BladeCenter Management Module
BladeCenter T Management Module

Command-Line Interface Reference Guide

BladeCenter Management Module
BladeCenter T Management Module

Command-Line Interface Reference Guide

Note: Before using this information and the product it supports, read the general information in "Getting help and technical assistance," on page 145 and "Notices" on page 147.

Fifteenth Edition (November 2008)

Contents

Chapter 1. Introduction

This topic provides a short introduction to the BladeCenter management module command-line interface. Information about the command-line interface for the advanced management module is in a separate document.

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

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

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

You access the management-module CLI by establishing a Telnet connection to the IP address of the management module or through a Secure Shell (SSH) connection. You can initiate connections from the client system by 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, Esc (, that terminates an SOL session.

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

Before you begin

The following hardware and software is required for the command-line interface:

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 service processor firmware level of version 1.00 or later. See the *IBM BladeCenter Serial Over LAN Setup Guide* for information.

Firmware:

Make sure that you are using the latest versions of device drivers, firmware, and BIOS code for your blade server, management module, and other BladeCenter components. Go to http://www.ibm.com/systems/

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

Accessibility features for the BladeCenter management module

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

Accessibility for the BladeCenter management module interface is provided through the command-line interface. The remote control video feed is not accessible to a screen reader.

The BladeCenter Information Center is accessibility-enabled. The accessibility features of the information center include:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers. (The Java access bridge must be installed to make Java applets available to the JAWS screen reader.)
- The attachment of alternative input and output devices

Keyboard navigation

This product uses standard Microsoft® Windows® navigation keys.

Related accessibility information

You can view the publications for IBM BladeCenter in Adobe® Portable Document Format (PDF) using the Adobe Acrobat® Reader. The PDFs are provided on a CD that is packaged with the product, or you can access them through the IBM BladeCenter Information Center.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Chapter 2. Using the command-line interface

This topic tells you how to use the management module command-line interface.

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

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 113. See the *IBM BladeCenter Serial Over LAN Setup Guide* for SOL setup instructions and the documentation for your operating system for information about commands that you can enter through an SOL connection.

Command-line interface guidelines

This topic gives general guidelines for using the BladeCenter command-line interface.

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. The following examples illustrate valid command option syntax:

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

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 you use the command-line interface:

- Case sensitivity

  All commands, command options, and predefined command option parameters are case sensitive.

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

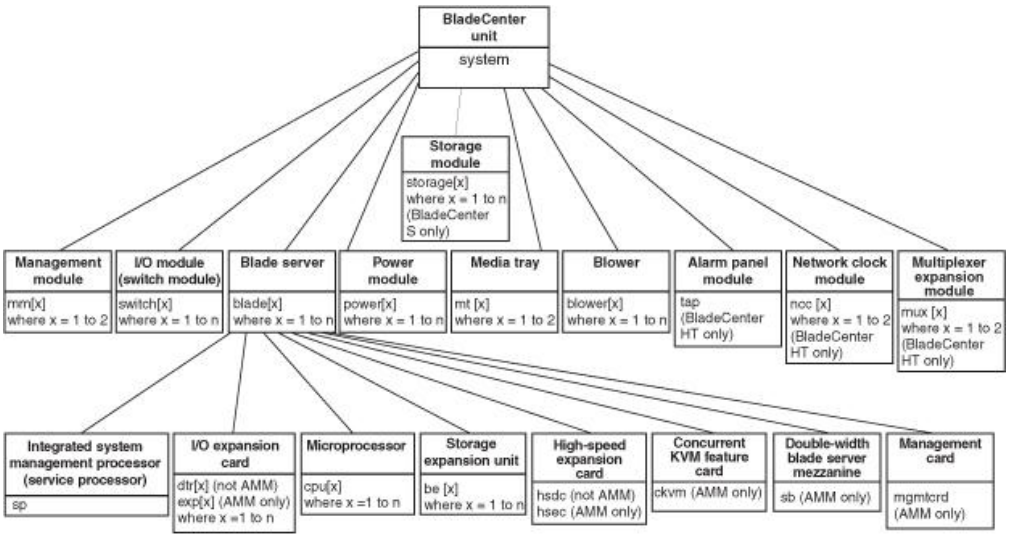
  The ip_address data type uses a predefined formatted string of xxx.xxx.xxx.xxx, where xxx is a number from 0 to 255.
- Delimiters
  - Options are delimited with a minus sign.
  - In a command that requires parameters, a single space is expected between an option and its parameter. Any additional spaces 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 that contain spaces must be enclosed in quotation marks, for example, `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 you entered.

Selecting the command target

This topic describes command targets and the persistent command environment.

You can use the command-line interface to target commands to the management module or to other devices in the BladeCenter unit. The command-line prompt indicates the persistent command environment: the environment in which commands are entered unless they are 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. This illustration shows command targets for all management module and BladeCenter unit types.



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 44). When you list the target as a command attribute by using the `-T` option, you change the target environment for the command that you are entering, temporarily overriding the persistent command environment. You can specify target environments by using the full path name or by using a partial path name that is 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 service processor in the blade server in blade server bay 3, when the persistent command environment is set to the blade server in blade server 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 always acts 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 by using the `list` command (see "list (system physical configuration) command" on page 69).

Commands and user authority

This topic lists command-line interface commands and the user authority levels needed to run them.

Some commands in the command-line interface can be executed only by users who are assigned a required level of authority. Users with Supervisor command authority can 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 execute all commands that display information.
- Users with Chassis Operator custom command authority can execute commands that display information about the common BladeCenter unit components.
- Users with Blade Operator custom command authority can execute commands that display information about the blade servers.
- Users with Switch Operator custom command authority can execute commands that display information about the I/O modules.

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

- The commands in this table apply only to the command variants that set values or cause an action: display variants of the commands do not require any special command authority.
- If a command requires only one command authority at a time, each of the applicable command authorities is indicated by a dot (•). If a command requires a combination of two or more command authorities, the applicable command authorities are indicate by ♢ or ‡. For example, the `boot -c` command is available to a user with the Supervisor command authority and to a user with both the Blade Administration and Blade Remote Presence command authorities.

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

Note: LDAP authority levels are not supported by the management-module Web interface.

Table 1. Command authority relationships

Command	Authority									
	Supervisor	Chassis Account Management	Chassis Log Management	Chassis Administration	Chassis Configuration	Blade Administration	Blade Configuration	Blade Remote Presence	I/O Module Administration	I/O Module Configuration
alarm -c, -r, -s	•				•		•			•
alarm -q -g	•					•		•		

Table 1. Command authority relationships (continued)

Command	Authority									
	Supervisor	Chassis Account Management	Chassis Log Management	Chassis Administration	Chassis Configuration	Blade Administration	Blade Configuration	Blade Remote Presence	I/O Module Administration	I/O Module Configuration
alertentries	•				•					
boot (blade server target)	•					•				
boot -c	•					◇		◇		
boot -p	•					•				
clear	•			◇	◇				‡	‡
clearlog	•		•							
clock	•				•					
config (blade server)	•						•			
config (management module)	•				•					
console	•							•		
dns	•				•					
fuelg	•				•					
identify	•				•		•			
ifconfig (blade server target)	•						•			
ifconfig (blade server ISMP, system targets)	•				•					
kvm -local	•				•					
mt -b	•							•		
mt -local, -remote	•				•					
power -on, -off, -softoff, -cycle	•					•				
power -on -c, -cycle -c	•					◇		◇		
reset (blade server or ISMP targets)	•					•				
reset (I/O module target)	•								•	
reset (management module target)	•			•						
reset -c, -clr, -dg, -ddg, -sft (blade server target)	•					◇		◇		
reset -exd, -full, -std (I/O module target)	•								•	

Table 1. Command authority relationships (continued)

Command	Authority									
	Supervisor	Chassis Account Management	Chassis Log Management	Chassis Administration	Chassis Configuration	Blade Administration	Blade Configuration	Blade Remote Presence	I/O Module Administration	I/O Module Configuration
reset -f (management module target)	•			•						
shutdown	•					•				
slp	•				•					
smtp	•				•					
snmp	•				•					
sol	•				•		•			
tcpcmdmode	•				•					
telnetcfg	•				•					
update (see Note 2)	•			•		•			•	
uplink	•				•					
users	•	•								

Note:

1. Firmware operations for the Server Connectivity Module for IBM BladeCenter require Chassis Administration authority.

Cabling the management module

This topic describes how to cable the management module.

You must connect a client system to the management module to configure and manage operation of the BladeCenter unit. All management modules support a remote management and console (Ethernet) connection.

You can manage the BladeCenter unit by using by using the command-line interface that you access through Telnet. You can also use the graphical user interface that is provided by the management-module Web interface to manage the BladeCenter unit and blade servers that support KVM. To make management connections to blade servers that do not support KVM, use an SOL session through the management-module command-line interface.

To access the management-module command-line interface, you need the following equipment and information:

- A system with Ethernet capability. To facilitate connections at multiple locations, you can use a notebook computer.
- The management-module MAC address (listed on the label on the management module).
- For networked connection to the management module, you need a standard Ethernet cable and a local Ethernet network port (facility connection).
- For direct connection of a system to the management-module remote management and console (Ethernet) connector, you need an Ethernet crossover cable.

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

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

Networked connection

This topic describes how to connect the management module to a network.

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

Direct connection

This topic tells you how to connect a client computer directly to the management module.

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

Starting the command-line interface

Access the management-module command-line interface from a client system 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, use a serial or SSH connection. SSH ensures that all data that is sent over the network is encrypted and secure.

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

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

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

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

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

- IP address: 192.168.70.125 (primary management module)
- IP address: 192.168.70.124 (standby management module)
- Subnet: 255.255.255.0
- User ID: USERID (all capital letters)
- Password: PASSW0RD (note the number zero, not the letter O, in PASSW0RD)

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

Telnet connection

This topic tells you how to establish a Telnet session with the management module.

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

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

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

Secure Shell (SSH) connection

This topic tell you how to establish a Secure Shell (SSH) connection with the management module.

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

1. Make sure that the SSH service on the network-management workstation is enabled. See your operating-system documentation for instructions.
2. Make sure that the SSH server on the BladeCenter management module is enabled. See the *BladeCenter Management Module User's Guide* for instructions.
3. Start an SSH session to the management module, using the SSH client of your choice. For example, if you are using the cygwin client, from a command prompt on the network-management workstation, type `ssh 192.168.70.125`, and press Enter. The IP address 192.168.70.125 is the default IP address of the management module; if a new IP address has been assigned to the management module, use that one instead.
4. Type the management-module user ID when you are prompted. At the password prompt, type the management-module password. The user ID and password are case sensitive and are the same as those that are used for management-module Web access. The default management-module user name is USERID, and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

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

Using the Secure Shell server

This topic tells you how to use the management module Secure Shell server.

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

- The SSH clients that are distributed with operating systems such as Linux, AIX®, and UNIX® (see your operating-system documentation for information).
- The SSH client of cygwin (see http://www.cygwin.com for information).

If you are using the Secure Shell client that is based on OpenSSH, such as the client that is included in Red Hat Linux version 7.3, to start an interactive command-line Secure Shell session to a management module with network address 192.168.70.2, type a command similar to the following example:

ssh -x -l USERID 192.168.70.2

where -x indicates no X Window System forwarding and -l indicates that the session is to use the login ID USERID.

BladeCenter unit configuration

You must configure the BladeCenter unit for command-line interface operation.

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

To communicate with network resources and with the I/O modules in the BladeCenter unit, you must configure IP addresses for the management module and I/O modules. You can configure management-module IP addresses by using the Web interface or command-line interface. You can configure the I/O modules through the management-module Web interface or through an external I/O-module port that is enabled through the management module, using a Telnet interface, or a Web browser. See the documentation that comes with each I/O module for information and instructions.

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

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

Configuring the management module

You must configure the management module for command-line interface operation.

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

If the management module that you installed is a replacement for the only management module in the BladeCenter unit and you saved the configuration file before you replaced the management module, you can apply the saved configuration file to the replacement management module. Management modules must have their configurations restored through the management-module Web interface (see the *BladeCenter Management Module User's Guide* for information).

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

- The external Ethernet (remote management) port (eth0) of the management module. The initial automatic management module configuration enables a remote console to connect to the management module to configure the port completely and to configure the rest of the BladeCenter unit.
- The internal Ethernet port (eth1) on the management module for communication with the I/O modules.

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

- If you have an accessible, active, and configured dynamic host configuration protocol (DHCP) server on the network, the IP address, gateway address, subnet mask, and DNS server IP address are set automatically. The host name is set to the management-module MAC address by default, and the domain server cannot change it.
- If the DHCP server does not respond within 2 minutes after the port is connected, the management module uses the factory-defined static IP address and default subnet address.

  Note: If the management-module DHCP setting is set to try the DHCP server and then use the static IP address, the management module uses the static IP address when the DHCP server is not available during management-module startup. When this occurs, the IP address might not be reachable if multiple management modules were started with the same static IP address.

Important: You cannot connect your system to the management module by using the factory-defined static IP address and default subnet address until at least 3 minutes after management-module startup.

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

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

1. Connect your system to the management-module command-line interface (see "Starting the command-line interface" on page 9 for more information).
2. Configure the internal Ethernet interface (eth1), using the **ifconfig** command (see "ifconfig command" on page 59 for instructions).

Notes:

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

Ethernet port, the I/O-module internal network interface and the management-module internal and external interfaces must be on the same subnet.

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

Starting an SOL session

After you start a Telnet or SSH session to the BladeCenter management module, you can start an SOL session to any individual blade server that supports SOL.

Note: Serial over LAN (SOL) must be enabled for both the BladeCenter unit and the blade server before you can start an SOL session with the blade server. See "sol (serial over LAN) command" on page 91 and the *BladeCenter Serial over LAN Setup Guide* for information about setting up and enabling SOL.

Because you can start up to 20 separate Web interface, Telnet, or SSH sessions to the BladeCenter management module, simultaneous SOL sessions can be active for each blade server installed in the BladeCenter unit.

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

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

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

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

See "sol (serial over LAN) command" on page 91 and the *IBM BladeCenter Serial over LAN Setup Guide* for information about configuring a blade server for SOL. See your operating-system documentation for information about SOL commands that you can enter by using the command-line interface.

Ending an SOL session

To end an SOL session, press Esc followed by an opening parenthesis.

When the SOL session ends, the command-line interface returns 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 topic contains command function, usage information, and examples.

Commands in "Command syntax" on page 17 are listed in alphabetic order. The commands are also listed in the following two topics:

- "Alphabetic command list"
- "Command list by function" on page 16

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.

Alphabetic command list

In alphabetic order, the commands are as follows:

Command list by function

By function, the commands are as follows:

- **Built-in commands**

  Use these commands to perform top-level functions within the command-line interface:
  - "env (environment) command" on page 44
  - "help command" on page 55
  - "history command" on page 57
  - "list (system physical configuration) command" on page 69

- **Common commands**

  Use these commands to monitor and control operation of BladeCenter components:
  - "health command" on page 52
  - "info (configuration information) command" on page 65

- **Configuration commands**

  Use these commands to view and configure network settings, Ethernet interfaces, and other functions:
  - "alertentries command" on page 23
  - "clock command" on page 32
  - "config command" on page 36
  - "dhcpinfo command" on page 40
  - "dns command" on page 42
  - "health command" on page 52
  - "ifconfig command" on page 59
  - "info (configuration information) command" on page 65
  - "kvm (keyboard, video, mouse) command" on page 67
  - "mt (media tray) command" on page 70
  - "slp command" on page 80
  - "smtp command" on page 81
  - "snmp command" on page 82
  - "sol (serial over LAN) command" on page 91
  - "tcpcmdmode command" on page 95
  - "telnetcfg (Telnet configuration) command" on page 97
  - "uplink (management module failover) command" on page 101
  - "users command" on page 103

- **Event log commands**

  Use these commands to view and clear primary management-module event log entries:
  - "clearlog command" on page 31
  - "displaylog command" on page 41
- **LED commands**

  Use these commands to monitor and control operation of BladeCenter unit LEDs:
  - "identify (location LED) command" on page 58
- **Memory commands**

  Use these commands to reset the management-module configuration and perform firmware updates:
  - "clear command" on page 30
  - "update (update firmware) command" on page 98
- **Power-control commands**

  Use these commands to control operation of the BladeCenter unit, blade servers, and I/O (switch) modules:
  - "boot command" on page 29
  - "power command" on page 72
  - "reset command" on page 76
  - "shutdown command" on page 79
- **Power-management commands**

  Use these commands to monitor power consumption of the BladeCenter unit and installed components:
  - "fuelg command" on page 49
- **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" on page 39
  - "exit command" on page 48
- **Systems-management commands (BladeCenter T only)**

  Use these commands to manage alarms for monitored parameters of the BladeCenter T unit:
  - "alarm command (BladeCenter T only)" on page 18

Command syntax

Each of the following topics describes a command-line interface command and its syntax. Each command description also includes an example of command use.

alarm command (BladeCenter T only)

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

Table 2. alarm command

Function	What it does	Command	Valid targets

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

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

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

Table 2. alarm command (continued)

Function	What it does	Command	Valid targets

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

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

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

Acknowledge alarm (specified by alarm generator ID)	Acknowledge the alarm specified by the generator ID.	`alarm -r -g` *value*
		
		where *value* is the generator ID.
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:power[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the primary management-module, blade server, I/O module, power module, or blower bay number.

Table 2. alarm command (continued)

Function	What it does	Command	Valid targets

Acknowledge alarm (specified by generator information)	Acknowledge the alarm specified by the generator information.	`alarm -r -o` *value*
		
		where *value* is the generator information.
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:power[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the primary management-module, blade server, I/O module, power module, or blower bay number.

Acknowledge alarm (specified by alarm ID)	Acknowledge the alarm specified by the alarm ID.	`alarm -r -a` *value*
		
		where *value* is the alarm ID.
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:power[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the primary management-module, blade server, I/O module, power module, or blower bay number.

Acknowledge alarm (specified by complete alarm key)	Acknowledge the alarm specified by the complete alarm key.	`alarm -r -k` *m:g:o:a*
		
		where *m:g:o:a* is the complete alarm key:
		• *m* is the module ID
		• *g* is the generator ID
		• *o* is the generator information
		• *a* is the alarm ID
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:power[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the primary management-module, blade server, I/O module, power module, or blower bay number.

Clear alarm (specified by alarm generator ID)	Clear the alarm specified by the generator ID.	`alarm -c -g` *value*
		
		where *value* is the generator ID.
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:power[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the primary management-module, blade server, I/O module, power module, or blower bay number.

Table 2. alarm command (continued)

Function	What it does	Command	Valid targets

Clear alarm (specified by generator information)	Clear the alarm specified by the generator information.	`alarm -c -o` *value*
		
		where *value* is the generator information.
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:power[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the primary management-module, blade server, I/O module, power module, or blower bay number.

Clear alarm (specified by alarm ID)	Clear the alarm specified by the alarm ID.	`alarm -c -a` *value*
		
		where *value* is the alarm ID.
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:power[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the primary management-module, blade server, I/O module, power module, or blower bay number.

Clear alarm (specified by complete alarm key)	Clear the alarm specified by the complete alarm key.	`alarm -c -k` *m:g:o:a*
		
		where *m:g:o:a* is the complete alarm key:
		• *m* is the module ID
		• *g* is the generator ID
		• *o* is the generator information
		• *a* is the alarm ID
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:power[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the primary management-module, blade server, I/O module, power module, or blower bay number.

Set alarm	Set an alarm for the specified target, including severity level and description.	`alarm -s -l` *level desc*
		
		where
		• *level* is the severity level:
		– `CRT` (critical)
		– `MJR` (major)
		– `MNR` (minor)
		• *desc* is a short text description of the alarm
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:power[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the primary management-module, blade server, I/O module, power module, or blower bay number.

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

```
alarm -q
```

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] -q
```

The following example shows the information that is returned from a series of alarm commands.

```
system> alarm -q
Alarms Summary List
Module                ACK  Severity  Power  Software
===========           ===  ========  =====  ========
mm[1]                 No    Major           No        No
power[2]              No    Critical        Yes       No

system> alarm -q -p
Alarms Summary List
Module         ACK  Severity  Power  Software
===========    ===  ========  =====  ========
power[2]       No   Critical   Yes       No

system> alarm -q -T mm[1]
Alarms Detailed List
ACK Severity PWR SW  Descript                                          Key
=== =======  === === ================================================ ============
No  Major    No  No (05/21/08, 13:46:11) Insufficient chassis power 255:81:1:2:3
No  Minor    No  No (05/21/08, 13:45:26) Event log full             255:81:1:1:1

system>
```

alertentries command

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

Table 3. alertentries command

Function	What it does	Command	Valid targets
Display alert properties for all recipients	Displays alert properties for all management-module alert recipients. Returned values for each alert recipient are: • recipient name • notification method (E-Mail over LAN/Director comp./SNMP over LAN) • type of alerts received (Receives critical alerts only/Receives all alerts/Disabled)	`alertentries`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display alert properties for alert recipients	Displays alert properties for the specified management-module alert recipient profile. Returned values are: • -status *alert_recipient_status* (on/off) • -n *alert_recipient_name* • -f *alert_type* (critical/none) • -t *notification_method* (email/director/snmp) • -e *email_address* (used for e-mail notifications) • -i *static_IP_addr/hostname* (used for IBM Director notifications)	`alertentries` *-recip_number* where *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Delete alert recipient	Delete the specified alert recipient.	`alertentries` *-recip_number* `-del` where *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. It is possible to delete an empty alert recipient. Command use restricted (see “Commands and user authority” on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 3. alertentries command (continued)

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

Table 3. alertentries command (continued)

Function	What it does	Command	Valid targets
Create alert recipient *(continued)*		• *ip_addr/hostname* is a valid static IP address or an alphanumeric hostname string for the recipient that is up to 49 characters in length that can include periods (.), hyphens (-), and underscores (_). Command use restricted (see "Commands and user authority" on page 6).	
Set alert recipient name	Sets a name for the specified alert recipient.	`alertentries -recip_number -n recip_name` where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *recip_name* is a alphanumeric string up to 31 characters in length that can include any character, including spaces, except for angle brackets (< and >). If the name includes spaces, it must be enclosed in double-quotes. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set alert recipient status	Sets status for the specified alert recipient. The status determines if a recipient will receive alarm notifications.	`alertentries -recip_number -status alert_status` where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *alert_status* is on or off. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 3. alertentries command (continued)

Function	What it does	Command	Valid targets
Set alert types received	Filters the types of alert that are received by the specified alert recipient.	`alertentries` *-recip_number* `-f` *filter_type* where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *alert_type* filters the alert types received: `critical` (receive critical alerts only) or `none` (receive all alerts). Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set alert notification method	Sets the alert notification method for the specified alert recipient.	`alertentries` *-recip_number* `-t` *notification_method* where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *notification_method* is – `email` – `director` (IBM Director) – `snmp` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 3. alertentries command (continued)

Function	What it does	Command	Valid targets
Set alert recipient e-mail address	Sets the e-mail address for the specified alert recipient. This e-mail address is used to send alerts to the recipient via e-mail. The e-mail address can be set only if the alert notification method (-t option) is set to email. The -t and -e options can be combined within the same command.	`alertentries` *-recip_number* `-e` *email_addr* where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *email_addr* is a valid e-mail address string up to 63 characters in length. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set alert recipient IP address or hostname	Sets the IP address or hostname used to send alert notifications to the specified alert recipient using IBM Director. The IP address or hostname used to send alert notifications can be set only if the alert notification method (-t option) is set to director (IBM Director). The -t and -i options can be combined within the same command.	`alertentries` *-recip_number* `-i` *ip_addr/hostname* where: • *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. • *ip_addr/hostname* is a valid static IP address or an alphanumeric hostname string up to 49 characters in length that can include periods (.), hyphens (-), and underscores (_). Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

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

```
alertentries -1
```

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

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

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

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

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

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

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

```
system:mm[1]> alertentries -1
-status on
-n test1
-f critical
-t email
-e test1@us.ibm.com
system:mm[1]> alertentries -2 -n test2 -status on -f critical -t email
-e test2@us.ibm.com
OK
system:mm[1]> alertentries -3 -n test3 -status on -f none -t director
-i 192.168.70.140
OK
system:mm[1]> alertentries -4 -n test4 -status on -f none -t snmp
OK
system:mm[1]>
```

boot command

This command resets blade servers with several different restart options.

Table 4. boot command

Function	What it does	Command	Valid targets
Reset blade server	Performs an immediate reset and restart of the specified blade server. This command will start a blade server that is turned off.	`boot` Command use restricted (see "Commands and user authority" on page 6).	`-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 6).	`-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 6).	`-T system:blade[x]` where *x* is the blade server bay number.
Reset blade server	Performs an immediate reset and restart of the specified blade server. This command will start a blade server that is turned off.	`boot -p reset` Command use restricted (see "Commands and user authority" on page 6).	`-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]>
```

clear command

This command restores the primary management module configuration or an I/O (switch) module configuration to the default settings.

The clear command must always include the `-config` option.

Table 5. clear command

Function	What it does	Command	Valid targets
Restore default configuration of primary management module	Restores the default configuration of the primary management module; then, resets the management module. No results are returned from this command because it resets the management module. When you restore the management-module configuration, the Ethernet configuration method is set to a value of dthens. After the management module resets, this causes the management module to try dhcp configuration and then default to the static IP configuration, which might cause the management module to remain offline for longer than normal. See "ifconfig command" on page 59 for information.	`clear -config` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Restore default configuration of I/O module	Restores the configuration of the specified I/O module to the default settings.	`clear -config` Command use restricted (see "Commands and user authority" on page 6).	`-T system:switch[x]` where *x* is the I/O-module bay number.

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

```
clear -config
```

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

clearlog command

This command clears the management-module audit event log, the system event log, or both.

Table 6. clearlog (clear management-module event log) command

Function	What it does	Command	Valid targets
Clear management-module event log	Clears the management-module event log and displays a message confirming that the specified event log was cleared.	`clearlog` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example: To clear the management-module audit 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]>
```

clock command

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

Table 7. clock command

Function	What it does	Command	Valid targets
Display management module clock information	Displays the following information for the management module clock: • current date and time • GMT (Greenwich-Mean Time) offset • daylight-savings time setting	`clock`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management module date	Sets the date for the management module clock.	`clock -d` *date* where *date* is the current calendar date in mm/dd/yyyy format. The month and day can be input as single digits. The year must be a four-digit number between 2000 and 2089, inclusive. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management module time	Sets the time for the management module clock.	`clock -t` *time* where *time* is the current time in 24-hour hh:mm:ss format. The hours, minutes, and seconds can all be input as single digits. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 7. clock command (continued)

Function	What it does	Command	Valid targets
Set management module clock GMT offset	Sets the time for the management module clock.	`clock -g` *offset* where *offset* is a value between +12 and -12, in hours and minutes. Positive offsets are entered using the form: GMT+hh:mm, +hh:mm, +hh, hh:mm, or hh; where, the hours and minutes can be input as single digits. Negative offsets are entered using the form: GMT-hh:mm, -hh:mm, or -hh; where, the hours and minutes can be input as single digits. Valid offsets are: • `GMT+0:00` • `GMT+1:00` • `GMT+2:00` • `GMT+3:00` • `GMT+3:30` • `GMT+4:00` • `GMT+4:30` • `GMT+5:00` • `GMT+5:30` • `GMT+6:00` • `GMT+7:00` • `GMT+8:00` • `GMT+9:00` • `GMT+9:30` • `GMT+10:00` • `GMT+11:00` • `GMT+12:00` • `GMT-12:00` • `GMT-11:00` • `GMT-10:00` • `GMT-9:00` • `GMT-8:00` • `GMT-7:00` • `GMT-6:00` • `GMT-5:00` • `GMT-4:00` • `GMT-3:30` • `GMT-3:00` • `GMT-2:00` • `GMT-1:00` *(continued on next page)*	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 7. clock command (continued)

Function	What it does	Command	Valid targets
Set management module clock GMT offset (continued)		For some time zones that use daylight-savings time (GMT +10, +2, -5, -6, -7, -8, -9), a special value for the `-dst` option must be specified to identify the correct daylight-savings time scheme to use in that time zone. Command use restricted (see "Commands and user authority" on page 6).	
Set management module clock daylight-savings time mode	Sets the daylight-savings time mode for the management module clock.	`clock -dst` *dst_mode* where *dst_mode* is one of the following: • `off` • `on` • for `GMT+2:00`: – `off` – `ee` (Eastern Europe) – `gtb` (Great Britain) – `egt` (Egypt) – `fle` (Finland) • for GMT+10:00: – `off` – `ea` (Eastern Australia) – `tas` (Tasmania) – `vlad` (Vladivostok) • for GMT-9:00 to GMT-5:00: – `off` – `uc` (United States and Canada) – `other` (other locations) • for GMT-4:00: – `off` – `can` (Canada) – `other` (other locations) Daylight-savings time is not observed in the following GMT offsets: GMT+4:00, GMT+4:30, GMT+5:30, GMT+6:00, GMT+7:00, GMT+8:00, GMT+11:00, GMT-12:00, GMT-11:00, and GMT-10:00. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example: To set the management-module for operation in the US Eastern time zone in compliance with new daylight-savings time rules, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
clock -g +5 -dst uc
```

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

```
clock
```

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

```
system:mm[1]> clock -g +5 -dst uc
OK
system:mm[1]> clock
10/17/2006 02:27:11 GMT+5:00 dst uc
system:mm[1]>
```

config command

This command sets and displays the name of the management module or blade server and the location and contact name for the management module.

Table 8. config command

Function	What it does	Command	Valid targets
Display name of blade server	Displays the name of the specified blade server.	`config`	`-T system:blade[x]` where *x* is the blade server bay number.
Display name of management module	Displays the following information for the command target: • Name • Location • Contact name	`config`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display identifying information for BladeCenter unit	Displays the following information for the command target: • Universally unique identifier • Serial number • Type/model	`config`	`-T system`

Set name of management module or blade server	Sets the name of the primary management module or specified blade server.	`config -name` *name*
		
		where *name* is up to 15 characters in length.
		
		Blade server names cannot contain angle brackets ("<" and ">"), and management module names can only contain alphanumeric characters, hyphens, pound signs, underscores, and periods.
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:mm[x]`
			`-T system:blade[x]`
			
			where *x* is the primary management-module or a blade server bay number.

Set location of management module	Sets the location of the primary management module.	`config -loc` *"location"* where *"location"* is up to 47 characters in length and contained within double-quotes. Management module locations can contain any character other than "<" and ">". Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 8. config command (continued)

Function	What it does	Command	Valid targets
Set contact name for management module	Sets the contact name for the primary management module.	`config -contact "contact_name"` where *"contact_name"* is up to 47 characters in length and contained within double-quotes. Management module contact names can contain any character other than "<" and ">". Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set universally unique identifier (UUID) for BladeCenter unit	Sets the universally unique identifier for the BladeCenter unit. **Notes:** • Change the -uuid value only if you are certain it was not programmed correctly on the hardware. To prevent disrupting the operation of IBM Director, you should edit this field only if the midplane of your system has been replaced with a new midplane that does not have this information programmed on it. • If you change the UUID on an existing system to a random new value, IBM Director will treat this as a new system, distinct from the one identified by the old UUID. • Changes to the UUID take effect after the next restart of the management module.	`config -uuid "unique_id"` where *"unique_id"* is 32 hexadecimal digits and is contained within double-quotes. Command use restricted (see "Commands and user authority" on page 6).	`-T system`
Set type/model for BladeCenter unit	Sets the type or model designator for the BladeCenter unit. **Notes:** • Change the -tm value only if you are certain it was not programmed correctly on the hardware. To prevent disrupting the operation of IBM Director, you should edit this field only if the midplane of your system has been replaced with a new midplane that does not have this information programmed on it. • Changes to the type/model take effect after the next restart of the management module.	`config -tm "type_model"` where *"type_model"* is up to seven characters in length and contained within double-quotes. Management module type / model designators can contain any character other than "<" and ">". Command use restricted (see "Commands and user authority" on page 6).	`-T system`

Table 8. config command (continued)

Function	What it does	Command	Valid targets
Set serial number for BladeCenter unit	Sets the serial number for the BladeCenter unit. **Notes:** • Change the -sn value only if you are certain it was not programmed correctly on the hardware. To prevent disrupting the operation of IBM Director, you should edit this field only if the midplane of your system has been replaced with a new midplane that does not have this information programmed on it. • Changes to the serial number take effect after the next restart of the management module.	`config -sn "serial_number"` where *"serial_number"* is up to seven characters in length and contained within double-quotes. Management module serial numbers can contain any character other than "<" and ">". Command use restricted (see "Commands and user authority" on page 6).	`-T system`

Example:

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

```
config -name IBM_lab
```

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

```
config
```

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

```
system:mm[1]> config -name IBM_lab
OK
system:mm[1]> config
-name IBM_lab
-contact John_Doe
-loc Main_Lab
system:mm[1]>
```

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 9. console command

Function	What it does	Command	Valid targets
Create SOL session with blade server	Creates an SOL connection to the specified blade server.	`console` Command use restricted (see "Commands and user authority" on page 6).	`-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 6).	`-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

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

dhcpinfo command

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

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

Table 10. dhcpinfo command

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

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

```
dhcpinfo -eth0
```

The following example shows the information that is returned:

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

displaylog command

This command displays management-module event log entries.

Table 11. displaylog (display management-module event log) command

Function	What it does	Command	Valid targets
Display management-module event log entries	Displays five entries from the management-module event log. The first time the command is executed, the five most recent log entries are displayed. Each subsequent time the command is issued, the next five entries in the log display.	`displaylog`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display management-module event log entries (reset counter)	Resets the counter and displays the first five most recent 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 all log entries generated by the management module in bay 1 other than those in the audit log, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
displaylog -src !Audit -T mm[1]
```

To display audit log entries generated by the management module in bay 1, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
displaylog -src Audit -T mm[1]
```

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

```
system> displaylog -src !Audit -T mm[1]
1       I       SERVPROC   08/04/08    14:18:06     Recovery Event log full
2       I       SERVPROC   08/04/08    14:18:06     Alarm Manager removed a MNR
                                                    alert during recovery of
                                                    Event log full

(There are no more entries in the event log.)
system> displaylog -src audit -T mm[1]
1       I       Audit      08/04/08    14:28:38     Remote logoff successful for
                                                    user 'spdev'from Telnet at
                                                    IP 9.44.124.157
2       I       Audit      08/04/08    14:28:18     Remote login successful for
                                                    user 'spdev' from Telnet at
                                                    IP 9.44.124.157
3       I       Audit      08/04/08    14:18:15     Audit log cleared by 'spdev'.
(There are no more entries in the event log.)
system>
```

dns command

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

Table 12. dns command

Function	What it does	Command	Valid targets
Display DNS configuration of management module	Displays the current DNS configuration of the management module. Possible return values are: • enabled • disabled • -i1 *first ip_address* • -i2 *second ip_address* • -i3 *third ip_address*	`dns`	`-T system:mm[x]` where *x* is the primary management-module bay number.
DNS - enable / disable	Enables or disables the management-module DNS configuration.	`dns -state` where *state* is `on` or `off`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
DNS first IP address - set	Checks syntax and sets the first IP address.	`dns -i1 ip_address` where *ip_address* is the first IP address. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
DNS second IP address - set	Checks syntax and sets the second IP address.	`dns -i2 ip_address` where *ip_address* is the second IP address. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
DNS third IP address - set	Checks syntax and sets the third IP address.	`dns -i3 ip_address` where *ip_address* is the third IP address. Command use restricted (see "Commands and user authority" on page 6).	`-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]>
```

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 by using a colon (:).

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

Table 13. Components and command paths

Component	Target path
BladeCenter unit	system
Management module	system:mm[*x*]
Blade server	system:blade[*x*]
Blade server integrated system management processor (BMC or service processor)	system:blade[*x*]:sp
Blade server I/O-expansion card	system:blade[*x*]:dtr[*y*]
Blade server high-speed expansion card	system:blade[*x*]:hsdc
Blade server microprocessor	system:blade[*x*]:cpu[*y*]
Blade server storage expansion unit	system:blade[*x*]:be
I/O (switch) module	system:switch[*x*]
Power module	system:power[*x*]
Blower	system:blower[*x*]
Media tray	system:mt

Table 14. env (environment) command

Function	What it does	Command	Valid targets
Set BladeCenter unit as command target	Sets the BladeCenter unit as the persistent target for commands during the current session. This is the persistent command environment you are in at the beginning of each command-line interface session, indicated by the `system>` prompt.	env `env -T system`	The env command can be directed to any installed device.

Table 14. env (environment) command (continued)

Function	What it does	Command	Valid targets
Set management module as command target	Sets the management module as the persistent target for commands during the current session.	`env -T system:mm[x]` where *x* is the bay (1 or 2) that identifies the management module.	The env command can be directed to any installed device, in this case `-T system:mm[x]` where *x* is the management-module bay number.
Set blade server as command target	Sets the specified blade server as the persistent target for commands during the current session.	`env -T system:blade[x]` where *x* is the blade bay that identifies the blade server. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies.	The env command can be directed to any installed device, in this case `-T system:blade[x]` where *x* is the blade bay that identifies the blade server.
Set blade server sub-component as command target	Sets the specified sub-component on the specified blade server as the persistent target for commands during the current session. Valid sub-components are: • Integrated system management processor (BMC or service processor) • I/O-expansion card • Microprocessor • High-speed expansion card • Storage expansion unit	`env -T system:blade[x]:comp` where *x* is the blade bay that identifies the blade server on which the sub-component is installed. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies. where *comp* is the sub-component: • `sp` for BMC or service processor • `dtr[x]` for I/O-expansion card (where *x* identifies the expansion card) • `cpu[x]` for microprocessor (where *x* identifies the microprocessor) • `hsdc` for high-speed expansion card • `be[x]` for storage expansion unit (where *x* identifies the expansion unit)	The env command can be directed to any installed device, in this case `-T system:blade[x]:comp` where *x* is the blade bay that identifies the blade server on which the integrated system management processor is installed. where *comp* is the sub-component: • `sp` for BMC or service processor • `dtr[x]` for I/O-expansion card (where *x* identifies the expansion card) • `hsdc` for high-speed expansion card • `cpu[x]` for microprocessor (where *x* identifies the microprocessor) • `be[x]` for storage expansion unit (where *x* identifies the expansion unit)

Table 14. env (environment) command (continued)

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

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

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

The following example shows the information that is returned:

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

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

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

The following example shows the information that is returned:

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

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

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

exit command

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

Table 15. exit command

Function	What it does	Command	Valid targets
Exit	Terminates the current command-line interface session.	`exit` **Note:** You can also use the Ctrl-D key combination to end the current session and exit the command-line interface.	Any installed device.

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

```
exit
```

fuelg command

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

Table 16. fuelg command

Function	What it does	Command	Valid targets
Display power domain status overview	Displays health status and total power usage information for all power domains	`fuelg`	`-T system`
Display detailed power domain status	Displays detailed status and usage information for the specified power domains	`fuelg` *domain* where *domain* is: • `pd1` for power domain 1. • `pd2` for power domain 2. • If no *domain* is specified, a status overview for all power domains displays.	`-T system`
Set power domain redundancy loss policy	Sets how the BladeCenter unit responds to a condition that could cause a loss of redundant power.	`fuelg` *domain* `-os` *policy* where: • *domain* is: – `pd1` for power domain 1. – `pd2` for power domain 2. – If no *domain* is specified, the *policy* is applied to all power domains. • *policy* of: – `none` (default) allows loss of redundancy. – `nonrecov` prevents components from turning on that will cause loss of power redundancy. – `recov` power throttles components to maintain power redundancy and prevents components from turning on that will cause loss of power redundancy. Command use restricted (see “Commands and user authority” on page 6).	`-T system`

Table 16. fuelg command (continued)

Function	What it does	Command	Valid targets
Thermal event response (quiet mode)	Sets how the BladeCenter unit blowers respond to thermal events.	`fuelg -qm` *setting* where the quiet-mode *setting* of: • `off` (default) allows blowers to increase speed to provide additional cooling. • `on` keeps blowers at a fixed speed and power throttles BladeCenter components to reduce power consumption (only for BladeCenter components that support power throttling). Command use restricted (see "Commands and user authority" on page 6).	`-T system`

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

```
fuelg
```

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

```
fuelg -qm on
```

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

```
fuelg pd1
```

The following example shows the information that is returned when the fuelg command is run.

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

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

Power Domain 2
--------------
Status: Power domain status is good.
Modules:
  Bay 3: 1800
```

```
  Bay 4: 1800
Power Budget:  2880
Reserved Power:  0
Remaining Power:  2880
Power in Use:  0

-qm off
system>  fuelg -qm on
OK
system>  fuelg pd1
                            Power  -- Allocated Power --
Bay(s)  Module              State  Current   Max    Min
======  ==================  =====  =======  =====  =====
Chassis Components
        Midplane             On         10     10     10
no media tray
Blowers
     1  Blower 1 (NP)        On        120    120    120
     2  Blower 2 (NP)        On        120    120    120
Management Modules
     1  WMN315619689         On         25     25     25
     2  Backup MM (NP)                  25     25     25
I/O Modules
     1  I/O Module 2 (NP)               45     45     45
     2  I/O Module 2 (NP)               45     45     45
Domain totals:
  Allocated Power                      390    390    390

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

-os none
system>
```

health command

This command displays the current health status of the command target. It can also be used to display the alerts that are active for the command target.

You can only specify one command target each time you run the health command.

Table 17. health command

Function	What it does	Command	Valid targets

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

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

Table 17. health command (continued)

Function	What it does	Command	Valid targets

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

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

```
health
```

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

```
health -l a
```

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

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

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

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

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

```
system> health
system:major
system> health -l a
system: Major
          mm[1]    :          OK
         blade[1]  :          OK
         blade[3]  :          OK
         blade[5]  :          Minor
         power[1]  :          OK
         power[2]  :          Minor
         blower[1] :          OK
         blower[2] :          OK
         blower[3] :          OK
         blower[4] :          OK
         switch[1] :          Major
system> health -T system:blade[5]
system: blade[5]   :          Minor
system> 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>
```

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 18. 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 the management module in bay 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> help
           ?- Display commands
alertentries- View/edit remote alert recipients
        boot- Boot target
       clear- Clear the config
    clearlog- Clear the event log
       clock- View/edit date, time, GMT offset, and dst setting
      config- View/edit general settings
     console- Start SOL session to a blade
    dhcpinfo- View DHCP server assigned settings
  displaylog- Display log entries
         dns- View/edit DNS config
         env- Set persistent command target
        exit- Log off
       fuelg- Power management
      health- View system health status
        help- Display command list
     history- Display command history
    identify- Control target location LED
    ifconfig- View/edit network interface config
        info- Display identity and config of target
         kvm- Controls the kvm owner
        list- Display installed targets
          mt- Controls the media tray owner
       power- Control target power
       reset- Reset target
    shutdown- Shutdown target
         slp- View/edit SLP parameters
        smtp- View/edit SMTP config
        snmp- View/edit SNMP config
         sol- View SOL status and view/edit SOL config
  tcpcmdmode- View/edit TCP command mode config
   telnetcfg- View/edit telnet config
      update- Update firmware from TFTP server
      uplink- View/edit failover on network uplink loss config
       users- View/edit user login profiles

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

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

- env -h
- env -help
- env ?

history command

This command displays the last eight commands that were entered, allowing the user to choose and re-enter one of these commands.

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

Table 19. 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]>
```

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 20. identify (location LED) command

Function	What it does	Command	Valid targets

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

Set location LED state	Sets the state of the location LED in the command target.	`identify -s` *state*
		
		where *state* is
		• `on`
		• `off`
		• `blink`
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system`
			`-T system:blade[x]`
			
			where *x* is the blade bay number.

Turn on BladeCenter unit location LED for specified period of time	Turns on the location LED in the BladeCenter unit for a specified period of time before turning it off automatically.	`identify -s on -d` *time* where *time* is the number of seconds the location LED will remain lit. Command use restricted (see "Commands and user authority" on page 6).	`-T system`

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

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

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

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

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

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

ifconfig command

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

Table 21. ifconfig command

Function	What it does	Command	Valid targets
Display Ethernet channel 0 configuration	Displays the current configuration of Ethernet channel 0. Possible return values are: • enabled • disabled • -i *static_ip_address* • -g *gateway_address* • -s *subnet_mask* • -n *hostname* • -c *config_method* • -r *data_rate* • -d *duplex_mode* • -m *mtu* • -l *locally_administered_mac_addr* • -b *burnedin_mac_address*	`ifconfig -eth0`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 static IP address	Checks syntax and sets the static IP address for Ethernet channel 0.	`ifconfig -eth0 -i` *ip_address* where *ip_address* is the static IP address for Ethernet channel 0. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 gateway IP address	Checks syntax and sets the gateway IP address for Ethernet channel 0.	`ifconfig -eth0 -g` *ip_address* where *ip_address* is the gateway IP address for Ethernet channel 0. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 subnet mask	Checks syntax and sets the subnet mask for Ethernet channel 0.	`ifconfig -eth0 -s` *sub_mask* where *sub_mask* is the subnet mask for Ethernet channel 0. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 21. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set Ethernet channel 0 hostname	Checks syntax and sets the host name for Ethernet channel 0.	`ifconfig -eth0 -n` *hostname* where *hostname* is the host name for Ethernet channel 0. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 configuration method	Checks syntax and sets the configuration method for Ethernet channel 0. A value of dthens will try the DHCP configuration and default to the static IP configuration if DHCP is unsuccessful. A value of dthens will try the DHCP configuration and default to the static IP configuration if DHCP is unsuccessful after 2 minutes. **Note:** If the management module DHCP setting is set to try the DHCP server and then use the static IP address, the management module will use the static IP address when the DHCP server is not available during management module start up. When this occurs, the IP address might not be reachable if multiple management modules were started with the same static IP address.	`ifconfig -eth0 -c` *config_method* where *config_method* is • `dhcp` • `static` • `dthens` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 data rate	Checks syntax and sets the data rate for Ethernet channel 0.	`ifconfig -eth0 -r` *data_rate* where *data_rate* is • `auto` • `10` • `100` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 duplex mode	Checks syntax and sets the duplex mode for Ethernet channel 0.	`ifconfig -eth0 -d` *duplex_mode* where *duplex_mode* is • `auto` • `half` • `full` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 21. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set Ethernet channel 0 MTU	Checks syntax and sets the MTU (maximum transmission unit) for Ethernet channel 0.	`ifconfig -eth0 -m` *mtu* where *mtu* is between 60 and 1500, inclusive. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set Ethernet channel 0 static MAC address (locally administered)	Checks syntax and sets the locally administered MAC address to the specified MAC address for Ethernet channel 0.	`ifconfig -eth0 -l` *address* where *address* is the locally administered MAC address for Ethernet channel 0. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display Ethernet channel 1 configuration	Displays the current configuration of Ethernet channel 1. Possible return values are: • enabled • disabled • -i *static_ip_address* • -g *gateway_address* • -s *subnet_mask* • -r *data_rate* • -d *duplex_mode* • -m *mtu* • -l *locally_administered_mac_addr* • -b *burnedin_mac_address*	`ifconfig -eth1`	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set Ethernet channel 1 static IP address	Checks syntax and sets the static IP address for Ethernet channel 1.	`ifconfig -eth1 -i` *ip_address* where *ip_address* is the static IP address for Ethernet channel 1. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set Ethernet channel 1 gateway IP address	Checks syntax and sets the gateway IP address for Ethernet channel 1.	`ifconfig -eth1 -g` *ip_address* where *ip_address* is the gateway IP address for Ethernet channel 1. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 21. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set Ethernet channel 1 subnet mask	Checks syntax and sets the subnet mask for Ethernet channel 1.	`ifconfig -eth1 -s` *sub_mask* where *sub_mask* is the subnet mask for Ethernet channel 1. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set Ethernet channel 1 static MAC address (locally administered)	Checks syntax and sets the locally administered MAC address to the specified MAC address for Ethernet channel 1.	`ifconfig -eth1 -l` *address* where *address* is the locally administered MAC address for Ethernet channel 1. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable Ethernet channel 1	Enables Ethernet channel 1.	`ifconfig -eth1 -up` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Disable Ethernet channel 1	Disables Ethernet channel 1.	`ifconfig -eth1 -down` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display starting IP address for blade server integrated system management processor	Displays the starting point of the integrated system management processor IP addresses for blade servers that are installed in the BladeCenter unit.	`ifconfig`	`-T system:blade[1]:sp`
Set starting IP address for blade server integrated system management processor	Sets the starting point of the integrated system management processor IP addresses for blade servers that are installed in the BladeCenter unit.	`ifconfig -i` *ip_address* where *ip_address* is the starting IP address for all blade servers that are installed in the BladeCenter unit. Command use restricted (see "Commands and user authority" on page 6).	`-T system:blade[1]:sp`

Table 21. ifconfig command (continued)

Function	What it does	Command	Valid targets
Display network settings for I/O module	Displays network settings for the specified I/O module. Depending on the type of I/O module targeted, valid return values might include one or more of the following: • I/O-module type • Config. Method *config_method* • -i *ip_address* • -s *subnet_mask* • -g *gateway_address* • -em *ext_mgt_status* • -ep *ext_port_status*	`ifconfig`	`-T system:switch[x]` where *x* is the I/O-module bay number.
Set starting IP address for I/O module	Sets the IP addresses for a specified I/O module that supports IP address configuration.	`ifconfig -i` *ip_address* where *ip_address* is the IP address of the specified I/O module. Command use restricted (see "Commands and user authority" on page 6).	`-T system:switch[x]` where *x* is the I/O-module bay number.
Enable / disable external management for I/O module	Enables or disables external management on all ports for a specified I/O module that supports this feature.	`ifconfig -em` *state* where *state* is `enabled` or `disabled`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:switch[x]` where *x* is the I/O-module bay number.
Enable / disable external ports for I/O module	Enables or disables external ports for the specified I/O module that supports this feature.	`ifconfig -ep` *state* where *state* is `enabled` or `disabled`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:switch[x]` where *x* is the I/O-module bay number.

Example:

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

```
ifconfig -eth0
```

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

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

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

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

info (configuration information) command

This command displays information about BladeCenter components and their configuration, and how to reload the component information.

Table 22. info (configuration information) command

Function	What it does	Command	Valid targets

Display component information	Displays identification and configuration information for the command target.	`info`
		
		Note: Only one target at a time can be viewed with the info command.
			`-T system`
			`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:blower[x]`
			`-T system:ncc[x]`
			`-T system:mux[x]`
			`-T system:tap`
			`-T system:blade[x]:dtr[y]`
			`-T system:blade[x]:hsdc`
			`-T system:blade[x]:sp`
			`-T system:blade[x]:be`
			`-T system:blade[x]:cpu[y]`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:mt`
			
			where:
			• *x* is the management-module bay number, blade server bay number, I/O-module bay number, microprocessor number, power module bay number, or daughter-card number.
			• *y* is the:
			– blade server I/O expansion card number (dtr).
			– microprocessor number (CPU).

Reload component information for firmware	Reloads vital product data (VPD) for firmware.	`info -reload fw`	`-T system`
Reload component information for hardware	Reloads vital product data (VPD) for hardware.	`info -reload hw`	`-T system`
Reload information on MAC addresses	Reloads vital product data (VPD) for MAC addresses.	`info -reload mac`	`-T system`
Reload WWN and GUID information	Reloads vital product data (VPD) for world-wide name (WWN) and globally-unique identifier (GUID).	`info -reload wwn`	`-T system`

Table 22. info (configuration information) command (continued)

Function	What it does	Command	Valid targets
Reload all component information	Forces reload of all VPD and MAC address information.	`info -reload all`	`-T system`

Notes:

1. The command targets `-T system:blade[x]:cpu[y]` and `-T system:blade[x]:dtr[y]` are shown with a line break before the `:cpu[y]` or `:dtr[y]`. When these command targets are entered, the entire entry must all be on one line.
2. This command returns vital product data (VPD) information that is unique for each command target.
3. Even if the command target is specified, the -reload option acts globally, reloading information not just for the specified target but for all targets in the corresponding category; for example, all MAC addresses are reloaded for all targets when the command is info -reload mac with system:blade[x] as the target.

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

```
info
```

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

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

kvm (keyboard, video, mouse) command

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

Table 23. kvm command

Function	What it does	Command	Valid targets
Display KVM owner	Displays the number of the blade server that has KVM ownership and the global local KVM switching state for all blade servers. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies. A return value of 0 indicates that no owner is set.	`kvm`	`-T system`
Set KVM owner	Sets a blade server as the KVM owner.	`kvm -b` *blade_server* where *blade_server* is the blade-bay number that identifies the blade server. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies. A setting of 0 sets no owner. Command use restricted (see "Commands and user authority" on page 6).	`-T system`
Enable / disable local KVM switching globally	Enable or disable local KVM switching globally for all blade servers.	`kvm -local` *state* where *state* is `enabled` or `disabled`. Command use restricted (see "Commands and user authority" on page 6).	`-T system`

Example:

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

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

To display the KVM owner and global local KVM switching state for all blade servers, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
kvm -T system
```

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

```
system:mm[1]> kvm -T system -b 1
OK
system:mm[1]> kvm -T system
-b 1
-local enabled
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 24. 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 standby (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 standby (redundant). For components that have been assigned a name, this name will be displayed next to the component bay number.	`list -l` *depth* where *depth* is • `all` or `a` for full tree display, starting at the command target level • `1` to display the current command target • `2` displays the content of the current command target plus one level below it	Any installed device.

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

```
list -l a
```

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

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

```
system> list -l a
system
        mm[1]     primary
        power[4]
        blower[1]
        blower[2]
        switch[1]
        switch[2]
        switch[3]
        switch[4]
        blade[1]
                sp
                dtr[1]
        blade[5]
                sp
        blade[6]
                sp
        blade[7]
                sp
        blade[8]
                sp
        mt
system>
```

mt (media tray) command

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

Table 25. mt command

Function	What it does	Command	Valid targets
Display media tray owner	Displays the number of the blade server that has media tray ownership and the global local and remote media tray switching states for all blade servers. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies. A return value of 0 indicates that no owner is set.	`mt`	`-T system`
Set media tray owner	Sets a blade server as the media tray owner.	`mt -b` *blade_server* where *blade_server* is the blade bay that identifies the blade server. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies. A setting of 0 sets no owner. Command use restricted (see "Commands and user authority" on page 6).	`-T system`
Enable / disable local media tray switching globally	Enable or disable local media tray switching globally for all blade servers.	`mt -local` *state* where *state* is `enabled` or `disabled`. Command use restricted (see "Commands and user authority" on page 6).	`-T system`
Enable / disable remote media tray switching globally	Enable or disable remote media tray switching globally for all blade servers.	`mt -remote` *state* where *state* is `enabled` or `disabled`. Command use restricted (see "Commands and user authority" on page 6).	`-T system`

Example:

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

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

To display the media tray owner and the global local and remote media tray switching states for all blade servers, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
mt -T system
```

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

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

power command

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

Table 26. power command

Function	What it does	Command	Valid targets

Power on	Turns on the specified command target.	`power -on`
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:blade[x]`
			`-T system:switch[x]`
			
			where *x* is the blade server or I/O-module bay.

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 6).	`-T system:blade[x]` where *x* is the blade server bay number.

Power off	Turns off the specified command target.	`power -off`
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:blade[x]`
			`-T system:switch[x]`
			
			where *x* is the blade server, I/O-module bay, or network clock module number.

Shutdown and power off blade server	Shuts down the operating system and turns off the specified blade server.	`power -softoff` Command use restricted (see "Commands and user authority" on page 6).	`-T system:blade[x]` where *x* is the blade server number.

Power cycle	Cycles power for the specified blade server or I/O module. If the blade server or I/O module is off, it will turn on. If the blade server or I/O module is on, it will turn off and then turn on.	`power -cycle`
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-T system:blade[x]`
			`-T system:switch[x]`
			
			where *x* is the blade server or I/O-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 6).	`-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 module. Possible return values are off, on, standby, or hibernate.	`power -state`	`-T system:blade[x]`
			`-T system:switch[x]`
			
			where *x* is the blade server or I/O-module bay number.

Enable / disable Wake on LAN globally	Enables or disables Wake on LAN globally for all blade servers.	`power -wol` *state* where *state* is `enabled` or `disabled`. Command use restricted (see "Commands and user authority" on page 6).	`-T system`

Table 26. power command (continued)

Function	What it does	Command	Valid targets
Enable / disable Wake on LAN for blade server	Enables or disables Wake on LAN for the specified blade server.	`power -wol` *state* where *state* is `enabled` or `disabled`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:blade[`*x*`]` where *x* is the blade server bay number.
Enable / disable local power control globally	Enables or disables local power control globally for all blade servers.	`power -local` *state* where *state* is `enabled` or `disabled`. Command use restricted (see "Commands and user authority" on page 6).	`-T system`
Enable / disable local power control for blade server	Enables local power control for the specified blade server.	`power -local` *state* where *state* is `enabled` or `disabled`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:blade[`*x*`]` where *x* is the blade server bay number.
Display fast POST setting for I/O module	Displays the current fast POST setting for specified I/O module. **Note:** This target works only for some I/O modules.	`power`	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.
Enable / disable fast POST for I/O module	Enables or disables fast POST globally for the specified I/O module. **Note:** This option works only for some I/O modules.	`power -fp` *state* where *state* is `enabled` or `disabled`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 26. power command (continued)

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

Example:

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

```
power -state
```

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

```
power -on
```

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

```
power -state
```

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

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

reset command

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

Table 27. reset command

Function	What it does	Command	Valid targets

Reset	Performs an immediate reset and restart of the specified device.	`reset`
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-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-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 6).	`-T system:blade[x]` where *x* is the blade server bay number.
Reset with failover	Resets the specified command target, enabling failover if a redundant (standby) component for the command target is present. An error message is displayed if you try to failover a management module when a standby management module is not installed or if the firmware in the one of the management modules is updating.	`reset -f` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Reset I/O module with standard diagnostics	Performs an immediate reset and restart of the specified device, running standard diagnostics on the I/O module after it restarts. Running the `reset -std` command gives the same result as running the `reset` command on a I/O module.	`reset -std` Command use restricted (see "Commands and user authority" on page 6).	`-T system:switch[x]` where *x* is the I/O-module bay number.
Reset I/O module with extended diagnostics	Performs an immediate reset and restart of the specified device, running extended diagnostics on the I/O module after it restarts.	`reset -exd` Command use restricted (see "Commands and user authority" on page 6).	`-T system:switch[x]` where *x* is the I/O-module bay number.
Reset I/O module with full diagnostics	Performs an immediate reset and restart of the specified device, running full diagnostics on the I/O module after it restarts.	`reset -full` Command use restricted (see "Commands and user authority" on page 6).	`-T system:switch[x]` where *x* is the I/O-module bay number.

Table 27. reset command (continued)

Function	What it does	Command	Valid targets
Restart blade server with NMI	Performs an immediate reset and restart of the specified blade server. Command results depend on the blade server model that is specified: • For a JS12 or JS22 blade server, this option is not available. • 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 6).	`-T system:blade[x]` where *x* is the blade server bay number.
Restart blade server and clear NVRAM	Performs an immediate reset and restart of the specified blade server. Command results depend on the blade server model that is specified: • For a JS12 or JS22 blade server, this option is not available. • 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 6).	`-T system:blade[x]` where *x* is the blade server bay number.
Restart blade server and run diagnostics	Performs an immediate reset and restart of the specified blade server. Command results depend on the blade server model that is specified: • For a JS12 or JS22 blade server, this option is not available. • 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 6).	`-T system:blade[x]` where *x* is the blade server bay number.

Table 27. reset command (continued)

Function	What it does	Command	Valid targets
Restart blade server and run diagnostics using default boot sequence	Performs an immediate reset and restart of the specified blade server. Command results depend on the blade server model that is specified: • For a JS12 or JS22 blade server, this option is not available. • For a JS20 blade server, the command performs an immediate reset and restart of the specified JS20 blade server and runs diagnostics using the default boot sequence configured for the blade server. • For all other blade servers, the command performs an immediate reset and restart of the specified blade server.	`reset -ddg` Command use restricted (see "Commands and user authority" on page 6).	`-T system:blade[x]` where *x* is the blade server bay number.

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

```
reset
```

The following example shows the information that is returned:

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

shutdown command

This command forces a blade server to shut down.

Table 28. shutdown command

Function	What it does	Command	Valid targets
Shutdown blade server	Forces a shutdown for the specified blade server.	`shutdown -f` Command use restricted (see "Commands and user authority" on page 6).	`-T system:blade[x]` where *x* is the blade server bay number.

Example:

To force a shutdown 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

```
shutdown -f
```

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

```
system:blade[5]> shutdown -f
OK
system:blade[5]>
```

slp command

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

Table 29. slp command

Function	What it does	Command	Valid targets
Display management-module SLP settings	Displays the SLP settings for the primary management module. Returned values are: • -t *address_type* • -i *multicast_addr*	`slp`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management-module SLP address type	Sets the SLP address type for the primary management module.	`slp -t` *address_type* where *address_type* is `multicast` or `broadcast`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management-module SLP multicast address	Sets the SLP multicast address for the primary management module.	`slp -i` *multicast_addr* where *multicast_addr* is the multicast IP address. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

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

```
slp -t multicast
```

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

```
slp
```

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

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

smtp command

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

Table 30. smtp command

Function	What it does	Command	Valid targets
Display SMTP server host name or IP address	Displays the SMTP server host name or IP address.	`smtp`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Server host name or IP address - set	Checks syntax and sets the server host name or IP address.	`smtp -s` *hostname/ip_address* where *hostname/ip_address* is the host name or IP address of the server. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

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

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

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

```
smtp
```

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

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

snmp command

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

Table 31. snmp command

Function	What it does	Command	Valid targets
Display SNMP configuration of management module	Displays the current SNMP configuration of the management module.	`snmp`	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMPv1 agent - enable/disable	Enables or disables the management-module SNMPv1 agent.	`snmp -a -`*state* where *state* is `on` or `off`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMPv3 agent - enable/disable	Enables or disables the management-module SNMPv3 agent.	`snmp -a3 -`*state* where *state* is `on` or `off`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMP traps - enable/disable	Enables or disables the management-module SNMP traps.	`snmp -t -`*state* where *state* is `on` or `off`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMP community 1 name - set	Sets the name of community 1.	`snmp -c1` *name* where *name* is a descriptive name of community 1. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 31. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP Community 1, first host name - set access to SET (wildcard)	Sets the access type for community 1 to SET.	`snmp –ca1 set -c1i1 0.0.0.0` • With the access type of SET, anyone can query the management information base (MIB) and set MIB values. Using 0.0.0.0 IP address with SET access allows open access to the management module for write (SET) operations. A 0.0.0.0 address cannot be a trap receiver. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 31. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP Community 1, first host name or IP address - set access to GET (wildcard)	Sets the access type for community 1 to GET.	`snmp –ca1 get -c1i1 0.0.0.0` • With the access type of GET, anyone can query the MIB. Using 0.0.0.0 IP address with GET access allows open access to the management module for read (GET). A 0.0.0.0 address cannot be a trap receiver. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-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 hostname/ip_address` where *hostname/ip_address* is the second host name or IP address of community 1. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 31. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 1 third host name or IP address - set	Checks syntax and sets the third host name or IP address of community 1.	`snmp -c1i3` *hostname/ip_address* where *hostname/ip_address* is the third host name or IP address of community 1. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMPv3 community 1 view type - set	Sets the SNMPv3 view type for community 1.	`snmp -ca1` *type* where *type* is • `get` • `set` • `trap` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
SNMP community 2 name - set	Sets the name of community 2.	`snmp -c2` *name* where *name* is a descriptive name of community 2. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 31. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 2 first host name or IP address - set	Checks syntax and sets the first host name or IP address of community 2.	`snmp -c2i1` *hostname/ip_address* where *hostname/ip_address* is the first host name or IP address of community 2. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* 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.	`snmp -c2i2` *hostname/ip_address* where *hostname/ip_address* is the second host name or IP address of community 2. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 31. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 2 third host name or IP address - set	Checks syntax and sets the third host name or IP address of community 2.	`snmp -c2i3` *hostname/ip_address* where *hostname/ip_address* is the third host name or IP address of community 2. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SNMPv3 community 2 view type - set	Sets the SNMPv3 view type for community 2.	`snmp -ca2` *type* where *type* is • `get` • `set` • `trap` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SNMP community 3 name - set	Sets the name of community 3.	`snmp -c3` *name* where *name* is a descriptive name of community 3. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 31. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 3 first host name or IP address - set	Checks syntax and sets the first host name or IP address of community 3.	`snmp -c3i1` *hostname/ip_address* where *hostname/ip_address* is the first host name or IP address of community 3. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* 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.	`snmp -c3i2` *hostname/ip_address* where *hostname/ip_address* is the second host name or IP address of community 3. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 31. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 3 third host name or IP address - set	Checks syntax and sets the third host name or IP address of community 3.	`snmp -c3i3` *hostname/ip_address* where *hostname/ip_address* is the third host name or IP address of community 3. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SNMPv3 community 3 view type - set	Sets the SNMPv3 view type for community 3.	`snmp -ca3` *type* where *type* is • `get` • `set` • `trap` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SNMP contact name - set	Sets the contact name.	`snmp -cn` *contact_name* where *contact_name* is the name of the party to be contacted when SNMP traps an event. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 31. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP location - set	Sets the location.	`snmp -l` *hostname/ip_address* where *hostname/ip_address* identifies the web site supporting SNMP for this management module. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • If this argument is not specified, the snmp command clears this option. • You can also clear this option by assigning an empty string as its value. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

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

```
snmp
```

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

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

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

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

sol (serial over LAN) command

This command configures SOL functions and indicates SOL status.

Table 32. sol (serial over LAN) command

Function	What it does	Command	Valid targets

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

SOL retry interval - set	Sets the SOL retry interval to the input value.	`sol -i value` where *value* is from 10 ms to 2550 ms, inclusive, in 10 ms increments. If you enter a value less than 10 ms, the retry interval will be set to 10 ms. If you enter a value greater than 2550 ms, the retry interval will be set to 2550 ms. Command use restricted (see “Commands and user authority” on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 32. sol (serial over LAN) command (continued)

Function	What it does	Command	Valid targets
SOL retry count - set	Sets the SOL retry count to the input value.	`sol -c` *value* where *value* is from 0 to 7, inclusive. If you enter a value of 0, no retries will be attempted. If you enter a value greater than 7, an error will be displayed. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SOL send threshold - set	Sets the SOL send threshold to the input value. Setting the threshold value to 1 causes the blade server integrated system management processor to send an SOL packet as soon as the first character is received.	`sol -s` *value* where *value* is from 1 to 251, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SOL accumulate timeout - set	Sets the SOL accumulate timeout to the input value.	`sol -t` *value* where *value* is from 5 ms to 1275 ms, inclusive. If you enter a value less than 5 ms, the accumulate timeout will be set to 5 ms. If you enter a value greater than 1275 ms, an error will be displayed. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SOL enable - global	Enables SOL globally for the BladeCenter unit. The global SOL enable command does not affect the SOL session status for each blade server.	`sol -status on` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SOL enable - blade server	Enables SOL for the specified blade server.	`sol -status on` Command use restricted (see "Commands and user authority" on page 6).	`-T system:blade[`*x*`]` where *x* is the blade server bay number.
SOL disable - global	Disables SOL globally for the BladeCenter unit. The global SOL disable command does not affect the SOL session status for each blade server.	`sol -status off` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SOL disable - blade server	Disables SOL for the specified blade server.	`sol -status off` Command use restricted (see "Commands and user authority" on page 6).	`-T system:blade[`*x*`]` where *x* is the blade server bay number.

Table 32. sol (serial over LAN) command (continued)

Function	What it does	Command	Valid targets
SOL VLAN ID - set	Sets the SOL VLAN ID to the input value.	`sol -v` *value* where *value* is from 1 to 4095, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
CLI key sequence - set	Sets the key sequence that is used to enter the CLI while a Telnet session in SOL mode.	`sol -e` *value* where *value* is the key sequence. In this sequence, a ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example: • `^[` (the carat symbol followed by a left bracket) means `Esc` • `^M` (the carat symbol followed by a capitol M) means carriage return. Refer to an ASCII-to-key conversion table for a complete listing of control-key sequences. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* 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` *value* where *value* is the key sequence. In this sequence, a ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example: • `^[` (the carat symbol followed by a left bracket) means `Esc` • `^M` (the carat symbol followed by a capitol M) means carriage return. Refer to an ASCII-to-key conversion table for a complete listing of control-key sequences. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

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

```
sol -t 25
```

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

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

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

```
sol
```

To display the SOL settings for the server blade in the third bay, while blade 3 is set as the persistent command environment, at the system:blade[3]> prompt, type

```
sol
```

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

```
system:mm[1]> sol -t 25
OK
system:mm[1]> sol
-status enabled
-c 3
-e ^[(
-i 250
-r ^[R^[r^[R
-s 250
-t 5
VLAN ID 4095
system:mm[1]>

system:blade[3]> sol
-status enabled
SOL Session: Not Ready
SOL retry interval: 250 ms
SOL retry count: 3
SOL bytes sent: 0
SOL bytes received: 0
SOL destination IP address: 10.10.10.80
SOL destination MAC: 00:00:00:00:00:00
SOL I/O module slot number: 0
SOL console user ID:
SOL console login from:
SOL console session started:
SOL console session stopped:
Blade power state: On
SOL recommended action: Internal network path between the AMM and this
blade server is currently not available.  Please refer to AMM user guide for
troubleshooting information.
system:blade[3]>
```

tcpcmdmode command

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

Table 33. tcpcmdmode command

Function	What it does	Command	Valid targets
Display TCP command-mode session status and timeout	Displays the TCP command-mode session status (on or off) and timeout.	`tcpcmdmode`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set TCP command-mode session timeout	Sets the TCP command-mode session timeout value.	`tcpcmdmode -t` *timeout* where *timeout* is from 0 seconds (no timeout) to 4294967295 seconds, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable / disable TCP command-mode sessions	Enables or disables TCP command-mode sessions that are used by IBM Director software for out-of-band communication with the management module.	`tcpcmdmode -status` *state* where *state* is `on` or `off`. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

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

```
tcpcmdmode -status on
```

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

```
tcpcmdmode -t 360
```

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

```
tcpcmdmode
```

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

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

telnetcfg (Telnet configuration) command

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

Table 34. telnetcfg (Telnet configuration) command

Function	What it does	Command	Valid targets
Display command-line session configuration	Displays the command-line session configuration of the primary management module.	`telnetcfg`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set command-line session timeout for primary management module	Sets the command-line session timeout value for the primary management module.	`telnetcfg -t` *timeout* where *timeout* is from 0 seconds (no timeout) to 4294967295 seconds, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

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

```
telnetcfg -t 360
```

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

```
telnetcfg
```

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

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

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 35. update (update firmware) command

Function	What it does	Command	Valid targets

Display firmware attributes	Displays attributes of the firmware installed in the command target. Return values are:
	• Firmware type
	• Build ID
	• Filename
	• Release date
	• Revision level
	Notes:
	• When the command target is the primary management module, this command will return the values for the currently active firmware and for the pending firmware, that will become active after the next management module reboot.
	• For I/O modules that support it, this command will also display firmware image information.
		`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 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.
	Note: The P6 blade server firmware is too large to be updated using this command. See the *User's Guide* for your P6 blade server for information about updating firmware.
		`update -i` *ip_address* `-l` *filename*
		where:
		• *ip_address* is the IP address of TFTP server.
		• *filename* is the path name of the of the firmware update file.
		Command use restricted (see "Commands and user authority" on page 6).
			`-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 module bay number.

Table 35. 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.
	Note: The P6 blade server firmware is too large to be updated using this command. See the *User's Guide* for your P6 blade server for information about updating firmware.
		`update -i` *ip_address* `-l` *filename* `-v`
		
		where:
		• *ip_address* is the IP address of TFTP server.
		• *filename* is the path name of the of the firmware update file.
		
		Command use restricted (see "Commands and user authority" on page 6).
			`-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 module bay number.

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

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

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

```
update -a
```

To update the service-processor firmware in the blade server in blade bay 8 (not using verbose mode), while the management module in management-module bay 1 is set as the persistent command environment, type the following command at the `system:mm[1]>` prompt. For this example, the IP address of the TFTP server is 192.168.70.120 and the firmware file containing the update is named h8.pkt.

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

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

```
system:mm[1]> update -v -i 192.168.70.120 -l dev_mm.pkt
TFTP file upload successful 1517829.
Starting flash packet preparation.
Flash preparation - packet percent complete 24.
Flash preparation - packet percent complete 48.
Flash preparation - packet percent complete 72.
Flash preparation - packet percent complete 96.
Flash preparation - packet percent complete 100.
Flash operation phase starting.
Flashing - packet percent complete 34.
Flashing - packet percent complete 38.
Flashing - packet percent complete 50.
Flashing - packet percent complete 55.
Flashing - packet percent complete 80.
```

```
Flashing - packet percent complete 90.
Flash operation complete. The new firmware will become active after the next
reset of the MM.
OK
system:mm[1]> update -a
Bay 1 Name 1
Firmware type: Main application
Build ID: BRETKD+
Filename: CNETMNUS.PKT
Released: 11-17-03
Revision: 16
Firmware type: Boot ROM
Build ID: BRBR1B+
Filename: CNETBRUS.PKT
Released: 10-27-03
Revision: 16
Firmware type: Remote control
Build ID: BRRG1B+
Filename: CNETRGUS.PKT
Released: 10-27-03
Revision: 16
OK
system:mm[1]> update -i 192.168.70.120 -l h8.pkt -T system:blade[8]:sp
OK
system:mm[1]>
```

uplink (management module failover) command

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

Table 36. uplink command

Function	What it does	Command	Valid targets
Display uplink failover status	Displays the management-module uplink failover status (enabled or disabled) and the failover delay.	`uplink`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set physical network uplink failover delay	Sets the amount of time between detection of a management-module physical uplink failure and failover to the standby management module.	`uplink -del delay` where *delay* is from 1 to 255 minutes, inclusive. If you enter a value outside this range, an error will be displayed. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable physical uplink failover	Enables failover to the standby management module if the external physical network interface of the primary management module fails.	`uplink -on` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.
Disable physical uplink failover	Disables failover to the standby management module if the external physical network interface of the primary management module fails.	`uplink -off` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

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

```
uplink -on
```

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

```
uplink -del 3
```

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

```
uplink
```

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

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

users command

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

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

Table 37. 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: • 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: • 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 6).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 37. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Create user profile	Create the specified management-module user profile. All fields must be specified when creating a user profile for the BladeCenter T management module. For management modules other than those installed in a BladeCenter T unit, only the following user-profile fields are required: • -*user_number* • -n *user_name* • -a *user_authority* • -p *user_password*	`users -`*user_number* `-n` *user_name* `-p` *user_password* `-a` *user_authority* `-cn` *context_name* `-ap` *auth_protocol* `-pp` *privacy_protocol* `-ppw` *privacy_pwd* `-at` *access_type* `-i` *ip_addr/hostname* where: • *user_number* is a number from 1 to 12 that corresponds to an unused user number in the "Display all user profiles" list. • *user_name* is a alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_). Each of the 12 user names must be unique. • *user_password* can be blank or an alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_), and must include at least one alphabetic and one non-alphabetic character. • *user_authority* is one of the following: – `operator` (read-only) – `rbs` (see Set user authority level for more information) • *context_name* is a string for SNMPv3 context that is up to 31 characters in length. Each of the 12 context names must be unique. *(continued on next page)*	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 37. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Create user profile *(continued)*		• *auth_protocol* is an SNMPv3 authentication protocol of – `sha` – `md5` – blank (no entry) for none • *privacy_protocol* is an SNMPv3 privacy protocol of `des` or blank (no entry) for none. If the privacy protocol is set to none, no `-ppw` command option (privacy password) is required. • *privacy_pwd* is an SNMPv3 privacy password string of up to 31 characters in length. If the privacy protocol is set to none, the `-ppw` command option does not need to be used unless a privacy password is required. • *access_type* is an SNMPv3 access type of – `read` – `write` – `traps` • *ip_addr/hostname* is a valid SNMPv3 static IP address or an alphanumeric hostname string up to 63 characters in length. Command use restricted (see "Commands and user authority" on page 6).	

Table 37. 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.	`users -`*user_number* `-n` *user_name* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *user_name* is a alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_). Each of the 12 user names must be unique. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set user password	Sets a user password in the specified management-module user profile.	`users -`*user_number* `-p` *user_password* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *user_password* can be blank or an alphanumeric string up to 15 characters in length that can include periods (.) and underscores (_), and must include at least one alphabetic and one non-alphabetic character. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 37. users (management-module users) command (continued)

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

Table 37. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Set user authority level ***(continued)***		where the *devices* are one or more of the following devices, separated by a vertical bar (|). Ranges of devices are separated by a dash (-). • c*n* (Chassis *n*, where *n* is a valid chassis number. Use c1 for single-chassis environments.) • b*n* (Blade *n*, where *n* is a valid blade bay number in the chassis) • s*n* (I/O module *n*, where *n* is a valid I/O module bay number in the chassis) Command use restricted (see "Commands and user authority" on page 6).	
Set SNMPv3 user context name	Sets an SNMPv3 context name in the specified management-module user profile. The context name defines the context the SNMPv3 user is working in. A context name can be shared by multiple users.	`users -`*user_number* `-cn` *context_name* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *context_name* is a string up to 31 characters in length. Each of the 12 context names must be unique. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 37. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Set SNMPv3 user authentication protocol	Sets the SNMPv3 authentication protocol to be used for the specified management-module user profile.	`users -`*user_number* `-ap` *auth_protocol* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *auth_protocol* is – `sha`, – `md5` – blank (no entry) for none Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set SNMPv3 user privacy protocol	Sets the SNMPv3 privacy protocol to be used for the specified management-module user profile. If the privacy protocol is set to none, no -ppw command option (privacy password) is required.	`users -`*user_number* `-pp` *privacy_protocol* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *privacy_protocol* is `des` or blank (no entry) for none. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set privacy password for SNMPv3 user	Sets an SNMPv3 privacy password in the specified management-module user profile.	`users -`*user_number* `-ppw` *privacy_pwd* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *privacy_pwd* is a string up to 31 characters in length. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 37. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Set access type for SNMPv3 user	Sets an SNMPv3 access type for the specified management-module user profile. This command supports the following access types: • read: the user can query Management Information Base (MIB) objects and receive traps. • write: the user can query and set MIB objects and receive traps. • traps: the user can only receive traps.	`users -`*user_number* `-at` *access_type* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *access_type* is – `read` – `write` – `traps` Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set IP address or hostname for SNMPv3 trap receiver	Sets the IP address or hostname that will receive SNMPv3 traps for the specified management-module user profile.	`users -`*user_number* `-i` *ip_addr/hostname* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *ip_addr/hostname* is a valid static IP address or an alphanumeric hostname string up to 63 characters in length. Command use restricted (see "Commands and user authority" on page 6).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

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

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

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

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

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

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

```
users
```

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

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

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

Chapter 4. Error messages

This topic lists error messages for the BladeCenter command-line interface.

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

This topic 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 38. Common errors

Error message	Definition
Alarm panel card is not present in this slot.	The user tries to issue a command to an empty alarm panel card slot.
Backplane Mux card is not present in this slot.	The user tries to issue a command to an empty backplane mux card slot.
Command cannot be issued to this target. Type env - h for help on changing targets.	The user tries to issue a command to a target that does not support that command.
Command line contains extraneous arguments.	Extra command arguments were entered.
Duplicate option: *option* where *option* identifies the command option that was entered more than once.	A user tries to enter the same command option in a single command multiple times. For example, `dns -i 192.168.70.29 -i`
Each option can only be used once per command.	A user tries to enter the same command option in a single command multiple times. For example, `env -T system:blade[4] -T system:blade[5]`.
Error: Command not recognized. Type 'help' to get a list of supported commands.	A user tries to enter a command that does not exist.
Error reading data for the option - *option* where *option* identifies the command option that is returning an error.	An error occurs while the management module is reading data of a option.
Error writing data for the option *option* where *option* identifies the command option that is returning an error.	An error occurs while the management module is writing a command option value.
Firmware update is in progress. Try again later.	Firmware update is in progress.
Illegal option: *option* where *option* identifies the illegal short command option that was entered.	An illegal short command option is entered.
Integer argument out of range (*range* - *range*) for *option*: *argument* where: • *range* identifies the range limits • *option* identifies the command option • *argument* identifies the integer that is out of range	An integer is entered that is out of range.
Internal error.	An internal error occurs.
Invalid integer argument for *option*: *argument* where: • *option* identifies the command option • *argument* identifies the invalid argument	An invalid integer is entered.
Invalid option.	An invalid command option is entered.

Table 38. Common errors (continued)

Error message	Definition
Invalid option argument for *option*: *argument* where: • *option* identifies the command option • *argument* identifies the invalid argument	An invalid argument for a command option is entered.
Invalid option for this target: *option* where *option* identifies the option that is invalid.	A user tries to issue a command with an invalid option for the target.
Invalid parameter. Input must be numeric.	A user tries to enter a non-numeric argument.
Invalid syntax. Type *command* - h for help. where *command* identifies the command that is returning an error.	A user tries to enter a command that is not syntactically correct.
Invalid target path.	A user tries to issue a command to a target that is not valid.
Long option *option* requires an argument where *option* identifies the long command option that is missing an argument.	A long command option is entered without a required argument.
Missing option name	A dash (-) is entered without a command option name.
Network Clock card is not present in this slot.	The user tries to issue a command to an empty network card slot.
Read/write command error.	An error occurs while the management module is executing the command.
Short option *option* requires an argument where *option* identifies the short command option that is missing an argument.	A short command option is entered without a required argument.
Syntax error. Type *command* -h for help. where *command* identifies the command that is returning an error.	A user tries to enter a command improperly.
That blade is presently not available. Please try again shortly.	A user tries to connect to a blade that is already in use.
The argument for the option *arg* is outside the valid range. where *arg* identifies the command option that is out of range.	A user tries to enter an arg outside the option's valid range.
The target bay is empty.	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.	A user tries to issue a command to a target that is out of range for that target. For example, the `env -T system:blade[15]` command is out of range because the BladeCenter unit has only 14 blade bays.
The target slot is out of range.	The user tries to issue a command to a target which is out of range for that target.
There is no blade present in that bay.	The user tries to issue a command to an empty blade bay.

Table 38. Common errors (continued)

Error message	Definition
There is no blower present in that bay.	The user tries to issue a command to an empty chassis cooling unit bay.
There is no management module present in that bay.	The user tries to issue a command to an empty management module bay.
There is no power source present in that bay.	The user tries to issue a command to an empty power module bay.
There is no switch present in that bay.	The user tries to issue a command to an empty I/O module bay.
Unknown long option: *option* where *option* identifies the command option that is unknown.	A user tries to enter a long option that is not valid for the command.
Unknown option: *option* where *option* identifies the command option that is unknown.	An unknown option is used.
Unrecognized long option: *option* where *option* identifies the illegal long command option that was entered.	An illegal long command option is entered.
Unsupported target type.	A user tries to issue a command to an unsupported target.
User does not have the authority to issue this command.	A user lacks the authority level necessary to execute a command.

alarm command errors

This topic lists error messages for the alarm command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 39. alarm command errors

Error message	Definition
A duplicate option is found in the requested command.	A duplicate argument is entered.
Alarm Description must be provided for setting an alarm.	The user tries to set an alarm without providing an alarm description.
Alarm ID must be from 1 to 255.	An invalid alarm ID is entered.
Category must be from 1 to 255.	An invalid category argument is entered.
Generator ID must be from 1 to 255.	An invalid generator ID is entered.
Generator ID must be provided.	A generator information ID is provided without a generator ID.
Module ID must be from 1 to 255.	An invalid module ID is entered.
No active alarm.	No active alarm is found for the command target.
No matching alarm.	No matching alarm is found for the command target.
Reading system health summary failed.	An error occurs while the management module is getting the system health summary.

Table 39. alarm command errors (continued)

Error message	Definition
Severity level must be provided for setting an alarm.	The user tries to set an alarm without specifying the severity level.
Software Generator ID must be from 1 to 255.	The user tries to enter an invalid generator information.
The entered Alarm Key is not in proper format.	The user tries to enter an invalid alarm key.
Unable to acknowledge the requested alarm.	An error occurs while the management module is acknowledging an alarm.
Unable to clear the requested alarm.	An error occurs while the management module is clearing an alarm.
Unable to set the requested alarm.	An error occurs while the management module is setting an alarm.

alertentries command errors

This topic lists error messages for the alertentries command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 40. alertentries command errors

Error message	Definition
-test must be used exclusive of other options.	The user tries to issue a command with the -test option at the same time as the other options.
An entry cannot be modified and deleted in the same command.	A user tries to modify an entry and delete it in the same command.
Arguments containing spaces must be enclosed in quotation marks.	A user tries to enter a string containing spaces that has an opening quotation mark without a closing quotation mark.
Enabling the application alert failed.	An error occurs while the management module is enabling the application alert.
Generating test alert failed.	An error occurs while the management module is generating a test alert.
Invalid input. Angle brackets are not allowed in the name field.	A user tries to enter a string parameter containing < or > for the -n (name) command option.
Invalid option.	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.	A user tries to enter a parameter value containing non-numeric characters for a command option requiring numeric input.
Restoring previous configured value for the application alert failed.	An error occurs while the management module is restoring previous configured value for the application alert.
Syntax error. -e can only be used in conjunction with the email argument.	A user tries to enter an invalid email address for the -e command option.
Syntax error. -i can only be used in conjunction with the director argument.	A user tries to enter an invalid IP address for the -i command option.
Syntax error. Type alertentries -h for help.	An alert entry number is entered without the leading dash (-).

Table 40. alertentries command errors (continued)

Error message	Definition
The name must be less than 32 characters long.	A user tries to enter too many characters in an input field.
When creating a new entry, all options are required.	A required command option is missing when creating a user.

boot command errors

This topic lists errors for the boot command.

There are no unique errors for the boot command. See "Common errors" on page 114 for a list of error messages that apply to all commands.

clear command errors

This topic lists error messages for the clear command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 41. clear command errors

Error message	Definition
Firmware update is in progress. Try again later.	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.	An error occurs while the management module is resetting the management module to its default configuration. The error message displays and the management-module configuration does not reset.

clearlog command errors

This topic lists error messages for the clearlog command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 42. clearlog command errors

Error message	Definition
Error clearing the event log.	An error occurs while the management module is clearing the event log.

clock command errors

This topic lists error messages for the clock command.

See “Common errors” on page 114 for a list of error messages that apply to all commands.

Table 43. clock command errors

Error message	Definition
GMT+2:00 requires one of the following dst values: off, ee, gtb, egt, or fle	The user tries to change the Greenwich mean-time (GMT) offset to +2:00 without adjusting the DST setting.
GMT+10:00 requires one of the following dst values: off, ea, tas, or vlad	The user tries to change the GMT offset to +10:00 without adjusting the DST setting.
GMT*offset* requires one of the following dst values: off, uc, other where *offset* is the daylight-savings time offset.	The user tries to change the GMT offset to -9, -8, -7, -6, or -5 without adjusting the DST setting.
Invalid dst setting for GMT+10:00: *setting* where *setting* is the illegal daylight-savings time setting that was entered.	The user tries to enter an invalid -dst setting for a GMT offset of 10.
Invalid dst setting for GMT+2:00: *setting* where *setting* is the illegal daylight-savings time setting that was entered.	The user tries to enter an invalid -dst setting for a GMT offset of 2.
Invalid dst setting for GMT*offset*: *setting* where *setting* is the daylight-savings time offset and *setting* is the illegal daylight-savings time setting that was entered.	The user tries to enter an invalid -dst setting for a GMT offset of -9, -8, -7, -6, or -5.
Invalid dst setting. The gmt offset does not support dst.	The user tries to turn on dst for a GMT offset that does not support daylight-savings time.
Invalid input for -dst.	A user tries to enter an invalid argument for the option -dst.
Reading date and time failed.	An error occurs while the management module is reading the date and time.
Reading GMT offset failed.	An error occurs while the management module is reading the GMT offset.
Reading status of daylight savings time failed.	An error occurs while the management module is reading the daylight savings time status.
The gmt offset you entered does not support dst. Turning dst off.	A user tries to enter a GMT offset that does not support daylight savings time.

config command errors

This topic lists error messages for the config command.

See “Common errors” on page 114 for a list of error messages that apply to all commands.

Table 44. config command errors

Error message	Definition
Arguments containing spaces must be enclosed in quotation marks.	The user tries to enter an management module Contact or Location without ending double quotes.
Contact must be enclosed in quotation marks.	The user tries to enter an management module Contact without enclosing it in double quotes.
Invalid input. Contact may not contain angle brackets.	The user tries to enter an management module Contact containing angle brackets ("<" and ">").
Invalid input. Location may not contain angle brackets.	The user tries to enter an management module Location containing angle brackets ("<" and ">").
Invalid input. Name must be less than 16 characters.	The user tries to enter a name that is more than 15 characters in length.
Invalid input. Name may not contain angle brackets.	The user tries to enter a blade server name that contains angle brackets: "<" or ">".
Invalid input. Only alphanumeric characters, underscores, hyphens, pound signs, and periods are allowed.	The user tries to enter a name for the management module that is not valid.
Invalid input. -sn should have exactly seven alphanumeric characters.	The user tries to enter a serial number that is not exactly seven alphanumeric characters.
Invalid input. -tm should have exactly seven alphanumeric characters.	The user tries to enter a type or model name that is not exactly seven alphanumeric characters.
Invalid input. -uuid should have exactly 32 hex digits.	The user tries to enter a universally unique ID that is not exactly 32 hex digits.
Location must be enclosed in quotation marks.	The user tries to enter an management module Location without enclosing it in double quotes.
Reading SNMPv1/SNMPv3 status failed.	An internal errors occurs while the management module is reading the SNMPv1/v3status.
System location and contact must be defined when SNMPv1 or SNMPv3 agent is enabled.	The user tries to undefine the system location or contact information while an SNMPv1 or SNMPv3 agent is enabled.

console command errors

This topic lists error messages for the console command.

See “Common errors” on page 114 for a list of error messages that apply to all commands.

Table 45. console command errors

Error message	Definition
A SOL session socket was not available.	The command-line interface fails to establish an SOL connection to a blade server.
Error entering console mode.	An error occurs while the management module is trying to establish an SOL connection.

Table 45. console command errors (continued)

Error message	Definition
Global SOL is not enabled	SOL is not enabled globally.
Internal Error	An error occurs while the management module is processing the command.
SOL is not ready	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	SOL is not enabled on the blade server where the user is trying to start an SOL session.
SOL session is already active	The user cannot start an SOL session with a blade server because an SOL session with that blade server is already in progress.
The maximum number of sessions to this blade has been reached.	The blade server has no available sessions for a user to connect to.
Unknown error occurred while attempting to connect.	An unknown error occurs when connecting to a blade server.

dhcpinfo command errors

This topic lists errors for the dhcpinfo command.

There are no unique errors for the dhcpinfo command. See "Common errors" on page 114 for a list of error messages that apply to all commands.

displaylog command errors

This topic lists error messages for the displaylog command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 46. displaylog command errors

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

dns command errors

This topic lists error messages for the dns command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 47. dns command errors

Error message	Definition
-on and -off cannot both be used in the same command.	A user tries to enable and disable DNS in the same command.
At least one address is required to enable DNS.	A user tries to enable DNS without configuring at least one address.
DNS State Can not be determined.	An error occurs while the management module is reading the DNS state.

Table 47. dns command errors (continued)

Error message	Definition
Input length is greater than the maximum characters allowed.	A user tries to enter too many characters in an input field.
Invalid ip address	A user tries to set an invalid IP address.
Reading status of DNS failed.	An error occurs while the management module is reading the DNS state.
Reading status of interface failed.	An error occurs while the management module is reading the status of an interface.

env command errors

This topic lists errors for the env command.

There are no unique errors for the env command. See "Common errors" on page 114 for a list of error messages that apply to all commands.

exit command errors

This topic lists errors for the exit command.

There are no unique errors for the exit command. See "Common errors" on page 114 for a list of error messages that apply to all commands.

fuelg command errors

This topic lists error messages for the fuelg command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 48. fuelg command errors

Error message	Definition
-am cannot be enabled while -e is set to nebs.	The user attempts to enable the acoustic mode while the environment is set to nebs.
-ps and -dps cannot be enabled at the same time.	The user attempts to enable -ps and idps at the same time.
A power module failure in domain *domain_number* can result in an immediate shutdown. where *domain_number* identifies the power domain.	A power module fails and the domain in which it is installed loses redundancy. The BladeCenter unit might turn itself off, based on the power management configuration.
Blade *blade_number* is not allowed to power on because of insufficient power. where *blade_number* identifies the blade server.	There is insufficient power available in the power domain to turn on this blade server.
Blade *blade_number* is throttled. where *blade_number* identifies the blade server.	The specified blade server has reduced power (power throttling) in response to a thermal event or oversubscription condition.
Blade *blade_number* was instructed to power off due to power budget restrictions. where *blade_number* identifies the blade server.	BladeCenter power management turns off a blade server that is already on in response to a oversubscription condition.

Table 48. fuelg command errors (continued)

Error message	Definition
Blade must be powered on to enable/disable dps.	The user attempts to enable or disable dynamic power server mode for a blade server while its power is off.
Checking if power is preallocated to switch *number* failed. where the *number* I/O-module bay number.	An error occurs while the management module is checking if power is preallocated for the specified I/O module.
Demand exceeds a single power module. Throttling can occur in power domain *domain_number*. where *domain_number* identifies the power domain.	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.
Getting blade health state parameters failed.	An error occurs while the management module is reading the blade server health state parameters.
Getting blade pcap maximum value failed.	An error occurs while the management module is reading the blade server power cap maximum value.
Getting blade pcap minimum value failed.	An error occurs while the management module is reading the blade server power cap minimum value.
Getting blade power cap level failed.	An error occurs while the management module is reading the blade server power cap level.
Getting data of domain 1 (or 2) failed.	An error occurs while the management module is reading the data of power domain 1 (or 2).
Getting domain latest power sample failed.	An error occurs while the management module is reading the latest power domain sample.
Getting duty cycle numbers failed.	An error occurs while the management module is reading the duty cycle numbers.
Getting duty cycle numbers of blade *blade_number* failed. where *blade_number* identifies the blade server.	An error occurs while the management module is reading the duty cycle numbers of specified blade server.
Getting dynamic power management capabilty of blade*blade_number* failed. where *blade_number* identifies the blade server.	An error occurs while the management module is reading the dynamic power management capability of specified blade server.
Getting information of power*number* failed. where the *number* identifies the specified power module.	An error occurs while the management module is reading data of specified power module.
Getting module domain map for blower*number* failed. where the *number* identifies the specified chassis cooling unit.	An error occurs while the management module is reading module domain map of specified chassis cooling unit.
Getting module domain map for midplane failed.	An error occurs while the management module is reading the module domain map for midplane.
Getting module domain map for MM*number* failed. where the *number* identifies the specified management module.	An error occurs while the management module is reading the module domain map of specified management module.
Getting module domain map for mux*number* failed. where the *number* identifies the location of the component.	An error occurs while the management module is reading the module domain map of specified mux.

Table 48. fuelg command errors (continued)

Error message	Definition
Getting module domain map for NC*number* failed. where the *number* identifies the location of the component.	An error occurs while the management module is reading the module domain map of specified network clock module.
Getting module domain map of mt*number* failed. where the *number* identifies the specified mt.	An error occurs while the management module is reading the module domain map of specified mt.
Getting module domain map of PM Cooling Device *number* failed. where *number* identifies the blade server.	An error occurs while the management module is reading the module domain map of specified power module Cooling Device.
Getting module domain map of switch*number* failed. where the *number* represents the specified I/O module.	An error occurs while the management module is reading the module domain map of specified I/O module.
Getting module domain map of Telco alarm panel failed.	An error occurs while the management module is reading the module domain map of Telco alarm panel.
Getting power management policy for domain *domain_number* failed where *domain_number* is the number of the domain that was entered.	An error occurs while the management module is reading the power management policy of specified domain.
Getting power state of blade*blade_number* failed. where *blade_number* identifies the blade server.	An error occurs while the management module is reading the power state of specified blade server.
Getting power values for blower*number* failed. where the *number* identifies the location of the component.	An error occurs while the management module is reading the power values of specified chassis cooling unit.
Getting power values for DSS*number* failed. where the *number* represents the specified DSS.	An error occurs while the management module is reading the power values of specified DSS.
Getting power values for MM*number* failed. where the *number* identifies the location of the component.	An error occurs while the management module is reading the power values of specified management module.
Getting power values for NC*number* failed. where the *number* represents the specified NC.	An error occurs while the management module is reading the power values of specified network clock module.
Getting power values for switch*number* failed. where the *number* represents the specified I/O module.	An error occurs while the management module is reading the power values of specified I/O module.
Getting power values of midplane within domain failed.	An error occurs while the management module is reading the power values of midplane within domain.
Getting power values of mt*number* within domain failed. where the *number* represents the specified mt.	An error occurs while the management module is reading the power values within domain of specified media tray.
Getting power values of mux*number* within domain failed. where the *number* represents the specified mux.	An error occurs while the management module is reading the power values within domain of specified mux.

Table 48. fuelg command errors (continued)

Error message	Definition
Getting power values of PM Cooling Device *number* failed where the *number* represents the specified PM cooling device.	An error occurs while the management module is reading the power values of specified power module cooling device.
Getting power values of Telco alarm panel within domain failed.	An error occurs while the management module is reading the power values of Telco alarm panel within domain.
Getting status of domain *domain_number* failed where *domain_number* identifies the power domain.	An error occurs while the management module is reading the status of specified domain.
Getting the power control setting on blade failed.	An error occurs while the management module is reading the power control setting on blade server.
Invalid option for this blade: *option* where *option* identifies the unacceptable option.	The user attempts to issue a command with an option which is invalid for the targeted blade server.
Maximum CPU Speed not available.	An error occurs while the management module is reading maximum CPU Speed.
pcap must be between *min* and *max* Watts. where *min* and *max* represent the minimum and maximum wattage values permitted.	The user input for power cap is out of the range.
Power value is not in the guaranteed capping range.	The user attempts to set a power value that is out of range.
Setting -e to nebs automatically disables -am, so "-am on" will be ignored.	The user attempts to set the environment to nebs and to enable the acoustic mode at the same time.
There are mismatched power modules in power domain *domain_number*. where *domain_number* identifies the power domain.	The power modules installed in a power domain have different ratings.
There is no thermal trending data to display.	An error occurs while the management module is reading thermal trending data.
There is no trending data to display.	An error occurs while the management module is reading power trending data.
Unable to change power management settings, domain may be oversubscribed.	An error occurs while the management module is configuring the power management policy.

health command errors

This topic lists errors for the health command.

See “Common errors” on page 114 for a list of error messages that apply to all commands.

Table 49. health command errors

Error message	Definition
Getting system health summary failed.	An error occurs while the management module is reading the system health summary.

help command errors

This topic lists errors for the help command.

There are no unique errors for the help command. See “Common errors” on page 114 for a list of error messages that apply to all commands.

history command errors

This topic lists errors for the history command.

There are no unique errors for the history command. See “Common errors” on page 114 for a list of error messages that apply to all commands.

identify command errors

This section lists error messages for the identify command.

See “Common errors” on page 114 for a list of error messages that apply to all commands.

Table 50. identify command errors

Error message	Definition
-d can only be used on the system target.	The user tries to issue a command with the -d option to a target other than system.
-d can only be used with the -s on.	The user tries to issue a command with the -d option without -s on setting.
Delay value must be less than *max* where *max* is the preset maximum.	The user input for option -d exceeds the maximum.
Delay value must be less than 60.	A user tries to enter a -d value that is greater than 60 seconds.
Error accessing remote LED.	An error occurs while the management module is accessing a remote LED.
Error getting LED status.	An error occurs while the management module is reading the blade LED status.
Error reading system LED state.	An error occurs while the management module is reading the system LED status.
Error setting system LED.	An error occurs while the management module is setting the system LED.
Error unknown command.	The user tries to enter unrecognized command.
Identify: Error accessing remote LED.	An error occurs while the management module is processing the command.
Identify: error getting LED status.	An error occurs while the management module is processing the command.
Identify: error setting Management Module LED.	An error occurs while the management module is processing the command.
Identify: Error unknown command.	An error occurs while the management module is processing the command.
Identify: LED status not supported.	The user tries to get the status of an LED that is not supported by a blade server.

Table 50. identify command errors (continued)

Error message	Definition
Identify: unknown LED state *state* where *state* identifies the LED state that was returned.	An LED state other than on, off, or blinking is returned.
Identify: Unknown return status *status* where the *status* value varies based on the problem that was encountered.	An error occurs while the management module is processing the command.
Syntax error.	The user tries to enter an invalid command option. Type `identify -h` for command help.
The chassis identification LED cannot be turned off at this time because one or more blades have their location LED active.	The user tries to turn off the chassis identification LED under conditions that do not permit this action.

ifconfig command errors

This topic lists error messages for the ifconfig command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 51. ifconfig command errors

Error message	Definition
-*option* is not supported by this type of I/O Module. where *option* is ir, gr, or sr.	The user tries to issue a command with an option -ir, -gr, or -sr which is not supported by the targeted I/O module.
-up and -down can not be both used in same line.	The user tries to issue a command with both the -up and -down options.
Cannot apply network configuration. Blade in configuration phase.	An error occurs while the management module is setting the network configuration.
Configuration not supported on this I/O Module type.	The user tries to issue a command for the configuration which is not supported by targeted I/O module type.
Configuration not supported on this switch type.	The user tries to issue a command to an unsupported I/O module type.
Enabling/Disabling new IP configuration failed.	An error occurs while the management module is enabling or disabling the new IP configuration.
Error reading gateway address.	An error occurs while the management module is reading the gateway address of a network interface (eth0 or eth1).
Error reading IP Address.	An error occurs while the management module is 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.	An error occurs while the management module is reading the burned-in MAC address of a network interface (eth0 or eth1).
Error reading the data rate.	An error occurs while the management module is reading the data rate setting of a network interface (eth0 or eth1).

Table 51. ifconfig command errors (continued)

Error message	Definition
Error reading the DHCP configuration.	An error occurs while the management module is reading the DHCP setting of a network interface (eth0).
Error reading the duplex setting.	An error occurs while the management module is reading the duplex setting of a network interface (eth0 or eth1).
Error reading the hostname.	An error occurs while the management module is reading the host name of a network interface (eth0).
Error reading the locally administered MAC address.	An error occurs while the management module is reading the locally administered MAC address of a network interface (eth0 or eth1).
Error reading the maximum transmission unit.	An error occurs while the management module is reading the maximum transmission unit (MTU) setting of a network interface (eth0 or eth1).
Error reading the subnet mask.	An error occurs while the management module is reading the subnet mask of a network interface (eth0 or eth1).
Error writing IP Address.	An error occurs while the management module is setting the IP address of the integrated system management processor on a blade server.
Getting interface status failed.	An error occurs while the management module is reading the interface status.
I/O Module is in Stacking Mode and cannot change its Gateway configuration.	The user tries to issue a command to change the Gateway configuration with the I/O Module in Stacking Mode.
I/O Module is in Stacking Mode and cannot change its IP configuration.	The user tries to issue a command to change the IP configuration with the I/O Module in Stacking Mode.
I/O Module is in Stacking Mode and cannot change its Subnet configuration.	The user tries to issue a command to change Subnet configuration with I/O Module in Stacking Mode.
Invalid gateway address.	The user tries to enter an invalid gateway address.
Invalid hostname.	The user tries to enter an invalid hostname.
Invalid hostname arg for *option*: *hostname*. Consecutive dots where: • *option* identifies the command option • *hostname* identifies the invalid hostname argument	The user tries to enter consecutive periods (.) as part of a hostname.
Invalid hostname arg for *option*: *hostname*. Length has to be < 64 characters where: • *option* identifies the command option • *hostname* identifies the invalid hostname argument	The user tries to enter a hostname longer than 63 characters.
Invalid hostname arg for *option*: *hostname*. Only alphanumeric chars and._- allowed where: • *option* identifies the command option • *hostname* identifies the invalid hostname argument	The user tries to enter an hostname that contains invalid characters. Valid characters that can be used in a hostname are letters, numbers, periods (.), dashes (-), and underscores (_).

Table 51. ifconfig command errors (continued)

Error message	Definition
Invalid ip address.	Displays for one of the following errors: • A user tries to set the IP address of system:blade[1]:sp to an invalid IP address. • A user tries to set an IP address whose last part is greater than 255 (the maximum number of blade servers). • A user tries to enter an invalid IP address for the -i (static IP address) command option.
Invalid IP arg for *option*: *ip_address*. Each byte has to be in the range (0-255) where: • *option* identifies the command option • *ip_address* identifies the invalid IP address argument	The user tries to enter an IP address that is out of range. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255.
Invalid IP arg for *option*: *ip_address*. Enter 4 bytes separated by 3 dots where: • *option* identifies the command option • *ip_address* identifies the invalid IP address argument	The user tries to enter an IP address that is too long. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255.
Invalid IP arg for *option*: *ip_address*. Too few bytes where: • *option* identifies the command option • *ip_address* identifies the invalid IP address argument	The user tries to enter an IP address with too few bytes. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255.
Invalid IP arg for *option*: *ip_address*. Too many bytes where: • *option* identifies the command option • *ip_address* identifies the invalid IP address argument	The user tries to enter an IP address with too many bytes. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255.
Invalid mac address.	The user tries to enter an invalid MAC address.
Invalid MAC arg for *option*: *address*. Invalid syntax where: • *option* identifies the command option • *address* identifies the invalid MAC address argument	The user tries to enter an invalid MAC address.
Invalid MAC arg for *option*: *address*. Multicast addresses not allowed where: • *option* identifies the command option • *address* identifies the invalid MAC address argument	The user tries to enter a multicast address.
Invalid MAC arg for *option*: *address*. Too few bytes where: • *option* identifies the command option • *address* identifies the invalid MAC address argument	The user tries to enter a MAC address with too few bytes.
Invalid MAC arg for *option*: *address*. Too many bytes where: • *option* identifies the command option • *address* identifies the invalid MAC address argument	The user tries to enter a MAC address with too many bytes.
Invalid option for ethernet interface.	A user tries to change a static property of eth1 (hostname, DHCP, data rate, duplex).

Table 51. ifconfig command errors (continued)

Error message	Definition
Invalid parameter. The locally administered MAC address cannot be a multicast address.	The user tries to set the locally administered MAC address to a multicast address.
Invalid parameter. The MTU must be between 60 and 1500, inclusive.	The user tries to enter an MTU outside the valid range.
Invalid parameter. Valid values for -c are dhcp, static, or dthens.	A user tries to enter an invalid parameter for the -c (Ethernet configuration method) command option.
Invalid parameter. Valid values for -d are auto, half, and full.	The user tries to enter an invalid parameter with the -d option.
Invalid parameter. Valid values for -r are auto, 10, and 100.	The user tries to enter an invalid parameter with the -r option.
Invalid subnet mask.	The user tries to enter an invalid subnet mask.
Maybe blade network configuration is still in discovery phase. Please check and try again.	An error occurs while the management module is reading the blade network configuration.
Please check blade health status and try again.	An error occurs while the management module is reading the blade health status.
The target must be system:blade[1]:sp for this command	A user tries to issue the `ifconfig -i` *`ip address`* `-T system:blade[`*`x`*`]:sp` to a blade server other than blade[1]. where *ip address* is a valid ip address and *x* identifies the selected blade server.

info command errors

This topic lists error messages for the info command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 52. info command errors

Error message	Definition
Device not found	No VPD is available for the targeted device.
Getting blade H8 firmware VPD data of blade *blade_number* failed. where *blade_number* identifies the blade server.	An error occurs while the management module is reading the blade H8 firmware VPD data of the targeted blade server.
Getting compact flash cards information failed.	An error occurs while the management module is reading the compact flash cards information.
Getting firmware's VPD data of *type* failed.	An error occurs while the management module is reading the firmware's VPD data of targeted type.
Getting name of blade *blade_number* failed. where *blade_number* identifies the blade server.	An error occurs while the management module is reading the name of the targeted blade server.
Getting name of mm *bay_number* failed. where the *bay_number* specifies the management module.	An error occurs while the management module is reading the name of the targeted management module.
Reload Firmware VPD failed.	An error occurs while the management module is reloading the firmware VPD.
Reload Hardware VPD failed.	An error occurs while the management module is reloading the hardware VPD.

Table 52. info command errors (continued)

Error message	Definition
Reload all failed.	An error occurs while the management module is reloading all VPD and MAC addresses.
Reload MAC address failed.	An error occurs while the management module is reloading the MAC address.
Reload WWN failed.	An error occurs while the management module is reloading WWN.
Status: Unable to read status.	An error occurs while the management module is reading the firmware update status.
Unknown device type.	The command is targeted to an unknown device type.

kvm command errors

This topic lists errors for the kvm command.

There are no unique errors for the kvm command. See "Common errors" on page 114 for a list of error messages that apply to all commands.

list command errors

This topic lists error messages for the list command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 53. list command errors

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

mt command errors

This topic lists errors for the mt command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 54. mt command errors

Error message	Definition
Remote media tray switching must be enabled to change the media tray owner.	A user tries to issue a command to change the media tray owner while media tray switching is not enabled.

power command errors

This topic lists error messages for the power command.

See “Common errors” on page 114 for a list of error messages that apply to all commands.

Table 55. power command errors

Error message	Definition
Invalid POST results.	The POST results are not valid.
Not supported by this type of I/O module. Type env -h for help on changing targets.	The user attempts to apply the -fp option to an I/O module that does not support this option.
POST results could not be read.	An error occurs during POST.
POST results not complete: *hex_code* where the *hex_code* value varies based on the problem that was encountered.	The POST results are not available. See the documentation that comes with the device that failed to respond correctly to the `power` command for information about the *hex_code* value.
Powering on/off blade failed.	An error occurs while powering the blade server on or off.
Powering on/off I/O Module failed.	An error occurs while the management module is powering the I/O module on or off.
Resetting blade failed.	An error occurs while the management module is resetting the blade server.
Shutting down OS and powering off blade failed.	An error occurs while the management module is shutting down the operating system and powering off the blade server.

reset command errors

This topic lists error messages for the reset command.

See “Common errors” on page 114 for a list of error messages that apply to all commands.

Table 56. reset command errors

Error message	Definition
An error occurred while disabling failover.	An error occurs while the management module is disabling failover.
An error occurred while enabling failover.	An error occurs while the management module is enabling failover.
Firmware update is in progress. Try again later.	The user tries to reset the management module during a firmware update. The error message displays and the management module does not reset.
Rebooting blade failed.	An error occurs while the management module is rebooting the blade server.
Resetting and running standard/extended/full diagnostics for I/O module failed.	An error occurs while the management module is resetting and running diagnostics for the I/O module.
Resetting I/O module failed.	An error occurs while the management module is resetting the I/O module.
There is no backup management module installed.	A user tries to enable failover on a management-module reset and there is no standby management module.

Table 56. reset command errors (continued)

Error message	Definition
Resetting blade *blade_number* with NMI not supported. where the *blade_number* identifies the blade server.	A user tries to reset a blade server that does not support non-maskable interrupts (NMI).
Resetting blade *blade_number* with NMI failed. where the *blade_number* identifies the blade server.	An error occurs while the management module is resetting a blade server with NMI.

shutdown command errors

This topic lists errors for the shutdown command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 57. shutdown command errors

Error message	Definition
Invalid option. This command must have the -f option.	The user tries to issue a command without the -f option.

slp command errors

This topic lists errors for the slp command.

There are no unique errors for the slp command. See "Common errors" on page 114 for a list of error messages that apply to all commands.

smtp command errors

This topic lists error messages for the smtp command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 58. smtp command errors

Error message	Definition
Getting SMTP server host name or IP address failed.	An error occurs while the management module is reading the SMTP server host name or IP address.
Input length is greater than the maximum characters allowed.	A user tries to enter too many characters in an input field.
Invalid host name or ip address.	A user tries to set the SMTP host name or IP address to an invalid value.
Removing SMTP server name or IP address failed.	An error occurs while the management module is removing an SMTP server host name or IP address.
Setting SMTP server name or IP address failed.	An error occurs while the management module is setting an SMTP server host name or IP address.
SMTP server host name or IP address is not set.	A user tries to view the SMTP host name or IP address when the values are not set.

snmp command errors

This topic lists error messages for the snmp command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 59. snmp command errors

Error message	Definition
Arguments containing spaces must be enclosed in quotation marks	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.	A user tries to enable SNMP without configuring at least one community name.
Config failed. IP address of 0.0.0.0 is allowed only for the first host name in the first community.	A user tries to set an IP address of 0.0.0.0 for something other than the first host name of the first community.
Config failed. IP address of 0.0.0.0 is allowed only when the first community is configured as Get access type.	A user tries to set an IP address of 0.0.0.0 for the first host name of the first community when the first community is not configured with the Get access type.
Config failed. You defined a community without an IP address or host name.	A user tries to define a community without specifying an IP address or host name.
Config failed. You defined a duplicate community name.	A user tries to define a two communities with the same name.
Enabling/Disabling snmp interface failed.	An error occurs while the management module is enabling or disabling an snmp interface.
Enabling/Disabling snmp traps failed.	An error occurs while the management module is enabling or disabling the snmp traps.
Enabling/Disabling SNMPv3 Agent failed.	An error occurs while the management module is enabling or disabling the SNMPv3 Agent.
Input length is greater than the maximum characters allowed.	A user tries to enter too many characters in an input field.
Invalid community name.	A user tries to set a community name to an invalid value.
Invalid host name or ip address.	A user tries to set the SNMP host name or IP address to an invalid value.
Setting access type of *type* for SNMPv3 failed where *type* is the type of SNMPv3 access desired.	An error occurs while the management module is setting access type for an SNMPv3.
Setting location/contact of the SNMP agent failed.	An error occurs while the management module is setting the location or contact of the SNMP agent.

sol command errors

This topic lists error messages for the sol command.

See “Common errors” on page 114 for a list of error messages that apply to all commands.

Table 60. sol command errors

Error message	Definition
An error occurred while disabling SOL globally.	An error occurs while the management module is disabling SOL globally.
An error occurred while disabling SOL on that blade.	An error occurs while the management module is disabling SOL on a blade server.
An error occurred while enabling SOL globally.	An error occurs while the management module is enabling SOL globally.
An error occurred while enabling SOL on that blade.	An error occurs while the management module is enabling SOL on a blade server.
An error occurred while reading the global SOL status.	An error occurs while the management module is reading the global SOL status.
An error occurred while reading the SOL accumulate timeout.	An error occurs while the management module is reading the SOL accumulate timeout.
An error occurred while reading the SOL retry count.	An error occurs while the management module is reading the SOL retry count.
An error occurred while reading the SOL retry interval.	An error occurs while the management module is reading the SOL retry interval.
An error occurred while reading the SOL send threshold.	An error occurs while the management module is reading the SOL send threshold.
An error occurred while reading the SOL session status on that blade.	An error occurs while the management module is reading the SOL session status on a blade server.
An error occurred while reading the SOL VLAN ID.	An error occurs while the management module is reading the SOL VLAN ID.
An error occurred while setting the SOL accumulate timeout.	An error occurs while the management module is setting the SOL accumulate timeout.
An error occurred while setting the SOL blade reset sequence.	An error occurs while the management module is processing the command.
An error occurred while setting the SOL escape sequence.	An error occurs while the management module is processing the command.
An error occurred while setting the SOL retry count.	An error occurs while the management module is setting the SOL retry count.
An error occurred while setting the SOL retry interval.	An error occurs while the management module is setting the SOL retry interval.
An error occurred while setting the SOL send threshold.	An error occurs while the management module is setting the SOL send threshold.
An error occurred while setting the SOL vlan id.	An error occurs while the management module is processing the command.
Checking if this blade supports SOL failed.	An error occurs while the management module is checking if the selected blade supports SOL.
Invalid arg for -status. Must be on or off.	A user tries to enter an invalid argument for the -status command option.

Table 60. sol command errors (continued)

Error message	Definition
Invalid arg for -status. Must be enabled or off.	A user tries to enter an invalid argument for the -status command option.
Invalid parameter. The accumulate timeout must be between 1 and 251 inclusive.	A user tries to enter an accumulate timeout that is outside of the valid range.
Invalid parameter. The retry count must be between 0 and 7, inclusive.	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.	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.	A user tries to enter a VLAN ID that is out of range.
Retry interval range is too large. Setting to 2550.	A user tries to enter a retry interval that is greater than 2550 ms. If the user tries to enter a retry interval greater than 2550 ms, the retry interval will be set to 2550 ms.
Setting retry interval to 2500 failed.	An error occurs while the management module is setting the retry interval to 2550.
This blade does not support SOL.	A user tries to issue the SOL command to a blade server that does not support SOL.

tcpcmdmode command errors

This topic lists error messages for the tcpcmdmode command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 61. tcpcmdmode command errors

Error message	Definition
Error changing TCP command mode connection.	An error occurs while the management module is changing the TCP command mode Connection.
Error disabling tcpcmdmode.	An error occurs while the management module is disabling the TCP command mode.
Error enabling TCP command mode.	An error occurs while the management module is enabling the TCP command mode.
Invalid parameter. Input must be numeric.	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.	A user tries to enter a parameter value for the -t (timeout) command option that is outside of the valid range.
Maximum connections can not exceed *maximum* where *maximum* designates the total number of permitted connections.	A user attempted to configure more connections than the maximum number of connections supported.
No valid server certificate is in place for Secure TCP Command Mode. Use the sslcfg command to generate a certificate.	The user issues a command to enable the Secure TCP Command Mode when a valid server certificate is not in place.

Table 61. tcpcmdmode command errors (continued)

Error message	Definition
The total number of secure and legacy connections of TCP Command Mode cannot exceed *maximum* where *maximum* designates the total number of permitted connections.	A user attempted to configure more TCP Command Mode connections than the maximum number of secure and legacy connections supported.
Warning: Communication with IBM Director via Secure TCP Command Mode has been disabled.	A user has disabled the Secure TCP command mode.
Warning: Communication with IBM Director via TCP Command Mode has been disabled.	A user has disabled the TCP command mode.

telnetcfg command errors

This topic lists error messages for the telnetcfg command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 62. telnetcfg command errors

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

update command errors

This topic lists error messages for the update command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 63. update command errors

Error message	Definition
Cannot perform this command right now. The agent is not active.	A user tries to enter a command while the agent is not active.
Disabling failover failed.	An error occurs while the management module is turning off the automatic failover feature.
Error reading information for firmware image *index.maximum* where *index* specifies the firmware image.	An error occurs while the management module is reading information for a specified firmware image.
Error reading the number of firmware images.	An error occurs while the management module is reading the number of firmware images.
Flash operation failed.	An error occurs during the flash firmware update.

Table 63. update command errors (continued)

Error message	Definition
Flash operation failed status *percentage* where the *percentage* value varies based on when the problem was encountered.	An error occurs during the flash firmware update.
Flash operation not in process or status unavailable.	An error occurs during the flash firmware update.
Flash operation timed out *percentage*. where the *percentage* value varies based on when the problem was encountered.	An error occurs during the flash firmware update.
Flash preparation - error sending packet file *filename*. where *filename* identifies the file being updated.	An error occurs during the flash firmware update.
Flash preparation error. Packet percent complete *percentage*. Flash percent complete *percentage*. where the *percentage* value varies based on when the problem was encountered.	An error occurs during the flash firmware update.
Flash preparation error. Timeout on packet preparation operation *percentage*. where the *percentage* value varies based on when the problem was encountered.	An error occurs during the flash firmware update.
Flashing not supported on this target.	A user attempts to run the update command on a module that does not support flash firmware updates.
Getting data encryption setting failed. If data encryption is enabled and you are updating the firmware to a level which does not support data encryption, you will lose all your configuration settings as a result.	An error occurs while the management module is reading the data encryption setting.
Getting name of mm *bay_number* failed. where the *bay_number* identifies the management module specified.	An error occurs while the management module is reading the name of the management module in designated bay.
Invalid image index. Index must be less than *maximum* where *maximum* designates the largest permitted index value.	A user tries to enter an image index that is greater than the maximum permitted index value.
Invalid option.	An invalid command option is entered. For the update command, invalid command option errors include: • the -i (IP address) command option does not have an IP address parameter • the -i (IP address) command option specifies an invalid IP address • attempting to enter the -i (IP address) command option without the -n (filename) command option • the -n (filename) command option does not have a file name parameter • attempting to enter the -n (filename) command option without the -i (IP address) command option • attempting to enter the -v (verbose) command option without the -i (IP address) command option and -n (filename) command option • attempting to enter the -v (verbose) command option with the -a command option

Table 63. update command errors (continued)

Error message	Definition
Management Module *bay_number* is not installed. where the *bay_number* identifies the management module specified.	The command is targeted to a management module bay where no management module is installed.
Status: Unable to read status.	An error occurs while the management module is reading status.
TFTP Error: *error_code*. where the *error_code* can have one of the following values: • Access violation. • Connection failure. • Disk full or allocation exceeded. • File already exists. • File error. • File not found. • Illegal option negotiation. • Illegal TFTP operation. • Unable to allocate memory. • Unknown transfer ID. • Unknown user.	An error occurs when the user attempts to set up the TFTP connection.
Unable to read blade server VPD bay *bay_number name*. where the *bay_number* and *name* identify the blade server by location and name.	The command specifies an empty blade server bay or an error occurs when reading the VPD.
Unable to read I/O Module VPD bay *bay_number name*. where the *bay_number* and *name* identify the I/O module by location and name.	The command specifies an empty I/O-module bay or an error occurs when reading the VPD.
Unable to read MM VPD bay *bay_number name*. where the *bay_number* and *name* identify the management module by location and name.	The command specifies an empty management module bay or an error occurs when reading the VPD.
Unable to read VPD for Blade *blade_number name*. where the *blade_number* and *name* identify the blade server by location and name.	An error occurs while the management module is reading the VPD of the targeted blade server.
Unknown device type.	The command is targeted to an unknown device type.
Update error. Invalid destination.	A user tries to issue a command to a target that is not valid.
Update Failed, there was a problem retrieving the file.	The management module was unable to complete the update because it was unable to retrieve the file from the TFTP server.

uplink command errors

This topic lists error messages for the uplink command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 64. uplink command errors

Error message	Definition
-ip must be a valid IP address before enabling -el	The user tries to issue a command to enable the -el without a valid -ip setting.
Getting status of failver on Lose/Logical of Physical Link failed.	An error occurs while the management module is reading status of failver on Lose/Logical of Physical Link.
Invalid uplink delay value.	A user tries to enter a delay value that is less than 1 or greater than 255. For example, `uplink -del 0`.
The option argument for *option* is out of the valid range (between 1 and 2880 minutes). where *option* is the number of minutes specified.	The user input for an option is out of the range.
The option argument for *option* is out of the valid range (between 10 and 172800 seconds). where *option* is the number of seconds specified.	The user input for an option is out of the range.

users command errors

This topic lists error messages for the users command.

See "Common errors" on page 114 for a list of error messages that apply to all commands.

Table 65. users command errors

Error message	Definition
-af contains invalid characters. Only alphanumeric, comma, asterisk, question mark, hyphen, period, and exclamation point characters are valid.	The user input for the -af option is invalid.
-af must start with from=.	The user input for the -af option is invalid.
-cm is greater than 255 characters.	The user input for the -cm option exceeds the maximum.
-cm must be quote-delimited.	The user input for the -cm option is not quote-delimited.
An entry cannot be modified and deleted in the same command.	A user tries to simultaneously modify and delete a user in the same command.
Arguments containing spaces must be enclosed in quotation marks.	A user tries to enter a context name containing spaces that does not have opening and closing quotation marks.
Checking if passwords are required failed.	An error occurs while the management module is checking if passwords are required.
Deleting user failed.	An error occurs while the management module is deleting an user.
Error: the RBS permissions capability is not enabled.	The user tries to run use the -a rbs: command option on management-module firmware that does not support this option.

Table 65. users command errors (continued)

Error message	Definition
Error converting RBS permissions.	An error occurs while the management module is converting permissions data to the role-based security (RBS) format.
Error creating user.	An error occurs while the management module is creating a user.
Error creating user: The authentication protocol cannot be none because the security settings require passwords.	The user tries to issue a command to create a user with no authentication protocol when the security settings require passwords.
Error reading certificate details.	An error occurs while the management module is reading certificate details.
Error reading key.	An error occurs while the management module is reading the key.
Error setting the access type.	An error occurs while the management module is setting the access type.
Error setting the authentication protocol.	An error occurs while the management module is setting the authentication protocol.
Error setting the authority level.	An error occurs while the management module is setting the authority level.
Error setting the context name.	An error occurs while the management module is setting the context name.
Error setting the hostname/IP address.	An error occurs while the management module is setting the hostname or IP address.
Error setting the password.	An error occurs while the management module is setting the password.
Error setting the password. The new password is not compliant.	The user tries to issue a command to set the new password which is not compliant.
Error setting the privacy password.	An error occurs while the management module is setting the privacy password.
Error setting the privacy protocol.	An error occurs while the management module is setting the privacy protocol.
Error setting the username.	An error occurs while the management module is setting the username.
Error transferring file.	An error occurs while the management module is transferring file.
Getting a summary of all keys of user *index* failed. where the *index* value varies based on the problem that was encountered.	An error occurs while the management module is reading a summary of all keys of the targeted user.
Getting authority level of user *index* failed. where the *index* value varies based on the problem that was encountered.	An error occurs while the management module is reading authority level of the targeted user.
Getting role-based security level of user *index* failed. where the *index* value varies based on the problem that was encountered.	An error occurs while the management module is reading role-based security level of the targeted user.
Incorrect login permission option: *permission* where the *permission* value varies based on the problem that was encountered.	A user tries to specify an invalid login permission for the -a command option.

Table 65. users command errors (continued)

Error message	Definition
Invalid argument. Valid arguments for -at are read, write, and traps.	A user tries to set an invalid argument for the -at command option.
Invalid argument. Valid choices are des or <none>.	A user tries to set an invalid argument for the -pp command option.
Invalid argument. Valid choices are md5, sha, or <none>.	A user tries to set an invalid argument for the -ap command option.
Invalid authority level.	This error message indicates one of the following errors: • A user tries to set an authority level that is invalid. • A user tries to set a custom authority level without specifying any customization information.
Invalid device number (first number must be smaller): *device_A-device_B*. where *device_A* and *device_B* identify the ends of the invalid device range being specified.	A user specifies an invalid device range while trying to create or modify a user.
Invalid device number: *device_number*. where *device_number* identifies the device number that is invalid.	A user provides a device number that is out of range while trying to create or modify a user.
Invalid hostname or ip address.	A user tries to set an invalid host name or IP address for the -i command option.
Invalid key index for this command.	The user input for index is invalid.
Invalid rbs device: *device*. where *device* identifies the device that is invalid.	A user specifies an invalid device while trying to create or modify a user.
Invalid rbs device: Must specify device number	A user specifies an invalid device number while trying to create or modify a user.
Invalid rbs device list.	A user does not specify a device list while trying to create or modify a user.
Invalid rbs device (must be same device): *device*. where *device* identifies the device that is invalid.	A user specifies an invalid device while trying to create or modify a user.
Invalid rbs role: *role*. where *role* identifies the role that is invalid.	A user specifies an invalid role while trying to create or modify a user.
Invalid rbs role list.	A user fails to specify a role list while trying to modify or create a user.
Invalid username. The username can only contain numbers, letters, dots, and underscores.	The user tries to enter The username that contains invalid characters. Valid characters that can be used in a username are letters, numbers, periods (.), and underscores (_).
Max retries changing password reached.	The user tries to issue a command to change a password after the max retries of changing password limit is reached.
Must be set at least one rbs role for this user.	The user tries to issue a command to create a user without the rbs role settings.
Old password is incorrect.	The user tries to issue a command to change a password with an incorrect old password.
Old password must be specified by long option op.	The user tries to issue a command to change a password without the -op option.

Table 65. users command errors (continued)

Error message	Definition
Specify your new password with '-p' option.	The user tries to issue a command to change a password without the -p option.
Syntax error. -a option must have an argument.	A user tries to attempt to enter the command with an -a command option that has no argument.
Syntax error. -at option must have an argument.	A user tries to attempt to enter the command with an -at command option that has no argument.
Syntax error. -cn option must have an argument.	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.	A user tries to attempt to enter the command with an -i command option that has no argument.
Syntax error. -n option must have an argument.	A user tries to attempt to enter the command with an -n command option that has no argument.
Syntax error. -ppw option must have an argument.	A user tries to attempt to enter the command with a -ppw command option that has no argument.
Syntax error. Multiple -a options found.	A user tries to enter the -a command option in a single command multiple times.
Syntax error. Multiple -ap options found.	A user tries to enter the -ap option flag in a single command multiple times.
Syntax error. Multiple -at options found.	A user tries to enter the -at option flag in a single command multiple times.
Syntax error. Multiple -cn options found.	A user tries to enter the -cn option flag in a single command multiple times.
Syntax error. Multiple -i options found.	A user tries to enter the -i option flag in a single command multiple times.
Syntax error. Multiple -n options found.	A user tries to enter the -n option flag in a single command multiple times.
Syntax error. Multiple -p options found.	A user tries to enter the -p option flag in a single command multiple times.
Syntax error. Multiple -pp options found.	A user tries to enter the -pp option flag in a single command multiple times.
Syntax error. Multiple -ppw options found.	A user tries to enter the -ppw option flag in a single command multiple times.
Syntax error. Type users -h for help.	A user tries to set an invalid value for a command option.
The context name must be less than 32 characters long.	A user tries to set a context name that is longer than 31 characters.
The -i and -l options must both be specified when using -upld.	The user tries to issue a -upld command without -i and -l.
The accept_from_string must be quote-delimited.	The user input for the -af option is not quote-delimited.
The key is greater than 6000 bytes.	The user input for the key exceeds the maximum.
The password must be at least 5 characters long, but no more than 15 characters long.	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.	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).

Table 65. users command errors (continued)

Error message	Definition
The privacy password must be less than 32 characters long.	A user tries to set a privacy password that is longer than 31 characters.
The user index must be different than that of the current user.	The user tries to issue a command to delete the account of current user.
The username cannot be longer than 15 characters.	A user tries to set a user name that is longer than 15 characters.
There was a problem retrieving the file.	An error occurs while the management module is retrieving the file.
Unable to change password. The minimum password change interval has not expired. Please try again later.	The user tries to issue a command to change a password while the minimum password change interval has not expired.
Unable to read the complex password requirement.	An error occurs while the management module is reading the complex password requirement.
Unable to read the password required setting.	An error occurs while the management module is reading the password required setting.
Unexpected error: Unable to change password.	An error occurs while the management module is changing the password.
When creating a new user, a username and authority level must be specified.	The user tries to issue a command to create a user without the -n and -a options.
When creating a new user, all options are required.	A user tries to create a new user without defining all of the command options and arguments.

Appendix. 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 section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your system, 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 *Problem Determination and Service Guide* on the IBM *Documentation* CD that comes with your system.
- Go to the IBM support Web site at http://www.ibm.com/systems/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 IBM systems also describes the diagnostic tests that you can perform. Most 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 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/systems/support/ and follow the instructions. Also, some documents are available through the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

Getting help and information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM systems, optional devices, services, and support. The address for IBM System x and xSeries information is http://www.ibm.com/systems/x/. The address for IBM BladeCenter information is http://www.ibm.com/systems/bladecenter/. The address for IBM IntelliStation® information is http://www.ibm.com/intellistation/.

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

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x and 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 your IBM reseller or IBM Services. To locate a reseller authorized by IBM to provide warranty service, go to http://www.ibm.com/partnerworld/ and click **Find a Business Partner** on the right side of the page. For IBM support telephone numbers, see http://www.ibm.com/planetwide/. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

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

IBM Taiwan product service

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

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

Notices

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

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

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

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

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

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

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

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

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common

law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information”at http://www.ibm.com/legal/copytrade.shtml.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

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

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

Linux is a registered trademark of Linus Torvalds 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.

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 or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 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 might 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.

Index

Special characters

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Part Number: 44R5372

Printed in USA

(1P) P/N: 44R5372