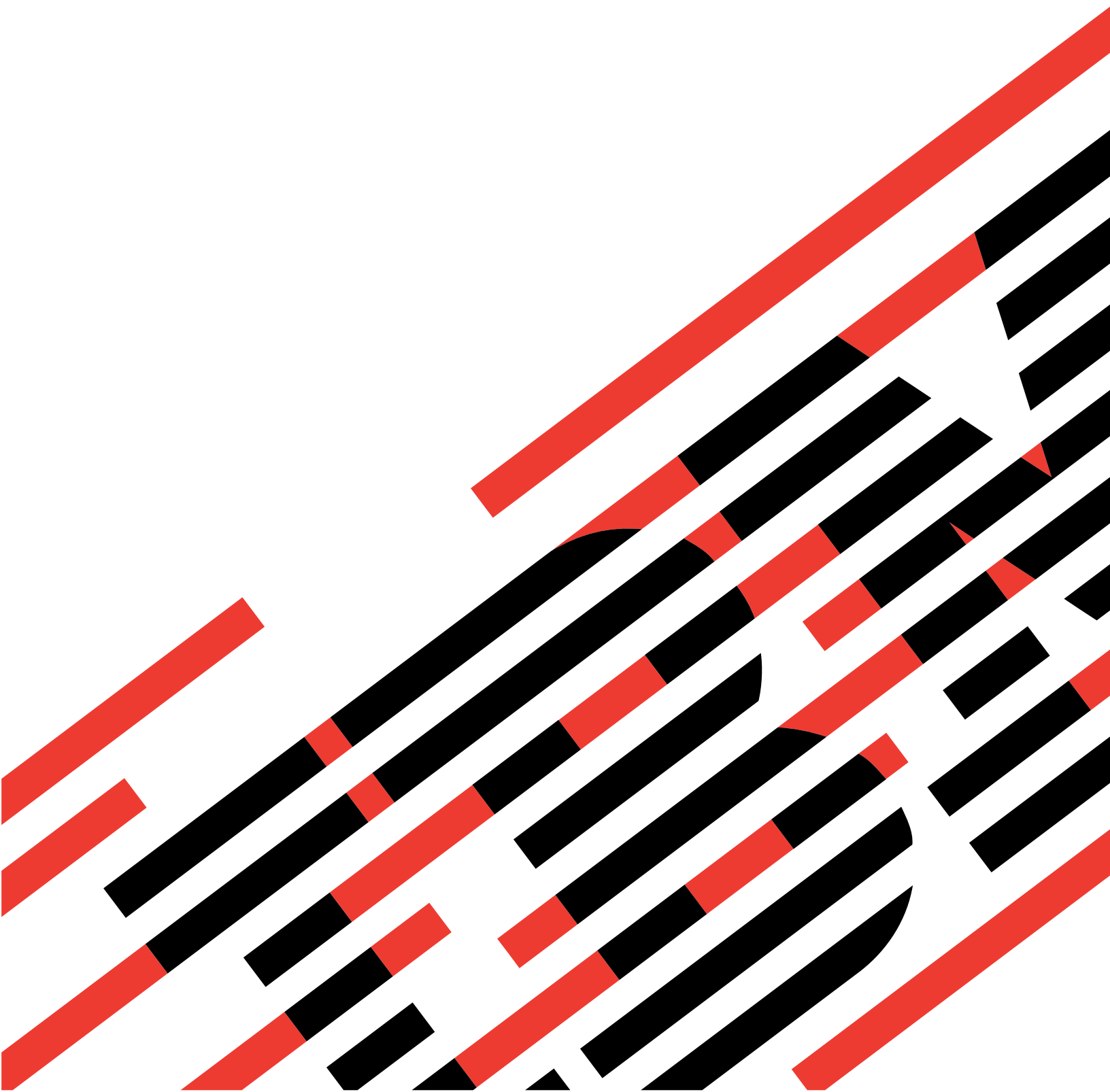




BladeCenter

Management Module Command-Line Interface
Reference Guide





@server

BladeCenter

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 107 and Appendix B, “Notices,” on page 109.

Fourth Edition (July 2005)

© Copyright International Business Machines Corporation 2005. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

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
Starting the command-line interface	12
Telnet connection	12
Secure Shell (SSH) connection	13
Starting an SOL session	13
Ending an SOL session	14
Chapter 3. Command reference	15
Built-in commands	16
env (environment) command	16
help command	18
history command	19
list (system physical configuration) command	20
Common commands	21
health commands	21
identify (location LED) command	24
info (configuration information) command	26
update (update firmware) command	27
Configuration commands	30
alertentries command	30
clear command	36
dhcpinfo command	37
dns command	38
ifconfig command	40
smtp command	43
snmp command	45
sol (serial over LAN) commands	50
tppcmdmode command	53
telnetcfg (Telnet configuration) command	54
uplink (management module failover) command	55
users (management-module users) command	57
Event-log commands	67
clearlog command	67
displaylog command	68
Power-control commands	69
boot command	69
fuelg command	70
power command	73
reset command	75
Session commands	78
console command	78
exit command	78
System management commands (for BladeCenter T only)	79
alarm command	79
thres (alarm threshold) command	85
Chapter 4. Error messages	89

Common errors	90
alarm command errors	91
alertentries command errors	92
boot command errors	92
clear command errors	92
clearlog command errors	93
console command errors	93
dhcpinfo command errors	93
displaylog command errors	93
dns command errors	94
fuelg command errors	94
health command errors	94
identify command errors	95
ifconfig command errors	95
info command errors	97
list command errors	98
power command errors	98
reset command errors	98
smtp command errors	99
snmp command errors	99
sol command errors	99
tcpcmdmode command errors	101
telnetcfg command errors	101
thres command errors	101
update command errors	102
uplink command errors	104
users command errors	104
Appendix A. Getting help and technical assistance	107
Before you call	107
Using the documentation	107
Getting help and information from the World Wide Web	108
Software service and support	108
Hardware service and support	108
Appendix B. Notices	109
Edition notice	109
Trademarks	110
Important notes	110
Product recycling and disposal	111
Battery return program	112
Electronic emission notices	113
Federal Communications Commission (FCC) statement	113
Industry Canada Class A emission compliance statement	113
Australia and New Zealand Class A statement	113
United Kingdom telecommunications safety requirement	113
European Union EMC Directive conformance statement	113
Taiwanese Class A warning statement	114
Chinese Class A warning statement	114
Japanese Voluntary Control Council for Interference (VCCI) statement	114
Index	115

Chapter 1. Introduction

The IBM® @server® BladeCenter™ Management Module Command-Line Interfaces provide 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 in a BladeCenter unit. All IBM @server BladeCenter units, including the BladeCenter T unit, are also referred to throughout this book as the BladeCenter unit. Unless otherwise noted, all commands can be run on all 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 @server BladeCenter Serial Over LAN Setup Guide* for information about SOL and setup instructions.

You access the Management Module Command-Line Interface 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 the IBM Web site at <http://www.ibm.com/pc/support/>.

Before you begin

The BladeCenter unit must be correctly configured before you can use the management-module command-line interface. 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 @server 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 the IBM Support Web site, <http://www.ibm.com/pc/support/> 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 Command-Line Interface 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 @server BladeCenter Serial Over LAN Setup Guide* for information.

Chapter 2. Using the command-line interface

The IBM Management Module Command-Line Interface 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”
- “Starting the command-line interface” on page 12
- “Starting an SOL session” on page 13
- “Ending an SOL session” on page 14

See Chapter 3, “Command reference,” on page 15 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 89. See the *IBM @server 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 `?`.

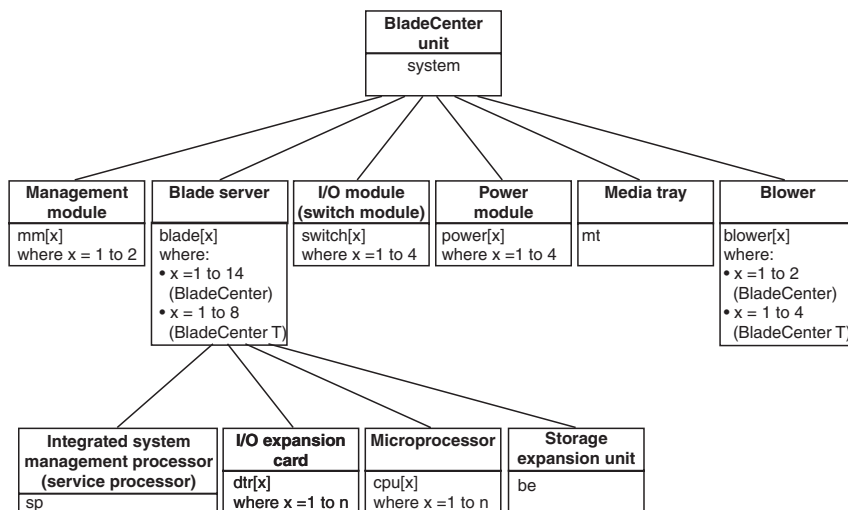
- Data types

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 16). 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 20).

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.

The following tables show command-line interface commands and their required authority levels. Command authorities for the latest version of management-module firmware are shown in Table 1 on page 6. Table 2 on page 9 shows the command authorities for previous versions of management-module firmware. To use the tables, 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, in Table 2 the `clearlog` command is available to users with the “Supervisor” command authority or to users with the “Ability to Clear Event Logs” 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, in Table 2 one available authority combination for the power -on -c command is the “Blade Server Remote Control Access” command authority and the “Blade and I/O Module Power/Restart Access” 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.

Table 1. Command authority relationships (latest management-module firmware version)

Command	Authority										
	Supervisor	Chassis User Account Management	Blade Server Remote Presence	Chassis Administration	Blade Administration	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration	
alarm -c, -r, -s	•										
								•			
									•		
alarm -q -g	•										
			•		•						
alertentries	•										
								•			
boot	•										
					•						
boot -c	•										
			◇		◇						
boot -p	•										
					•						
clear -config	•										
								•			
										•	
clearlog	•										
							•				
console	•										
			•								

Table 1. Command authority relationships (latest management-module firmware version) (continued)

Command	Authority										
	Supervisor	Chassis User Account Management	Blade Server Remote Presence	Chassis Administration	Blade Administration	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration	
console -o	•		•								
dns	•							•			
fuelg	•							•			
identify	•							•			
ifconfig	•							•			
									•		
										•	
power -on, -off, -cycle	•										
					•						
power -on -c, -cycle -c	•										
			◇		◇						
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)	•										
										•	

Table 1. Command authority relationships (latest management-module firmware version) (continued)

Command	Authority										
	Supervisor	Chassis User Account Management	Blade Server Remote Presence	Chassis Administration	Blade Administration	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration	
reset -f (management module)	•			•							
smtp	•							•			
snmp	•							•			
sol	•							•			
									•		
tcpcmdmode	•							•			
telnetcfg	•							•			
thres	•							•			
update	•			•							
					•						
						•					
uplink -del, -off, -on	•							•			
users	•										
		•									

Table 2. Command authority relationships (previous management-module firmware versions)

Command	Authority									
	Supervisor	User Account Management	Blade Server Remote Console Access	Blade Server Remote Console and Virtual Media Access	Blade and I/O Module Power/Restart Access	Ability to Clear Event Logs	Basic Configuration (MM, I/O Modules, Blades)	Network and Security Configuration	Advanced Configuration (MM, I/O Modules, Blades)	
alarm -c, -r, -s, -q -g	.						.		.	
alertentries	.	.								
boot	.				.					
boot -c	.		◇	◇	◇					
boot -p	.				.					
clear -config	.								.	
clearlog	.					.				
console	.		.	.						
console -o	.		.	.						
dns	.						.		.	
fuelg	.						.		.	
identify	.						.		.	

Table 2. Command authority relationships (previous management-module firmware versions) (continued)

Command	Authority									
	Supervisor	User Account Management	Blade Server Remote Console Access	Blade Server Remote Console and Virtual Media Access	Blade and I/O Module Power/Restart Access	Ability to Clear Event Logs	Basic Configuration (MM, I/O Modules, Blades)	Network and Security Configuration	Advanced Configuration (MM, I/O Modules, Blades)	
ifconfig	•							•	•	
power -on, -off, -cycle	•				•					
power -on -c, -cycle -c	•		◇	◇	◇					
reset (blade server, ISMP, or 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)	•							•		
smtp	•						•	•		
snmp	•						•	•		
sol	•						•	•		

Table 2. Command authority relationships (previous management-module firmware versions) (continued)

Command	Authority									
	Supervisor	User Account Management	Blade Server Remote Console Access	Blade Server Remote Console and Virtual Media Access	Blade and I/O Module Power/Restart Access	Ability to Clear Event Logs	Basic Configuration (MM, I/O Modules, Blades)	Network and Security Configuration	Advanced Configuration (MM, I/O Modules, Blades)	
tcpcmdmode	•							•		
									•	
telnetcfg	•							•		
									•	
thres	•						•			
									•	
update	•								•	
									•	
uplink -del, -off, -on	•							•		
									•	
users	•									
		•								

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. You can establish up to 20 separate Telnet 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, 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/~sgatham/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

Telnet connection

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

1. Open a command-line window 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.

A command-prompt window opens.

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.

A 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 *IBM @server BladeCenter Management Module User's Guide* for instructions.
3. Start a SSH session to the management module using the SSH client of your choice. For example, if you are using the cygwin client, open a command-line window 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.

A command prompt window opens.

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.

A command prompt is displayed. You can now enter commands for the management 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) commands” on page 50 and the *IBM @server BladeCenter Serial over LAN Setup Guide* for information about setting up and enabling SOL.

After you start a Telnet or SSL session to the BladeCenter management module, you can start an SOL session to any individual blade server that supports SOL using the **console** command. Since you can start up to 20 separate Telnet or SSL 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.

Use 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]
```

A blade server 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) commands” on page 50 and the *IBM @server 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 and usage information and examples. It is divided into the following subsections:

- “Built-in commands” on page 16
 - env (environment) command
 - help command
 - history command
 - list (system physical configuration) command
- “Common commands” on page 21
 - health commands
 - identify (location LED) command
 - info (configuration information) command
 - update (update firmware) command
- “Configuration commands” on page 30
 - alertentries command
 - clear command
 - dhcpinfo command
 - dns command
 - ifconfig command
 - smtp command
 - snmp command
 - sol (serial over LAN) commands
 - tpcmdmode command
 - telnetcfg (Telnet configuration) command
 - uplink (management module failover) command
 - users (management-module users) command
- “Event-log commands” on page 67
 - clearlog command
 - displaylog command
- “Power-control commands” on page 69
 - boot command
 - fuelg command
 - power command
 - reset command
- “Session commands” on page 78
 - console command
 - exit command
- “System management commands (for BladeCenter T only)” on page 79
 - alarm command
 - thres (alarm threshold) 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 “.”.

Table 3. 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 <code>system></code> prompt.	<code>env</code> <code>env -T system</code>	The any installed device.
Set management module as command target	Sets the management module as the persistent target for commands during the current session.	<code>env -T system:mm[x]</code> where <i>x</i> is the bay (1 or 2) that identifies the management module.	The env command can be directed to any installed device, in this case <code>-T system:mm[x]</code> where <i>x</i> 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.	<code>env -T system:blade[x]</code> where <i>x</i> 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 <code>-T system:blade[x]</code> where <i>x</i> is the blade bay that identifies the blade server.

Table 3. env (environment) command (continued)

Function	What it does	Command	Valid targets
Set blade server integrated system management processor as command target	Sets the integrated system management processor on the specified blade server as the persistent target for commands during the current session.	env -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. 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]:sp where x is the blade bay that identifies the blade server on which the integrated system management processor is installed.
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 (1 - 4) 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 (1 - 4) where the I/O (switch) module is installed.

Example:

To set the persistent target of commands to the ISMP 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 ISMP 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 1 while the management module is set as the default command target, at the system:mm[x]> prompt, type

```
reset -T system:blade[1]
```

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 4. 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
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
list- Display installed targets
power- Control target power
reset- Reset target
shutdown- Shutdown target
smtp- View/edit SMTP config
snmp- View/edit SNMP config
sol- View SOL status and view/edit SOL 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)
thres- Manage Telco System threshold(s)
threshold- Manage Telco system threshold(s)
```

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. Users 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. Users can also recall one of the past eight previously entered commands using the up-arrow and down-arrow keys.

Table 5. 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 6. 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 <i>depth</i> where <i>depth</i> is "all" or "a" for full tree display, starting at the command target level. Specifying a <i>depth</i> of "1" displays the current command target. Specifying a <i>depth</i> of "2" displays the content of the current command target.	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:

```
system> list -l a
system
  mm[1]    primary
  power[4]
  blower[1]
  blower[2]
  blade[1]
    sp
    dtr[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 commands
- identify (location LED) command
- info (configuration information) command
- update (update firmware) command

health commands

These commands display the current health status of the command target. They 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 7. health commands

Function	What it does	Command	Valid targets
Display health status	<p>Displays the current health status of the command target. Return values are different for the BladeCenter and BladeCenter T configurations.</p> <ul style="list-style-type: none"> • Possible return values for the BladeCenter configuration are: <ul style="list-style-type: none"> – ok – warning – critical • Possible return values for the BladeCenter T configurations are: <ul style="list-style-type: none"> – ok – minor – major – critical 	health	<ul style="list-style-type: none"> -T system -T system:mm[x] -T system:blade[x] -T system:switch[x] -T system:power[x] -T system:blower[x] <p>where <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.</p>
Display health status for tree	<p>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.</p> <ul style="list-style-type: none"> • Possible return values for the BladeCenter configuration are: <ul style="list-style-type: none"> – ok – warning – critical • Possible return values for the BladeCenter T configurations are: <ul style="list-style-type: none"> – ok – minor – major – critical 	<p>health -l <i>depth</i></p> <p>where <i>depth</i> is “2”, “all”, or “a” for full tree display, starting at the command target level.</p> <p>Specifying a <i>depth</i> of “1” displays health status of the current command target.</p>	<ul style="list-style-type: none"> -T system -T system:mm[x] -T system:blade[x] -T system:switch[x] -T system:power[x] -T system:blower[x] <p>where <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.</p>

Table 7. health commands (continued)

Function	What it does	Command	Valid targets
Display health status and alerts	<p>Displays the current health status and active alerts for the command target. Return values are different for the BladeCenter and BladeCenter T configurations.</p> <ul style="list-style-type: none"> • Possible return values for the health status of the BladeCenter configuration are: <ul style="list-style-type: none"> – ok – warning – critical • Possible return values for the health status of the BladeCenter T configurations are: <ul style="list-style-type: none"> – ok – minor – major – critical • Active alert information provides short text descriptions of alerts that are active for each monitored component. <p>The total amount of information returned from the <code>health -f</code> command is limited to 1024 bytes.</p>	<code>health -f</code>	<ul style="list-style-type: none"> -T system -T system:mm[x] -T system:blade[x] -T system:switch[x] -T system:power[x] -T system:blower[x] <p>where x is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.</p>

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 8. 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. This command returns the identity of the command target, System or blade server bay (slot) number, followed by the current state of the target location LED. Possible LED states are: <ul style="list-style-type: none"> • off • on • blink 	identify -s	-T system -T system:blade[x] where x is the blade bay number.
Turn off location LED	Turns off the location LED in the command target.	identify -off Command use restricted (see “Commands and user authority” on page 5).	-T system -T system:blade[x] where x is the blade bay number.
Light location LED	Lights the location LED in the command target.	identify identify -on Command use restricted (see “Commands and user authority” on page 5).	-T system -T system:blade[x] where x is the blade bay number.
Flash location LED	Flashes the location LED in the command target.	identify -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 -on <i>time</i> where <i>time</i> 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 module while the BladeCenter unit is set as the persistent command environment, at the system> prompt, type

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

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

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

or

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

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

```
system> identify -s -T system:blade[4]
Identify: LED in slot 4 is off
system> identify -on -T system:blade[4]
OK
system> identify -s -T system:blade[4]
Identify: LED in slot 4 is on
system>
```

info (configuration information) command

This command displays information about BladeCenter components and their configuration.

Table 9. info (configuration information) command

Function	What it does	Command	Valid targets
Display component information	Displays identification and configuration information for the specified 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]:dtr[x] -T system:blade[x]:sp -T system:blade[x]:be -T system:switch[x] -T system:power[x] -T system:mt where x is the management module bay number, blade server, I/O (switch) module bay number, power module bay number, or daughter-card number.

Note: The command target -T system:blade[x]:dtr[x] is shown with a line break before :dtr[x]. When this command target is entered, the entire entry must all be on one line.

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 -T system:mm[1]
```

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

```
system:mm[1]> info -T system:mm[1]
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 10. 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, or I/O (switch) module bay number.
Display firmware attributes	Displays attributes of the firmware installed in the command target. Return values are: <ul style="list-style-type: none"> • 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, 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 <i>ip_address</i> -n <i>filename</i> where: <ul style="list-style-type: none"> • <i>ip_address</i> is the IP address of TFTP server. • <i>filename</i> is the name 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, or I/O (switch) module bay number.

Table 10. update (update firmware) command (continued)

Function	What it does	Command	Valid targets
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 <i>ip_address</i> -n <i>filename</i> -v where: <ul style="list-style-type: none"> <i>ip_address</i> is the IP address of TFTP server. <i>filename</i> is the name 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, 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 -n 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 -n 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 -n 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 -n 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
- dhcpinfo command
- dns command
- ifconfig command
- smtp command
- snmp command
- sol (serial over LAN) commands
- tpcmdmode command
- telnetcfg (Telnet configuration) command
- uplink (management module failover) command
- users (management-module users) command

alertentries command

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

Table 11. 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • -status <i>alert_recipient_status</i> (on/off) • -n <i>alert_recipient_name</i> • -f <i>alert_type</i> (critical/none) • -t <i>notification_method</i> (email/director/snmp) • -e <i>email_address</i> (used for e-mail notifications) • -i <i>static_IP_addr/hostname</i> (used for IBM Director notifications) 	alertentries - <i>recip_number</i> where <i>recip_number</i> 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.

Table 11. alertentries command (continued)

Function	What it does	Command	Valid targets
Delete alert recipient	Delete the specified alert recipient.	<p>alertentries -<i>recip_number</i> -del</p> <p>where <i>recip_number</i> 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.</p> <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where <i>x</i> is the primary management module bay number.</p>

Table 11. alertentries command (continued)

Function	What it does	Command	Valid targets
Create alert recipient	<p>Create the specified alert recipient.</p> <p>All fields must be specified when creating an alert recipient.</p>	<pre> alertentries -recip_number -n recip_name -status alert_status -f filter_type -t notification_method -e email_addr -i ip_addr/hostname </pre> <p>where:</p> <ul style="list-style-type: none"> • <i>recip_number</i> is a number from 1 to 12 that corresponds to an unused recipient number in the "Display alert properties for all recipients" list. • <i>recip_name</i> 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. • <i>alert_status</i> is on or off for receipt of alerts. • <i>filter_type</i> filters the alert types received: critical (receive critical alerts only) or none (receive all alerts). • <i>notification_method</i> is e-mail, director (IBM Director) or snmp. <ul style="list-style-type: none"> – 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. • <i>email_addr</i> is a valid e-mail address string up to 63 characters in length. <p>(continued on next page)</p>	<p>-T system:mm[x]</p> <p>where x is the primary management module bay number.</p>

Table 11. *alertentries* command (continued)

Function	What it does	Command	Valid targets
Create alert recipient <i>(continued)</i>		<ul style="list-style-type: none"> <i>ip_addr/hostname</i> 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 (_). <p>Command use restricted (see “Commands and user authority” on page 5).</p>	
Set alert recipient name	Sets a name for the specified alert recipient.	<p><code>alertentries -<i>recip_number</i> -n <i>recip_name</i></code></p> <p>where:</p> <ul style="list-style-type: none"> <i>recip_number</i> is a number from 1 to 12 that corresponds to the recipient number assigned in the “Display alert properties for all recipients” list. <i>recip_name</i> 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. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where x is the primary management module bay number.</p>
Set alert recipient status	Sets status for the specified alert recipient. The status determines if a recipient will receive alarm notifications.	<p><code>alertentries -<i>recip_number</i> -status <i>alert_status</i></code></p> <p>where:</p> <ul style="list-style-type: none"> <i>recip_number</i> is a number from 1 to 12 that corresponds to the recipient number assigned in the “Display alert properties for all recipients” list. <i>alert_status</i> is on or off. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where x is the primary management module bay number.</p>

Table 11. 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.	<p>alertentries <i>-recip_number</i> <i>-f filter_type</i></p> <p>where:</p> <ul style="list-style-type: none"> <i>recip_number</i> is a number from 1 to 12 that corresponds to the recipient number assigned in the “Display alert properties for all recipients” list. <i>alert_type</i> filters the alert types received: critical (receive critical alerts only) or none (receive all alerts). <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where x is the primary management module bay number.</p>
Set alert notification method	Sets the alert notification method for the specified alert recipient.	<p>alertentries <i>-recip_number</i> <i>-t notification_method</i></p> <p>where:</p> <ul style="list-style-type: none"> <i>recip_number</i> is a number from 1 to 12 that corresponds to the recipient number assigned in the “Display alert properties for all recipients” list. <i>notification_method</i> is e-mail, director (IBM Director) or snmp. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where x is the primary management module bay number.</p>
Set alert recipient e-mail address	<p>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.</p> <p>The e-mail address can be set only if the alert notification method (-t option) is set to e-mail. The -t and -e options can be combined within the same command.</p>	<p>alertentries <i>-recip_number</i> <i>-e email_addr</i></p> <p>where:</p> <ul style="list-style-type: none"> <i>recip_number</i> is a number from 1 to 12 that corresponds to the recipient number assigned in the “Display alert properties for all recipients” list. <i>email_addr</i> is a valid e-mail address string up to 63 characters in length. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where x is the primary management module bay number.</p>

Table 11. alertentries command (continued)

Function	What it does	Command	Valid targets
Set alert recipient IP address or hostname	<p>Sets the IP address or hostname used to send alert notifications to the specified alert recipient using IBM Director.</p> <p>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.</p>	<p>alertentries -<i>recip_number</i> -i <i>ip_addr/hostname</i></p> <p>where:</p> <ul style="list-style-type: none"> <i>recip_number</i> is a number from 1 to 12 that corresponds to the recipient number assigned in the “Display alert properties for all recipients” list. <i>ip_addr/hostname</i> is a valid static IP address or an alphanumeric hostname string up to 49 characters in length that can include periods (.), hyphens (-), and underscores (_). <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where x is the primary management module bay number.</p>

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

This command resets 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 12. `clear` command

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

Example:

To reset 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.

dhcpcinfo command

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

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

Table 13. *dhcpcinfo* commands

Function	What it does	Command	Valid targets
Display Ethernet channel 0 DHCP configuration	<p>If the IP configuration for <code>eth0</code> 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 <code>eth0</code> is <i>not</i> assigned by a DHCP server, an error message is displayed. Possible configuration values returned are:</p> <ul style="list-style-type: none">• <code>-server dhcp_ip_address</code>• <code>-n hostname</code>• <code>-i ip_address</code>• <code>-g gateway_address</code>• <code>-s subnet_mask</code>• <code>-d domainname</code>• <code>-dns1 primary_dns_ip_address</code>• <code>-dns2 secondary_dns_ip_address</code>• <code>-dns3 tertiary_dns_ip_1address</code>	<code>dhcpcinfo -eth0</code>	<p><code>-T system:mm[x]</code></p> <p>where <code>x</code> is the primary management module bay number.</p>

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

```
dhcpcinfo -eth0
```

The following example shows the information that is returned:

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

dns command

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

Table 14. dns commands

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: <ul style="list-style-type: none"> • enabled • disabled • -i1 <i>first ip_address</i> • -i2 <i>second ip_address</i> • -i3 <i>third ip_address</i> 	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.
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 <i>ip_address</i> where <i>ip_address</i> 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 <i>ip_address</i> where <i>ip_address</i> 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 <i>ip_address</i> where <i>ip_address</i> 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

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

Table 15. *ifconfig* commands

Function	What it does	Command	Valid targets
Display Ethernet channel 0 configuration	Displays the current configuration of Ethernet channel 0. Possible return values are: <ul style="list-style-type: none"> • enabled • disabled • -i <i>static_ip_address</i> • -g <i>gateway_address</i> • -s <i>subnet_mask</i> • -n <i>hostname</i> • -c <i>config_method</i> • -r <i>data_rate</i> • -d <i>duplex_mode</i> • -m <i>mtu</i> • -l <i>locally_administered_mac_addr</i> • -b <i>burnedin_mac_address</i> 	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 <i>ip_address</i> where <i>ip_address</i> 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 <i>ip_address</i> where <i>ip_address</i> 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 <i>ip_address</i> where <i>ip_address</i> 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 Ethernet channel 0 hostname	Checks syntax and sets the host name for Ethernet channel 0.	ifconfig -eth0 -n <i>hostname</i> where <i>hostname</i> 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.

Table 15. *ifconfig* commands (continued)

Function	What it does	Command	Valid targets
Set Ethernet channel 0 configuration method	Checks syntax and sets the configuration method for Ethernet channel 0. A value of <i>dthens</i> will try the dhcp configuration and default to the static IP configuration if dhcp is unsuccessful.	<code>ifconfig -eth0 -c <i>config_method</i></code> where <i>config_method</i> is <i>dhcp</i> , <i>static</i> , or <i>dthens</i> . Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> is the primary management module bay number.
Set Ethernet channel 0 data rate	Checks syntax and sets the data rate for Ethernet channel 0.	<code>ifconfig -eth0 -r <i>data_rate</i></code> where <i>data_rate</i> is <i>auto</i> , <i>10</i> , or <i>100</i> . Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> is the primary management module bay number.
Set Ethernet channel 0 duplex mode	Checks syntax and sets the duplex mode for Ethernet channel 0.	<code>ifconfig -eth0 -d <i>duplex_mode</i></code> where <i>duplex_mode</i> is <i>auto</i> , <i>half</i> , or <i>full</i> . Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> is the primary management module bay number.
Set Ethernet channel 0 MTU	Checks syntax and sets the MTU for Ethernet channel 0.	<code>ifconfig -eth0 -m <i>mtu</i></code> where <i>mtu</i> is between 60 and 1500, inclusive. Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> 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.	<code>ifconfig -eth0 -l <i>address</i></code> where <i>address</i> 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 <i>x</i> is the primary management module bay number.
Display Ethernet channel 1 configuration	Displays the current configuration of Ethernet channel 1. Possible return values are: <ul style="list-style-type: none"> • <i>enabled</i> • <i>disabled</i> • -i <i>static_ip_address</i> • -g <i>gateway_address</i> • -s <i>subnet_mask</i> • -r <i>data_rate</i> • -d <i>duplex_mode</i> • -m <i>mtu</i> • -l <i>locally_administered_mac_addr</i> • -b <i>burnedin_mac_address</i> 	<code>ifconfig -eth1</code>	-T system:mm[x] where <i>x</i> is the primary management module bay number.

Table 15. *ifconfig* commands (continued)

Function	What it does	Command	Valid targets
Set Ethernet channel 1 static IP address	Checks syntax and sets the static IP address for Ethernet channel 1.	<code>ifconfig -eth1 -i <i>ip_address</i></code> where <i>ip_address</i> 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 <i>x</i> 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.	<code>ifconfig -eth1 -g <i>ip_address</i></code> where <i>ip_address</i> 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 <i>x</i> is the primary management module bay number.
Set Ethernet channel 1 subnet mask	Checks syntax and sets the subnet mask for Ethernet channel 1.	<code>ifconfig -eth1 -s <i>ip_address</i></code> where <i>ip_address</i> is the subnet mask for Ethernet channel 1. Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> 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.	<code>ifconfig -eth1 -l <i>address</i></code> where <i>address</i> 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 <i>x</i> is the primary management module bay number.
Enable Ethernet channel 1	Enables Ethernet channel 1.	<code>ifconfig -eth1 -up</code> Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> is the primary management module bay number.
Disable Ethernet channel 1	Disables Ethernet channel 1.	<code>ifconfig -eth1 -down</code> Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> is the primary management module bay number.

Table 15. *ifconfig* commands (continued)

Function	What it does	Command	Valid targets
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.	<code>ifconfig -i <i>ip_address</i></code> where <i>ip_address</i> 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]>
```

smtp command

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

Table 16. *smtp* commands

Function	What it does	Command	Valid targets
Display SMTP server host name or IP address	Displays the SMTP server host name or IP address.	<code>smtp</code>	-T system:mm[x] where <i>x</i> is the primary management module bay number.

Table 16. *smtp* commands (continued)

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

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 17. snmp commands

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: <ul style="list-style-type: none"> • -a enabled/disabled • -t enabled/disabled • -c1 <i>community1_name</i> • -c1i1 <i>community1_ipaddr1_or_hstname</i> • -c1i2 <i>community1_ipaddr2_or_hstname</i> • -c1i3 <i>community1_ipaddr3_or_hstname</i> • -c2 <i>community2_name</i> • -c2i1 <i>community2_ipaddr1_or_hstname</i> • -c2i2 <i>community2_ipaddr2_or_hstname</i> • -c2i3 <i>community2_ipaddr3_or_hstname</i> • -c3 <i>community3_name</i> • -c3i1 <i>community3_ipaddr1_or_hstname</i> • -c3i2 <i>community3_ipaddr2_or_hstname</i> • -c3i3 <i>community3_ipaddr3_or_hstname</i> • -cn <i>contact_name</i> • -l <i>location</i> 	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 46, 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.
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 58, 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.

Table 17. snmp commands (continued)

Function	What it does	Command	Valid targets
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 <i>name</i> where <i>name</i> 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 <i>hostname/ip_address</i> where <i>hostname/ip_address</i> 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.
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 <i>hostname/ip_address</i> where <i>hostname/ip_address</i> 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 <i>hostname/ip_address</i> where <i>hostname/ip_address</i> 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.

Table 17. *snmp* commands (continued)

Function	What it does	Command	Valid targets
SNMPv3 community 1 view type - set	Sets the SNMPv3 view type for community 1.	<code>snmp -ca1 type</code> where <i>type</i> is get, set, or trap. Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> is the primary management module bay number.
SNMP community 2 name - set	Sets the name of community 2.	<code>snmp -c2 name</code> where <i>name</i> is a descriptive name of community 2. Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> 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.	<code>snmp -c2i1 hostname/ip_address</code> where <i>hostname/ip_address</i> 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 <i>x</i> is the primary management module bay number.
SNMP community 2 second host name or IP address - set	Checks syntax and sets the second host name or IP address of community 2.	<code>snmp -c2i2 hostname/ip_address</code> where <i>hostname/ip_address</i> 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 <i>x</i> 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.	<code>snmp -c2i3 hostname/ip_address</code> where <i>hostname/ip_address</i> 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 <i>x</i> is the primary management module bay number.

Table 17. *snmp* commands (continued)

Function	What it does	Command	Valid targets
SNMPv3 community 2 view type - set	Sets the SNMPv3 view type for community 2.	<code>snmp -ca2 <i>type</i></code> where <i>type</i> is get, set, or trap. Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> is the primary management module bay number.
SNMP community 3 name - set	Sets the name of community 3.	<code>snmp -c3 <i>name</i></code> where <i>name</i> is a descriptive name of community 3. Command use restricted (see “Commands and user authority” on page 5).	-T system:mm[x] where <i>x</i> 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.	<code>snmp -c3i1 <i>hostname/ip_address</i></code> where <i>hostname/ip_address</i> 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 <i>x</i> is the primary management module bay number.
SNMP community 3 second host name or IP address - set	Checks syntax and sets the second host name or IP address of community 3.	<code>snmp -c3i2 <i>hostname/ip_address</i></code> where <i>hostname/ip_address</i> 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 <i>x</i> 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.	<code>snmp -c3i3 <i>hostname/ip_address</i></code> where <i>hostname/ip_address</i> 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 <i>x</i> is the primary management module bay number.

Table 17. snmp commands (continued)

Function	What it does	Command	Valid targets
SNMPv3 community 3 view type - set	Sets the SNMPv3 view type for community 3.	snmp -ca3 <i>type</i> where <i>type</i> 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 <i>contact_name</i> 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 <i>hostname/ip_address</i> 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) commands

These commands configure SOL functions and indicate SOL status.

Table 18. sol (serial over LAN) commands

Function	What it does	Command	Valid targets
Display SOL status	<p>Displays the SOL status for the targeted device:</p> <ul style="list-style-type: none"> • When the command target is the primary management module, it displays the following values: <ul style="list-style-type: none"> – -status <i>on/off</i> (global SOL status) – -c <i>retry_count</i> – -e <i>CLI_key_sequence</i> – -i <i>retry_interval</i> – -r <i>reset_blade_key_seq</i> – -s <i>send_threshold</i> – -t <i>accumulate_timeout</i> – -v <i>VLAN_id</i> • When the command target is a blade server, it displays the following: <ul style="list-style-type: none"> – -status <i>on/off</i> (SOL status for the blade server) – Status of any SOL sessions for that blade server: <ul style="list-style-type: none"> - 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. 	<p>sol</p>	<p>-T system:mm[x] -T system:blade[x]</p> <p>where x is the primary management module or blade server bay number.</p>
SOL retry interval - set	<p>Sets the SOL retry interval to the input value.</p>	<p>sol -i <i>value</i></p> <p>where <i>value</i> 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.</p> <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where x is the primary management module bay number.</p>

Table 18. sol (serial over LAN) commands (continued)

Function	What it does	Command	Valid targets
SOL retry count - set	Sets the SOL retry count to the input value.	sol -c <i>value</i> where <i>value</i> 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 <i>x</i> 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 <i>value</i> where <i>value</i> 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 <i>x</i> is the primary management module bay number.
SOL accumulate timeout - set	Sets the SOL accumulate timeout to the input value.	sol -t <i>value</i> where <i>value</i> 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 <i>x</i> 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 <i>x</i> 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 <i>x</i> 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 <i>x</i> 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 <i>x</i> is the blade server bay number.

Table 18. sol (serial over LAN) commands (continued)

Function	What it does	Command	Valid targets
SOL VLAN ID - set	Sets the SOL VLAN ID to the input value.	sol -v <i>value</i> where <i>value</i> 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 <i>x</i> 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 <i>value</i> where <i>value</i> is the key sequence. In this sequence, a ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example: <ul style="list-style-type: none"> • ^[(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 <i>x</i> is the primary management module bay number.
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 <i>value</i> where <i>value</i> is the key sequence. In this sequence, a ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example: <ul style="list-style-type: none"> • ^[(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 <i>x</i> 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]>
```

tcpcmdmode command

These commands display and change 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 19. *tcpcmdmode* commands

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.	<code>tcpcmdmode</code>	<code>-T system:mm[x]</code> where <i>x</i> is the primary management module bay number.
Set TCP command-mode session timeout	Sets the TCP command-mode session timeout value.	<code>tcpcmdmode -t <i>timeout</i></code> where <i>timeout</i> 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).	<code>-T system:mm[x]</code> where <i>x</i> is the primary management module bay number.

Table 19. *tcpcmdmode* commands (continued)

Function	What it does	Command	Valid targets
Enable TCP command-mode sessions	Enables TCP command-mode sessions that are used by <i>IBM Director</i> software for out-of-band communication with the management module.	<code>tcpcmdmode -on</code> Command use restricted (see “Commands and user authority” on page 5).	<code>-T system:mm[x]</code> where <i>x</i> is the primary management module bay number.
Disable TCP command-mode sessions	Disables TCP command-mode sessions that are used by <i>IBM Director</i> software for out-of-band communication with the management module.	<code>tcpcmdmode -off</code> Command use restricted (see “Commands and user authority” on page 5).	<code>-T system:mm[x]</code> where <i>x</i> 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 -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 -on
OK
system:mm[1]> tcpcmdmode -t 360
OK
system:mm[1]> tcpcmdmode
-on
-t 360
system:mm[1]>
```

telnetcfg (Telnet configuration) command

These commands display and configure the telnet parameters of the primary management module.

Table 20. *telnetcfg* (Telnet configuration) commands

Function	What it does	Command	Valid targets
Display telnet configuration	Displays the telnet configuration of the primary management module.	<code>telnetcfg</code>	<code>-T system:mm[x]</code> where <i>x</i> is the primary management module bay number.

Table 20. *telnetcfg* (Telnet configuration) commands (continued)

Function	What it does	Command	Valid targets
Display telnet timeout	Displays the telnet 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 telnet timeout for primary management module	Sets the telnet timeout value for the primary management module.	telnetcfg -t <i>timeout</i> where <i>timeout</i> 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 telnet 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 telnet 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

These commands display and configure 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 21. *uplink* commands

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.

Table 21. uplink commands (continued)

Function	What it does	Command	Valid targets
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 <i>delay</i> where <i>delay</i> 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 (management-module users) command

This command displays and configures user accounts 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 22. users (management-module users) command

Function	What it does	Command	Valid targets
Display all user profiles	Displays all 12 management-module user profiles. Returned values are: <ul style="list-style-type: none"> • User name • Authority level 	users	-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: <ul style="list-style-type: none"> • 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 22. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Create user profile	<p>Create the specified management-module user profile.</p> <p>All fields must be specified when creating a user profile for the BladeCenter T management module.</p>	<pre>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</pre> <p>where:</p> <ul style="list-style-type: none"> • <i>user_number</i> is a number from 1 to 12 that corresponds to an unused user number in the “Display all user profiles” list. • <i>user_name</i> 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. • <i>user_password</i> is a 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. • <i>user_authority</i> is one of the following: <ul style="list-style-type: none"> – ro (read-only) – super (Supervisor) – custom (see “Set user authority level” on page 61 for more information) <p>for previous versions of management-module firmware, <i>user_authority</i> was one of the following:</p> <ul style="list-style-type: none"> – operator (read-only) – super (Supervisor) – rbs (see “Set user authority level” on page 63 for more information) <p>(continued on next page)</p>	<p>-T system:mm[x]</p> <p>where x is the primary management module bay number.</p>

Table 22. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
<p>Create user profile <i>(continued)</i></p>		<ul style="list-style-type: none"> • <i>context_name</i> is a string for SNMPv3 context that is up to 31 characters in length. Each of the 12 context names must be unique. • <i>auth_protocol</i> is an SNMPv3 authentication protocol of sha, md5, or blank (no entry) for none. • <i>privacy_protocol</i> 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. • <i>privacy_pwd</i> 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. • <i>access_type</i> is an SNMPv3 access type of read, write, or traps. • <i>ip_addr/hostname</i> is a valid SNMPv3 static IP address or an alphanumeric hostname string up to 63 characters in length. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	

Table 22. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Set user name	Sets a user name in the specified management-module user profile.	<p>users -<i>user_number</i> -n <i>user_name</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>user_number</i> is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • <i>user_name</i> 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. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where <i>x</i> is the primary management module bay number.</p>
Set user password	Sets a user password in the specified management-module user profile.	<p>users -<i>user_number</i> -p <i>user_password</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>user_number</i> is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • <i>user_password</i> is a 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. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where <i>x</i> is the primary management module bay number.</p>

Table 22. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Set user authority level (latest level of management-module firmware)	Sets a user authority level in the specified management-module user profile.	<p>users -<i>user_number</i> -a <i>user_authority</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>user_number</i> is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • <i>user_authority</i> is one of the following: <ul style="list-style-type: none"> – operator (read-only) – super (Supervisor) – rbs (custom) <p>The custom authority level parameter is specified using the following syntax:</p> <p>rbs:<i>levels</i>:<i>devices</i></p> <p>where the <i>levels</i> are one or more of the following authority levels, separated by a vertical bar ():</p> <ul style="list-style-type: none"> • 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) <p>(continued on next page)</p>	<p>-T system:mm[x]</p> <p>where x is the primary management module bay number.</p>

Table 22. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
<p>Set user authority level (latest level of management-module firmware) (continued)</p>		<p>where the <i>devices</i> are one or more of the following devices, separated by a vertical bar (). Ranges of devices are separated by a dash (-).</p> <ul style="list-style-type: none"> • <i>cn</i> (Chassis <i>n</i>, where <i>n</i> is a valid chassis number. Use c1 for single-chassis environments.) • <i>bn</i> (Blade <i>n</i>, where <i>n</i> is a valid blade bay number in the chassis) • <i>sn</i> (I/O module <i>n</i>, where <i>n</i> is a valid I/O module bay number in the chassis) <p>Command use restricted (see “Commands and user authority” on page 5).</p>	

Table 22. *users* (management-module users) command (continued)

Function	What it does	Command	Valid targets
<p>Set user authority level (previous levels of management-module firmware)</p>	<p>Sets a user authority level in the specified management-module user profile.</p>	<p><code>users -user_number -a user_authority</code></p> <p>where:</p> <ul style="list-style-type: none"> • <i>user_number</i> is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. • <i>user_authority</i> is one of the following: <ul style="list-style-type: none"> – ro (read-only) – super (Supervisor) – custom <p>The custom authority level parameter is specified using the following syntax:</p> <p>custom:<i>level1</i> <i>level2</i></p> <p>where the <i>levels</i> are one or more of the following authority levels, separated by a vertical bar (): <ul style="list-style-type: none"> • 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) </p> <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where <i>x</i> is the primary management module bay number.</p>

Table 22. users (management-module users) command (continued)

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

Table 22. *users* (management-module users) command (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.	<p><code>users -user_number -ppw privacy_pwd</code></p> <p>where:</p> <ul style="list-style-type: none"> <code>user_number</code> is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. <code>privacy_pwd</code> is a string up to 31 characters in length. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where <i>x</i> is the primary management module bay number.</p>
Set access type for SNMPv3 user	<p>Sets an SNMPv3 access type for the specified management-module user profile.</p> <p>This command supports the following access types:</p> <ul style="list-style-type: none"> 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. 	<p><code>users -user_number -at access_type</code></p> <p>where:</p> <ul style="list-style-type: none"> <code>user_number</code> is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. <code>access_type</code> is read, write, or traps. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where <i>x</i> is the primary management module bay number.</p>
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.	<p><code>users -user_number -i ip_addr/hostname</code></p> <p>where:</p> <ul style="list-style-type: none"> <code>user_number</code> is a number from 1 to 12 that corresponds to the user number assigned in the “Display all user profiles” list. <code>ip_addr/hostname</code> is a valid static IP address or an alphanumeric hostname string up to 63 characters in length. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:mm[x]</p> <p>where <i>x</i> is the primary management module bay number.</p>

Example:

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

```
users -3 -n user3 -p passwd -a super -cn joe -ap md5 -pp des -ppw passwd  
-at read -I 192.168.70.129
```

Note: The entry beginning with users -3 -n... is shown with a line break after passwd. 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|c
```

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 passwd -a super -cn joe -ap md5 -pp des  
-ppw passwd -at read -I 192.168.70.129  
OK  
system:mm[1]> users  
1. USERID      Read/Write  
2. <not used>  
3. user3       Read/Write  
4. user4       Read/Write  
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 -pp des. When this command is entered, the entire entry must all be on one line.

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 23. clearlog (clear management-module event log) commands

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

These commands display management-module event log entries.

Table 24. *displaylog* (display management-module event log) commands

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.

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
- power command
- reset command

boot command

These commands reset blade servers with several different restart options.

Table 25. boot commands

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.

Table 25. boot commands (continued)

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 -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

These commands display 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. These commands also configure the power domain policies for oversubscription and quiet mode

Table 26. fuelg commands

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 <i>domain</i> where <i>domain</i> is “pd1” for power domain 1 and “pd2” for power domain 2. If no <i>domain</i> is specified, a status overview for all power domains displays.	-T system

Table 26. *fuelg* commands (continued)

Function	What it does	Command	Valid targets
Set power domain oversubscription policy	Sets how the BladeCenter unit responds to an oversubscription condition that could cause a loss of redundant power.	<p><i>fuelg domain -os policy</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>domain</i> is “pd1” for power domain 1 and “pd2” for power domain 2. If no <i>domain</i> is specified, the <i>policy</i> is applied to all power domains. • <i>policy</i> of: <ul style="list-style-type: none"> – “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. <p>Command use restricted (see “Commands and user authority” on page 5).</p>	-T system
Thermal event response (quiet mode)	Sets how the BladeCenter unit blowers respond to thermal events.	<p><i>fuelg -qm setting</i></p> <p>where the quiet-mode <i>setting</i> of:</p> <ul style="list-style-type: none"> • “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). <p>Command use restricted (see “Commands and user authority” on page 5).</p>	-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 turn on quiet mode for all power domains while the BladeCenter unit is set as the persistent command environment, 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:

```
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
```

Bay(s)	Module	Power State	Current	Allocated Max	Power Min
Chassis Components					
	Midplane	0n	10	10	10
no media tray					
Blowers					
1	Blower 1 (NP)	0n	120	120	120
2	Blower 2 (NP)	0n	120	120	120
Management Modules					
1	WMN315619689	0n	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:
```

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>
```

power command

These commands turn on and turn off blade servers and I/O (switch) modules.

Table 27. power commands

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 27. power commands (continued)

Function	What it does	Command	Valid targets
Display POST status for I/O (switch) module	<p>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:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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. <p>Where <i>hex_code</i> is a hexadecimal code. See the documentation that comes with your I/O module for information.</p> <p>Note: This command option is not supported for serial concentrator I/O (switch) modules.</p>	power -state -post	<p>-T system:switch[x]</p> <p>where x is the I/O (switch) module bay number.</p>

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

These commands reset blade servers, blade server integrated system management processors, I/O (switch) modules, or the primary management module.

Table 28. reset commands

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 28. reset commands (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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 28. reset commands (continued)

Function	What it does	Command	Valid targets
Restart blade server and run diagnostics using default boot sequence	<p>Command results depend on the blade server model that is specified:</p> <ul style="list-style-type: none"> • 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. 	<p>reset -ddg</p> <p>Command use restricted (see “Commands and user authority” on page 5).</p>	<p>-T system:blade[x]</p> <p>where x is the blade server bay number.</p>

Example:

To reset the ISMP 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

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 29. console commands

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.
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 30. 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
```

System management commands (for BladeCenter T only)

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

- alarm command
- thres (alarm threshold) command

alarm command

These commands display alarm information, acknowledge alarms, and clear alarms for the specified command target.

Table 31. alarm commands

Function	What it does	Command	Valid targets
Display all alarms	<p>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.</p> <p>Detailed alarm listings include an alarm key that can be used to acknowledge or clear an alarm.</p>	alarm	<p>-T system -T system:mm[x] -T system:blade[x] -T system:switch[x] -T system:power[x] -T system:blower[x]</p> <p>where x is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.</p>
Display power alarms	<p>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.</p> <p>Detailed alarm listings include an alarm key that can be used to acknowledge or clear an alarm.</p>	alarm -p	<p>-T system -T system:mm[x] -T system:blade[x] -T system:switch[x] -T system:power[x] -T system:blower[x]</p> <p>where x is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.</p>

Table 31. alarm commands (continued)

Function	What it does	Command	Valid targets
Display alarm information (specified by alarm generator ID)	Display information for alarm specified by the generator ID.	alarm -q -g <i>value</i> where <i>value</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.
Display alarm information (specified by alarm ID)	Display information for alarm specified by the alarm ID.	alarm -q -a <i>value</i> where <i>value</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower 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 <i>value</i> where <i>value</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.

Table 31. alarm commands (continued)

Function	What it does	Command	Valid targets
Display alarm information (specified by complete alarm key)	Display information for alarm specified by the complete alarm key.	alarm -q -k <i>m:g:o:a</i> where <i>m:g:o:a</i> is the complete alarm key: <ul style="list-style-type: none"> • <i>m</i> is the module ID • <i>g</i> is the generator ID • <i>o</i> is the generator information • <i>a</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.
Acknowledge alarm (specified by alarm generator ID)	Acknowledge the alarm specified by the generator ID.	alarm -r -g <i>value</i> where <i>value</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.
Acknowledge alarm (specified by generator information)	Acknowledge the alarm specified by the generator information.	alarm -r -o <i>value</i> where <i>value</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.

Table 31. alarm commands (continued)

Function	What it does	Command	Valid targets
Acknowledge alarm (specified by alarm ID)	Acknowledge the alarm specified by the alarm ID.	alarm -r -a <i>value</i> where <i>value</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.
Acknowledge alarm (specified by complete alarm key)	Acknowledge the alarm specified by the complete alarm key.	alarm -r -k <i>m:g:o:a</i> where <i>m:g:o:a</i> is the complete alarm key: <ul style="list-style-type: none"> • <i>m</i> is the module ID • <i>g</i> is the generator ID • <i>o</i> is the generator information • <i>a</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.
Clear alarm (specified by alarm generator ID)	Clear the alarm specified by the generator ID.	alarm -c -g <i>value</i> where <i>value</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.

Table 31. alarm commands (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 <i>value</i> where <i>value</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.
Clear alarm (specified by alarm ID)	Clear the alarm specified by the alarm ID.	alarm -c -a <i>value</i> where <i>value</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.
Clear alarm (specified by complete alarm key)	Clear the alarm specified by the complete alarm key.	alarm -c -k <i>m:g:o:a</i> where <i>m:g:o:a</i> is the complete alarm key: <ul style="list-style-type: none"> • <i>m</i> is the module ID • <i>g</i> is the generator ID • <i>o</i> is the generator information • <i>a</i> 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 <i>x</i> is the primary management module bay number, blade server, I/O (switch) module bay number, power module bay number, or blower number.

Table 31. alarm commands (continued)

Function	What it does	Command	Valid targets
Set alarm	Set an alarm for the specified target, including severity level and description.	alarm -s -l <i>level desc</i> where <ul style="list-style-type: none"> • <i>level</i> is the severity level: <ul style="list-style-type: none"> – CRT (critical) – MJR (major) – MNR (minor) • <i>desc</i> 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 bay number, blade server, I/O (switch) module bay number, power module bay number, or blower 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>

```

thres (alarm threshold) command

These commands display and set alarm thresholds for the BladeCenter T unit.

Table 32. *thres* (alarm threshold) commands

Function	What it does	Command	Valid targets
Display specified threshold settings	Displays the current settings of threshold values for the specified source.	<p><code>thres -q -source</code></p> <p>where <i>source</i> is the set of threshold values to display:</p> <ul style="list-style-type: none"> • MM (management module ambient temperature) • SYS (system temperature) • P12V (plus 12 voltage) • P5V (plus 5 voltage) • P3.3V (plus 3.3 voltage) • P2.5V (plus 2.5 voltage) • P1.8V (plus 1.8 voltage) • M5V (minus 5 voltage) 	<p><code>-T system:mm[x]</code></p> <p>where <i>x</i> is the primary management module bay number.</p>

Table 32. *thres* (alarm threshold) commands (continued)

Function	What it does	Command	Valid targets
Display specified threshold setting	Checks syntax and sets the specified threshold value.	<p><i>thres -s -source -type value</i></p> <p>where</p> <ul style="list-style-type: none"> • <i>source</i> is a set of threshold values: <ul style="list-style-type: none"> – MM (management module ambient temperature) – SYS (system temperature) – P12V (plus 12 voltage) – P5V (plus 5 voltage) – P3.3V (plus 3.3 voltage) – P2.5V (plus 2.5 voltage) – P1.8V (plus 1.8 voltage) – M5V (minus 5 voltage) • <i>type</i> is a specific threshold to set for the indicated source: <ul style="list-style-type: none"> – HCRT (high critical) – HMJR (high major) – HMNR (high minor) – LCRT (low critical) – LMJR (low major) – LMNR (low minor) – HCRTH (high critical hysteresis reset) – HMJRH (high major hysteresis reset) – HMNRH (high minor hysteresis reset) – LCRTH (low critical hysteresis reset) – LMJRH (low major hysteresis reset) – LMNRH (low minor hysteresis reset) <p><i>(continued on next page)</i></p>	<p>-T system:mm[x]</p> <p>where <i>x</i> is the primary management module bay number.</p>

Table 32. thres (alarm threshold) commands (continued)

Function	What it does	Command	Valid targets
Display specified threshold setting (continued)		<p>where</p> <ul style="list-style-type: none"> • <i>value</i> is a threshold value or -DEFAULT to set the threshold to the factory preset value. The default threshold value is Disable (no setting), with the following exceptions: <ul style="list-style-type: none"> – SYS HMNR: 60 – SYS HMNRH: 55 – MM HMNR: 39 – MM HMNRH: 30 – P1.8V LMNR: +1.62 – P1.8V LMNRH: +1.74 – P1.8V HMNR: +1.89 – P1.8V HMNRH: +1.86 – P2.5V LMNR: +2.25 – P2.5V LMNRH: +2.42 – P2.5V HMNR: +2.63 – P2.5V HMNRH: +2.58 – P3.3V LMNR: +3.00 – P3.3V LMNRH: +3.20 – P3.3V HMNR: +3.47 – P3.3V HMNRH: +3.40 – P5V LMNR: +4.50 – P5V LMNRH: +4.85 – P5V HMNR: +5.25 – P5V HMNRH: +5.15 – P12V LMNR: +10.80 – P12V LMNRH: +11.64 – P12V HMNR: +12.60 – P12V HMNRH: +12.36 – M5V LMNR: -5.50 – M5V LMNRH: -5.15 – M5V HMNR: -4.75 – M5V HMNRH: -4.85 <p><i>(continued on next page)</i></p>	
Display specified threshold setting (continued)		<p>Command use restricted (see “Commands and user authority” on page 5).</p>	

Example:

To display the management-module ambient temperature thresholds for the BladeCenter T unit while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
thres -q -MM
```

To set the management-module ambient temperature low major threshold for the BladeCenter T unit while the BladeCenter T unit is set as the persistent command environment, at the `system>` prompt, type

```
thres -s -MM -LMJR 45
```

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

```
system:mm[1]> thres -q -MM
Management Module Temperature Thresholds Detail in Centigrade
LCRT      LCRTH    LMJR      LMJRH     LMNR      LMNRH
=====  =====  =====  =====  =====  =====
Disable   Disable  Disable   Disable   Disable   Disable

HMNRH     HMNR     HMJRH     HMJR      HCRTH     HCRT
=====  =====  =====  =====  =====  =====
+55.00    +60.00   Disable   Disable   Disable   Disable
system:mm[1]> thres -s -MM -LMJR 45
OK
system:mm[1]> thres -q -MM
Management Module Temperature Thresholds Detail in Centigrade
LCRT      LCRTH    LMJR      LMJRH     LMNR      LMNRH
=====  =====  =====  =====  =====  =====
Disable   Disable   +45.00    Disable   Disable   Disable

HMNRH     HMNR     HMJRH     HMJR      HCRTH     HCRT
=====  =====  =====  =====  =====  =====
+55.00    +60.00   Disable   Disable   Disable   Disable
system:mm[1]>
```

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 90
- “alarm command errors” on page 91
- “alertentries command errors” on page 92
- “boot command errors” on page 92
- “clear command errors” on page 92
- “clearlog command errors” on page 93
- “console command errors” on page 93
- “dhcpinfo command errors” on page 93
- “displaylog command errors” on page 93
- “dns command errors” on page 94
- “fuelg command errors” on page 94
- “health command errors” on page 94
- “identify command errors” on page 95
- “ifconfig command errors” on page 95
- “info command errors” on page 97
- “list command errors” on page 98
- “power command errors” on page 98
- “reset command errors” on page 98
- “smtp command errors” on page 99
- “snmp command errors” on page 99
- “sol command errors” on page 99
- “tcpcmdmode command errors” on page 101
- “telnetcfg command errors” on page 101
- “thres command errors” on page 101
- “update command errors” on page 102
- “uplink command errors” on page 104
- “users command errors” on page 104

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 33. Common errors

Error message	Definition
Command line contains extraneous arguments	Displays when extra command arguments are entered.
Duplicate option: <i>option</i> where <i>option</i> 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, <code>dns -i 192.168.70.29 -i</code>
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, <code>env -T system:blade[4] -T system:blade[5]</code> .
Error writing data for option <i>option</i> where <i>option</i> identifies the command option that is returning an error.	Displays when an internal error occurs while writing a command option value.
Illegal option: <i>option</i> where <i>option</i> identifies the illegal short command option that was entered.	Displays when an illegal short command option is entered.
Integer argument out of range (<i>range - range</i>) for <i>option: argument</i> where: <ul style="list-style-type: none"> • <i>range</i> identifies the range limits • <i>option</i> identifies the command option • <i>argument</i> identifies the integer that is out of range 	Displays when an integer is entered that is out of range.
Invalid integer argument for <i>option: argument</i> where: <ul style="list-style-type: none"> • <i>option</i> identifies the command option • <i>argument</i> 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 <i>option: argument</i> where: <ul style="list-style-type: none"> • <i>option</i> identifies the command option • <i>argument</i> 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 <i>option</i> requires an argument where <i>option</i> 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 33. Common errors (continued)

Error message	Definition
Short option <i>option</i> requires an argument where <i>option</i> 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 <code>env -T system:blade[15]</code> command is out of range because the BladeCenter unit has only 14 blade bays.
Unrecognized long option: <i>option</i> where <i>option</i> 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 90 for a list of error messages that apply to all commands.

Table 34. 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 90 for a list of error messages that apply to all commands.

Table 35. 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 90 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 90 for a list of error messages that apply to all commands.

Table 36. 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 90 for a list of error messages that apply to all commands.

Table 37. 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 90 for a list of error messages that apply to all commands.

Table 38. 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.

dhcpcinfo command errors

There are no unique errors for the dhcpcinfo command. See “Common errors” on page 90 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 90 for a list of error messages that apply to all commands.

Table 39. 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.

dns command errors

The following table lists error messages for the dns command. See “Common errors” on page 90 for a list of error messages that apply to all commands.

Table 40. 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 90 for a list of error messages that apply to all commands.

Table 41. fuelg command errors

Error message	Definition
A power module failure in domain <i>domain_number</i> can result in an immediate shutdown. where <i>domain_number</i> 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 <i>blade_number</i> is not allowed to power on because of insufficient power. where <i>blade_number</i> identifies the blade server.	Displays when there is insufficient power available in the power domain to turn on this blade server.
Blade <i>blade_number</i> is throttled. where <i>blade_number</i> 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 <i>blade_number</i> was instructed to power off due to power budget restrictions. where <i>blade_number</i> 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 <i>domain_number</i> . where <i>domain_number</i> 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 <i>domain_number</i> . where <i>domain_number</i> 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 90 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 90 for a list of error messages that apply to all commands.

Table 42. 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 <i>state</i> where <i>state</i> identifies the LED state that was returned.	Displays when an LED state other than on, off, or blinking is returned.
Identify: Unknown return status <i>status</i> where the <i>status</i> 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 <code>identify -h</code> for command help.

ifconfig command errors

The following table lists error messages for the ifconfig command. See “Common errors” on page 90 for a list of error messages that apply to all commands.

Table 43. 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).
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).

Table 43. *ifconfig* command errors (continued)

Error message	Definition
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 <i>option: ip_address</i> . Each byte has to be in the range (0-255) where: <ul style="list-style-type: none"> • <i>option</i> identifies the command option • <i>ip_address</i> 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: <i>xxx.xxx.xxx.xxx</i> , where each <i>xxx</i> is a number from 0 to 255.
Invalid IP arg for <i>option: ip_address</i> . Enter 4 bytes separated by 3 dots where: <ul style="list-style-type: none"> • <i>option</i> identifies the command option • <i>ip_address</i> 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: <i>xxx.xxx.xxx.xxx</i> , where each <i>xxx</i> is a number from 0 to 255.
Invalid IP arg for <i>option: ip_address</i> . Too few bytes where: <ul style="list-style-type: none"> • <i>option</i> identifies the command option • <i>ip_address</i> 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: <i>xxx.xxx.xxx.xxx</i> , where each <i>xxx</i> is a number from 0 to 255.
Invalid IP arg for <i>option: ip_address</i> . Too many bytes where: <ul style="list-style-type: none"> • <i>option</i> identifies the command option • <i>ip_address</i> 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: <i>xxx.xxx.xxx.xxx</i> , where each <i>xxx</i> is a number from 0 to 255.
Invalid hostname arg for <i>option: hostname</i> . Consecutive dots where: <ul style="list-style-type: none"> • <i>option</i> identifies the command option • <i>hostname</i> identifies the invalid hostname argument 	Displays when the user tries to enter consecutive periods (.) as part of a hostname.
Invalid hostname arg for <i>option: hostname</i> . Length has to be < 64 characters where: <ul style="list-style-type: none"> • <i>option</i> identifies the command option • <i>hostname</i> identifies the invalid hostname argument 	Displays when the user tries to enter a hostname longer than 63 characters.
Invalid hostname arg for <i>option: hostname</i> . Only alphanumeric chars and <i>._-</i> allowed where: <ul style="list-style-type: none"> • <i>option</i> identifies the command option • <i>hostname</i> identifies the invalid hostname argument 	Displays when the user tries to enter a hostname that contains invalid characters. Valid characters that can be used in a hostname are letters, numbers, periods (.), dashes (-), and underscores (_).

Table 43. *ifconfig* command errors (continued)

Error message	Definition
Invalid ip address.	Displays for one of the following errors: <ul style="list-style-type: none"> 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 <i>option: address</i> . Invalid syntax where: <ul style="list-style-type: none"> <i>option</i> identifies the command option <i>address</i> identifies the invalid MAC address argument 	Displays when the user tries to enter an invalid MAC address.
Invalid MAC arg for <i>option: address</i> . Multicast addresses not allowed where: <ul style="list-style-type: none"> <i>option</i> identifies the command option <i>address</i> identifies the invalid MAC address argument 	Displays when the user tries to enter a multicast address.
Invalid MAC arg for <i>option: address</i> . Too few bytes where: <ul style="list-style-type: none"> <i>option</i> identifies the command option <i>address</i> identifies the invalid MAC address argument 	Displays when the user tries to enter a MAC address with too few bytes.
Invalid MAC arg for <i>option: address</i> . Too many bytes where: <ul style="list-style-type: none"> <i>option</i> identifies the command option <i>address</i> 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 <code>ifconfig -i <ip address> -T system:blade[x]:sp</code> 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 90 for a list of error messages that apply to all commands.

Table 44. *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.

list command errors

The following table lists error messages for the list command. See “Common errors” on page 90 for a list of error messages that apply to all commands.

Table 45. 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.

power command errors

The following table lists error messages for the power command. See “Common errors” on page 90 for a list of error messages that apply to all commands.

Table 46. 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: <i>hex_code</i> where the <i>hex_code</i> 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 <i>hex_code</i> value.

reset command errors

The following table lists error messages for the reset command. See “Common errors” on page 90 for a list of error messages that apply to all commands.

Table 47. 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.

smtp command errors

The following table lists error messages for the smtp command. See “Common errors” on page 90 for a list of error messages that apply to all commands.

Table 48. 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 90 for a list of error messages that apply to all commands.

Table 49. 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 90 for a list of error messages that apply to all commands.

Table 50. 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 50. 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 a 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.

tcpcmdmode command errors

The following table lists error messages for the tcpcmdmode command. See “Common errors” on page 90 for a list of error messages that apply to all commands.

Table 51. tcpcmdmode command errors

Error message	Definition
-on and -off cannot be used in the same command.	Displays when a user tries to enable and disable TCP command mode in the same command.
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 90 for a list of error messages that apply to all commands.

Table 52. 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.

thres command errors

The following table lists error messages for the thres command. See “Common errors” on page 90 for a list of error messages that apply to all commands.

Table 53. thres command errors

Error message	Definition
Invalid threshold value.	Displays when an invalid threshold value is entered.
Unable to query the threshold request.	Displays when an internal error occurs while processing the query threshold request.
Unable to set the requested threshold.	Displays when an internal error occurs while setting an threshold.

update command errors

The following table lists error messages for the update command. See “Common errors” on page 90 for a list of error messages that apply to all commands.

Table 54. update command errors

Error message	Definition
Flash operation failed.	Displays when an internal error occurs during flash firmware update.
Flash operation failed status <i>percentage</i> where the <i>percentage</i> 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 <i>percentage</i> where the <i>percentage</i> value varies based on when the problem was encountered.	Displays when an internal error occurs during flash firmware update.
Flash preparation - error sending packet file <i>filename</i> where the <i>filename</i> value varies based on the file being updated.	Displays when an internal error occurs during flash firmware update.
Flash preparation error.Packet percent complete <i>percentage</i> . Flash percent complete <i>percentage</i> . where the <i>percentage</i> 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 <i>percentage</i> where the <i>percentage</i> 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: <ul style="list-style-type: none"> 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 <i>bay_number</i> is not installed. where the <i>bay_number</i> 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.

Table 54. update command errors (continued)

Error message	Definition
TFTP Error <i>error_code</i> where the <i>error_code</i> 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.
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 <i>bay_number name</i> . where the <i>bay_number</i> and <i>name</i> 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 <i>bay_number name</i> . where the <i>bay_number</i> and <i>name</i> 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 <i>bay_number name</i> . where the <i>bay_number</i> and <i>name</i> 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 90 for a list of error messages that apply to all commands.

Table 55. 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, <code>uplink -del 0</code> .

users command errors

The following table lists error messages for the users command. See “Common errors” on page 90 for a list of error messages that apply to all commands.

Table 56. 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.
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 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: <i>permission</i> where the <i>permission</i> value varies based on the problem that was encountered.	Displays when a user tries to specify an invalid login permission for the <code>-a</code> command option.
Invalid argument. Valid arguments for <code>-at</code> are read, write, and traps.	Displays when a user tries to set an invalid argument for the <code>-at</code> command option.
Invalid argument. Valid choices are des or <none>.	Displays when a user tries to set an invalid argument for the <code>-pp</code> command option.

Table 56. users command errors (continued)

Error message	Definition
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: <ul style="list-style-type: none"> • 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 hostname or ip address.	Displays when a user tries to set an invalid host name or IP address for the -i command option.
Invalid username. The username can only contain numbers, letters, dots, and underscores.	Displays when the user tries to enter a 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.
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.

Table 56. users command errors (continued)

Error message	Definition
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.

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 @server or IntelliStation® system 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.

Note: For some IntelliStation models, the *Hardware Maintenance Manual and Troubleshooting Guide* is available only from the IBM support Web site.

- Go to the IBM support Web site at <http://www.ibm.com/pc/support/> to check for technical information, hints, tips, and new device drivers or to submit a request for information.

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 @server and IntelliStation systems also describes the diagnostic tests that you can perform. Most @server and IntelliStation 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 operating system or program.

Using the documentation

Information about your IBM @server or IntelliStation 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/pc/support/> and follow the instructions. Also, some documents are available through the IBM Publications Ordering System at <http://www.elink.ibm.com/public/applications/publications/cgibin/pbi.cgi>.

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 @server and IntelliStation systems, optional devices, services, and support. The address for IBM xSeries® and BladeCenter information is <http://www.ibm.com/eserver/xseries/>. The address for IBM IntelliStation information is <http://www.ibm.com/pc/us/intellistation/>.

You can find service information for IBM systems and optional devices at <http://www.ibm.com/pc/support/>.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with xSeries servers, BladeCenter products, IntelliStation workstations, and appliances. 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.

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.

Edition notice

© Copyright International Business Machines Corporation 2005. All rights reserved.

U.S. Government Users Restricted Rights — Use, duplication, or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Trademarks

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

Active Memory	Predictive Failure Analysis
Active PCI	PS/2
Active PCI-X	ServeRAID
Alert on LAN	ServerGuide
BladeCenter	ServerProven
C2T Interconnect	TechConnect
Chipkill	ThinkPad
EtherJet	Tivoli
e-business logo	Tivoli Enterprise
@server	Update Connector
FlashCopy	Wake on LAN
IBM	XA-32
IBM (logo)	XA-64
IntelliStation	X-Architecture
NetBAY	XcelL4
Netfinity	XpandOnDemand
NetView	xSeries
OS/2 WARP	

Intel, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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-ROM 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.

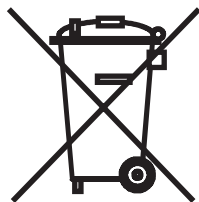
IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven[®], including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

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>.



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'étiquette 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.

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.

In the Netherlands, the following applies.



For Taiwan: Please recycle batteries.



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

聲 明
此為 A 級產品。在生活環境中，該產品可能會造成無線電干擾。在這種情況下，可能需要用戶對其干擾採取切实可行的措施。

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

! 19
? 18

A

accumulate timeout
 set for SOL 51
acknowledge alarms
 alarm ID 82
 complete alarm key 82
 generator ID 81
 generator information 81
alarm 79
 acknowledge (alarm ID) 82
 acknowledge (complete alarm key) 82
 acknowledge (generator ID) 81
 acknowledge (generator information) 81
 clear (alarm ID) 83
 clear (complete alarm key) 83
 clear (generator ID) 82
 clear (generator information) 83
 display (alarm ID) 80
 display (all) 79
 display (complete alarm key) 81
 display (generator ID) 80
 display (generator information) 80
 display (power) 79
 options
 c, a 83
 c, g 82
 c, k 83
 c, o 83
 p 79
 q, a 80
 q, g 80
 q, k 81
 q, o 80
 r, a 82
 r, g 81
 r, k 82
 r, o 81
 s, l 84
 set 84
alarm command 79
alarm command errors 91
alarm commands
 example 84
alert notification method, set 34
alert recipient, create 32, 33
alert recipient, delete 31
alert recipient, set email address 34
alert recipient, set hostname for alerts 35
alert recipient, set IP address for alerts 35
alert recipient, set name 33
alert recipient, set status 33
alert recipients, manage 30

alert type, filter 34
alert type, set 34
alertentries 30
 options
 1 through 12 30
 create (n, status, f, t, e, i) 32
 del 31
 e 34
 f 34
 i 35
 n 33
 status 33
 t 34
alertentries command 30
alertentries command errors 92
alertentries commands
 example 35
alerts, display 22
algorithms, encryption 12
attributes, display for firmware 27
authority, command 5

B

blade server
 boot 69, 70
 boot (to console) 69
 command target 16
 cycle power 69, 73
 display power state 73
 power off 73
 power on 73
 power on (to console) 73
 reset 69, 70, 75
 reset (clear NVRAM) 76
 reset (run diagnostics with boot sequence) 77
 reset (run diagnostics) 76
 reset (to console) 69, 75
 reset (with NMI) 76
 turn off 73
 turn on 73
 turn on (to console) 73
blade servers
 set starting IP address 43
BladeCenter T specific commands 79, 89
BladeCenter unit
 command target 16
blink location LED 24
boot 69
 blade server 69, 70
 options
 -p powercycle 69
 -p reset 70
 c 69
boot (to console)
 blade server 69
boot command errors 92
boot commands 69

boot commands *(continued)*

example 70

built-in commands 16, 20

C

change command environment 15, 16

Class A electronic emission notice 113

clear

options

config 36

clear alarms

alarm ID 83

complete alarm key 83

generator ID 82

generator information 83

clear command 36

clear command errors 92

clear commands

example 36

clear event log

management module 67

clear management module event log commands 67

example 67

clearlog

example 67

clearlog command errors 93

clearlog commands 67

example 67

CLI key sequence

set for SOL 52

command

health 21, 22

system physical configuration 20

command authority 5

command environment selecting 4

command history 19

command redirect 15, 16

command target 15, 16

blade server 16

BladeCenter unit 16

I/O module 17

integrated system management processor 17

management module 16

switch module 17

temporary 4

view 20

command target selection 4

command-line interface

guidelines 3

case sensitivity 3

command history 4

data types 3

delimiters 4

help 4

options 3

output format 4

strings 4

starting 12

using 3, 15

commands

alarm 79, 84

alertentries 30, 35

boot 69, 70

built-in 16, 20

clear 36

clear management module event log 67

clearlog 67

commands

management module failover 56

common 21, 29

configuration 30, 66

console 78

dhcpinfo 37

display management module event log 68

displaylog 68

dns 38

environment 16, 17

event log, clear for management module 67

event log, display for management module 68

examples

alarm 84

alertentries 35

boot 70

clear 36

clear management module event log 67

clearlog 67

console 78

DHCP settings for management module 37

dhcpinfo 37

display management module event log 68

displaylog 68

DNS 38

env 17

environment 17

environment redirect 17

Ethernet network settings for management

module 43

exit 78

fuelg 71

health 22

help 18

history 19

identify 24

ifconfig 43

info 26

list 20

management module DHCP settings 37

management module DNS 38

management module Ethernet network

settings 43

management module event log clear 67

management module event log display 68

management module SMTP settings 44

management module SNMP settings 49

management module telnet configuration 55

management module uplink failover 56

power 74

reset 77

Serial Over LAN 53

smtp 44

- commands *(continued)*
 - examples *(continued)*
 - SMTP settings for management module 44
 - snmp 49
 - SNMP settings for management module 49
 - sol 53
 - syntax help 18
 - tcpcmdmode 54
 - telnetcfg 55
 - thres 88
 - update 28
 - uplink 56
 - users 66
 - exit 78
 - fuelg 70, 71
 - help 18
 - history 19
 - identify 24
 - ifconfig 40, 43
 - info 26
 - list 20
 - management module event log 67, 69
 - management module failover 55
 - power 73, 74
 - power control 69, 77
 - reset 75, 77
 - reset command 69, 77
 - Serial Over LAN 50, 53
 - session command 78, 79
 - smtp 43, 44
 - snmp 45, 49
 - SOL 50, 53
 - system management command 79, 89
 - tcpcmdmode 53, 54
 - telnet configuration 54, 55
 - telnetcfg 54, 55
 - thres 85, 88
 - update 27, 28
 - uplink 55, 56
 - users 57, 66
- common commands 21, 29
- common errors 90
- communicating with IBM Director 53
- communication
 - out-of-band 53
- component information 26
- component information display 26
- configuration
 - view for management module 20
 - view tree for system 20
- configuration commands 30, 66
- configuration method
 - set for channel 0 of management module 41
- console 78
 - create override SOL session 78
 - create SOL session 78
 - options
 - o 78
- console command 78
- console command errors 93

- console commands
 - example 78
- create alert recipient 32, 33
- create override SOL session 78
- create SOL session 78
- create user 58, 59
- cycle power
 - blade server 69, 73
 - I/O module 73
 - switch module 73

D

- data rate
 - set for channel 0 of management module 41
- delete alert recipient 31
- delete user 57
- DHCP settings for management module commands
 - example 37
- dhcpinfo
 - options
 - eth0 37
- dhcpinfo command errors 93
- dhcpinfo commands 37
 - example 37
- disable
 - TCP command mode 54
- disable DNS
 - management module 38
- disable power domain quiet mode 71
- disable SNMP agent
 - management module (SNMPv1) 45
 - management module (SNMPv3) 45
- disable SNMP traps
 - management module 46
- disable SOL
 - global 51
- disable uplink failover
 - management module 56
- display
 - TCP command-mode session status 53
 - TCP command-mode session timeout 53
- display (reset counter) event log
 - management module 68
- display alarms
 - alarm ID 80
 - all 79
 - complete alarm key 81
 - generator ID 80
 - generator information 80
 - power 79
- display alert properties (all recipients) 30
- display alert properties (single recipient) 30
- display alerts 22
- display all users 57
- display component information 26
- display DNS configuration
 - management module 38
- display Ethernet channel 0 configuration
 - management module 40

- display Ethernet channel 0 DHCP configuration management module 37
- display Ethernet channel 1 configuration management module 41
- display event log management module 68
- display failover configuration management module 55
- display firmware attributes 27
- display health status 21, 22
- display health status (tree) 21
- display management module event log commands 68
 - example 68
- display POST status
 - I/O module 74
 - switch module 74
- display power domain information details 70
- display power domain information overview 70
- display power state
 - blade server 73
 - I/O module 73
 - switch module 73
- display single user 57
- display SMTP server host name management module 43
- display SMTP server IP address management module 43
- display SNMP configuration management module 45
- display state
 - location LED 24
- display telnet configuration management module 54
- display telnet timeout management module 55
- display threshold (specific) 85
- display uplink configuration management module 55
- displaylog 68
 - options
 - f 68
- displaylog command errors 93
- displaylog commands 68
 - example 68
- dns 38
 - options
 - i1 38
 - i2 38
 - i3 38
 - off 38
 - on 38
- DNS
 - disable for management module 38
 - enable for management module 38
- dns command errors 94
- dns commands 38
 - example 38
- DNS configuration
 - display for management module 38
- DNS first IP address
 - set for management module 38

- DNS second IP address
 - set for management module 38
- DNS third IP address
 - set for management module 38
- duplex mode
 - set for channel 0 of management module 41

E

- electronic emission Class A notice 113
- enable
 - TCP command mode 54
- enable DNS
 - management module 38
- enable power domain quiet mode 71
- enable SNMP agent
 - management module (SNMPv1) 45
 - management module (SNMPv3) 45
- enable SNMP traps
 - management module 46
- enable SOL
 - global 51
- enable uplink failover
 - management module 56
- encryption algorithms 12
- end session 78
- ending an SOL session 14, 78
- env 16
 - options
 - blade 16, 17
 - switch 17
 - system (management module) 16
- env command errors 90
- env commands
 - example 17
- environment
 - blade server 16
 - BladeCenter unit 16
 - I/O module 17
 - integrated system management processor 17
 - management module 16
 - switch module 17
- environment commands 16
 - example 17
- errors
 - alarm command 91
 - alertentries command 92
 - boot command 92
 - clear command 92
 - clearlog command 93
 - common 90
 - console command 93
 - dhcinfo command 93
 - displaylog command 93
 - dns command 94
 - env command 90
 - exit command 90
 - fuelg command 94
 - health command 94
 - help command 90
 - history command 90

- errors *(continued)*
 - identify command 95
 - ifconfig command 95
 - info command 97
 - list command 98
 - power command 98
 - reset command 98
 - smtp command 99
 - snmp command 99
 - sol command 99
 - tpcmdmode command 101
 - telnetcfg command 101
 - thres command 101
 - update command 102
 - uplink command 104
 - users command 104
- Ethernet channel 0 configuration
 - display for management module 40
- Ethernet channel 0 configuration method
 - set for management module 41
- Ethernet channel 0 data rate
 - set for management module 41
- Ethernet channel 0 DHCP configuration
 - display for management module 37
- Ethernet channel 0 duplex mode
 - set for management module 41
- Ethernet channel 0 gateway IP address
 - set for management module 40
- Ethernet channel 0 hostname
 - set for management module 40
- Ethernet channel 0 MAC address
 - set for management module 41
- Ethernet channel 0 MTU
 - set for management module 41
- Ethernet channel 0 static IP address
 - set for management module 40
- Ethernet channel 0 subnet mask
 - set for management module 40
- Ethernet channel 1
 - disable for management module 42
 - enable for management module 42
- Ethernet channel 1 configuration
 - display for management module 41
- Ethernet channel 1 gateway IP address
 - set for management module 42
- Ethernet channel 1 MAC address
 - set for management module 42
- Ethernet channel 1 static IP address
 - set for management module 42
- Ethernet channel 1 subnet mask
 - set for management module 42
- Ethernet network settings for management module
 - commands
 - example 43
- event log
 - clear for management module 67
 - display (reset counter) for management module 68
 - display for management module 68
- event log, clear for management module
 - commands 67

- event log, display for management module
 - commands 68
- exit 78
- exit command 78
- exit command errors 90
- exit commands
 - example 78

F

- failover configuration
 - display for management module 55
- FCC Class A notice 113
- filter alert type 34
- firmware
 - display attributes 27
 - update 27
 - update (verbose) 28
- firmware requirements 2
- firmware update 27
- flash location LED 24
- fuelg 70
 - options
 - os 71
 - qm 71
- fuelg command errors 94
- fuelg commands 70
 - example 71

G

- gateway IP address
 - set for channel 0 of management module 40
 - set for channel 1 of management module 42
- global disable
 - SOL 51
- global enable
 - SOL 51
- guidelines
 - case sensitivity 3
 - command history 4
 - data types 3
 - delimiters 4
 - help 4
 - options 3
 - output format 4
 - overview of 3
 - strings 4

H

- hardware requirements 2
- health 21
 - display status 21
 - display status (tree) 21
 - display status and alerts 22
 - options
 - f 22
 - l 21
- health command 21, 22
 - example 22

- health command errors 94
- help 15, 18
- help command 18
- help command errors 90
- help commands
 - example 18
- help for update command 27
- history 19
- history command 19
- history command errors 90
- history commands
 - example 19
- host name
 - set for channel 0 of management module 40

I

- I/O module
 - command target 17
 - cycle power 73
 - display POST status 74
 - display power state 73
 - power off 73
 - power on 73
 - reset 75
 - reset (extended diagnostics) 76
 - reset (full diagnostics) 76
 - reset (standard diagnostics) 75
 - reset configuration 36
 - turn off 73
 - turn on 73

- IBM Director
 - communication 53

- identify 24
 - options
 - blink 24
 - off 24
 - on 24
 - s 24

- identify command 24

- identify command errors 95

- identify commands
 - example 24

- ifconfig

- options
 - eth0 40
 - eth0, c 41
 - eth0, d 41
 - eth0, g 40
 - eth0, i 40
 - eth0, l 41
 - eth0, m 41
 - eth0, n 40
 - eth0, r 41
 - eth0, s 40
 - eth1 41
 - eth1, down 42
 - eth1, g 42
 - eth1, i 42
 - eth1, l 42
 - eth1, s 42

- ifconfig (*continued*)
 - options (*continued*)
 - eth1, up 42
 - i 43

- ifconfig command errors 95

- ifconfig commands 40
 - example 43

- info 26

- info command 26

- info command errors 97

- info commands
 - example 26

- information about components 26

- information display, component 26

- information display, power domain (detailed) 70

- information display, power domain (overview) 70

- integrated system management processor

- command target 17

- IP address

- set starting for blade servers 43

- ISMP

- reset 75

J

- JS20 blade server commands

- reset (clear NVRAM) 76

- reset (run diagnostics with boot sequence) 77

- reset (run diagnostics) 76

- reset (with NMI) 76

L

- LED (location), control 24

- light location LED 24

- light location LED (BladeCenter unit)

- time period 24

- list 20

- options

- l 20

- list command

- example 20

- list command errors 98

- location LED

- blink 24

- display state 24

- flash 24

- light 24

- light (BladeCenter unit)

- time period 24

- turn off 24

- location LED control 24

M

- MAC address

- set for channel 0 of management module 41

- set for channel 1 of management module 42

- manage alert recipients 30

- management module

- clear event log 67

management module (*continued*)

- clear event log commands
 - example 67
- command target 16
- create alert recipient 32, 33
- create user 58, 59
- delete alert recipient 31
- delete user 57
- DHCP settings commands
 - example 37
- dhcpinfo commands 37
- disable DNS 38
- disable Ethernet channel 1 42
- disable SNMP agent (SNMPv1) 45
- disable SNMP agent (SNMPv3) 45
- disable SNMP traps 46
- disable uplink failover 56
- display (reset counter) event log 68
- display alert properties (all recipients) 30
- display alert properties (single recipient) 30
- display all users 57
- display DNS configuration 38
- display Ethernet channel 0 configuration 40
- display Ethernet channel 0 DHCP configuration 37
- display Ethernet channel 1 configuration 41
- display event log 68
- display event log commands
 - example 68
- display single user 57
- display SMTP server host name 43
- display SMTP server IP address 43
- display SNMP configuration 45
- dns commands 38
 - example 38
- enable DNS 38
- enable Ethernet channel 1 42
- enable SNMP agent (SNMPv1) 45
- enable SNMP agent (SNMPv3) 45
- enable SNMP traps 46
- enable uplink failover 56
- Ethernet network settings commands
 - example 43
- failover configuration 55
- filter alert type 34
- IBM Director communication 53
- ifconfig commands 40, 43
- reset 75
- reset (failover) 75
- reset configuration 36
- set alert notification method 34
- set alert recipient email address 34
- set alert recipient name 33
- set alert recipient status 33
- set alert type 34
- set DNS first IP address 38
- set DNS second IP address 38
- set DNS third IP address 38
- set Ethernet channel 0 configuration method 41
- set Ethernet channel 0 data rate 41
- set Ethernet channel 0 duplex mode 41
- set Ethernet channel 0 gateway IP address 40

management module (*continued*)

- set Ethernet channel 0 hostname 40
- set Ethernet channel 0 MAC address 41
- set Ethernet channel 0 MTU 41
- set Ethernet channel 0 static IP address 40
- set Ethernet channel 0 subnet mask 40
- set Ethernet channel 1 gateway IP address 42
- set Ethernet channel 1 MAC address 42
- set Ethernet channel 1 static IP address 42
- set Ethernet channel 1 subnet mask 42
- set hostname for alerts 35
- set IP address for alerts 35
- set privacy password (SNMPv3) 65
- set server host name 44
- set server IP address 44
- set SNMP community 1 first host name 46
- set SNMP community 1 IP address (first host) 46
- set SNMP community 1 IP address (second host) 46
- set SNMP community 1 IP address (third host) 46
- set SNMP community 1 name 46
- set SNMP community 1 second host name 46
- set SNMP community 1 third host name 46
- set SNMP community 1 view type (SNMPv3) 47
- set SNMP community 2 first host name 47
- set SNMP community 2 IP address (first host) 47
- set SNMP community 2 IP address (second host) 47
- set SNMP community 2 IP address (third host) 47
- set SNMP community 2 name 47
- set SNMP community 2 second host name 47
- set SNMP community 2 third host name 47
- set SNMP community 2 view type (SNMPv3) 48
- set SNMP community 3 first host name 48
- set SNMP community 3 IP address (first host) 48
- set SNMP community 3 IP address (second host) 48
- set SNMP community 3 IP address (third host) 48
- set SNMP community 3 name 48
- set SNMP community 3 second host name 48
- set SNMP community 3 third host name 48
- set SNMP community 3 view type (SNMPv3) 49
- set SNMP contact name 49
- set SNMP location 49
- set user access type (SNMPv3) 65
- set user authentication protocol (SNMPv3) 64
- set user authority level 61, 62, 63
- set user context name (SNMPv3) 64
- set user hostname (SNMPv3 traps) 65
- set user IP address (SNMPv3 traps) 65
- set user name 60
- set user password 60
- set user privacy protocol (SNMPv3) 64
- smtp commands 43, 44
- SMTP settings commands
 - example 44
- snmp commands 45, 49
- SNMP settings commands
 - example 49
- telnet configuration 54
- telnet timeout 55

- management module (*continued*)
 - uplink configuration 55
 - uplink failover delay 56
 - view configuration 20
- management module event log commands 67, 69
- management module failover commands 55
- management module telnet configuration commands
 - example 55
- management module uplink failover commands
 - example 56
- management module, user accounts 57
- management-module firmware 2
- MTU
 - set for channel 0 of management module 41

N

- notes, important 110
- notices
 - electronic emission 113
 - FCC, Class A 113
- notification method, set for alerts 34

O

- online documentation 1
- out-of-band communication, IBM Director 53
- override persistent command environment 4
- oversubscription policy, power domain (set) 71

P

- persistent command environment
 - override 4
- persistent command target 4
- POST status
 - display for I/O module 74
 - display for switch module 74
- power
 - options
 - cycle 73
 - cycle, c 73
 - off 73
 - on 73
 - on, c 73
 - state 73
 - state, post 74
- power command errors 98
- power commands 73
 - example 74
- power control commands 69, 77
- power domain
 - disable quiet mode 71
 - enable quiet mode 71
- power domain information display (detailed) 70
- power domain information display (overview) 70
- power domain oversubscription policy, set 71
- power off
 - blade server 73
 - I/O module 73
 - switch module 73

- power on
 - blade server 73
 - I/O module 73
 - switch module 73
- power on (to console)
 - blade server 73
- power state
 - display for blade server 73
 - display for I/O module 73
 - display for switch module 73
- primary management module 5

Q

- quiet mode, disable 71
- quiet mode, enable 71

R

- redirect command 15, 16
- redundant management modules 5
- required, firmware 2
- required, hardware 2
- reset 75
 - blade server 69, 70, 75
 - I/O module 75
 - ISMP 75
 - management module 75
 - options
 - c 75
 - clr 76
 - ddg 77
 - dg 76
 - exd 76
 - f 75
 - full 76
 - sft 76
 - std 75
 - switch module 75
- reset (clear NVRAM)
 - blade server 76
- reset (extended diagnostics)
 - I/O module 76
 - switch module 76
- reset (failover)
 - management module 75
- reset (full diagnostics)
 - I/O module 76
 - switch module 76
- reset (run diagnostics with boot sequence)
 - blade server 77
- reset (run diagnostics)
 - blade server 76
- reset (standard diagnostics)
 - I/O module 75
 - switch module 75
- reset (to console)
 - blade server 69, 75
- reset (with NMI)
 - blade server 76

- reset blase server key sequence
 - set for SOL 52
- reset command 69, 77
- reset command errors 98
- reset commands 75
 - example 77
- reset configuration
 - I/O module 36
 - management module 36
 - switch module 36
- reset default configuration 36
- responding to thermal events 71
- retry count
 - set for SOL 51
- retry interval
 - set for SOL 50

S

- 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 51
- Serial Over LAN 13
- Serial Over LAN commands 50
 - example 53
- server host name
 - set for management module 44
- server IP address
 - set for management module 44
- session command 78, 79
- set
 - TCP command-mode session timeout 53
- set accumulate timeout
 - SOL 51
- set alarm 84
- set alert notification method 34
- set alert recipient email address 34
- set alert recipient name 33
- set alert recipient status 33
- set alert type 34
- set CLI key sequence
 - SOL 52
- set DNS first IP address
 - management module 38
- set DNS second IP address
 - management module 38
- set DNS third IP address
 - management module 38
- set Ethernet channel 0 configuration method
 - management module 41
- set Ethernet channel 0 data rate
 - management module 41
- set Ethernet channel 0 duplex mode
 - management module 41
- set Ethernet channel 0 gateway IP address
 - management module 40
- set Ethernet channel 0 hostname
 - management module 40
- set Ethernet channel 0 MAC address
 - management module 41
- set Ethernet channel 0 MTU
 - management module 41
- set Ethernet channel 0 static IP address
 - management module 40
- set Ethernet channel 0 subnet mask
 - management module 40
- set Ethernet channel 1 gateway IP address
 - management module 42
- set Ethernet channel 1 MAC address
 - management module 42
- set Ethernet channel 1 static IP address
 - management module 42
- set Ethernet channel 1 subnet mask
 - management module 42
- set hostname for alerts 35
- set IP address for alerts 35
- set power domain oversubscription policy 71
- set privacy password (SNMPv3) 65
- set reset blase server key sequence
 - SOL 52
- set retry count
 - SOL 51
- set retry interval
 - SOL 50
- set send threshold
 - SOL 51
- set server host name
 - management module 44
- set server IP address
 - management module 44
- set SNMP community 1 first host name
 - management module 46
- set SNMP community 1 IP address (first host)
 - management module 46
- set SNMP community 1 IP address (second host)
 - management module 46
- set SNMP community 1 IP address (third host)
 - management module 46
- set SNMP community 1 name
 - management module 46
- set SNMP community 1 second host name
 - management module 46
- set SNMP community 1 third host name
 - management module 46
- set SNMP community 1 view type (SNMPv3)
 - management module 47
- set SNMP community 2 first host name
 - management module 47
- set SNMP community 2 IP address (first host)
 - management module 47
- set SNMP community 2 IP address (second host)
 - management module 47
- set SNMP community 2 IP address (third host)
 - management module 47
- set SNMP community 2 name
 - management module 47

- set SNMP community 2 second host name
 - management module 47
- set SNMP community 2 third host name
 - management module 47
- set SNMP community 2 view type (SNMPv3)
 - management module 48
- set SNMP community 3 first host name
 - management module 48
- set SNMP community 3 IP address (first host)
 - management module 48
- set SNMP community 3 IP address (second host)
 - management module 48
- set SNMP community 3 IP address (third host)
 - management module 48
- set SNMP community 3 name
 - management module 48
- set SNMP community 3 second host name
 - management module 48
- set SNMP community 3 third host name
 - management module 48
- set SNMP community 3 view type (SNMPv3)
 - management module 49
- set SNMP contact name
 - management module 49
- set SNMP location
 - management module 49
- set starting IP address
 - blade servers 43
- set telnet timeout
 - management module 55
- set threshold 86, 87
- set uplink failover delay
 - management module 56
- set user access type (SNMPv3) 65
- set user authentication protocol (SNMPv3) 64
- set user authority level 61, 62, 63
- set user context name (SNMPv3) 64
- set user hostname (SNMPv3 traps) 65
- set user IP address (SNMPv3 traps) 65
- set user name 60
- set user password 60
- set user privacy protocol (SNMPv3) 64
- set VLAN ID
 - SOL 52
- smtp 43
 - options
 - s 44
- smtp command errors 99
- smtp commands 43
 - example 44
- SMTP server host name
 - display for management module 43
- SMTP server IP address
 - display for management module 43
- SMTP settings for management module commands
 - example 44
- snmp 45
 - options
 - a, off 45
 - a, on 45
 - a3, off 45
- snmp *(continued)*
 - options *(continued)*
 - a3, on 45
 - c1 46
 - c1i1 46
 - c1i2 46
 - c1i3 46
 - c2 47
 - c2i1 47
 - c2i2 47
 - c2i3 47
 - c3 48
 - c3i1 48
 - c3i2 48
 - c3i3 48
 - ca1 47
 - ca2 48
 - ca3 49
 - cn 49
 - l 49
 - t, off 46
 - t, on 46
 - SNMP agent
 - disable for management module (SNMPv1)
 - SNMPv1 45
 - disable for management module (SNMPv3)
 - SNMPv3 45
 - enable for management module (SNMPv1)
 - SNMPv1 45
 - enable for management module (SNMPv3)
 - SNMPv3 45
 - snmp command errors 99
 - snmp commands 45
 - example 49
 - SNMP community 1 first host name
 - set for management module 46
 - SNMP community 1 IP address (first host)
 - set for management module 46
 - SNMP community 1 IP address (second host)
 - set for management module 46
 - SNMP community 1 IP address (third host)
 - set for management module 46
 - SNMP community 1 name
 - set for management module 46
 - SNMP community 1 second host name
 - set for management module 46
 - SNMP community 1 third host name
 - set for management module 46
 - SNMP community 1 view type
 - set for management module (SNMPv3) 47
 - SNMP community 2 first host name
 - set for management module 47
 - SNMP community 2 IP address (first host)
 - set for management module 47
 - SNMP community 2 IP address (second host)
 - set for management module 47
 - SNMP community 2 IP address (third host)
 - set for management module 47
 - SNMP community 2 name
 - set for management module 47

- SNMP community 2 second host name
 - set for management module 47
- SNMP community 2 third host name
 - set for management module 47
- SNMP community 2 view type
 - set for management module (SNMPv3) 48
- SNMP community 3 first host name
 - set for management module 48
- SNMP community 3 IP address (first host)
 - set for management module 48
- SNMP community 3 IP address (second host)
 - set for management module 48
- SNMP community 3 IP address (third host)
 - set for management module 48
- SNMP community 3 name
 - set for management module 48
- SNMP community 3 second host name
 - set for management module 48
- SNMP community 3 third host name
 - set for management module 48
- SNMP community 3 view type
 - set for management module (SNMPv3) 49
- SNMP configuration
 - display for management module 45
- SNMP contact name
 - set for management module 49
- SNMP location
 - set for management module 49
- SNMP settings for management module commands
 - example 49
- SNMP traps
 - disable for management module 46
 - enable for management module 46
- SNMPv3
 - community 1 view type 47
 - community 2 view type 48
 - community 3 view type 49
 - privacy password 65
 - trap receiver IP address or hostname 65
 - user access type 65
 - user authentication protocol 64
 - user context name 64
 - user privacy protocol 64
- sol 50
 - options
 - c 51
 - e 52
 - i 50
 - r 52
 - s 51
 - status 51
 - t 51
 - v 52
- SOL 13, 14, 78
 - global disable 51
 - global enable 51
 - set accumulate timeout 51
 - set CLI key sequence 52
 - set reset base server key sequence 52
 - set retry count 51
 - set retry interval 50
- SOL (*continued*)
 - set send threshold 51
 - set VLAN ID 52
 - status 50
- sol command errors 99
- sol commands
 - example 53
- SOL commands 50
- SOL session
 - ending 14, 78
 - starting 13
- SSH clients 12
- SSH connection 13
- starting a session using SSH 13
- starting a session using Telnet 12
- starting an SOL session 13
- starting command-line interface 12
- static IP address
 - set for channel 0 of management module 40
 - set for channel 1 of management module 42
- status
 - SOL 50
- subnet mask
 - set for channel 0 of management module 40
 - set for channel 1 of management module 42
- switch module
 - command target 17
 - cycle power 73
 - display POST status 74
 - display power state 73
 - power off 73
 - power on 73
 - reset 75
 - reset (extended diagnostics) 76
 - reset (full diagnostics) 76
 - reset (standard diagnostics) 75
 - reset configuration 36
 - turn off 73
 - turn on 73
- syntax help 18
- syntax help commands
 - example 18
- system
 - view configuration tree 20
- system management command 79, 89
- system physical configuration command 20

T

- target 15, 16
- TCP command mode
 - disable 54
 - enable 54
- TCP command-mode session status
 - display 53
- TCP command-mode session timeout
 - display 53
 - set 53
- tcpcmdmode 53
 - options
 - off 54

- tcpcmdmode *(continued)*
 - options *(continued)*
 - on 54
 - t 53
- tcpcmdmode command errors 101
- tcpcmdmode commands 53
 - example 54
- telnet configuration
 - display for management module 54
- telnet configuration commands 54
- Telnet connection 12
- telnet timeout
 - display for management module 55
 - set for management module 55
- telnetcfg 54
 - options
 - t 55
- telnetcfg command errors 101
- telnetcfg commands 54
 - example 55
- temporary command target 4
- terminate session 78
- thermal event response 71
- thres
 - options
 - q 85
 - s 86, 87
- thres command 85
- thres command errors 101
- thres commands
 - example 88
- threshold
 - display (specific) 85
 - set 86, 87
- threshold command 85
- trademarks 110
- turn off
 - blade server 73
 - I/O module 73
 - switch module 73
- turn off location LED 24
- turn on
 - blade server 73
 - I/O module 73
 - switch module 73
- turn on (to console)
 - blade server 73

U

- United States electronic emission Class A notice 113
- United States FCC Class A notice 113
- update 27
 - options
 - a 27
 - i, n 27, 28
- update command 27
- update command errors 102
- update command help 27
- update commands
 - example 28
- update firmware 27
- update firmware (verbose) 28
- uplink 55
 - options
 - del 56
 - off 56
 - on 56
- uplink command errors 104
- uplink commands 55
 - example 56
- uplink configuration
 - display for management module 55
- uplink failover
 - disable for management module 56
 - enable for management module 56
- uplink failover delay
 - set for management module 56
- users 57
 - options
 - 1 through 12 57
 - a 61, 63
 - ap 64
 - at 65
 - clear 57
 - cn 64
 - create (n, p, a, cn, ap, pp, ppw, at, i) 58
 - i 65
 - n 60
 - p 60
 - pp 64
 - ppw 65
- users command 57
- users command errors 104
- users commands
 - example 66
- users, create 58, 59
- users, delete 57
- users, display (all) 57
- users, display (single) 57
- users, management module 57
- users, set access type (SNMPv3) 65
- users, set authentication protocol (SNMPv3) 64
- users, set authority level 61, 62, 63
- users, set context name (SNMPv3) 64
- users, set hostname (SNMPv3 traps) 65
- users, set IP address (SNMPv3 traps) 65
- users, set name 60
- users, set password 60
- users, set privacy password (SNMPv3) 65
- users, set privacy protocol (SNMPv3) 64
- using the command-line interface 3

V

- view command target 20
- VLAN ID
 - set for SOL 52



Part Number: 59P4363

Printed in USA

(1P) P/N: 59P4363

