to enter an IP address with too many bytes. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255.
Invalid hostname arg for *option*: *hostname*. Consecutive dots where: • *option* identifies the command option • *hostname* identifies the invalid hostname argument	Displays when the user tries to enter consecutive periods (.) as part of a hostname.
Invalid hostname arg for *option*: *hostname*. Length has to be < 64 characters where: • *option* identifies the command option • *hostname* identifies the invalid hostname argument	Displays when the user tries to enter a hostname longer than 63 characters.

Table 59. ifconfig command errors (continued)

Error message	Definition
Invalid hostname arg for *option*: *hostname*. Only alphanumeric chars and ._- allowed where: • *option* identifies the command option • *hostname* identifies the invalid hostname argument	Displays when the user tries to enter an hostname that contains invalid characters. Valid characters that can be used in a hostname are letters, numbers, periods (.), dashes (-), and underscores (_).
Invalid ip address.	Displays for one of the following errors: • A user tries to set the IP address of system:blade[1]:sp either to an invalid IP address, or an IP address whose last part is greater than 255 (the max number of blade servers). • A user tries to enter an invalid IP address for the -i (static IP address) command option.
Invalid MAC arg for *option*: *address*. Invalid syntax where: • *option* identifies the command option • *address* identifies the invalid MAC address argument	Displays when the user tries to enter an invalid MAC address.
Invalid MAC arg for *option*: *address*. Multicast addresses not allowed where: • *option* identifies the command option • *address* identifies the invalid MAC address argument	Displays when the user tries to enter a multicast address.
Invalid MAC arg for *option*: *address*. Too few bytes where: • *option* identifies the command option • *address* identifies the invalid MAC address argument	Displays when the user tries to enter a MAC address with too few bytes.
Invalid MAC arg for *option*: *address*. Too many bytes where: • *option* identifies the command option • *address* identifies the invalid MAC address argument	Displays when the user tries to enter a MAC address with too many bytes.
Invalid parameter. Valid values for -c are dhcp, static, or dthens.	Displays when a user tries to enter an invalid parameter for the -c (Ethernet configuration method) command option.
The target must be system:blade[1]:sp for this command	Displays when a user tries to issue the `ifconfig -i <ip address> -T system:blade[x]:sp` to a blade server other than blade[1].

info command errors

The following table lists error messages for the info command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 60. info command errors

Error message	Definition
Device not found	Displays when no VPD is available for the targeted device.
Unknown device type.	Displays when the command is targeted to an unknown device type.

kvm command errors

There are no unique errors for the kvm command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

ldapcfg command errors

The following table lists error messages for the ldapcfg command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 61. ldapcfg command errors

Error message	Definition
AMM target name is limited to 63 characters.	Displays when a user tries to set an AMM target name that is longer than 63 characters.

list command errors

The following table lists error messages for the list command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 62. list command errors

Error message	Definition
The level must be non-zero.	Displays when the user tries to enter a level of depth for tree-structure display of 0.

mt command errors

There are no unique errors for the mt command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

nat command errors

The following table lists error messages for the nat command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 63. nat command errors

Error message	Definition
NAT configuration is not supported on this IO module.	Displays when the user tries to direct a nat command to an I/O module that does not support the network address table.
Error reading -pi	Displays when an internal error occurs while reading the protocol ID for the specified row in the NAT table for the specified I/O module.
Error reading -ep	Displays when an internal error occurs while reading the external port number for the specified row in the NAT table for the specified I/O module.
Error reading -ip	Displays when an internal error occurs while reading the internal port number for the specified row in the NAT table for the specified I/O module.
Error reading -en	Displays when an internal error occurs while reading the state of the specified row in the NAT table for the specified I/O module.

Table 63. nat command errors (continued)

Error message	Definition
The first two rules' protocol names cannot be changed.	Displays when the user tries to change a rule for a protocol name that is static.
When creating a new rule, all fields must be specified.	Displays when the user does not specify all fields when creating a rule.

portcfg command errors

There are no unique errors for the portcfg command. See "Common errors" on page 128 for a list of error messages that apply to all commands.

ports command errors

The following table lists error messages for the ports command. See "Common errors" on page 128 for a list of error messages that apply to all commands.

Table 64. ports command errors

Error message	Definition
A certificate must first be in place before SSL can be enabled. Use the web interface to generate one.	Displays when the user tries to enable SSL before setting up a valid SSL certificate and private encryption key.
An SSH server key must first be in place before SSH can be enabled. Use the web interface to generate one.	Displays when the user tries to enable SSH before setting up a valid SSH server key.
Duplicate port number entered.	Displays when the user tries to enter a port number that is already in use.
Invalid parameter. The timeout must be between 0 and 4294967295 seconds.	Displays when a user tries to enter a timeout that is outside of the valid range.
Port number out of range.	Displays when the user tries to enter a port number that is outside of the valid range.
Reserved port number entered.	Displays when the user tries to enter a port number that has been reserved.
Secure SMASH CLP cannot be enabled without a valid SSH server key in place.	Displays when the user tries to enable the secure SMASH CLP before setting up a valid SSH server key.

power command errors

The following table lists error messages for the power command. See "Common errors" on page 128 for a list of error messages that apply to all commands.

Table 65. power command errors

Error message	Definition
Invalid POST results.	Displays when the POST results are not valid.
POST results could not be read.	Displays when an internal error occurs during POST.
POST results not complete: *hex_code* where the *hex_code* value varies based on the problem that was encountered.	Displays when the POST results are not available. See the documentation that comes with the device that failed to respond correctly to the `power` command for information about the *hex_code* value.

read command errors

The following table lists error messages for the read command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 66. read command errors

Error message	Definition
Firmware update is in progress. Try again later.	Displays when a user tries to restore the management-module configuration from the BladeCenter unit midplane while the management-module firmware is updating.
Configuration restore from the chassis failed: operation not supported.	Displays when an internal error occurs while restoring the management-module configuration from the BladeCenter unit midplane due to a failed system check.
Configuration restore from the chassis failed: i2c bus read error	Displays when an internal error occurs while restoring the management-module configuration from the BladeCenter unit midplane due to an i2ct read error.
Configuration restore from the chassis failed: NVRAM compression error	Displays when an internal error occurs while restoring the management-module configuration from the BladeCenter unit midplane due to an EEPROM compression error.
Configuration restore from the chassis failed: unsupported midplane data format	Displays when an internal error occurs while restoring the management-module configuration from the BladeCenter unit midplane due to an unsupported EEPROM format.

reset command errors

The following table lists error messages for the reset command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 67. reset command errors

Error message	Definition
An error occurred while disabling failover.	Displays when an internal error occurs while disabling failover.
An error occurred while enabling failover.	Displays when an internal error occurs while enabling failover.
Firmware update is in progress. Try again later.	Displays when the user tries to reset the management module during a firmware update. The error message displays and the management module does not reset.
There is no backup management module installed.	Displays when a user tries to enable failover on a management-module reset and there is no back-up management module.

service command errors

There are no unique errors for the service command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

slp command errors

There are no unique errors for the slp command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

smtp command errors

The following table lists error messages for the smtp command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 68. smtp command errors

Error message	Definition
Input length is greater than the maximum characters allowed.	Displays when a user tries to enter too many characters in an input field.
Invalid host name or ip address	Displays when a user tries to set the SMTP host name or IP address to an invalid value.
SMTP server host name or IP address is not set	Displays when a user tries to view the SMTP host name or IP address and the values are not set.

snmp command errors

The following table lists error messages for the snmp command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 69. snmp command errors

Error message	Definition
Arguments containing spaces must be enclosed in quotation marks	Displays when a user tries to enter a string containing spaces that has an opening quotation mark without a closing quotation mark.
At least one configured community is required to enable SNMP.	Displays when a user tries to enable SNMP without configuring at least one community name.
Input length is greater than the maximum characters allowed.	Displays when a user tries to enter too many characters in an input field.
Invalid community name	Displays when a user tries to set a community name to an invalid value.
Invalid host name or ip address	Displays when a user tries to set the SNMP host name or IP address to an invalid value.

sol command errors

The following table lists error messages for the sol command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 70. sol command errors

Error message	Definition
An error occurred while disabling SOL globally	Displays when an internal error occurs while disabling SOL globally.
An error occurred while disabling SOL on that blade	Displays when an internal error occurs while disabling SOL on a blade server.
An error occurred while enabling SOL globally	Displays when an internal error occurs while enabling SOL globally
An error occurred while enabling SOL on that blade	Displays when an internal error occurs while enabling SOL on a blade server.
An error occurred while reading the global SOL status	Displays when an internal error occurs while reading the global SOL status.

Table 70. sol command errors (continued)

Error message	Definition
An error occurred while reading the SOL accumulate timeout	Displays when an internal error occurs while reading the SOL accumulate timeout.
An error occurred while reading the SOL retry count	Displays when an internal error occurs while reading the SOL retry count.
An error occurred while reading the SOL retry interval	Displays when an internal error occurs while reading the SOL retry interval.
An error occurred while reading the SOL send threshold	Displays when an internal error occurs while reading the SOL send threshold.
An error occurred while reading the SOL session status on that blade	Displays when an internal error occurs while reading the SOL session status on a blade server.
An error occurred while reading the SOL VLAN ID	Displays when an internal error occurs while reading the SOL VLAN ID.
An error occurred while setting the SOL accumulate timeout	Displays when an internal error occurs while setting the SOL accumulate timeout.
An error occurred while setting the SOL blade reset sequence	Displays when an internal error occurs while processing the command.
An error occurred while setting the SOL escape sequence	Displays when an internal error occurs while processing the command.
An error occurred while setting the SOL retry count	Displays when an internal error occurs while setting the SOL retry count.
An error occurred while setting the SOL retry interval	Displays when an internal error occurs while setting the SOL retry interval.
An error occurred while setting the SOL send threshold	Displays when an internal error occurs while setting the SOL send threshold.
An error occurred while setting the SOL vlan id	Displays when an internal error occurs while processing the command.
Invalid arg for -status. Must be on or off.	Displays if a user tries to enter an invalid argument for the -status command option.
Invalid parameter. The accumulate timeout must be between 1 and 1275 inclusive.	Displays when a user tries to enter an accumulate timeout that is outside of the valid range.
Invalid parameter. The retry count must be between 0 and 7, inclusive.	Displays when a user tries to enter a retry count that is outside of the valid range.
Invalid parameter. The send threshold must be between 1 and 251 inclusive.	Displays when a user tries to enter a send threshold that is outside of the valid range.
Invalid parameter. The vlan id must be between 1 and 4095 inclusive.	Displayed if a user tries to enter a VLAN ID that is out of range.
Retry interval range is too large. Setting to 250.	Displays when a user tries to enter a retry interval that is greater than 250 ms. If the user tries to enter a retry interval greater than 250 ms, the retry interval will be set to 250 ms.
This blade does not support SOL	Displays if a user tries to issue the SOL command to a blade server that does not support SOL.

sshcfg command errors

There are no unique errors for the sshcfg command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

tcpcmdmode command errors

The following table lists error messages for the tcpcmdmode command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 71. tcpcmdmode command errors

Error message	Definition
Error disabling tcpcmdmode	Displays when an internal error occurs while disabling TCP command mode.
Error enabling TCP command mode	Displays when an internal error occurs while enabling TCP command mode.
Invalid parameter. Input must be numeric.	Displays when a user tries to enter a parameter value for the -t (timeout) command option containing non-numeric characters. For example, `tcpcmdmode -t 200m`.
Invalid parameter. The timeout must be between 0 and 4294967295 seconds.	Displays when a user tries to enter a parameter value for the -t (timeout) command option that is outside of the valid range.

telnetcfg command errors

The following table lists error messages for the telnetcfg command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 72. telnetcfg command errors

Error message	Definition
Invalid parameter. Input must be numeric.	Displays when a user tries to enter a Telnet timeout value containing non-numeric characters. For example, `telnetcfg -t 200w`.
Invalid parameter. The timeout must be between 0 and 4294967295 seconds.	Displays when a user tries to enter a Telnet timeout value that is out of range.

update command errors

The following table lists error messages for the update command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 73. update command errors

Error message	Definition
Flash operation failed.	Displays when an internal error occurs during flash firmware update.
Flash operation failed status *percentage* where the *percentage* value varies based on when the problem was encountered.	Displays when an internal error occurs during flash firmware update.
Flash operation not in process or status unavailable.	Displays when an internal error occurs during flash firmware update.
Flash operation timed out *percentage* where the *percentage* value varies based on when the problem was encountered.	Displays when an internal error occurs during flash firmware update.

Table 73. update command errors (continued)

Error message	Definition
Flash preparation - error sending packet file *filename* where the *filename* value varies based on the file being updated.	Displays when an internal error occurs during flash firmware update.
Flash preparation error.Packet percent complete *percentage*. Flash percent complete *percentage*. where the *percentage* value varies based on when the problem was encountered.	Displays when an internal error occurs during flash firmware update.
Flash preparation error.Timeout on packet preparation operation *percentage* where the *percentage* value varies based on when the problem was encountered.	Displays when an internal error occurs during flash firmware update.
Flashing not supported on this target	Displays when a user targets the command to a I/O module that does not support flash firmware updates.
Invalid option	Displays when an invalid command option is entered. For the update command, invalid command option errors include: • the -i (IP address) command option does not have an IP address parameter • the -i (IP address) command option specifies an invalid IP address • attempting to enter the -i (IP address) command option without the -n (filename) command option • the -n (filename) command option does not have a file name parameter • attempting to enter the -n (filename) command option without the -i (IP address) command option • attempting to enter the -v (verbose) command option without the -i (IP address) command option and -n (filename) command option • attempting to enter the -v (verbose) command option with the -a command option
Management Module *bay_number* is not installed. where the *bay_number* value varies based on the problem that was encountered.	Displays when the command is targeted to a management-module bay where no management module is installed.
TFTP Error *error_code* where the *error_code* value varies based on the problem that was encountered.	Displays when an internal error occurs for the TFTP connection.
TFTP Error. Access violation.	Displays when an internal error occurs for the TFTP connection.
TFTP Error. Connection failure.	Displays when an internal error occurs for the TFTP connection.
TFTP Error. Disk full or allocation exceeded.	Displays when an internal error occurs for the TFTP connection.
TFTP Error. File already exists.	Displays when an internal error occurs for the TFTP connection.
TFTP Error. File error.	Displays when an internal error occurs for the TFTP connection.

Table 73. update command errors (continued)

Error message	Definition
TFTP Error. File not found.	Displays when an internal error occurs for the TFTP connection.
TFTP Error. Illegal option negotiation.	Displays when an internal error occurs for the TFTP connection.
TFTP Error. Illegal TFTP operation.	Displays when an internal error occurs for the TFTP connection.
TFTP Error. Unable to allocate memory.	Displays when an internal error occurs for the TFTP connection.
TFTP Error. Unknown transfer ID.	Displays when an internal error occurs for the TFTP connection.
TFTP Error. Unknown user.	Displays when an internal error occurs for the TFTP connection.
Unable to read blade server VPD bay *bay_number name*. where the *bay_number* and *name* values vary based on the problem that was encountered.	Displays when the command is specifies an empty bay or if an internal error occurs when reading the VPD.
Unable to read MM VPD bay *bay_number name*. where the *bay_number* and *name* values vary based on the problem that was encountered.	Displays when the command is specifies an empty bay or if an internal error occurs when reading the VPD.
Unable to read I/O Module VPD bay *bay_number name*. where the *bay_number* and *name* values vary based on the problem that was encountered.	Displays when the command is specifies an empty bay or if an internal error occurs when reading the VPD.
Unknown device type.	Displays when the command is targeted to an unknown device type.
Update error. Invalid destination.	Displays when a user tries to issue a command to a target that is not valid.

uplink command errors

The following table lists error messages for the uplink command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 74. uplink command errors

Error message	Definition
Invalid uplink delay value	Displays when a user tries to enter a delay value that is less than 1 or greater than 255. For example, `uplink -del 0`.

users command errors

The following table lists error messages for the users command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 75. users command errors

Error message	Definition
An entry cannot be modified and deleted in the same command.	Displays when a user tries to modify and delete a user in the same command.

Table 75. users command errors (continued)

Error message	Definition
Arguments containing spaces must be enclosed in quotation marks.	Displays when a user tries to enter a context name containing spaces that does not have opening and closing quotation marks.
Error: the RBS permissions capability is not enabled.	Displays when attempting to run use the -a rbs: command option on management-module firmware that does not support this option. (The -a rbs: command option is not supported for the advanced management module.)
Error converting RBS permissions	Displays when an internal error occurs while converting permissions data to role-based security (RBS) format.
Error creating user	Displays when an internal error occurs while creating a user.
Error setting the access type	Displays when an internal error occurs while setting the access type.
Error setting the authentication protocol	Displays when an internal error occurs while setting the authentication protocol.
Error setting the authority level	Displays when an internal error occurs while setting the authority level.
Error setting the context name	Displays when an internal error occurs while setting the context name.
Error setting the hostname/IP address	Displays when an internal error occurs while setting the hostname or IP address.
Error setting the password	Displays when an internal error occurs while setting the password.
Error setting the privacy password	Displays when an internal error occurs while setting the privacy password.
Error setting the privacy protocol	Displays when an internal error occurs while setting the privacy protocol.
Error setting the username	Displays when an internal error occurs while setting the username.
Incorrect login permission option: *permission* where the *permission* value varies based on the problem that was encountered.	Displays when a user tries to specify an invalid login permission for the -a command option.
Invalid argument. Valid arguments for -at are read, write, and traps.	Displays when a user tries to set an invalid argument for the -at command option.
Invalid argument. Valid choices are des or <none>.	Displays when a user tries to set an invalid argument for the -pp command option.
Invalid argument. Valid choices are md5, sha, or <none>.	Displays when a user tries to set an invalid argument for the -ap command option.
Invalid authority level.	Displays for one of the following errors: • A user tries to set an authority level that is invalid. • A user tries to set a custom authority level without specifying any customization information.
Invalid device number (first number must be smaller): *device_A-device_B*. where *device_A* and *device_B* identify the ends of the invalid device range being specified.	Displays when a user specifies an invalid device range while trying to create or modify a user.

Table 75. users command errors (continued)

Error message	Definition
Invalid device number: *device_number*. where *device_number* identifies the device number that is invalid.	Displays when a user provides a device number that is out of range while trying to create or modify a user.
Invalid hostname or ip address.	Displays when a user tries to set an invalid host name or IP address for the -i command option.
Invalid rbs device: *device*. where *device* identifies the device that is invalid.	Displays when a user specifies an invalid device while trying to create or modify a user.
Invalid rbs device: Must specify device number	Displays when a user specifies an invalid device number while trying to create or modify a user.
Invalid rbs device list.	Displays when a user does not specify a device list while trying to create or modify a user.
Invalid rbs device (must be same device): *device*. where *device* identifies the device that is invalid.	Displays when a user specifies an invalid device while trying to create or modify a user.
Invalid rbs role: *role*. where *role* identifies the role that is invalid.	Displays when a user specifies an invalid role while trying to create or modify a user.
Invalid username. The username can only contain numbers, letters, dots, and underscores.	Displays when the user tries to enter an username that contains invalid characters. Valid characters that can be used in a username are letters, numbers, periods (.), and underscores (_).
Syntax error. -a option must have an argument.	Displays when a user tries to attempt to enter the command with a -a command option that has no argument.
Syntax error. -at option must have an argument.	Displays when a user tries to attempt to enter the command with a -at command option that has no argument.
Syntax error. -cn option must have an argument.	Displays when a user tries to attempt to enter the command with a -cn command option that has no argument.
Syntax error. -i option must have an argument.	Displays when a user tries to attempt to enter the command with a -i command option that has no argument.
Syntax error. -n option must have an argument.	Displays when a user tries to attempt to enter the command with a -n command option that has no argument.
Syntax error. -ppw option must have an argument.	Displays when a user tries to attempt to enter the command with a -ppw command option that has no argument.
Syntax error. Multiple -a options found.	Displays when a user tries to enter the -a command option in a single command multiple times.
Syntax error. Multiple -ap options found.	Displays when a user tries to enter the -ap option flag in a single command multiple times.
Syntax error. Multiple -at options found.	Displays when a user tries to enter the -at option flag in a single command multiple times.
Syntax error. Multiple -cn options found.	Displays when a user tries to enter the -cn option flag in a single command multiple times.

Table 75. users command errors (continued)

Error message	Definition
Syntax error. Type users -h for help.	Displays when a user tries to set an invalid value for a command option.
Syntax error. Multiple -i options found.	Displays when a user tries to enter the -i option flag in a single command multiple times.
Syntax error. Multiple -n options found.	Displays when a user tries to enter the -n option flag in a single command multiple times.
Syntax error. Multiple -p options found.	Displays when a user tries to enter the -p option flag in a single command multiple times.
Syntax error. Multiple -pp options found.	Displays when a user tries to enter the -pp option flag in a single command multiple times.
Syntax error. Multiple -ppw options found.	Displays when a user tries to enter the -ppw option flag in a single command multiple times.
The context name must be less than 32 characters long.	Displays when a user tries to set a context name that is longer than 31 characters.
The password must be at least 5 characters long, but no more than 15 characters long.	Displays when the user tries to enter a password that is too short or too long.
The password must contain at least one alphabetic and one non-alphabetic character.	Displays when the user tries to enter a password that does not have at least one alphabetic and one non-alphabetic character.
The privacy password must also be set when setting the privacy protocol.	Displays if the user tries to set the privacy protocol to des without a specifying a privacy password (-ppw command option).
The privacy password must be less than 32 characters long.	Displays when a user tries to set a privacy password that is longer than 31 characters.
The username cannot be longer than 15 characters.	Displays when a user tries to set a user name that is longer than 15 characters.
When creating a new user, all options are required.	Displays when a user tries to create a new user without defining all command options and arguments.

write command errors

The following table lists error messages for the write command. See “Common errors” on page 128 for a list of error messages that apply to all commands.

Table 76. write command errors

Error message	Definition
Failed to save configuration settings to the chassis.	Displays when an internal error occurs while saving the management-module configuration to the BladeCenter unit midplane.
Firmware update is in progress. Try again later.	Displays when a user tries to save the management-module configuration to the BladeCenter unit midplane while the management-module firmware is updating.

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your BladeCenter® product or optional device, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Hardware Maintenance Manual and Troubleshooting Guide* or *Problem Determination and Service Guide* on the IBM *Documentation* CD that comes with your system.
- Go to http://www.ibm.com/servers/eserver/support/bladecenter/index.html to check for information to help you solve the problem.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with BladeCenter systems also describes the diagnostic tests that you can perform. Most BladeCenter systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the software.

Using the documentation

Information about your IBM BladeCenter system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/servers/eserver/support/bladecenter/index.html and follow the instructions. Also, some documents are available through the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

Getting help and information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM BladeCenter systems, optional devices, services, and support at http://www.ibm.com/servers/eserver/support/bladecenter/index.html.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with BladeCenter products. For information about which products are supported by Support Line in your country or region, see http://www.ibm.com/services/sl/products/.

For more information about Support Line and other IBM services, see http://www.ibm.com/services/, or see http://www.ibm.com/planetwide/ for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through IBM Services or through your IBM reseller, if your reseller is authorized by IBM to provide warranty service. See http://www.ibm.com/planetwide/ for support telephone numbers, or in the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan product service

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

IBM Taiwan product service contact information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Appendix B. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Active Memory	IBM	TechConnect
Active PCI	IBM (logo)	Tivoli
Active PCI-X	IntelliStation	Tivoli Enterprise
AIX	NetBAY	Update Connector
Alert on LAN	Netfinity	Wake on LAN

BladeCenter
Chipkill
e-business logo
@server
FlashCopy
i5/OS
Predictive Failure Analysis
ServeRAID
ServerGuide
ServerProven
System x
XA-32
XA-64
X-Architecture
XpandOnDemand
xSeries

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adaptec and HostRAID are trademarks of Adaptec, Inc., in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Red Hat, the Red Hat “Shadow Man” logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speeds indicate the internal clock speed of the microprocessor; other factors also affect application performance.

CD drive speeds list the variable read rate. Actual speeds vary and are often less than the maximum possible.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for approximately 1000 bytes, MB stands for approximately 1 000 000 bytes, and GB stands for approximately 1 000 000 000 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity may vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives available from IBM.

Maximum memory may require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven®, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

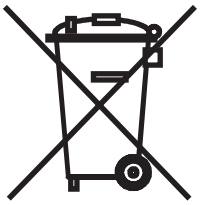
IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software may differ from its retail version (if available), and may not include user manuals or all program functionality.

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM http://www.ibm.com/ibm/environment/products/prp.shtml.



Notice: This mark applies only to countries within the European Union (EU) and Norway.

This appliance is labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

注意: このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

Remarque : Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'etiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

Battery return program

This product may contain a sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and battery packs from IBM equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Have the IBM part number listed on the battery available prior to your call.

For Taiwan: Please recycle batteries.

For the European Union:

For California: Perchlorate material – special handling may apply. See http://www.dtsc.ca.gov/hazardouswaste/perchlorate/.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5 Chapter 33. Best Management Practices for Perchlorate Materials. This product/part may include a lithium manganese dioxide battery which contains a perchlorate substance.

Electronic emission notices

Federal Communications Commission (FCC) statement

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

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

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

United Kingdom telecommunications safety requirement

Notice to Customers

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

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

Taiwanese Class A warning statement

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

Chinese Class A warning statement

声　　明
此为 A 级产品。在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Japanese Voluntary Control Council for Interference (VCCI) statement

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

Index

Special characters

! 23
? 22

A

accumulate timeout
  set for SOL 76
acknowledge alarms
  alarm ID 124
  complete alarm key 124
  generator ID 123
  generator information 124
acoustic mode, disable 112
acoustic mode, enable 112
activate network protocol settings
  I/O module 55
advanced management module commands
  clear 40
  displaysd 43
  fuelg 111
  ifconfig 49
  kvm 119
  ldapcfg 54
  mt 120
  nat 55
  portcfg 57
  ports 59
  read 66
  service 66
  slp 67
  sshcfg 79
  tcpcmdmode 81
  users 95
  write 104
alarm 122
  acknowledge (alarm ID) 124
  acknowledge (complete alarm key) 124
  acknowledge (generator ID) 123
  acknowledge (generator information) 124
  clear (alarm ID) 125
  clear (complete alarm key) 125
  clear (generator ID) 124
  clear (generator information) 125
  display (alarm ID) 123
  display (all) 122
  display (complete alarm key) 123
  display (generator ID) 122
  display (generator information) 123
  display (power) 122
  options
    c, a 125
    c, g 124
    c, k 125
    c, o 125
    p 122
    q, a 123
alarm *(continued)*
  options *(continued)*
    q, g 122
    q, k 123
    q, o 123
    r, a 124
    r, g 123
    r, k 124
    r, o 124
    s, l 125
  set 125
alarm command 122
alarm command errors 129
alarm commands
  example 126
alert notification method, set 37
alert recipient, create 35, 36
alert recipient, delete 34
alert recipient, set email address 37
alert recipient, set hostname for alerts 38
alert recipient, set IP address for alerts 38
alert recipient, set name 36
alert recipient, set status 36
alert recipients, manage 34
alert type, filter 37
alert type, set 37
alertentries 34
  options
    1 through 12 34
    create (n, status, f, t, e, i) 35
    del 34
    e 37
    f 37
    i 38
    n 36
    status 36
    t 37
alertentries command 34
alertentries command errors 130
alertentries commands
  example 38
alerts, display 26
algorithms, encryption 12
attributes, display for firmware 31
authority, command 5

B

baud rate
  set for serial port of management module 57
blade mezzanine
  command target 20
blade server
  boot 107
  boot (to console) 107
  command target 19
  cycle power 107, 114
  display cKVM status 51

blade server *(continued)*
display power state 114
power off 114
power on 114
power on (to console) 114
reset 107, 116
reset (clear NVRAM) 117
reset (run diagnostics with boot sequence) 118
reset (run diagnostics) 117
reset (to console) 107, 116
reset (with NMI) 117
set as KVM owner 120
set as media tray owner 121
turn off 114
turn on 114
turn on (to console) 114
blade servers
set starting IP address 48, 51
BladeCenter T specific commands 122, 127
BladeCenter unit
command target 19
configuring 14
display global cKVM status 52
display network settings 52
set starting BSMP IP address 51
set VLAN ID 52
blink location LED 28
blower
command target 21
BMC
command target 20
boot 107
blade server 107
options
-p powercycle 107
-p reset 107
c 107
boot (to console)
blade server 107
boot command errors 130
boot commands 107
example 107
built-in commands 18, 25

C

capture service information 43
change command environment 18
cKVM (global) status
display for BladeCenter unit 52
cKVM status
display (global) for BladeCenter unit 52
display for blade server 51
Class A electronic emission notice 153
clear
options
cnfg 40, 41
config 39, 41
clear alarms
alarm ID 125
complete alarm key 125
clear alarms *(continued)*
generator ID 124
generator information 125
clear command 39, 40
clear command errors 130
clear commands
example 40, 41
clear event log
management module 104
clear management module event log commands 104
example 104
clearlog
example 104
clearlog command errors 131
clearlog commands 104
example 104
CLI key sequence
set for SOL 77
command
health 25, 26
system physical configuration 24
command authority 5
command environment selecting 4
command history 23
command redirect 18
command target 18
blade mezzanine 20
blade server 19
BladeCenter unit 19
blower 21
BMC 20
high-speed expansion card 20
I/O module 21
I/O-expansion card 20
integrated system management processor 20
management module 19
media tray 21
microprocessor 20
power module 21
service processor 20
storage expansion unit 20
switch module 21
temporary 5
view 24
command target selection 4
command-line interface
guidelines 3
case sensitivity 3
command history 4
data types 4
delimiters 4
help 4
options 3
output format 4
strings 4
starting 12
using 3, 17
command-line session configuration
display for management module 82
command-line session timeout
display for management module 82

command-line timeout
set for management module 82
commands
alarm 122, 126
alertentries 34, 38
boot 107
built-in 18, 25
clear 39, 40, 41
clear management module event log 104
clearlog 104
common 25, 32
configuration 33, 104
console 118, 119
dhcpinfo 42
display management module event log 105
displaylog 105
displaysd 43
dns 43, 44
environment 18, 21
event log, clear for management module 104
event log, display for management module 105
examples
alarm 126
alertentries 38
boot 107
clear 40, 41
clear management module event log 104
clearlog 104
console 119
DHCP settings for management module 42
dhcpinfo 42
display KVM owner 120
display management module event log 105
display media tray owner 121
displaylog 105
displaysd 43
DNS 44
env 21
environment 21
environment redirect 22
Ethernet network settings for management module 48, 53
exit 119
fuelg 109, 112
health 26
help 22
history 23
I/O module network protocol configuration 57
identify 28
ifconfig 48, 53
info 30
kvm 120
LDAP configuration for management module 54
ldapcfg 54
list 24
management module DHCP settings 42
management module DNS 44
management module Ethernet network settings 48, 53
management module event log clear 104
management module event log display 105
commands *(continued)*
examples *(continued)*
management module LDAP configuration 54
management module network port configuration 65
management module restore configuration 66
management module save configuration 104
management module serial port settings 58
management module service 67
management module SLP configuration 68
management module SMTP settings 69
management module SNMP settings 73
management module SSH v1 79
management module telnet configuration 82
management module uplink failover 83
mt 121
nat 57
network port configuration for management module 65
network protocol configuration for I/O module 57
portcfg 58
ports 65
power 115
read 66
reset 118
restore configuration for management module 66
save configuration for management module 104
Serial Over LAN 78
serial port settings for management module 58
service 67
set KVM owner 120
set media tray owner 121
slp 68
SLP configuration for management module 68
smtp 69
SMTP settings for management module 69
snmp 73
SNMP settings for management module 73
sol 78
SSH v1 configuration for management module 79
sshcfg 79
syntax help 22
tcpcmdmode 80, 81
telnetcfg 82
update 31
uplink 83
users 94, 103
write 104
exit 119
fuelg 107, 109, 111, 112
help 22
history 23
identify 28
ifconfig 45, 48, 49, 53
info 29, 30
kvm 119, 120
ldapcfg 54
list 24
management module event log 104, 106
management module failover 83

commands *(continued)*
mt 120, 121
nat 55, 57
portcfg 57, 58
ports 59, 65
power 114, 115
power control 106, 118
read 66
reset 116, 118
reset command 106, 118
Serial Over LAN 75, 78
service 66, 67
session command 118, 121
slp 67, 68
smtp 68, 69
snmp 69, 73
SOL 75, 78
sshcfg 79
system management command 122, 127
tcpcmdmode 79, 80, 81
telnet configuration 82
telnetcfg 82
update 30, 31
uplink 83
users 84, 94, 95, 103
write 104
common commands 25, 32
common errors 128
communicating with IBM Director 79, 81
communication
out-of-band 79, 81
communication rate
set for serial port of management module 57
component information 29
component information display 29
configuration
disable automatic for management module 66
enable automatic for management module 66
restore for management module 66
save for management module 104
view for management module 24
view tree for system 24
configuration commands 33, 104
configuration method
set for channel 0 of management module 46, 50
configure LDAP command
example 54
configure network ports command
example 65
configure network protocols command
example 57
configure SLP command
example 68
console 118
create override SOL session 119
create SOL session 118
options
o 119
console command 118
console command errors 131
console commands
example 119
create alert recipient 35, 36
create override SOL session 119
create SOL session 118
create user 86, 87, 97
cycle power
blade server 107, 114
I/O module 114
switch module 114

D

data rate
set for channel 0 of management module 46, 50
default IP address 12
delete alert recipient 34
delete user 85, 96
DHCP settings for management module commands
example 42
dhcpinfo
options
eth0 42
dhcpinfo command errors 131
dhcpinfo commands 42
example 42
disable
TCP command mode 80, 81
disable automatic configuration
management module 66
disable DNS
management module 44
disable Ethernet channel 0
management module 51
disable external management
I/O module 53
disable external ports
I/O module 53
disable FTP
management module 63
disable HTTPS port
management module 63
disable NAT table
I/O module 56
disable NTP
management module 63
disable power domain acoustic mode 112
disable power domain quiet mode 109
disable SNMP agent
management module (SNMPv1) 70
management module (SNMPv3) 70
disable SNMP traps
management module 63, 70
disable SNMPv1 agent
management module 63
disable SNMPv3 agent
management module 63
disable SOL
global 76
disable SSH port
management module 64

disable SSH v1
  management module 79
disable TCP command mode
  management module 64
disable technician debug
  management module 67
disable Telnet port
  management module 64
disable TFTP
  management module 64
disable uplink failover
  management module 83
display
  TCP command-mode session status 80, 81
  TCP command-mode session timeout 80, 81
display (reset counter) event log
  management module 105
display active users 95
display alarms
  alarm ID 123
  all 122
  complete alarm key 123
  generator ID 122
  generator information 123
  power 122
display alert properties (all recipients) 34
display alert properties (single recipient) 34
display alerts 26
display all event log entries
  management module 105
display all users 84, 95
display cKVM status
  blade server 51
display command-line session configuration
  management module 82
display command-line session timeout
  management module 82
display component information 29
display DNS configuration
  management module 43
display Ethernet channel 0 configuration
  management module 45, 49
display Ethernet channel 0 DHCP configuration
  management module 42
display Ethernet channel 1 configuration
  management module 47
display event log
  management module 105
display failover configuration
  management module 83
display firmware attributes 31
display global cKVM status
  BladeCenter unit 52
display health status 25, 26
display health status (tree) 26
display KVM owner 119
display LDAP settings
  management module 54
display management module event log commands 105
  example 105
display management module status 43
display media tray owner 120
display network port settings
  management module 59
display network protocol settings
  I/O module 55
display network settings
  BladeCenter unit 52
  I/O module 52
display POST status
  I/O module 115
  switch module 115
display power domain information details 108, 111
display power domain information overview 108, 111
display power state
  blade server 114
  I/O module 114
  switch module 114
display serial port configuration
  management module 57
display service data command 43
display service information 43
display service setting
  management module 66
display single user 85, 95
display SLP settings
  management module 67
display SMTP server host name
  management module 68
display SMTP server IP address
  management module 68
display SNMP configuration
  management module 69
display SSH v1 status
  management module 79
display state
  location LED 28
display telnet configuration
  management module 82
display telnet timeout
  management module 82
display uplink configuration
  management module 83
displaylog 105
  options
    a 105
    f 105
displaylog command errors 131
displaylog commands 105
  example 105
displaysd 43
  options
    mmstat 43
displaysd command errors 132
displaysd commands 43
  example 43
dns 43
  options
    i1 44
    i2 44
    i3 44
    off 44

dns *(continued)*
options *(continued)*
on 43
DNS
disable for management module 44
enable for management module 43
dns command errors 132
dns commands 43
example 44
DNS configuration
display for management module 43
DNS first IP address
set for management module 44
DNS second IP address
set for management module 44
DNS third IP address
set for management module 44
duplex mode
set for channel 0 of management module 46, 50

E

electronic emission Class A notice 153
enable
TCP command mode 80, 81
enable automatic configuration
management module 66
enable DNS
management module 43
enable Ethernet channel 0
management module 51
enable external management
I/O module 53
enable external ports
I/O module 53
enable FTP
management module 62
enable HTTPS port
management module 63
enable NAT table
I/O module 56
enable NTP
management module 63
enable power domain acoustic mode 112
enable power domain quiet mode 109
enable SNMP agent
management module (SNMPv1) 69
management module (SNMPv3) 70
enable SNMP traps
management module 63, 70
enable SNMPv1 agent
management module 63
enable SNMPv3 agent
management module 63
enable SOL
global 76
enable SSH port
management module 64
enable SSH v1
management module 79
enable TCP command mode
management module 64
enable technician debug
management module 67
enable Telnet port
management module 64
enable TFTP
management module 64
enable uplink failover
management module 83
encryption algorithms 12
end session 119
ending an SOL session 16, 118
env 19
options
blade 19, 20
blower 21
mt 21
power 21
switch 21
system (management module) 19
env command errors 128
env commands
example 21
environment
blade mezzanine 20
blade server 19
BladeCenter unit 19
blower 21
BMC 20
high-speed expansion card 20
I/O module 21
I/O-expansion card 20
integrated system management processor 20
management module 19
media tray 21
microprocessor 20
power module 21
service processor 20
storage expansion unit 20
switch module 21
environment commands 18
example 21
errors
alarm command 129
alertentries command 130
boot command 130
clear command 130
clearlog command 131
common 128
console command 131
dhcpinfo command 131
displaylog command 131
displaysd command 132
dns command 132
env command 128
exit command 128
fuelg command 132
health command 133
help command 128
history command 128

errors *(continued)*
identify command 133
ifconfig command 133
info command 135
kvm command 136
ldapcfg command 136
list command 136
mt command 136
nat command 136
portcfg command 137
ports command 137
power command 137
read command 138
reset command 138
service command 138
slp command 138
smtp command 139
snmp command 139
sol command 139
sshcfg command 140
tcpcmdmode command 141
telnetcfg command 141
update command 141
uplink command 143
users command 143
write command 146
Ethernet
configuring remote connection 15
Ethernet channel 0
disable for management module 51
enable for management module 51
Ethernet channel 0 configuration
display for management module 45, 49
Ethernet channel 0 configuration method
set for management module 46, 50
Ethernet channel 0 data rate
set for management module 46, 50
Ethernet channel 0 DHCP configuration
display for management module 42
Ethernet channel 0 duplex mode
set for management module 46, 50
Ethernet channel 0 gateway IP address
set for management module 45, 49
Ethernet channel 0 hostname
set for management module 46, 50
Ethernet channel 0 MAC address
set for management module 46, 51
Ethernet channel 0 MTU
set for management module 46, 50
Ethernet channel 0 static IP address
set for management module 45, 49
Ethernet channel 0 subnet mask
set for management module 45, 50
Ethernet channel 1
disable for management module 48
enable for management module 47
Ethernet channel 1 configuration
display for management module 47
Ethernet channel 1 gateway IP address
set for management module 47
Ethernet channel 1 MAC address
set for management module 47
Ethernet channel 1 static IP address
set for management module 47
Ethernet channel 1 subnet mask
set for management module 47
Ethernet network settings for management module commands
example 48, 53
event log
clear for management module 104
display (reset counter) for management module 105
display all entries for management module 105
display for management module 105
event log, clear for management module commands 104
event log, display for management module commands 105
exit 119
exit command 119
exit command errors 128
exit commands
example 119
external management
disable for I/O module 53
enable for I/O module 53
external ports
disable for I/O module 53
enable for I/O module 53

F

failover configuration
display for management module 83
FCC Class A notice 153
filter alert type 37
firmware
display attributes 31
update 31
update (verbose) 31
firmware requirements 2
firmware update 30
flash location LED 28
FTP
disable for management module 63
enable for management module 62
FTP data port number
set for management module 60
FTP port number
set for management module 60
fuelg 108, 111
options
am 112
os 108
pm 108, 111
qm 109
fuelg command errors 132
fuelg commands 107, 111
example 109, 112

G

gateway IP address
  set for channel 0 of management module 45, 49
  set for channel 1 of management module 47
  set for I/O module 52
global disable
  SOL 76
global enable
  SOL 76
guidelines
  case sensitivity 3
  command history 4
  data types 4
  delimiters 4
  help 4
  options 3
  output format 4
  overview of 3
  strings 4

H

hardware requirements 2
health 25
  display status 25
  display status (tree) 26
  display status and alerts 26
  options
    f 26
    l 25, 26
health command 25, 26
  example 26
health command errors 133
help 18, 22
help command 22
help command errors 128
help commands
  example 22
help for update command 30
high-speed expansion card
  command target 20
history 23
history command 23
history command errors 128
history commands
  example 23
host name
  set for channel 0 of management module 46, 50
HTTP port number
  set for management module 60
HTTPS port
  disable for management module 63
  enable for management module 63
HTTPS port number
  set for management module 60

I

I/O module
  activate network protocol settings 55
I/O module *(continued)*
  command target 21
  cycle power 114
  disable external management 53
  disable external ports 53
  disable NAT table 56
  display network protocol settings 55
  display network settings 52
  display POST status 115
  display power state 114
  enable external management 53
  enable external ports 53
  enable NAT table 56
  nat command 55, 57
    example 57
  power off 114
  power on 114
  reset 116
  reset (extended diagnostics) 117
  reset (full diagnostics) 117
  reset (standard diagnostics) 116
  reset configuration 39, 41
  reset network protocol settings 55
  set gateway IP address 52
  set NAT external port number 56
  set NAT internal port number 56
  set NAT protocol ID 56
  set NAT protocol name 55
  set subnet mask 52
  turn off 114
  turn on 114
I/O-expansion card
  command target 20
IBM Director
  communication 79, 81
identify 28
  options
    s 28
    s, d 28
identify command 28
identify command errors 133
identify commands
  example 28
ifconfig 52
  options
    bsmp 51
    ckvm, disable 52
    ckvm, disabled 51
    ckvm, enable 52
    ckvm, enabled 51
    eth0 45, 49
    eth0, c 46, 50
    eth0, d 46, 50
    eth0, down 51
    eth0, g 45, 49
    eth0, i 45, 49
    eth0, l 46, 51
    eth0, m 46, 50
    eth0, n 46, 50
    eth0, r 46, 50
    eth0, s 45, 50

ifconfig *(continued)*
options *(continued)*
eth0, up 51
eth1 47
eth1, down 48
eth1, g 47
eth1, i 47
eth1, l 47
eth1, s 47
eth1, up 47
i 48, 51
intf, em, disabled 53
intf, em, enabled 53
intf, ep, disabled 53
intf, ep, enabled 53
intf, g 52
intf, s 52
v 52
ifconfig command errors 133
ifconfig commands 45, 49
example 48, 53
info 29
info command 29
info command errors 135
info commands
example 30
information about components 29
information display, component 29
information display, power domain (detailed) 108, 111
information display, power domain (overview) 108, 111
integrated system management processor
command target 20
IP address
set for management module 45, 49
set starting for blade servers 48, 51
IP address (BSMP)
set starting for BladeCenter unit 51
IP address, default 12
ISMP
reset 116

J

JS20 blade server commands
reset (clear NVRAM) 117
reset (run diagnostics with boot sequence) 118
reset (run diagnostics) 117
reset (with NMI) 117

K

kvm 119
options
b 120
KVM
display owner 119
set owner 120
kvm command errors 136
kvm commands 119
example 120
KVM port number
set for management module 61

L

LDAP name
set for management module 54
LDAP security version
set for management module 54
LDAP settings
display for management module 54
ldapcfg 54
options
t 54
v 54
ldapcfg command 54
example 54
ldapcfg command errors 136
LED (location), control 28
light location LED 28
light location LED (BladeCenter unit)
time period 28
list 24
options
l 24
list command
example 24
list command errors 136
location LED
blink 28
display state 28
flash 28
light 28
light (BladeCenter unit)
time period 28
turn off 28
location LED control 28

M

MAC address
set for channel 0 of management module 46, 51
set for channel 1 of management module 47
manage alert recipients 34
management module
clear event log 104
clear event log commands
example 104
command target 19
command-line session configuration 82
command-line session timeout 82
command-line timeout 82
create alert recipient 35, 36
create user 86, 87, 97
default IP address 12
delete alert recipient 34
delete user 85, 96
DHCP settings commands
example 42
dhcpinfo commands 42
disable automatic configuration 66

management module *(continued)*
disable DNS 44
disable Ethernet channel 0 51
disable Ethernet channel 1 48
disable FTP 63
disable HTTPS port 63
disable NTP 63
disable SNMP agent (SNMPv1) 70
disable SNMP agent (SNMPv3) 70
disable SNMP traps 63, 70
disable SNMPv1 agent 63
disable SNMPv3 agent 63
disable SSH port 64
disable SSH v1 79
disable TCP command mode 64
disable technician debug 67
disable Telnet port 64
disable TFTP 64
disable uplink failover 83
display (reset counter) event log 105
display active users 95
display alert properties (all recipients) 34
display alert properties (single recipient) 34
display all event log entries 105
display all users 84, 95
display DNS configuration 43
display Ethernet channel 0 configuration 45, 49
display Ethernet channel 0 DHCP configuration 42
display Ethernet channel 1 configuration 47
display event log 105
display event log commands
example 105
display LDAP settings 54
display network port settings 59
display serial port configuration 57
display service setting 66
display single user 85, 95
display SLP settings 67
display SMTP server host name 68
display SMTP server IP address 68
display SNMP configuration 69
display SSH v1 status 79
display status 43
dns commands 43, 44
example 44
enable automatic configuration 66
enable DNS 43
enable Ethernet channel 0 51
enable Ethernet channel 1 47
enable FTP 62
enable HTTPS port 63
enable NTP 63
enable SNMP agent (SNMPv1) 69
enable SNMP agent (SNMPv3) 70
enable SNMP traps 63, 70
enable SNMPv1 agent 63
enable SNMPv3 agent 63
enable SSH port 64
enable SSH v1 79
enable TCP command mode 64
enable technician debug 67
management module *(continued)*
enable Telnet port 64
enable TFTP 64
enable uplink failover 83
Ethernet network settings commands
example 48, 53
failover configuration 83
filter alert type 37
IBM Director communication 79, 81
ifconfig commands 45, 48, 49, 53
kvm commands 119, 120
ldapcfg command 54
example 54
mt commands 120, 121
portcfg commands 57, 58
ports command 59, 65
example 65
read command 66
example 66
reset 116
reset (failover) 116
reset configuration 39
reset configuration (delete logs) 41
reset configuration (keep logs) 40
reset network port settings 59
restore configuration 66
save configuration 104
serial port settings commands
example 58
service command
example 67
service commands 66, 67
set alert notification method 37
set alert recipient email address 37
set alert recipient name 36
set alert recipient status 36
set alert type 37
set DNS first IP address 44
set DNS second IP address 44
set DNS third IP address 44
set Ethernet channel 0 configuration method 46, 50
set Ethernet channel 0 data rate 46, 50
set Ethernet channel 0 duplex mode 46, 50
set Ethernet channel 0 gateway IP address 45, 49
set Ethernet channel 0 hostname 46, 50
set Ethernet channel 0 MAC address 46, 51
set Ethernet channel 0 MTU 46, 50
set Ethernet channel 0 static IP address 45, 49
set Ethernet channel 0 subnet mask 45, 50
set Ethernet channel 1 gateway IP address 47
set Ethernet channel 1 MAC address 47
set Ethernet channel 1 static IP address 47
set Ethernet channel 1 subnet mask 47
set FTP data port number 60
set FTP port number 60
set hostname for alerts 38
set HTTP port number 60
set HTTPS port number 60
set IP address 45, 49
set IP address for alerts 38
set KVM port number 61

management module *(continued)*
set LDAP name 54
set LDAP security version 54
set privacy password (SNMPv3) 93, 102
set remote disk on chip port number 61
set remote disk port number 61
set serial port baud rate 57
set serial port communication rate 57
set serial port parity 58
set serial port stop bits 58
set server host name 68
set server IP address 68
set SLP address type 67
set SLP multicast address 68
set SNMP agent port number 61
set SNMP community 1 first host name 70
set SNMP community 1 IP address (first host) 70
set SNMP community 1 IP address (second host) 71
set SNMP community 1 IP address (third host) 71
set SNMP community 1 name 70
set SNMP community 1 second host name 71
set SNMP community 1 third host name 71
set SNMP community 1 view type (SNMPv3) 71
set SNMP community 2 first host name 71
set SNMP community 2 IP address (first host) 71
set SNMP community 2 IP address (second host) 72
set SNMP community 2 IP address (third host) 72
set SNMP community 2 name 71
set SNMP community 2 second host name 72
set SNMP community 2 third host name 72
set SNMP community 2 view type (SNMPv3) 72
set SNMP community 3 first host name 72
set SNMP community 3 IP address (first host) 72
set SNMP community 3 IP address (second host) 73
set SNMP community 3 IP address (third host) 73
set SNMP community 3 name 72
set SNMP community 3 second host name 73
set SNMP community 3 third host name 73
set SNMP community 3 view type (SNMPv3) 73
set SNMP contact name 73
set SNMP location 73
set SNMP traps port number 62
set SSH port number 62
set TCP command-mode timeout 64
set Telnet port number 62
set Telnet port timeout 65
set TFTP port number 62
set user access type (SNMPv3) 93, 102
set user authentication protocol (SNMPv3) 92, 101
set user authority level 89, 90, 91, 99, 100
set user context name (SNMPv3) 92, 101
set user hostname (SNMPv3 traps) 93, 102
set user IP address (SNMPv3 traps) 93, 102
set user name 88, 98
set user password 88, 98
set user privacy protocol (SNMPv3) 92, 101
slp command 67, 68
example 68
management module *(continued)*
smtp commands 68, 69
SMTP settings commands
example 69
snmp commands 69, 73
SNMP settings commands
example 73
sshcfg command 79
example 79
telnet configuration 82
telnet timeout 82
uplink configuration 83
uplink failover delay 83
view configuration 24
write command 104
example 104
management module event log commands 104, 106
management module failover commands 83
management module telnet configuration commands
example 82
management module uplink failover commands
example 83
management module, user accounts 84, 95
management-module firmware 2
media tray
command target 21
display owner 120
set owner 121
microprocessor
command target 20
mt 120
options
b 121
mt command errors 136
mt commands 120
example 121
MTU
set for channel 0 of management module 46, 50

N

nat 55
options
activate 55
en 56
ep 56
ip 56
pi 56
pn 55
reset 55
nat command 55
example 57
nat command errors 136
NAT external port number
set for I/O module 56
NAT internal port number
set for I/O module 56
NAT protocol ID
set for I/O module 56
NAT protocol name
set for I/O module 55

NAT table
  disable for I/O module 56
  enable for I/O module 56
network port settings
  display for management module 59
  reset for management module 59
network protocol settings
  activate for I/O module 55
  display for I/O module 55
  reset for I/O module 55
network settings
  display for BladeCenter unit 52
  display for I/O module 52
notes, important 150
notices
  electronic emission 153
  FCC, Class A 153
notification method, set for alerts 37
NTP
  disable for management module 63
  enable for management module 63

O

online documentation 1
out-of-band communication, IBM Director 79, 81
override persistent command environment 5

P

parity
  set for serial port of management module 58
persistent command environment
  override 5
persistent command target 4
portcfg
  options
    com1 57
    com1, b 57
    com1, p 58
    com1, s 58
portcfg command errors 137
portcfg commands 57
  example 58
ports 59
  options
    ftpdp 60
    ftpe, off 63
    ftpe, on 62
    ftpp 60
    httpp 60
    httpse, off 63
    httpse, on 63
    httpsp 60
    kvmp 61
    ntpe, off 63
    ntpe, on 63
    rdocp 61
    rdp 61
    reset 59
    snmp1ae, off 63
ports *(continued)*
  options *(continued)*
    snmp1ae, on 63
    snmp3ae, off 63
    snmp3ae, on 63
    snmpap 61
    snmpte, off 63
    snmpte, on 63
    snmptp 62
    sshe, off 64
    sshe, on 64
    sshp 62
    tcme, off 64
    tcme, on 64
    tcmt 64
    telnete, off 64
    telnete, on 64
    telnetp 62
    telnett 65
    tftpe, off 64
    tftpe, on 64
    tftpp 62
ports command 59
  example 65
ports command errors 137
POST status
  display for I/O module 115
  display for switch module 115
power
  options
    cycle 114
    cycle, c 114
    off 114
    on 114
    on, c 114
    state 114
    state, post 115
power command errors 137
power commands 114
  example 115
power control commands 106, 118
power domain
  disable acoustic mode 112
  disable quiet mode 109
  enable acoustic mode 112
  enable quiet mode 109
power domain information display (detailed) 108, 111
power domain information display (overview) 108, 111
power domain redundancy loss policy, set 108, 111
power module
  command target 21
power off
  blade server 114
  I/O module 114
  switch module 114
power on
  blade server 114
  I/O module 114
  switch module 114
power on (to console)
  blade server 114

power state
display for blade server 114
display for I/O module 114
display for switch module 114
primary management module 5

Q

quiet mode, disable 109
quiet mode, enable 109

R

read
options
auto, off 66
auto, on 66
config 66
read command 66
example 66
read command errors 138
redirect command 18
redundancy loss policy, power domain (set) 108, 111
redundant management modules 5
remote disk on chip port number
set for management module 61
remote disk port number
set for management module 61
required, firmware 2
required, hardware 2
reset 116
blade server 107, 116
I/O module 116
ISMP 116
management module 116
options
c 116
clr 117
ddg 118
dg 117
exd 117
f 116
full 117
sft 117
std 116
service processor 116
switch module 116
reset (clear NVRAM)
blade server 117
reset (extended diagnostics)
I/O module 117
switch module 117
reset (failover)
management module 116
reset (full diagnostics)
I/O module 117
switch module 117
reset (run diagnostics with boot sequence)
blade server 118
reset (run diagnostics)
blade server 117
reset (standard diagnostics)
I/O module 116
switch module 116
reset (to console)
blade server 107, 116
reset (with NMI)
blade server 117
reset blase server key sequence
set for SOL 78
reset command 106, 118
reset command errors 138
reset commands 116
example 118
reset configuration
I/O module 39, 41
management module 39
switch module 39, 41
reset configuration (delete logs)
management module 41
reset configuration (keep logs)
management module 40
reset default configuration 39, 40
reset network port settings
management module 59
reset network protocol settings
I/O module 55
responding to thermal events 109, 112
restore configuration
management module 66
restore management module configuration command
example 66
retry count
set for SOL 76
retry interval
set for SOL 75

S

save configuration
management module 104
save management module configuration command
example 104
secure command-line interface 12
Secure Shell connection clients 12
security 12
selecting command environment 4
selecting command target 4
send threshold
set for SOL 76
Serial Over LAN 16
Serial Over LAN commands 75
example 78
serial port baud rate
set for management module 57
serial port communication rate
set for management module 57
serial port configuration
display for management module 57
serial port parity
set for management module 58

serial port settings for management module commands
example 58
serial port stop bits
set for management module 58
server host name
set for management module 68
server IP address
set for management module 68
service 66
options
disable 67
enable 67
service command
example 67
service command errors 138
service commands 66
service data
display command 43
service information
capture 43
display 43
service processor
command target 20
reset 116
service setting
display for management module 66
session command 118, 121
set
TCP command-mode session timeout 80, 81
set accumulate timeout
SOL 76
set alarm 125
set alert notification method 37
set alert recipient email address 37
set alert recipient name 36
set alert recipient status 36
set alert type 37
set CLI key sequence
SOL 77
set command-line timeout
management module 82
set DNS first IP address
management module 44
set DNS second IP address
management module 44
set DNS third IP address
management module 44
set Ethernet channel 0 configuration method
management module 46, 50
set Ethernet channel 0 data rate
management module 46, 50
set Ethernet channel 0 duplex mode
management module 46, 50
set Ethernet channel 0 gateway IP address
management module 45, 49
set Ethernet channel 0 hostname
management module 46, 50
set Ethernet channel 0 MAC address
management module 46, 51
set Ethernet channel 0 MTU
management module 46, 50
set Ethernet channel 0 static IP address
management module 45, 49
set Ethernet channel 0 subnet mask
management module 45, 50
set Ethernet channel 1 gateway IP address
management module 47
set Ethernet channel 1 MAC address
management module 47
set Ethernet channel 1 static IP address
management module 47
set Ethernet channel 1 subnet mask
management module 47
set FTP data port number
management module 60
set FTP port number
management module 60
set gateway IP address
I/O module 52
set hostname for alerts 38
set HTTP port number
management module 60
set HTTPS port number
management module 60
set IP address
management module 45, 49
set IP address for alerts 38
set KVM owner 120
set KVM port number
management module 61
set LDAP name
management module 54
set LDAP security version
management module 54
set media tray owner 121
set NAT external port number
I/O module 56
set NAT internal port number
I/O module 56
set NAT protocol ID
I/O module 56
set NAT protocol name
I/O module 55
set number of sessions
TCP command mode 81
set power domain redundancy loss policy 108, 111
set privacy password (SNMPv3) 93, 102
set remote disk on chip port number
management module 61
set remote disk port number
management module 61
set reset blase server key sequence
SOL 78
set retry count
SOL 76
set retry interval
SOL 75
set send threshold
SOL 76
set serial port baud rate
management module 57

set serial port communication rate
management module 57
set serial port parity
management module 58
set serial port stop bits
management module 58
set server host name
management module 68
set server IP address
management module 68
set SLP address type
management module 67
set SLP multicast address
management module 68
set SNMP agent port number
management module 61
set SNMP community 1 first host name
management module 70
set SNMP community 1 IP address (first host)
management module 70
set SNMP community 1 IP address (second host)
management module 71
set SNMP community 1 IP address (third host)
management module 71
set SNMP community 1 name
management module 70
set SNMP community 1 second host name
management module 71
set SNMP community 1 third host name
management module 71
set SNMP community 1 view type (SNMPv3)
management module 71
set SNMP community 2 first host name
management module 71
set SNMP community 2 IP address (first host)
management module 71
set SNMP community 2 IP address (second host)
management module 72
set SNMP community 2 IP address (third host)
management module 72
set SNMP community 2 name
management module 71
set SNMP community 2 second host name
management module 72
set SNMP community 2 third host name
management module 72
set SNMP community 2 view type (SNMPv3)
management module 72
set SNMP community 3 first host name
management module 72
set SNMP community 3 IP address (first host)
management module 72
set SNMP community 3 IP address (second host)
management module 73
set SNMP community 3 IP address (third host)
management module 73
set SNMP community 3 name
management module 72
set SNMP community 3 second host name
management module 73
set SNMP community 3 third host name
management module 73
set SNMP community 3 view type (SNMPv3)
management module 73
set SNMP contact name
management module 73
set SNMP location
management module 73
set SNMP traps port number
management module 62
set SSH port number
management module 62
set starting BSMP IP address
BladeCenter unit 51
set starting IP address
blade servers 48, 51
set subnet mask
I/O module 52
set TCP command-mode timeout
management module 64
set Telnet port number
management module 62
set Telnet port timeout
management module 65
set telnet timeout
management module 82
set TFTP port number
management module 62
set uplink failover delay
management module 83
set user access type (SNMPv3) 93, 102
set user authentication protocol (SNMPv3) 92, 101
set user authority level 89, 90, 91, 99, 100
set user context name (SNMPv3) 92, 101
set user hostname (SNMPv3 traps) 93, 102
set user IP address (SNMPv3 traps) 93, 102
set user name 88, 98
set user password 88, 98
set user privacy protocol (SNMPv3) 92, 101
set VLAN ID
BladeCenter unit 52
SOL 77
slp 67
options
i 68
t 67
SLP address type
set for management module 67
slp command 67
example 68
slp command errors 138
SLP multicast address
set for management module 68
SLP settings
display for management module 67
smtp 68
options
s 68
smtp command errors 139
smtp commands 68
example 69

SMTP server host name
display for management module 68
SMTP server IP address
display for management module 68
SMTP settings for management module commands
example 69
snmp 69
options
a, off 70
a, on 69
a3, off 70
a3, on 70
c1 70
c1i1 70
c1i2 71
c1i3 71
c2 71
c2i1 71
c2i2 72
c2i3 72
c3 72
c3i1 72
c3i2 73
c3i3 73
ca1 71
ca2 72
ca3 73
cn 73
l 73
t, off 70
t, on 70
SNMP agent
disable for management module (SNMPv1)
SNMPv1 70
disable for management module (SNMPv3)
SNMPv3 70
enable for management module (SNMPv1)
SNMPv1 69
enable for management module (SNMPv3)
SNMPv3 70
SNMP agent port number
set for management module 61
snmp command errors 139
snmp commands 69
example 73
SNMP community 1 first host name
set for management module 70
SNMP community 1 IP address (first host)
set for management module 70
SNMP community 1 IP address (second host)
set for management module 71
SNMP community 1 IP address (third host)
set for management module 71
SNMP community 1 name
set for management module 70
SNMP community 1 second host name
set for management module 71
SNMP community 1 third host name
set for management module 71
SNMP community 1 view type
set for management module (SNMPv3) 71
SNMP community 2 first host name
set for management module 71
SNMP community 2 IP address (first host)
set for management module 71
SNMP community 2 IP address (second host)
set for management module 72
SNMP community 2 IP address (third host)
set for management module 72
SNMP community 2 name
set for management module 71
SNMP community 2 second host name
set for management module 72
SNMP community 2 third host name
set for management module 72
SNMP community 2 view type
set for management module (SNMPv3) 72
SNMP community 3 first host name
set for management module 72
SNMP community 3 IP address (first host)
set for management module 72
SNMP community 3 IP address (second host)
set for management module 73
SNMP community 3 IP address (third host)
set for management module 73
SNMP community 3 name
set for management module 72
SNMP community 3 second host name
set for management module 73
SNMP community 3 third host name
set for management module 73
SNMP community 3 view type
set for management module (SNMPv3) 73
SNMP configuration
display for management module 69
SNMP contact name
set for management module 73
SNMP location
set for management module 73
SNMP settings for management module commands
example 73
SNMP traps
disable for management module 63, 70
enable for management module 63, 70
SNMP traps port number
set for management module 62
SNMPv1 agent
disable for management module 63
enable for management module 63
SNMPv3
community 1 view type 71
community 2 view type 72
community 3 view type 73
privacy password 93, 102
trap receiver IP address or hostname 93, 102
user access type 93, 102
user authentication protocol 92, 101
user context name 92, 101
user privacy protocol 92, 101
SNMPv3 agent
disable for management module 63
enable for management module 63

sol 75
options
c 76
e 77
i 75
r 78
s 76
status 76
t 76
v 77
SOL 16, 118
global disable 76
global enable 76
set accumulate timeout 76
set CLI key sequence 77
set reset blase server key sequence 78
set retry count 76
set retry interval 75
set send threshold 76
set VLAN ID 77
status 75
sol command errors 139
sol commands
example 78
SOL commands 75
SOL session
ending 16, 118
starting 16
SSH clients 12
SSH connection 13
SSH port
disable for management module 64
enable for management module 64
SSH port number
set for management module 62
SSH v1
disable for management module 79
enable for management module 79
SSH v1 enable command
example 79
SSH v1 status
display for management module 79
sshcfg 79
options
v1, off 79
v1, on 79
sshcfg command 79
example 79
sshcfg command errors 140
starting a session using SSH 13
starting a session using Telnet 13
starting an SOL session 16
starting command-line interface 12
static IP address
set for channel 0 of management module 45, 49
set for channel 1 of management module 47
status
display for management module 43
SOL 75
stop bits
set for serial port of management module 58
storage expansion unit
command target 20
subnet mask
set for channel 0 of management module 45, 50
set for channel 1 of management module 47
set for I/O module 52
switch module
command target 21
cycle power 114
display POST status 115
display power state 114
power off 114
power on 114
reset 116
reset (extended diagnostics) 117
reset (full diagnostics) 117
reset (standard diagnostics) 116
reset configuration 39, 41
turn off 114
turn on 114
syntax help 22
syntax help commands
example 22
system
view configuration tree 24
system management command 122, 127
system physical configuration command 24

T

target 18
TCP command mode
disable 80, 81
disable for management module 64
enable 80, 81
enable for management module 64
set number of sessions 81
TCP command-mode session status
display 80, 81
TCP command-mode session timeout
display 80, 81
set 80, 81
TCP command-mode timeout
set for management module 64
tcpcmdmode 80, 81
options
status, 0 81
status, 1 to 5 81
status, off 80
status, on 80
t 80, 81
tcpcmdmode command errors 141
tcpcmdmode commands 79, 81
example 80, 81
technician debug
disable for management module 67
enable for management module 67
telnet configuration
display for management module 82
telnet configuration commands 82
Telnet connection 12, 13

Telnet port
disable for management module 64
enable for management module 64
Telnet port number
set for management module 62
Telnet port timeout
set for management module 65
telnet timeout
display for management module 82
set for management module 82
telnetcfg 82
options
t 82
telnetcfg command errors 141
telnetcfg commands 82
example 82
temporary command target 5
terminate session 119
TFTP
disable for management module 64
enable for management module 64
TFTP port number
set for management module 62
thermal event response 109, 112
trademarks 149
turn off
blade server 114
I/O module 114
switch module 114
turn off location LED 28
turn on
blade server 114
I/O module 114
switch module 114
turn on (to console)
blade server 114

U

United States electronic emission Class A notice 153
United States FCC Class A notice 153
update 30
options
a 31
i, n 31
update command 30
update command errors 141
update command help 30
update commands
example 31
update firmware 30, 31
update firmware (verbose) 31
uplink 83
options
del 83
off 83
on 83
uplink command errors 143
uplink commands 83
example 83
uplink configuration
display for management module 83
uplink failover
disable for management module 83
enable for management module 83
uplink failover delay
set for management module 83
users 84, 95
options
1 through 12 85, 95
a 89, 91, 99
ap 92, 101
at 93, 102
clear 85, 96
cn 92, 101
create (n, p, a, cn, ap, pp, ppw, at, i) 86, 97
curr 95
i 93, 102
n 88, 98
p 88, 98
pp 92, 101
ppw 93, 102
users command 84, 95
users command errors 143
users commands
example 94, 103
users, create 86, 87, 97
users, delete 85, 96
users, display (active) 95
users, display (all) 84, 95
users, display (single) 85, 95
users, management module 84, 95
users, set access type (SNMPv3) 93, 102
users, set authentication protocol (SNMPv3) 92, 101
users, set authority level 89, 90, 91, 99, 100
users, set context name (SNMPv3) 92, 101
users, set hostname (SNMPv3 traps) 93, 102
users, set IP address (SNMPv3 traps) 93, 102
users, set name 88, 98
users, set password 88, 98
users, set privacy password (SNMPv3) 93, 102
users, set privacy protocol (SNMPv3) 92, 101
using the command-line interface 3

V

view command target 24
VLAN ID
set for BladeCenter unit 52
set for SOL 77

W

write
options
config 104
write command 104
example 104
write command errors 146

Part Number: 31R1756

Printed in USA

(1P) P/N: 31R1756