BladeCenter Advanced Management Module
BladeCenter T Advanced Management Module

Command-Line Interface Reference Guide

BladeCenter Advanced Management Module
BladeCenter T Advanced Management Module

Command-Line Interface Reference Guide

Note: Before using this information and the product it supports, read the general information in "Getting help and technical assistance," on page 489, "Notices" on page 493, the *Warranty Information* document, and the *Safety Information* and *Environmental Notices and User Guide* documents on the IBM *Documentation* CD.

Twenty-seventh Edition (October 2012)

Contents

Chapter 1. Introduction 1
Before you begin 2
Accessibility features for the BladeCenter management module 2

Chapter 2. Using the command-line interface 5
Command-line interface guidelines 5
Selecting the command target. 6
Commands and user authority 8
Cabling the management module 12
- Networked connection. 13
- Direct connection 13
- Serial connection 14

Starting the command-line interface 14
- IPv6 addressing for initial connection. 15
- Telnet connection 16
- Serial connection 17
- Secure Shell (SSH) connection 18

BladeCenter unit configuration 20
Configuring the management module 21
Starting an SOL session 22
Ending an SOL session 23

Chapter 3. Command reference 25
Alphabetic command list 25
Command list by function 27
Command syntax 29
- accseccfg command. 30
- advfailover command 40
- airfilter command (BladeCenter S only) 42
- alarm command (BladeCenter T and HT only). . 43
- alertcfg command 51
- alertentries command 53
- autoftp command 60
- baydata command 63
- bofm command 66
- boot command 72
- bootmode command 74
- bootseq command 75
- buildidcfg command 80
- chconfig command 87
- chlog command 93
- chmanual command 95
- cin command. 97
- cinstatus command 102
- clear command. 103
- clearlog command. 105
- clock command. 106
- config command 111
- console command 115
- dhcpinfo command 117
- displaylog command 119
- displaysd command 124
- dns command 126
- env (environment) command 131
- ethoverusb command. 137
- eventinfo command 138
- events command 140
- exit command 143
- feature command 144
- files command 147
- fuelg command. 149
- groups command 159
- health command 163
- help command 166
- history command 168
- identify (location LED) command 169
- ifconfig command 171
- info (configuration information) command . . 203
- iocomp command 206
- kvm (keyboard, video, mouse) command . . . 208
- ldapcfg command 210
- led command 220
- list (system physical configuration) command 225
- mcad command 227
- modactlog command 228
- monalerts command 229
- mt (media tray) command 239
- nat command 241
- ntp (network time protocol) command 245
- ping command 248
- pmpolicy command 251
- portcfg command 253
- ports command. 255
- power command 272
- rdoc command 278
- read command 280
- remacccfg command 283
- remotechassis command. 285
- reset command 288
- scale command. 293
- sddump command 301
- sdemail command. 303
- security command. 305
- service command 306
- shutdown command 308
- slp command 309
- smtp command. 311
- snmp command 314
- sol (serial over LAN) command 330
- sshcfg command 337
- sslcfg command 339
- syslog command 349
- tcpcmdmode command 353
- telnetcfg (Telnet configuration) command . . . 356
- temps command 357
- trespass command. 358
- uicfg command. 361
- update (update firmware) command 365
- uplink (management module failover) command 375

users command 379
vlan command 402
volts command 412
write command 413
zonecfg command 415

Chapter 4. Error messages 419
Common errors 421
accseccfg command errors 423
advfailover command errors 424
alarm command errors 425
alertcfg command errors. 426
alertentries command errors 426
autoftp command errors. 427
baydata command errors 427
bofm command errors 428
boot command errors. 429
bootmode command errors 429
bootseq command errors 430
buildidcfg command errors. 430
chconfig command errors 431
chlog command errors 432
chmanual command errors 433
cin command errors 433
clear command errors 435
clearlog command errors 435
clock command errors 435
config command errors 436
console command errors. 437
dhcpinfo command errors 438
displaylog command errors. 438
displaysd command errors 439
dns command errors 440
env command errors 440
ethoverusb command errors 440
eventinfo command errors 441
events command errors 441
exit command errors 442
feature command errors 442
files command errors 444
fuelg command errors 445
groups command errors 448
health command errors 448
help command errors. 449
history command errors 449
identify command errors 449
ifconfig command errors 450
info command errors 454
iocomp command errors. 455
kvm command errors. 455
ldapcfg command errors. 455
led command errors 456
list command errors 457
mcad command errors 457
modactlog command errors 457
monalerts command errors 457
monalertsleg command errors 458
mt command errors 458
nat command errors 458
ntp command errors 459
ping command errors 459
pmpolicy command errors 460
portcfg command errors. 460
ports command errors 460
power command errors 462
rdoc command errors. 462
read command errors. 463
remacccfg command errors 464
remotechassis command errors 464
reset command errors 465
scale command errors 465
sddump command errors 466
sdemail command errors 467
security command errors 467
service command errors 467
shutdown command errors 468
slp command errors 468
smtp command errors 468
snmp command errors 469
sol command errors 470
sshcfg command errors 471
sslcfg command errors 472
syslog command errors 474
tcpcmdmode command errors 475
telnetcfg command errors 475
temps command errors 476
thres command errors 476
trespass command errors 476
uicfg command errors 477
update command errors 478
uplink command errors 480
users command errors 481
vlan command errors. 485
volts command errors 486
write command errors 486
zonecfg command errors 487

Appendix. Getting help and technical assistance. 489
Before you call 489
Using the documentation 490
Getting help and information from the World Wide Web 490
How to send DSA data to IBM 490
Creating a personalized support web page . . . 490
Software service and support 491
Hardware service and support 491
IBM Taiwan product service 491

Notices 493
Trademarks 493
Important notes 494
Particulate contamination 495
Documentation format 496
Telecommunication regulatory statement 496
Electronic emission notices 496
Federal Communications Commission (FCC) statement. 496
Industry Canada Class A emission compliance statement. 497

Avis de conformité à la réglementation d'Industrie Canada 497
Australia and New Zealand Class A statement 497
European Union EMC Directive conformance statement. 497
Germany Class A statement 497
Japan VCCI Class A statement. 498
Korea Communications Commission (KCC) statement. 499
Russia Electromagnetic Interference (EMI) Class A statement 499
People's Republic of China Class A electronic emission statement 499
Taiwan Class A compliance statement 499

Index 501

Chapter 1. Introduction

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

The IBM® BladeCenter® advanced 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.

- When a command is labeled "BladeCenter H only", it can run on all types of BladeCenter H units (BladeCenter H and BladeCenter HT).
- When a command is labeled "BladeCenter T only", it can run on all types of BladeCenter T units (BladeCenter T and BladeCenter HT).
- When a command is labeled "Blade Center S only", it can run on all types of BladeCenter S units.

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/.

IBM Redbooks publications are developed and published by the IBM International Technical Support Organization (ITSO). The ITSO develops and delivers skills, technical know-how, and materials to IBM technical professionals, Business Partners, clients, and the marketplace in general. For IBM Redbooks publications for your BladeCenter, go to http://www.redbooks.ibm.com/portals/bladecenter.

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:

- "Command-line interface guidelines"
- "Selecting the command target" on page 6
- "Commands and user authority" on page 8
- "Cabling the management module" on page 12
- "Starting the command-line interface" on page 14
- "BladeCenter unit configuration" on page 20
- "Configuring the management module" on page 21
- "Starting an SOL session" on page 22
- "Ending an SOL session" on page 23

See Chapter 3, "Command reference," on page 25 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 419. 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

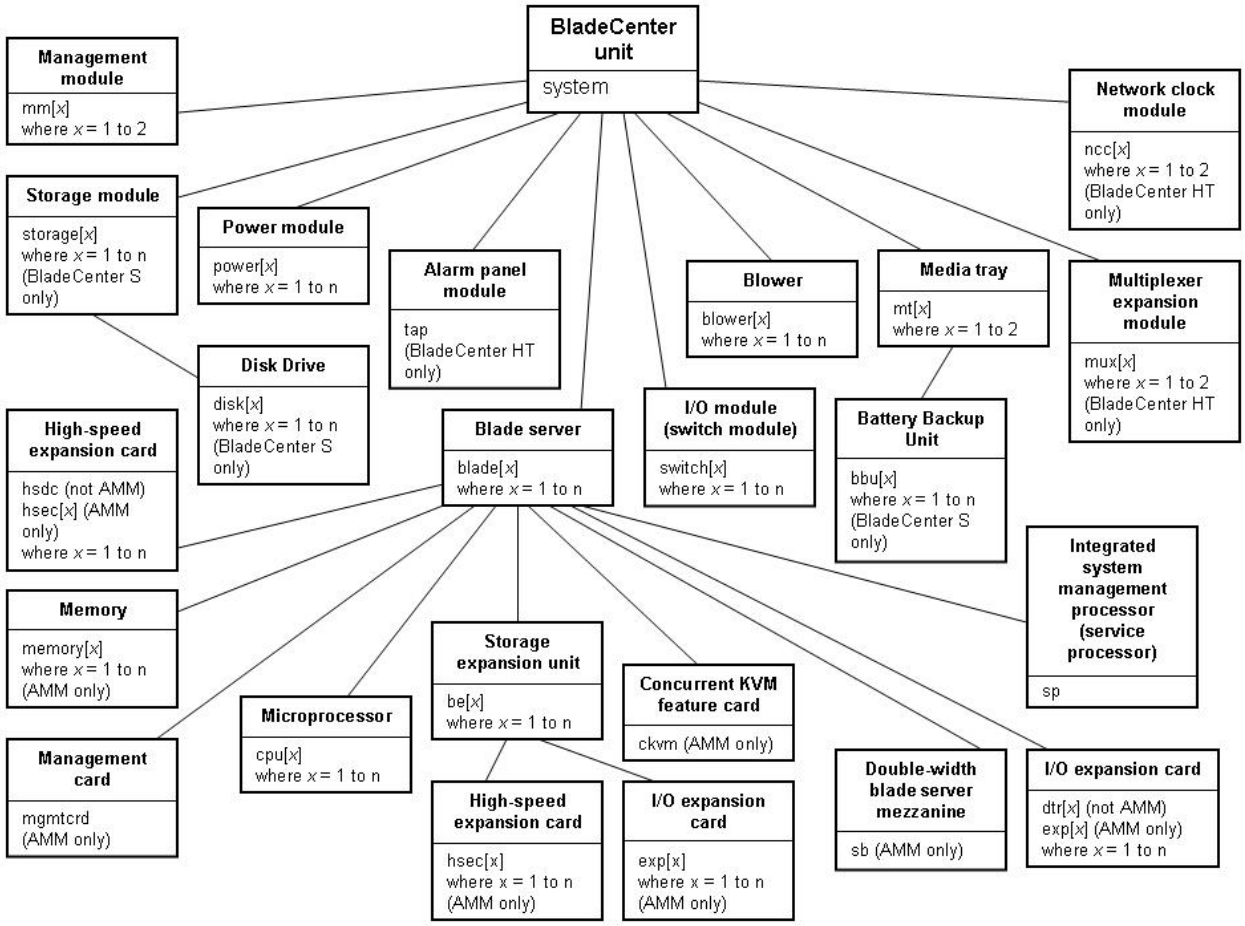
  The ip_address data type uses a predefined formatted string of xxx.xxx.xxx.xxx, where xxx is a number from 0 to 255.
- Delimiters
  - Options are delimited with a minus sign.
  - In a command that requires parameters, a single space is expected between an option and its parameter. Any additional spaces 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 131). 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 225).

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 on page 9 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 and require a special command authority: 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.

Notes:

1. LDAP (lightweight directory access protocol) authority levels are not supported by management modules other than the advanced management module.
2. LDAP authority levels are not supported by the management-module web interface.
3. To use the LDAP authority levels, you must make sure that the version of LDAP security that is used by the management module is set to v2 (enhanced role-based security model). See "ldapcfg command" on page 210 for information.

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**
accseccfg	•				•					
advfailover	•				•					
airfilter	•	•	•	•	•					
alarm -c, -r, -s	•				•		•			•
alarm -q -g	•					•		•		
alertcfg	•				•					
alertentries	•				•					
alertentries -test	•		•	•	•	•	•	•	•	•
autoftp	•				•					
baydata	•						•			
bofm	•				•					
boot (blade server)	•					•				
boot -c	•					◇		◇		
boot -p	•					•				
bootmode	•						•			
bootseq	•						•			
buildidcfg	•					•	•	•		
chconfig	•				•					
chlog	•				•					
chmanual	•	•	•	•	•	•	•	•	•	•
cin	•	◇			◇					
clear	•			◇	◇				‡	‡
clearlog	•		•							
clock	•				•					
config (blade server)	•						•			
config (management module or BladeCenter unit)	•				•					
console	•							•		
displaylog -lse	•		•							
dns	•				•					

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**
ethoverusb	•					•				
events -che	•	•	•	•	•	•	•	•	•	•
events -che -add -rm	•				•					
feature	•			•						
files -d	•			•	•	•	•		•	•
fuelg	•				•					
groups	•				•					
identify	•				•		•			
ifconfig (blade server target)	•						•			
ifconfig (blade server ISMP, management module, and system targets)	•				•					
ifconfig (I/O module target)	•									•
ifconfig -pip (I/O module target)	•								•	•
kvm -b	•							•		
kvm -local	•				•					
ldapcfg	•				•					
led -info, -d, -loc (system target)	•	•	•	•	•					
led -info, -loc (blade server target)	•					•	•	•		
mcad	•				•					
monalerts	•				•					
mt -b	•							•		
mt -local, -remote	•				•					
nat	•									•
ntp	•				•					
ping -i (see Note 1)	•								•	•
pmpolicy	•				•					
portcfg	•				•					
ports	•				•					

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**
ports (I/O module target)										•
power -on, -off, -softoff, -cycle	•					•			•	
power -on -c, -cycle -c	•					◇		◇		
power -wol, -local	•				•		•			
power -fp (global)	•				•					
power -fp (I/O module)	•								•	
rdoc	•							•		
read	•				•					
remacccfg	•				•					
reset (blade server or ISMP)	•					•				
reset (I/O module)	•								•	
reset (management module)	•			•						
reset -c, -clr, -dg, -ddg, -sft, (blade server)	•					◇		◇		
reset -sms (blade server)	•					•				
reset -exd, -full, -std (I/O module)	•								•	
reset -f, -standby, -force (management module)	•			•						
scale	•					•				
sddump	•					•				
sdemail	•	•	•	•	•	•	•	•	•	•
security	•				•					
service	•				•					
shutdown	•					•				
slp	•				•					
smtp	•				•					
snmp	•				•					

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
sol	•				•		•			
sshcfg	•				•					
sslcfg	•				•					
syslog	•				•					
tcpcmdmode	•				•					
telnetcfg	•				•					
trespass	•				•					
uicfg	•				•					
update	•			•		•			•	
uplink	•				•					
users	•	•								
users -disable, -enable, -unlock	•	•		•	•					
vlan	•				•					
write	•				•					
zonecfg	•									•

Note:

1. All users can execute the `ping -i` command directed to a specific IP address. Users with Supervisor, Operator (general operator), I/O Module Administration, I/O Module Configuration, or I/O Module Operator authority can execute the `ping -i` command option with no arguments or ping a specific IP address that is identified using its index number.

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. The advanced management module also supports connection through the serial management port.

You can manage the BladeCenter unit by using by using the command-line interface that you access through Telnet or through the serial management port. 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 or serial connection capability. To facilitate connections at multiple locations, you can use a notebook computer.
- The management-module MAC address (listed on the label on the management module).
- For networked connection to the management module, you need a standard Ethernet cable and a local Ethernet network port (facility connection).
- For direct connection of a system to the advanced management-module remote management and console (Ethernet) connector, you can use either a standard Ethernet cable or an Ethernet crossover cable.
- For serial connection of a system to the advanced management-module serial connector, you need a serial cable. See the *Installation Guide* for your management module for cabling information and instructions.

For information about accessing the management-module web interface, see the *BladeCenter Advanced 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 cable or 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.

Note: An advanced management module can perform an automatic media dependent interface (MDI) crossover, eliminating the need for crossover cables or cross-wired (MDIX) ports. You might have to use a crossover cable to connect your system to the advanced management module if the network interface card in the client system is very old.

Serial connection

You can connect a serial cable to the advanced management module.

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

Starting the command-line interface

Access the management-module command-line interface from a client system by establishing a Telnet connection to the IP address of the management module or by establishing a Secure Shell (SSH) connection.

For the advanced management module, you can also access the command-line interface using a serial connection. You can establish up to 20 separate Telnet, serial, or SSH sessions to the BladeCenter management module, giving you the ability to have 20 command-line interface sessions active at the same time.

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

The following SSH clients are available. 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 2.0 clients**
Public key exchange	Diffie-Hellman-group 1-sha-1
Host key type	DSA - 2048-bit
Bulk cipher algorithms	3-des-cbc or blowfish-cbc
MAC algorithms	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:

Note: The advanced management module does not have a fixed static IPv6 IP address by default. For initial access to the advanced management module in an IPv6 environment, users can either use the IPv4 IP address or the IPv6 link-local address. See "IPv6 addressing for initial connection" for information about determining IPv6 addressing for initial connection.

- IPv4 IP address: 192.168.70.125 (primary and secondary management module)
- IPv4 Subnet: 255.255.255.0
- User ID: USERID (all capital letters)
- Password: PASSW0RD (note the number zero, not the letter O, in PASSW0RD)

For IPv4, 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.

Note: For advanced management modules, the available password options depend on the password options that are configured for the BladeCenter unit.

IPv6 addressing for initial connection

When using IPv6 addressing, the only way to initially connect to the advanced management module is by using the IPv6 link-local address.

The link-local address is a unique IPv6 address for the advanced management module that is automatically generated based on its MAC address. It is of the form: `FE80::3BA7:94FF:FE07:CBD0`.

The link-local address for the advanced management module can be determined in one of the following ways:

- Some advanced management modules will list the link-local address on a label that is attached to the advanced management module.
- If you are able to log in to the management module command-line interface (CLI) using IPv4 addressing, the link-local address can be viewed using the `ifconfig` command (see "ifconfig command" on page 171 for information).
- If you are able to log in to the management module web interface using IPv4 addressing, the link-local address can be viewed in the Primary Management Module, IPv6 section of the **MM Control → Network Interfaces** page (see the *BladeCenter Advanced Management Module User's Guide* for information).

If the advanced management module does not have a label listing the link-local address and you are unable to access the advanced management module using IPv4, complete the following steps to calculate link-local address:

1. Write down the MAC address of the advanced management module. It is on a label on the management module, below the IP reset button. The label reads MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the MAC address. For example,

   `39-A7-94-07-CB-D0`
2. Split the MAC address into two parts and insert FF-FE in the middle. For example,

   `39-A7-94-`**`FF-FE`**`-07-CB-D0`

3. Convert the two hexadecimal digits at the left end of the string to binary. For example,
   - **39**-A7-94-FF-FE-07-CB-D0
   - **00111001**-A7-94-FF-FE-07-CB-D0
4. Invert the value for bit 7 of the binary string. For example,
   - 0011100**0**1-A7-94-FF-FE-07-CB-D0
   - 0011101**1**1-A7-94-FF-FE-07-CB-D0
5. Convert the binary digits at the left end of the string back to hexadecimal. For example,
   - **00111011**-A7-94-FF-FE-07-CB-D0
   - **3B**-A7-94-FF-FE-07-CB-D0
6. Combine the hexadecimal digit pairs into 4-digit groups. For example,
   - 3B-A7-94-FF-FE-07-CB-D0
   - 3BA7-94FF-FE07-CBD0
7. Replace dash (-) separators with colon (:) separators. For example,
   - 3BA7-94FF-FE07-CBD0
   - 3BA7**:**94FF**:**FE07**:**CBD0
8. Add FE80:: to the left of the string. For example,

   FE80::3BA7:94FF:FE07:CBD0

For a MAC address of 39-A7-94-07-CB-D0, the link-local address used for initial IPv6 access is FE80::3BA7:94FF:FE07:CBD0.

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` *`ip_address`* (where *ip_address* is the management module IP address), and press Enter. For the first connection to the management module, use the default IP address of the management module; if a new IP address has been assigned to the management module, use that one instead.

   Note: The factory-defined static IPv4 IP address is 192.168.70.125, the default IPv4 subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the burned-in MAC address. The MAC address is on a label on the management module, below the IP reset button. See "IPv6 addressing for initial connection" on page 15 for information about determining IPv6 addressing for initial connection.
2. At the login prompt, type the management-module user ID. At the password prompt, type the management-module password. The user ID and password are case sensitive and are the same as those that are used for management-module web access. The default management-module user name is USERID, and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

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

Serial connection

You can set up a serial connection with the management module.

After you connect a serial cable from the management module to the client system, complete the following steps:

1. Open a terminal session on the client system, and make sure that the serial port settings for the client system match the settings for the serial port on the management module. The default management-module serial port settings are as follows:
   - Baud rate (BPS): 57600
   - Data bits: 8
   - Parity: no parity
   - Stop bits: 1
   - Flow control: none
2. If any of the serial port settings for the client system were changed, reset the management module (see the *Installation Guide* for your management module for instructions).
3. At the login prompt, type the management-module user ID. At the password prompt, type the management-module password. The user ID and password are case sensitive and are the same as those that are used for management-module web access. The default management-module user name is USERID, and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

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

Secure Shell (SSH) connection

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 Advanced 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 ip_address` (where *ip_address* is the management module IP address), and press Enter. For the first connection to the management module, use the default IP address of the management module; if a new IP address has been assigned to the management module, use that one instead.

   Note: The factory-defined static IPv4 IP address is 192.168.70.125, the default IPv4 subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxx*, where *xxxxxxxxxxx* is the burned-in MAC address. The MAC address is on a label on the management module, below the IP reset button. See "IPv6 addressing for initial connection" on page 15 for information about determining IPv6 addressing for initial connection.
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.

The advanced management module supports non-interactive Secure Shell sessions. This is most useful when it is combined with public key authentication. Use this capability to issue a single CLI command by adding the command to the end of the `ssh` command. For example, to get a list of the current users of the advanced management module type

ssh -l USERID 192.168.70.2 users -T mm[1] -curr

If the CLI command requires special characters such as quotation marks, you must escape them so that they are not consumed by the command shell on your client system. For example, to set a new trespass warning, type a command similar to the following example:

ssh -l USERID 192.168.70.2 trespass -T mm[1] -tw \"New WARNING\"

To start a Serial over LAN text redirection session to a blade server, the process is similar, but in this case you must specify that the Secure Shell server session uses a pseudo-terminal (PTY) to get the correct output formatting and keystroke handling. In the following example, which starts a Serial over LAN session to the blade server in slot 2, the `-t` SSH client option specifies that a PTY is to be allocated.

ssh -t -l USERID 192.168.70.1 console -T blade[2]

Using SMASH

You can use the System Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) for the advanced management module. See the *IBM SMASH Proxy Installation and User's Guide* for more information.

To start an interactive SMASH CLP session by using an SSH client such as OpenSSH client with an advanced management module with networking address 192.168.70.2, type a command similar to the following example:

ssh -p 50022 -l USERID 192.168.70.2

where `-p 50022` specifes TCP port 50022, the default port number for Secure SMASH on the advanced management module, and `-l USERID` specifies one of the 12 local account login IDs.

The advanced management module supports non-interactive Secure SMASH sessions. This is most useful when it is combined with public key authentication. Use this capability to issue a single SMASH CLP command. To start a non-interactive SMASH session, you must specify that the Secure SMASH server uses a pseudo-terminal (PTY). If you fail to specify a PTY for the session the `Input Redirection not Supported` error message is displayed. For example, to get a list of the SMASH-addressable entities, type a command similar to the following example:

ssh -t -p 50022 -l USERID 192.168.70.2 show /modular1

where `-t` specifies that a PTY is required for the session and `show /modular1` is the SMASH command that is to be executed on the advanced management module.

If you are using a Telnet client to start an interactive SMASH CLP session, you must specify the correct TCP port number. By default, the port that is assigned to the SMASH protocol is 50023.

SSH CLI exit codes

The SSH CLI commands return exit codes.

All CLI commands that are run in an SSH client single-command environment provide exit codes to indicate their outcomes. The following table shows exit codes that are supported; other exit codes are reserved for future use.

Table 2. SSH CLI exit codes

Name	Value (decimal)	Description
EX_OK	0	Successful command execution.
EX_USAGE	64	Command-line usage error: syntax error, wrong command arguments or number of arguments, or invalid command target.
EX_DATAERR	65	Input data error: invalid configuration file or SSH key parsing error.
EX_NOINPUT	66	The input file does not exist or is not readable.
EX_UNAVAILABLE	69	The command-line interface is not available: CLI oversubscribed, CLI disabled, or the data returned by a command has an unexpected value.
EX_SOFTWARE	70	Internal software error. Check the management-module event log for other error indications.
EX_TEMPFAIL	75	The command could not perform a write operation because the device or management module was not in the correct state. Check for conflicting tasks or conditions and try to run the command again.
CLI_ERR_NOT_AUTHORIZED	126	Authorization error: the user does not have sufficient privileges to execute command.
CLI_ERR_CNF	127	Command not found.

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, a serial connection, 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 (redundant) 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. For advanced management modules, see "read command" on page 280 for information about applying a saved configuration file.

For the primary management module to communicate, you must configure the IP address for 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.

Note: The internal Ethernet ports (eth1) for the advanced management module cannot be configured.

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

- If you have an accessible, active, and configured dynamic host configuration protocol (DHCP) server on the network, 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 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 14 for more information).
2. Configure the external Ethernet interface (eth0), using the `ifconfig` command (see "ifconfig command" on page 171 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 Advanced 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® Systems 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 330 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, serial, 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 330 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 29 are listed in alphabetic order. The commands are also listed in the following two topics:

- "Alphabetic command list"
- "Command list by function" on page 27

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 6 for information.

Alphabetic command list

In alphabetic order, the commands are as follows:

- "accseccfg command" on page 30
- "advfailover command" on page 40
- "airfilter command (BladeCenter S only)" on page 42
- "alarm command (BladeCenter T and HT only)" on page 43
- "alertcfg command" on page 51
- "alertentries command" on page 53
- "autoftp command" on page 60
- "baydata command" on page 63
- "bofm command" on page 66
- "boot command" on page 72
- "bootmode command" on page 74
- "bootseq command" on page 75
- "buildidcfg command" on page 80
- "chconfig command" on page 87
- "chlog command" on page 93
- "chmanual command" on page 95
- "cin command" on page 97
- "cinstatus command" on page 102
- "clear command" on page 103
- "clearlog command" on page 105
- "clock command" on page 106
- "config command" on page 111
- "console command" on page 115
- "dhcpinfo command" on page 117
- "displaylog command" on page 119
- "displaysd command" on page 124
- "dns command" on page 126
- "env (environment) command" on page 131
- "ethoverusb command" on page 137

- "eventinfo command" on page 138
- "events command" on page 140
- "exit command" on page 143
- "feature command" on page 144
- "files command" on page 147
- "groups command" on page 159
- "fuelg command" on page 149
- "health command" on page 163
- "help command" on page 166
- "history command" on page 168
- "identify (location LED) command" on page 169
- "ifconfig command" on page 171
- "info (configuration information) command" on page 203
- "iocomp command" on page 206
- "kvm (keyboard, video, mouse) command" on page 208
- "ldapcfg command" on page 210
- "led command" on page 220
- "list (system physical configuration) command" on page 225
- "mcad command" on page 227
- "modactlog command" on page 228
- "monalerts command" on page 229
- "mt (media tray) command" on page 239
- "nat command" on page 241
- "ntp (network time protocol) command" on page 245
- "ping command" on page 248
- "pmpolicy command" on page 251
- "portcfg command" on page 253
- "ports command" on page 255
- "power command" on page 272
- "rdoc command" on page 278
- "read command" on page 280
- "read command" on page 280
- "remacccfg command" on page 283
- "remotechassis command" on page 285
- "reset command" on page 288
- "scale command" on page 293
- "sddump command" on page 301
- "sdemail command" on page 303
- "security command" on page 305
- "service command" on page 306
- "shutdown command" on page 308
- "slp command" on page 309
- "smtp command" on page 311
- "snmp command" on page 314
- "sol (serial over LAN) command" on page 330
- "sshcfg command" on page 337
- "sslcfg command" on page 339
- "syslog command" on page 349
- "tcpcmdmode command" on page 353
- "telnetcfg (Telnet configuration) command" on page 356
- "temps command" on page 357
- "trespass command" on page 358
- "uicfg command" on page 361
- "update (update firmware) command" on page 365
- "uplink (management module failover) command" on page 375
- "users command" on page 379

- "vlan command" on page 402
- "volts command" on page 412
- "write command" on page 413
- "zonecfg command" on page 415

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 131
  - "help command" on page 166
  - "history command" on page 168
  - "list (system physical configuration) command" on page 225

- **Common commands**

  Use these commands to monitor and control operation of BladeCenter components:
  - "cinstatus command" on page 102
  - "health command" on page 163
  - "info (configuration information) command" on page 203
  - "iocomp command" on page 206
  - "modactlog command" on page 228
  - "ping command" on page 248
  - "temps command" on page 357
  - "volts command" on page 412

- **Configuration commands**

  Use these commands to view and configure network settings, Ethernet interfaces, and other functions:
  - "accseccfg command" on page 30
  - "advfailover command" on page 40
  - "alertcfg command" on page 51
  - "alertentries command" on page 53
  - "autoftp command" on page 60
  - "baydata command" on page 63
  - "bofm command" on page 66
  - "bootmode command" on page 74
  - "bootseq command" on page 75
  - "buildidcfg command" on page 80
  - "cin command" on page 97
  - "cinstatus command" on page 102
  - "clock command" on page 106
  - "config command" on page 111
  - "dhcpinfo command" on page 117
  - "displaysd command" on page 124
  - "dns command" on page 126
  - "ethoverusb command" on page 137
  - "feature command" on page 144
  - "files command" on page 147
  - "groups command" on page 159
  - "health command" on page 163
  - "ifconfig command" on page 171
  - "info (configuration information) command" on page 203
  - "iocomp command" on page 206

  - "kvm (keyboard, video, mouse) command" on page 208
  - "ldapcfg command" on page 210
  - "mcad command" on page 227
  - "modactlog command" on page 228
  - "monalerts command" on page 229
  - "mt (media tray) command" on page 239
  - "nat command" on page 241
  - "ntp (network time protocol) command" on page 245
  - "pmpolicy command" on page 251
  - "ping command" on page 248
  - "portcfg command" on page 253
  - "ports command" on page 255
  - "read command" on page 280
  - "rdoc command" on page 278
  - "remotechassis command" on page 285
  - "scale command" on page 293
  - "sddump command" on page 301
  - "security command" on page 305
  - "service command" on page 306
  - "slp command" on page 309
  - "chconfig command" on page 87
  - "chmanual command" on page 95
  - "smtp command" on page 311
  - "snmp command" on page 314
  - "sol (serial over LAN) command" on page 330
  - "sshcfg command" on page 337
  - "sslcfg command" on page 339
  - "tcpcmdmode command" on page 353
  - "telnetcfg (Telnet configuration) command" on page 356
  - "temps command" on page 357
  - "trespass command" on page 358
  - "uicfg command" on page 361
  - "uplink (management module failover) command" on page 375
  - "users command" on page 379
  - "volts command" on page 412
  - "zonecfg command" on page 415

- **Discovery commands**

  Use these commands to locate other resources on the network:
  - "ping command" on page 248
  - "remotechassis command" on page 285

- **Event log commands**

  Use these commands to view and clear primary management-module event log entries:
  - "clearlog command" on page 105
  - "displaylog command" on page 119
  - "eventinfo command" on page 138
  - "events command" on page 140
  - "modactlog command" on page 228
  - "chlog command" on page 93
  - "syslog command" on page 349

- **LED commands**

  Use these commands to monitor and control operation of BladeCenter unit LEDs:
  - "identify (location LED) command" on page 169
  - "led command" on page 220
- **Memory commands**

  Use these commands to reset the management-module configuration and perform firmware updates:
  - "clear command" on page 103
  - "update (update firmware) command" on page 365
- **Power-control commands**

  Use these commands to control operation of the BladeCenter unit, blade servers, and I/O (switch) modules:
  - "boot command" on page 72
  - "power command" on page 272
  - "reset command" on page 288
  - "shutdown command" on page 308
- **Power-management commands**

  Use these commands to monitor power consumption of the BladeCenter unit and installed components:
  - "fuelg command" on page 149
  - "pmpolicy command" on page 251
  - "volts command" on page 412
- **Save and restore configuration commands**

  Use these commands to save and restore the management-module configuration:
  - "read command" on page 280
  - "write command" on page 413
- **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 115
  - "exit command" on page 143
- **Systems-management commands (BladeCenter T only)**

  Use these commands to manage alarms for monitored parameters of the BladeCenter T unit:
  - "alarm command (BladeCenter T and HT only)" on page 43

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.

accseccfg command

This command displays and configures account security settings for the advanced management module.

Table 3. accseccfg command

Function	What it does	Command	Valid targets
Display account security settings	Displays the user account security settings for the advanced management module. Returned values: • Default security settings used (legacy, high, or custom) • -am: user authentication method (local, ldap, localldap, or ldaplocal) • -alt: authentication logging timeout (in seconds) • -cp: complex password (on, off) • -ct: CLI inactivity session timeout (in seconds) • -dc: minimum different characters in the password (when -cp is enabled) • -de: default administration password expiration (on, off) • -ia: account inactivity alert time period (in days) • -ici: log new login events from same user (on, off) • -id: account inactivity disable time period (in days) • -lf: maximum login failures • -lp: lockout period after maximum login failures (in minutes) • -mls: maximum simultaneous user sessions • -pc: password change on first access (on, off) • -pe: password expiration time period (in days) • -pi: minimum password change interval (in hours) • -pr: password required (on, off) • -rc: password reuse cycle • -wt: web inactivity session timeout (in minutes, none, or based on length of user session)	`accseccfg`	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 3. accseccfg command (continued)

Function	What it does	Command	Valid targets
Set account defaults to legacy level	Sets management-module account security to a predefined legacy set of default values. Legacy default values: • -alt: retains set value • -am: retains set value • -cp: off • -ct: retains set value • -dc: 0 • -de: off • -ia: 0 • -ici: retains set value • -id: 0 • -lf: 5 • -lp: 2 • -mls: retains set value • -pc: off • -pe: 0 • -pi: 0 • -pr: off • -rc: 0 • -wt: retains set value **Note:** • The user who is running the accseccfg -legacy command must have a password assigned. • The -legacy option must be run alone and not in conjunction with any other accseccfg command options.	`accseccfg -legacy` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 3. accseccfg command (continued)

Function	What it does	Command	Valid targets
Set account defaults to high level	Sets management-module account security to a predefined high set of default values. High default values are: • -am: retains set value • -cp: on • -ct: retains set value • -dc: 2 • -de: on • -ia: 120 • -id: 180 • -lf: 5 • -lp: 60 • -pc: on • -pe: 90 • -pi: 24 • -pr: on • -rc: 5 • -wt: retains set value **Note:** • The user who is running the accseccfg -high command must have a password assigned. • The -high option must be run alone and not in conjunction with any other accseccfg command options.	`accseccfg -high` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set authentication logging timeout	Sets a custom value for the amount of time that the management module will not log repeated logins by the same user.	`accseccfg -alt` *timeout* where *timeout* is 0, 5, 30, 60, 300, 600, 1800, 3600, 43200, or 86400 seconds. If a value of `none` is entered, login logging is disabled. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 3. accseccfg command (continued)

Function	What it does	Command	Valid targets
Set user authentication method	Sets a custom value for management module user authentication method.	`accseccfg -am` *method* where *method* is • `local` • `ldap` • `localldap` • `ldaplocal` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable complex password	Enables or disables the complex password for management-module user authentication. **Note:** Enabling the complex password also turns on the password required (-pr) command option.	`accseccfg -cp` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set CLI inactivity timeout	Sets the custom value for management-module CLI inactivity session timeout.	`accseccfg -ct` *timeout* where *timeout* is from 0 to 4,294,967,295 seconds, inclusive. This command can only be run by users who have the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 3. accseccfg command (continued)

Function	What it does	Command	Valid targets
Set minimum number of different characters for password	Sets custom value for the minimum number of different characters to be used in a management-module password. **Note:** The minimum number of different characters applies only when complex passwords are enabled.	`accseccfg -dc` *number* where *number* is from 0 to 15, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable default administration password expiration	Enables or disables the default administration password expiration for the management module.	`accseccfg -de` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set account inactivity alert time	Sets custom value for management module account inactivity alert time. **Note:** The accseccfg -ia value must be less than the accseccfg -id value.	`accseccfg -ia` *time* where *time* is from 0 to 365 days, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 3. accseccfg command (continued)

Function	What it does	Command	Valid targets
Set state for logging of login events from same IP address	Enables or disables logging of new login events from the same user from the same IP address. **Note:** This value applies only if the value set by the `-alt` command option is set to something other than 0 or none.	`accseccfg -ici` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set account inactivity disable time	Sets the custom value for management-module account inactivity disable time. **Note:** The accseccfg -id value must be greater than the accseccfg -ia value.	`accseccfg -id` *time* where *time* is from 0 to 365 days, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set maximum number of login failures	Sets the custom value for the maximum number of login failures before the management module locks out a user.	`accseccfg -lf` *number* where *number* is from 0 to 10, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 3. accseccfg command (continued)

Function	What it does	Command	Valid targets
Set lockout period	Sets the custom value for management-module account lockout period, used when the maximum number of login failures is exceeded.	`accseccfg -lp` *time* where *time* is from 0 to 2880 minutes, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set maximum LDAP sessions for user	Sets the custom value for the maximum number of simultaneous login sessions allowed for a single LDAP user	`accseccfg -mls` *max_sessions* where *max_sessions* is from 0 to 20, inclusive. This command can only be run by users who have the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable password change at first login	Enables or disables the mandatory password change at first management-module login.	`accseccfg -pc` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 3. accseccfg command (continued)

Function	What it does	Command	Valid targets
Set password expiration time	Sets custom value for the management module password expiration time.	`accseccfg -pe` *time* where *time* is from 0 to 365 days, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set password minimum change interval	Sets custom value for the minimum amount of time between management module password changes.	`accseccfg -pi` *time* where *time* is from 0 to 1440 hours, inclusive, and less than password expiration period when that period is greater than 0. This command can only be run by users who have the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable password required	Enables or disables the password required for management module. **Notes:** • The user that is running the accseccfg -pr command must have a password assigned. • Disabling password required also turns off the complex password (-cp) command option.	`accseccfg -pr` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 3. accseccfg command (continued)

Function	What it does	Command	Valid targets
Set password reuse cycle	Sets custom value for the management module password reuse cycle. This setting determines how many times a password must be changed before being reused.	`accseccfg -rc` *number_reuses* where *number_reuses* is from 0 to 5, inclusive. This command can only be run by users who have the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set web interface inactivity timeout	Sets custom value for management module web interface inactivity session timeout.	`accseccfg -wt` *timeout* where *timeout* is 1, 5, 10, 15, or 20 minutes, `none` (no timeout), or `user` (user picks timeout each time they log in to the web interface). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

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

```
accseccfg -alt none
```

To set management-module account security to use the high level defaults, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
accseccfg -high
```

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

```
accseccfg
```

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

```
system:mm[1]> accseccfg -alt none
OK
system:mm[1]> accseccfg -high
OK
system:mm[1]> accseccfg
-high
-alt 600
-am local
-cp on
-ct 0
-dc 2
-de on
-ia 120
-ici on
-id 180
-lf 5
-lp 60
-mls 5
-pc on
-pe 90
-pi 24
-pr on
-rc 5
-wt user
system:mm[1]>
```

advfailover command

This command displays and configures the advanced failover settings for the advanced management module.

Table 4. advfailover command

Function	What it does	Command	Valid targets
Display management module advanced failover settings	Displays the advanced failover settings for the management module. Possible return values are: • off - disable network interface for the standby management module • swap - enable the standby management module network interface and swap IP addresses between the two management modules during failover • noswap - enable the standby management module network interface and do not swap IP addresses between the two management modules during failover **Note:** This command does not apply to the BladeCenter S unit, which supports only a single advanced management module.	`advfailover`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Disable network interface for standby management module	Disables the network interface for the standby management module, preventing failover.	`advfailover -ip off` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable network interface and allow IP address swap during failover	Enables the network interface for the standby management module and allows the IP addresses to swap between the two management modules during failover.	`advfailover -ip swap` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 4. advfailover command (continued)

Function	What it does	Command	Valid targets
Enable network interface and prevent IP address swap during failover	Enables the network interface for the standby management module and prevents the IP addresses from swapping between the two management modules during failover.	`advfailover -ip noswap` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

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

```
advfailover -ip off
```

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

```
advfailover
```

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

```
system:mm[1]> advfailover -ip off
OK
system:mm[1]> advfailover
-ip off
system:mm[1]>
```

airfilter command (BladeCenter S only)

This command sets the interval for air filter change notifications for a BladeCenter S unit.

Table 5. airfilter (set notification interval) command

Function	What it does	Command	Valid targets
Display air filter change notification interval	Displays the frequency of the chassis air filter reminder.	`airfilter`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set air filter change notification interval	Configures the frequency of the chassis air filter reminder. **Note:** The 1 month replacement interval is recommended for environments with a high amount of dust. Replacement every 3 months is recommended for environments with medium amounts of dust. Replacement every 6 months is recommended for environments with low amounts of dust.	`airfilter -freq` *frequency* where *frequency* is the interval, in months, between reminders to change the chassis air filter. Valid values are 0, 1, 3, and 6. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management • Chassis log management • Chassis administration • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

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

```
airfilter
```

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

```
airfilter -freq 3
```

The following example shows the information that is returned when these commands are entered:

```
system:mm[1]> airfilter
-freq 1
system:mm[1]>

system:mm[1]> airfilter -freq 3
OK
system:mm[1]>
```

alarm command (BladeCenter T and HT only)

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

Table 6. 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 -q`	`-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.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Blade administration
		• Blade remote presence
		
		See "Commands and user authority" on page 8 for additional 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.

Table 6. 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.

Table 6. alarm command (continued)

Function	What it does	Command	Valid targets

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.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for management module, power module, or blower)
		• Blade configuration (for blade server)
		• I/O module configuration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional 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.

Acknowledge alarm (specified by generator information)	Acknowledge the alarm specified by the generator information.	`alarm -r -o` *value*
		
		where *value* is the generator information.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for management module, power module, or blower)
		• Blade configuration (for blade server)
		• I/O module configuration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional 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.

Table 6. alarm command (continued)

Function	What it does	Command	Valid targets

Acknowledge alarm (specified by alarm ID)	Acknowledge the alarm specified by the alarm ID.	`alarm -r -a` *value*
		
		where *value* is the alarm ID.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for management module, power module, or blower)
		• Blade configuration (for blade server)
		• I/O module configuration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional 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.

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
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for management module, power module, or blower)
		• Blade configuration (for blade server)
		• I/O module configuration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional 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.

Table 6. alarm command (continued)

Function	What it does	Command	Valid targets

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.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for management module, power module, or blower)
		• Blade configuration (for blade server)
		• I/O module configuration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional 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.

Clear alarm (specified by generator information)	Clear the alarm specified by the generator information.	`alarm -c -o value`
		
		where *value* is the generator information.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for management module, power module, or blower)
		• Blade configuration (for blade server)
		• I/O module configuration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional 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.

Table 6. alarm command (continued)

Function	What it does	Command	Valid targets

Clear alarm (specified by alarm ID)	Clear the alarm specified by the alarm ID.	`alarm -c -a` *value*
		
		where *value* is the alarm ID.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for management module, power module, or blower)
		• Blade configuration (for blade server)
		• I/O module configuration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional 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.

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
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for management module, power module, or blower)
		• Blade configuration (for blade server)
		• I/O module configuration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional 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.

Table 6. alarm command (continued)

Function	What it does	Command	Valid targets

Set alarm	Set an alarm for the specified target, including severity level and description.	`alarm -s -l` *level desc*
		
		where
		• *level* is the severity level:
		– `CRT` (critical)
		– `MJR` (major)
		– `MNR` (minor)
		• *desc* is a short text description of the alarm
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for management module, power module, or blower)
		• Blade configuration (for blade server)
		• I/O module configuration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional 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.

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>
```

alertcfg command

This command displays and configures the global remote alert settings for the advanced management module.

Table 7. alertcfg command

Function	What it does	Command	Valid targets
Display global remote alert settings	Displays the global remote alert settings for the advanced management module.	`alertcfg`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set remote alert retry delay interval and number of retries	Sets the remote alert retry delay interval and permitted number of retries.	`alertcfg -dr` *delay* `-rl` *limit* where: • *delay* is from 0.5 minutes to 4.0 minutes, inclusive, in 0.5 minute increments. If you enter a value less than 0.5 minute, the retry interval will be set to 0.5 minute. If you enter a value greater than 4.0 minutes, the retry interval will be set to 4.0 minutes. • *limit* is the remote alert retry limit, ranging from 0 to 8. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Include / exclude service information with email alerts	Enables or disables inclusion of service information with email alerts.	`alertcfg -si` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 7. alertcfg command (continued)

Function	What it does	Command	Valid targets
Set remote alert retry limit	Sets the maximum number of times the system will attempt to send a remote alert, if previous attempts were unsuccessful.	`alertcfg -rl` *value* where *value* is from 0 to 8, inclusive. If you enter a value of 0, no retries will be attempted. If you enter a value greater than 8, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

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

```
alertcfg
```

To set the retry interval to 3.5 minutes, include service information in the alert, and set the remote alert retry limit to 7, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
alertcfg -dr 3.5 -si enabled -rl 7
```

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

```
system:mm[1]> alertcfg
-dr 2.0
-si disabled
-rl 6
system:mm[1]> alertcfg -dr 3.5 -si enabled -rl 7
OK
system:mm[1]> alertcfg
-dr 3.5
-si enabled
-rl 7
system:mm[1]>
```

alertentries command

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

Table 8. 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 (Email over LAN/Systems 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 email notifications) • -i *static_IP_addr/hostname* (used for IBM Systems 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 8. alertentries command (continued)

Function	What it does	Command	Valid targets
Create alert recipient	Create the specified alert recipient. All fields must be specified when creating an alert recipient.	`alertentries` *-recip_number* `-n` *recip_name* -status *alert_status* `-f` *filter_type* `-t` *notification_method* -e *email_addr* `-i` *ip_addr/hostname* where: • *recip_number* is a number from 1 to 12 that corresponds to an unused recipient number in the "Display alert properties for all recipients" list. • *recip_name* is a alphanumeric string up to 31 characters in length containing any character, including spaces, except for angle brackets (< and >). If the string includes spaces it must be enclosed in double-quotes. • *alert_status* is `on` or `off` for receipt of alerts. • *filter_type* filters the alert types received: `critical` (receive critical alerts only) or `none` (receive all alerts). • *notification_method* is `email`, `director` (IBM Systems Director) or `snmp`. – For `email`, you must specify an email 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 email 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 8. 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 (_). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 8. alertentries command (continued)

Function	What it does	Command	Valid targets
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
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). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 8. alertentries command (continued)

Function	What it does	Command	Valid targets
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 Systems Director) – `snmp` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set alert recipient email address	Sets the email address for the specified alert recipient. This email address is used to send alerts to the recipient via email. The email 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 email address string up to 63 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 8. alertentries command (continued)

Function	What it does	Command	Valid targets
Set alert recipient IP address or hostname	Sets the IP address or hostname used to send alert notifications to the specified alert recipient using IBM Systems 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 Systems 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 (_). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Generate test alert	Generates a test alert to verify correct alert response. **Notes:** • The `alertentries -test` command option must be used alone. • If autoftp is enabled, sending a test alert will cause the system to send out service data as well.	`alertentries -test` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis log management • Chassis administration • Chassis configuration • Blade administration • Blade configuration • Blade remote presence • I/O module administration • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-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 email, 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 Systems 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]>
```

autoftp command

This command displays and configures the automated FTP/TFTP problem report settings for the advanced management module.

Table 9. autoftp command

Function	What it does	Command	Valid targets
Display call-home settings for autoftp call home	Displays the Automated FTP/TFTP Problem Report settings that allow the advanced management module to automatically put service data onto a specified server when a call home event is detected.	`autoftp`	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 9. autoftp command (continued)

Function	What it does	Command	Valid targets
Configure call-home settings for autoftp call home	Configures the Automated FTP/TFTP Problem Report settings that allow the advanced management module to automatically put service data onto a specified server when a call home event is detected. **Note:** The system will wait five days before sending duplicate events if they are left unacknowledged in the activity log.	`autoftp -m` *mode* `-i` *ip_address* `-p` *port* `-u` *"user_name"* `-pw` *"password"* where: • *mode* is one of the following automated problem reporting modes: – `ftp` – `tftp` – `disabled` • *ip_address* is the IP address of the FTP or TFTP server • *port* is the FTP or TFTP transmission port, a number from 1 to 65535, inclusive. If you enter a value outside this range, an error message will be displayed. • *"user_name"* is the quote-delimited FTP User Name for automated problem reporting (63 characters maximum). • *"password"* is the quote-delimited FTP password for automated problem reporting (63 characters maximum). **Notes:** • For FTP, all fields must be set. • For TFTP, only -i and -p are needed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

To view the settings of the automated call-home message feature, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
autoftp
```

To configure the automated call-home message feature to report call-home events using TFTP to tftp.ibm.com over transmission port 69, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
autoftp -m tftp -i tftp.ibm.com -p 69
```

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

```
system:mm[1]> autoftp
-m ftp
-i ftp.ibm.com
-p 6
-u smlite
system:mm[1]> autoftp -m tftp -i tftp.ibm.com -p 69
OK
system:mm[1]>
```

baydata command

This command allows a user to set, assign, and display informational data assigned to the blade server bays.

Table 10. baydata command

Function	What it does	Command	Valid targets
Display bay data for all blade servers	Displays blade server bay data for bay number, bay data status, and defined bay data for all bays.	`baydata`	`-T system`
Display blade server bay data for a specific bay	Displays the information assigned to the specified blade bay using the -b option.	`baydata -b` *bay_num* where *bay_num* is the number of the specific bay to display. The bay number must be within the scope assigned to the user. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
Clear bay data	Clears the blade bay definition strings for all bays.	`baydata -clear` The bay number must be within the scope assigned to the user. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 10. baydata command (continued)

Function	What it does	Command	Valid targets
Clear bay data for specific bay	Clears the blade bay definition strings for the specified blade bay.	`baydata -b` *bay_num* `-clear` where *bay_num* is the number of the specified bay to clear of data. The bay number must be within the scope of the user. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
Set bay data	Sets blade bay data for all blade servers within the user's scope. This information can include: data about drivers or software, the BladeCenter unit shelf number and IP address, and whether the blade server is a master or member in a high-availability system. **Note:** To apply changes to the BIOS/SMBIOS structure, power-off and power-on the blade server, restart the blade server, or remove and reinstall the blade server.	`baydata -data` *"data_definition"* where *"data definition"* is the ASCII string of up to 60 characters enclosed in double quotation marks–"data definition". The quotation marks are not stored. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 10. baydata command (continued)

Function	What it does	Command	Valid targets
Set blade bay data definition for specific blade server	Sets blade bay data for the specified blade server using the -b option. **Note:** To apply changes to the BIOS/SMBIOS structure, power-off and power-on the blade server, restart the blade server, or remove and reinstall the blade server. If the command is issued to a specific bay, data is written to that blade server if it is in the user's scope.	`baydata -b` *bay_num* `-data` *"data_definition"* where: • *bay_num* is the blade bay • where *"data definition"* is the quote-delimited ASCII string of up to 60 characters This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Example: To view the bay data for all blades, while the management module is set as the persistend command environment, at the `system>` prompt, type

```
baydata
```

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

```
system> baydata
Bay  Status            Definition
1    Unsupported
2    No blade present
3    No blade present
4    No blade present
5    No blade present
6    No blade present
7    No blade present
8    No blade present
9    No blade present
10   No blade present
11   No blade present
12   No blade present
13   No blade present
14   No blade present
system>
```

bofm command

This command applies a new BladeCenter Open Fabric Manager (BOFM) configuration to all the specified BladeCenter units, bays, and ports.

Notes:

1. Open Fabric Manager is not a standard management module feature; it is offered and documented separately. See the *BladeCenter Open Fabric Manager Installation and Users Guide* for more detailed information.
2. If the number of advanced management module TCP command mode connections is zero, or if all available TCP command mode connections are in use, a connection failure message is generated by the BOFM feature. Make sure that the advanced management module TCP command mode connection limit is positive and that no more than the available number of connections are in use. See the *BladeCenter Open Fabric Manager Installation and Users Guide* for additional information.

Table 11. bofm command

Function	What it does	Command	Valid targets
Apply BOFM configuration to specified BladeCenter units, bays, and ports	Copies a configuration file from a TFTP server to the specified management module, which then configures BladeCenter units, blade servers, and I/O modules. The configuration file is a comma-separated values (CSV) file that assigns IP addresses and other values to BladeCenter units, bays, and ports.	`bofm -l` *filename* `-i` *ip_address* where: • *filename* is the name of the configuration file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the configuration file is located. **Note:** Both the `-l` *filename* option and the `-i` *ip_address* option need to be specified. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system:mm[x]` where x is the primary management-module bay number.

Table 11. bofm command (continued)

Function	What it does	Command	Valid targets
Apply BOFM configuration to specified BladeCenter units, bays and ports while ignoring duplicate lines in the configuration file	Copies a configuration file from a TFTP server to the specified management module, which then configures BladeCenter units, blade servers, and I/O modules, even if it encounters duplicate lines in the configuration file. The configuration file is a comma-separated values (CSV) file that assigns IP addresses and other values to BladeCenter units, bays, and ports.	`bofm -l` *filename* `-i` *ip_address* `-d off` where: • *filename* is the name of the configuration file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the configuration file is located. • The `-d off` option causes bofm to ignore duplicate lines in the configuration file. **Note:** Both the `-l` *filename* option and the `-i` *ip_address* option need to be specified. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where x is the primary management-module bay number.

Table 11. bofm command (continued)

Function	What it does	Command	Valid targets
Apply BOFM configuration to specified BladeCenter units, bays, and ports unless there are duplicate lines in the configuration file	Copies a configuration file from a TFTP server to the specified management module, which then configures BladeCenter units, blade servers, and I/O modules, but halts the operation if it encounters duplicate lines in the configuration file. The configuration file is a comma-separated values (CSV) file that assigns IP addresses and other values to BladeCenter units, bays, and ports.	`bofm -l` *filename* `-i` *ip_address* `-d on` where: • *filename* is the name of the configuration file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the configuration file is located. • The `-d on` option halts bofm if there are duplicate lines in the configuration file. **Note:** Both the `-l` *filename* option and the `-i` *ip_address* option need to be specified. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where x is the primary management-module bay number.

Table 11. bofm command (continued)

Function	What it does	Command	Valid targets
Apply BOFM configuration to specified BladeCenter units, bays, and ports even if the bays are powered on	Copies a configuration file from a TFTP server to the specified management module, which then configures BladeCenter units, blade servers, and I/O modules, after checking to make sure that the bays are not powered on. The configuration file is a comma-separated values (CSV) file that assigns IP addresses and other values to BladeCenter units, bays, and ports.	`bofm -l` *filename* `-i` *ip_address* `-p on` where: • *filename* is the name of the configuration file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the configuration file is located. • The `-p on` option halts the bofm command if bays are powered on. **Note:** Both the `-l` *filename* option and the `-i` *ip_address* option need to be specified. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where x is the primary management-module bay number.

Table 11. bofm command (continued)

Function	What it does	Command	Valid targets
Apply BOFM configuration to specified BladeCenter units, bays, and ports unless bays are powered on	Copies a configuration file from a TFTP server to the specified management module, which then configures BladeCenter units, blade servers, and I/O modules, without checking if the bays are powered on. The configuration file is a comma-separated values (CSV) file that assigns IP addresses and other values to BladeCenter units, bays, and ports. **Note:** Do not change the BOFM configuration while a blade server is powered on.	`bofm -l` *filename* `-i` *ip_address* `-p off` where: • *filename* is the name of the configuration file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the configuration file is located. • The `-p off` option forces BOFM to apply the configuration file to blade servers that are powered on. **Note:** Both the `-l` *filename* option and the `-i` *ip_address* option need to be specified. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where x is the primary management-module bay number.

Table 11. bofm command (continued)

Function	What it does	Command	Valid targets
Apply BOFM configuration to specified BladeCenter units, bays, and ports (verbose)	Copies a configuration file from a TFTP server to the specified management module, which then configures BladeCenter units, blade servers, and I/O modules, a process which might take several minutes. The detailed information is shown after the update is complete.	`bofm -l` *filename* `-i` *ip_address* `-v` where: • *filename* is the name of the configuration file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the configuration file is located. **Note:** Both the `-l` *filename* option and the `-i` *ip_address* option need to be specified. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where x is the primary management-module bay number.

Example:

To apply a new BOFM configuration file to a set of BladeCenter units and view details of the procedure, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
bofm -i 9.148.8.2 -l apply.csv -v
```

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

```
system:mm[1]> bofm -i 9.148.8.2 -l apply.csv -v
TFTP file upload successful.
Starting to apply new BOFM configuration on MM
Percent complete: 100%
Status: Confirmed configuration change.
Percent complete: 100%
Status: Configuration applied.
Applying new BOFM configuration on MM - Completed.
system:mm[1]>
```

boot command

This command resets blade servers with several different restart options.

Table 12. 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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration and blade remote presence See "Commands and user authority" on page 8 for additional information.	`-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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-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]>
```

bootmode command

This command sets and displays the boot mode settings for blade servers installed in the BladeCenter unit that support this feature.

Table 13. bootmode command

Function	What it does	Command	Valid targets
Display blade server boot mode	Displays the boot mode settings of the specified blade server. **Note:** This command will execute only on blade servers that support the bootmode feature.	`bootmode`	`-T system:blade[x]` where *x* is the blade server bay number.
Set blade server boot mode	Sets the copy of firmware that the specified blade server will use to boot: • Temporary: booting from the temporary copy is recommended since it typically contains the latest enhancements and fixes. • Permanent: booting from the permanent copy should be used only when booting from the temporary copy is no longer possible. Changes to the boot mode setting take effect after the next restart of the blade server. **Note:** This command will execute only on blade servers that support the bootmode feature.	`bootmode -p` *mode* where *mode* is: • `temp` for temporary firmware copy. • `perm` for permanent firmware copy. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade server bay number.

Example: To view the boot mode of the blade server in bay 2, while this blade server is set as the persistent command environment, at the `system:blade[2]>` prompt, type

```
bootmode
```

To set the boot mode of the blade server in bay 2 to permanent, while this blade server is set as the persistent command environment, at the `system:blade[2]>` prompt, type

```
bootmode -p perm
```

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

```
system:blade[2]> bootmode
active: temporary
pending: Invalid boot mode type
system:blade[2]> bootmode -p perm
Set the blade boot mode to permanent succeeded.
The setting will become active after the next reboot of the blade.
system:blade[2]> bootmode
active: temporary
pending: permanent
system:blade[2]>
```

bootseq command

This command sets and displays the boot sequence settings for blade servers installed in the BladeCenter unit.

Table 14. bootseq command

Function	What it does	Command	Valid targets
Display blade server boot sequence	Displays the boot sequence of the specified blade server. Possible return values are: • floppy (diskette drive) • usbdisk (USB device) • iscsi (iSCSI) • iscsicrt (iSCSI critical) • nw (network) • nodev (no device) • hd0 (hard disk drive 0) • hd1 (hard disk drive 1) • hd2 (hard disk drive 2 • hd3 (hard disk drive 3) • hd4 (hard disk drive 4) • cd (CD-ROM drive) • usb (media tray) • hyper (hypervisor) • uefi (unified extensible firmware interface) • legacy (UEFI-specified legacy sequence)	`bootseq`	`-T system:blade[x]` where *x* is the blade server bay number.

Table 14. bootseq command (continued)

Function	What it does	Command	Valid targets
Set boot sequence for blade server	Sets the boot sequence of the specified blade server.	`bootseq` *devicelist* where *devicelist* has one or more of the following boot devices specified, in order of preference: • `floppy` for the diskette drive (non-POWER-based blade servers only) • `usbdisk` for a USB device (not supported by all blade servers) • `iscsi` for iSCSI • `iscsicrt` for iSCSI critical • `nw` for network - PXE • `nodev` for no device • `hd0` for hard disk drive 0 • `hd1` for hard disk drive 1 • `hd2` for hard disk drive 2 • `hd3` for hard disk drive 3 • `hd4` for hard disk drive 4 • `cd` for the CD-ROM drive • `usb` for the media tray (non-POWER-based blade servers installed in BladeCenter T units only) • `hyper` for hypervisor (only for blade servers that use hypervisor virtualization) • `uefi` for unified extensible firmware interface (UEFI) (only for blade servers that support this feature) • `legacy` for the UEFI-specified legacy boot sequence (only for blade servers that support this feature) *(continued on next page)*	`-T system:blade[`*x*`]` where *x* is the blade server bay number.

Table 14. bootseq command (continued)

Function	What it does	Command	Valid targets
Set boot sequence for blade server *(continued)*		A boot sequence of up to four boot devices can be specified. If fewer than four devices are specified, the remaining items in the sequence are set to nodev. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	

Table 14. bootseq command (continued)

Function	What it does	Command	Valid targets
Set boot sequence for all blade servers	Sets the same boot sequence for all blade servers installed in the BladeCenter unit.	`bootseq -all` *devicelist* where *devicelist* has one or more of the following boot devices specified, in order of preference: • `floppy` for the diskette drive (non-POWER-based blade servers only) • `usbdisk` for a USB device (not supported by all blade servers) • `iscsi` for iSCSI • `iscsicrt` for iSCSI critical • `nw` for network - PXE • `nodev` for no device • `hd0` for hard disk drive 0 • `hd1` for hard disk drive 1 • `hd2` for hard disk drive 2 • `hd3` for hard disk drive 3 • `hd4` for hard disk drive 4 • `cd` for the CD-ROM drive • `usb` for the media tray (non-POWER-based blade servers installed in BladeCenter T units only) • `hyper` for hypervisor (only for blade servers that use hypervisor virtualization) • `uefi` for unified extensible firmware interface (only for blade servers that support this feature) *(continued on next page)*	`-T system:blade[`*x*`]` where *x* is the blade server bay number.

Table 14. bootseq command (continued)

Function	What it does	Command	Valid targets
Set boot sequence for all blade servers *(continued)*		• `legacy` for the UEFI-specified legacy boot sequence (only for blade servers that support this feature) A boot sequence of up to four boot devices can be specified. If fewer than four devices are specified, the remaining items in the sequence are set to `nodev`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	

Example: To set a boot sequence of diskette drive, CD-ROM drive, and hard disk drive 0 for the blade server in blade bay 3, while the blade server in blade bay 3 is set as the persistent command environment, at the `system:blade[3]>` prompt, type

```
bootseq floppy cd hd0
```

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

```
bootseq
```

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

```
system:blade[3]>  bootseq floppy cd hd0
OK
system:blade[3]>  bootseq
floppy
cd
hd0
nodev
system:blade[3]>
```

buildidcfg command

This command creates, displays, and configures the list of firmware build IDs for the blade servers.

Table 15. buildidcfg command

Function	What it does	Command	Valid targets
Display blade server firmware build IDs	Displays list of blade server firmware build IDs. **Note:** The build ID list must be built using the `-create` command option before it can be displayed.	`buildidcfg`	`-T system`
Create blade server build ID list	Creates an initial firmware build ID list for all blade servers installed in the BladeCenter unit. **Note:** The build ID list contains information for only those blade servers that have VPD which is fully accessible by the advanced management module. Any blade servers with VPD that is unavailable or failed will be ignored and not appear in the list..	`buildidcfg -create` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See “Commands and user authority” on page 8 for additional information.	`-T system`

Table 15. buildidcfg command (continued)

Function	What it does	Command	Valid targets
Add blade server build ID list entry	Adds a new blade server firmware build ID entry to the list. **Note:** All options must be specified when adding a new firmware build ID entry. The arguments for manufacturer, machine type, firmware type, and build ID cannot be blank or unspecified; however, the argument for build revision can be blank or not set.	`buildidcfg -ab -mfg` *manufacturer* `-mt` *machine_type* `-ft` *type* `-id` *build_id* `-rev` *build_rev* where: • *manufacturer* is a manufacturer name, up to 31 characters in length, enclosed in quotation marks. The manufacturer name can contain spaces, but no leading or trailing spaces are allowed. • *machine_type* is a machine type, up to 31 characters in length, enclosed in quotation marks. The machine type can contain spaces, but no leading or trailing spaces are allowed. • *firmware_type* is `bios`, `diags`, or `bmc`. • *build_id* is a firmware build ID, up to 31 characters in length, enclosed in quotation marks. The firmware build ID can contain spaces, but no leading or trailing spaces are allowed. • *build_rev* is a firmware build revision, up to 31 characters in length, enclosed in quotation marks. The firmware build revision can contain spaces, but no leading or trailing spaces are allowed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 15. buildidcfg command (continued)

Function	What it does	Command	Valid targets
Update blade server build ID list entry - manufacturer	Update the manufacturer for the specified blade server firmware build ID entry. **Note:** • The *index* number for each entry in the list is found by running the `buildidcfg` command with no options. • The argument for manufacturer cannot be blank or unspecified.	`buildidcfg -ub` *index* `-mfg` *manufacturer* where: • *index* is the index of the build ID list entry. • *manufacturer* is a manufacturer name, up to 31 characters in length, enclosed in quotation marks. The manufacturer name can contain spaces, but no leading or trailing spaces are allowed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system`
Update blade server build ID list entry - machine type	Update the machine type for the specified blade server firmware build ID entry. **Note:** • The *index* number for each entry in the list is found by running the `buildidcfg` command with no options. • The argument for machine type cannot be blank or unspecified.	`buildidcfg -ub` *index* `-mt` *machine_type* where: • *index* is the index of the build ID list entry. • *machine_type* is a machine type, up to 31 characters in length, enclosed in quotation marks. The machine type can contain spaces, but no leading or trailing spaces are allowed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 15. buildidcfg command (continued)

Function	What it does	Command	Valid targets
Update blade server build ID list entry - firmware type	Update the firmware type for the specified blade server firmware build ID entry. **Note:** • The *index* number for each entry in the list is found by running the `buildidcfg` command with no options. • The argument for firmware type cannot be blank or unspecified.	`buildidcfg -ub` *index* `-ft` *firmware_type* where: • *index* is the index of the build ID list entry. • *firmware_type* is `bios`, `diags`, or `bmc`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system`
Update blade server build ID list entry - firmware build ID	Update the firmware build ID for the specified blade server firmware build ID entry. **Note:** • The *index* number for each entry in the list is found by running the `buildidcfg` command with no options. • The argument for build ID cannot be blank or unspecified.	`buildidcfg -ub` *index* `-id` *build_id* where: • *index* is the index of the build ID list entry. • *build_id* is a firmware build ID, up to 31 characters in length, enclosed in quotation marks. The firmware build ID can contain spaces, but no leading or trailing spaces are allowed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 15. buildidcfg command (continued)

Function	What it does	Command	Valid targets
Update blade server build ID list entry - firmware build revision	Update the firmware build revision for the specified blade server firmware build ID entry. **Note:** • The *index* number for each entry in the list is found by running the `buildidcfg` command with no options. • The argument for the build revision can be blank or not set.	`buildidcfg -ub` *index* `-rev` *build_rev* where: • *index* is the index of the build ID list entry. • *build_rev* is a firmware build revision, up to 31 characters in length, enclosed in quotation marks. The firmware build revision can contain spaces, but no leading or trailing spaces are allowed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system`
Delete all entries from blade server build ID list	Delete all blade server firmware build ID entries from the list.	`buildidcfg -db all` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 15. buildidcfg command (continued)

Function	What it does	Command	Valid targets
Delete entry from blade server build ID list	Delete a specific blade server firmware build ID entry from the list. **Note:** The *index* number for each entry in the list is found by running the `buildidcfg` command with no options.	`buildidcfg -db` *index* where *index* is the index number of a specific build ID list entry to delete. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system`
Import blade server build ID list	Import a firmware build ID list from file. The file name to import must specify a qualified location for the build ID list image that indicates the protocol to be used. For example, tftp://192.168.0.1/tmp/buildid.txt.	`buildidcfg -import` *filename* where *filename* is a qualified location of up to 256 characters in length that indicates the protocol to be used (tftp, ftp, ftps, http, or https) and contains any character except the percent sign (%) or double-quote ("). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 15. buildidcfg command (continued)

Function	What it does	Command	Valid targets
Export blade server build ID list	Export the current build ID list to a specified TFTP server.	`buildidcfg -export` *ip_address* where *ip_address* is a valid IP address. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration • Blade configuration • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system`

Example: To create the initial build ID list, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
buildidcfg -create
```

To view the build ID list, while the BladeCenter unitis set as the persistent command environment, at the `system>` prompt, type

```
buildidcfg
```

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

```
system> buildidcfg -create
OK
system> buildidcfg
Index  Manufacture   Machine Type  Firmware Type            Build ID    Revision
1      IBM           8853          Blade Sys Mgmt Processor  BCBT58A     1.18

2      IBM           8853          Diagnostics               BCYT28AUS   1.06

3      IBM           8853          FW/BIOS                   BCE141AUS   1.17

4      IBM           7971          Blade Sys Mgmt Processor  BABT55A     1.32

5      IBM           7971          Diagnostics               BAYT37AUS   1.06

6      IBM           7971          FW/BIOS                   BAE155AUS   1.10

system>
```

chconfig command

This command configures the BladeCenter unit Service Advisor feature.

Table 16. chconfig command

Function	What it does	Command	Valid targets
Display Service Advisor configuration	Displays the contact information for the Service Advisor feature. Service Advisor resides on your advanced management module and monitors your BladeCenter unit for hardware events. Upon detecting a hardware event, Service Advisor captures the event, error logs, and service data, and can automatically report the event to IBM support. To send call home event to IBM support, you must enable and configure Service Advisor. For each call home event IBM receives, a service ticket will opened, and a follow-up call will be made. This feature will generate a message to IBM when events occur in the BladeCenter unit or one of its components that usually can be resolved without additional problem determination. **Note:** The system will wait five days before sending duplicate events if they are left unacknowledged in the activity log.	`chconfig`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display / accept Service Advisor terms and conditions	Displays or accepts the terms of the Service Advisor terms and conditions.	`chconfig -li` *license* where *license* is • `view` to view the Service Advisor terms and conditions. • `accept` to accept the Service Advisor terms and conditions. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 16. chconfig command (continued)

Function	What it does	Command	Valid targets
Enable / disable Service Advisor terms and conditions	Enables or disables the call-home terms and conditions. **Notes:** • All contact information fields are required before the Service Advisor can be enabled. • Call Home will connect to IBM through HTTPS and HTTP. HTTP Proxy fields must be set to permit for outbound traffic. • Service Advisor also needs to set up DNS server address on the advanced management module. • Changing the Service Advisor setting from disabled to enabled will automatically trigger a test call home and the Service Advisor Activity Log will record this test call home.	`chconfig -sa` *setting* `-sc` *support_center* where • *setting* is – `enable` to activate the Service Advisor terms and conditions. – `disable` to suspend the Service Advisor terms and conditions. • *support_center* is the 2–character ISO 3166 country code of the IBM support center location. For example, the country code for the United States is US. **Notes:** • Go to http://www.iso.org/iso/country_codes/iso_3166_code_lists/ for a complete list of country codes. • Valid country codes must refer to countries that have IBM support centers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 16. chconfig command (continued)

Function	What it does	Command	Valid targets
Set contact information for Service Advisor	Sets contact information for the Service Advisor.	`chconfig -co "company" -cn "name" -cph "phone" -ce email -ca "address" -cci "city" -cs state -sc support_center -cz "postalcode"` where: • *"company"* is the quote-delimited contact company name, of up to 30 characters in length. • *"name"* is the quote-delimited contact name, of 1 to 30 characters in length. • *"phone"* is the quote-delimited contact phone number, of 5 to 30 characters in length. • *email* is email address of the contact person in the form userid@hostname (30 characters maximum). The userid can be alphanumeric characters, ".", "-", or "_" but must begin and end with alphanumeric characters. The hostname can be alphanumeric characters, ".", "-", or "_". It must contain at least two domain items. Every domain item should begin and end with an alphanumeric character and the last domain item should be from 2 to 20 alphabetic characters. • *"address"* is the quote-delimited street address of the machine location, of 1 to 30 characters in length. • *"city"* is the quote-delimited city of the machine location, of 1 to 30 characters in length. *(continued on next page)*	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 16. chconfig command (continued)

Function	What it does	Command	Valid targets
Set contact information for Service Advisor *(continued)*		• *state* is the state of the machine location, of 2 to 3 characters in length. • *"postalcode"* is the quote-delimited postal code of the machine location, of 1 to 9 alphanumeric characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	

Table 16. chconfig command (continued)

Function	What it does	Command	Valid targets
Set up HTTP proxy for Service Advisor	Sets up HTTP proxy for Service Advisor.	`chconfig -ps` *setting* `-loc` *hostname* `-po` *port* `-u` *"username"* `-pw` *"password"* where: • *setting* is `enabled` or `disabled` • *hostname* is the fully qualified host name or IP address of the HTTP proxy, of 1 to 63 characters in length. • *port* is the port of the HTTP proxy, a number from 1 to 65535, inclusive. • *"username"* is the quote-delimited user name, of 1 to 30 characters in length. • *"password"* is the quote-delimited password of the HTTP proxy, of up to 15 characters in length This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

To accept the Service Advisor terms and conditions, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
chconfig -li accept
```

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

```
chconfig
```

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

```
system:mm[1]> chconfig -li accept
OK
system:mm[1]> chconfig
-sa enabled
-sc  US
-ca  No 399, Keyuan Rd,
-cci  Dallas
-ce  bob@cn.ibm.com
-cn  bob
-co  IBM
-cph  800-555-1111
-cs  TX
-cz  75210
-loc  google.cn
-po  8080
-ps disabled
-u  User-001
system:mm[1]>
```

chlog command

This command is used to display up to five call-home activity log entries and to mark a call-home event entry as acknowledged or unacknowledged.

Table 17. chlog (display call-home activity log) command

Function	What it does	Command	Valid targets
Display call-home activity log entries	Displays the last five entries from the call-home activity log. **Notes:** • The entries are displayed in reverse chronological order (most recent call-home entry first). • The system will wait 5 days before sending duplicate events if they are not acknowledged as corrected in the activity log. • Call-home events are usually those that can be resolved without additional problem determination.	`chlog`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display FTP/TFTP server call-home activity log entries	Displays the last five FTP/TFTP server entries from the call-home activity log. **Notes:** • The entries are displayed in reverse chronological order (most recent call-home entry first). • The system will wait 5 days before sending duplicate events if they are not acknowledged as corrected in the activity log.	`chlog -f`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display IBM Support call-home activity log entries	Displays the last five IBM Support entries from the call-home activity log. **Notes:** • The entries are displayed in reverse chronological order (most recent call-home entry first). • The system will wait 5 days before sending duplicate events if they are not acknowledged as corrected in the activity log. • Call-home events are usually those that can be resolved without additional problem determination.	`chlog -s`	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 17. chlog (display call-home activity log) command (continued)

Function	What it does	Command	Valid targets
Acknowledge / unacknowledge call-home activity log entries	Marks the selected call-home event as acknowledged (yes) or unacknowledged (no) when the call-home event has been corrected. **Note:** The system will wait five days before sending duplicate events if they are left unacknowledged in the activity log.	`chlog -`*index* `-ack` *option* where: • *index* is the index of the call-home event entry • *option* is `yes` or `no` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

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

```
chlog
```

To mark the call-home event with index number 14 as acknowledged, type

```
chlog -14 -ack yes
```

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

```
system:mm[1]> chlog
Index  Ack  Send Result   Assigned Num  Event ID    Sev  Source
            Time                    Message
14     No   Success        NULL          0x00016802  I    CHASSIS
06/04/08  09:11:11   Test Call Home generated  by USERID.
15     No   Pending       NULL          0x00016802  I    CHASSIS
06/04/08  09:11:12   Test Call Home generated  by USERID.

system:mm[1]>chlog -14 -ack yes
OK
system:mm[1]>
```

chmanual command

This command tests the BladeCenter unit call-home feature setup.

Table 18. chmanual command

Function	What it does	Command	Valid targets

Create call-home problem message	Create a call-home problem message for a management module or blade server.	`chmanual -desc "description"`
		
		where *"description"* is a quote-delimited problem description of 1 to 100 characters in length.
		
		This command can only be run by users who have one or more of the following command authorities:
		• 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
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system`
			`-T system:blade[x]`
			
			where *x* is the blade server bay number.

Table 18. chmanual command (continued)

Function	What it does	Command	Valid targets
Generate call-home test call home	Manually generate a test call-home event that transmits the sample call-home problem message.	`chmanual -test` This command can only be run by users who have one or more of the following command authorities: • 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 See "Commands and user authority" on page 8 for additional information.	`-T system`

Example:

To create a call-home test message, at the `system:>` prompt, type

```
chmanual -desc "This is a test."
```

To manually send a test message, while the system is set as the persistent command environment, at the `system>` prompt, type

```
chmanual -test
```

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

```
system> chmanual -desc "This is a test."
OK
system> chmanual -test
OK
system>
```

cin command

This command can be used to view and configure the chassis internal network for up to 14 supported chassis internal network (CIN) configurations, globally, or for specified entries. You can define a CIN by creating a pool of VLAN (virtual local area network) ID/IP address pairs, each of which is a CIN entry.

Table 19. cin command

Function	What it does	Command	Valid targets
Display CIN configuration table	Displays the configuration table for the chassis internal network. Possible return values are: • Global CIN enabled or disabled status • CIN index – VLAN ID – IP address – index entry enabled or disabled status	`cin`	`-T system`
Set global CIN state	Sets the global state of CIN to enabled or disabled.	`cin -global -en` *state* where *state* is • `on` • `off` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management and chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system`
Clear all CIN configuration entries	Deletes all CIN configuration entries.	`cin all -clear` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management and chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system`

Table 19. cin command (continued)

Function	What it does	Command	Valid targets
Turn all index entries on or off	Turns all CIN index entries on or off.	`cin all -en` *state* where *state* is • `on` • `off` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management and chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
Delete CIN configuration entry	Deletes the specified CIN configuration entry.	`cin -`*entry_index* `-clear` where *entry_index* is a number between 1 and 14 (inclusive). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management and chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
Set CIN configuration entry to enable or disable	Enables or disables a CIN configuration entry. If you enable or disable a non-existent entry, the action is ignored and no error message is returned.	`cin -`*entry_index* `-en` *state* where: • *entry_index* is a number between 1 and 14, and • *state* is – `on` – `off` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management and chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 19. cin command (continued)

Function	What it does	Command	Valid targets
Create a CIN configuration entry	Creates a CIN index entry. If the CIN index is currently empty, both -id and -ip must be specified. **Note:** The VLAN ID must be different from that of the blade server management module.	`cin` *-entry_index* -id *vlan_id* `-ip` *ip_address* where: • *entry_index* is a number between 1 and 14, • *vlan_id* is a VLAN ID number between 3 and 4094 (inclusive), • *ip_address* is a valid IP address. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management and chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
Specify valid IP address for CIN index entry	Specifies the IP address of the CIN index entry. The CIN IP address must be a valid IP address. An error is displayed if the IP address is invalid. **Note:** • If the index is not empty, the IP address can be specified separately. • CIN entries cannot have matching IP addresses unless they are 0.0.0.0. and have different VLAN IDs. • If the CIN IP address is 0.0.0.0, the blade server IP address for CIN which is configured in the blade server operating system cannot be in the same subnet as that of the advanced management module. • The IP address cannot be multi-cast and cannot match the IP address of the management module.	`cin` *-entry_index* `-ip` *ip_address* where: • *entry_index* is a number between 1 and 14 • *ip_address* is a valid IP address. You can overwrite parameters of an existing definition; for example, cin -1 -ip 0.0.0.0 overwrites the current CIN IP address of the first cin entry. If the entry does not exist, an error is returned. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management and chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 19. cin command (continued)

Function	What it does	Command	Valid targets
Specify VLAN ID for CIN entry	Set the VLAN ID for the specified CIN entry. **Note:** • If the index is not empty, the ID can be specified separately. • The VLAN ID must be different from that of the management module.	`cin -`*entry_index* `-id` *vlan_id* where: • *entry_index* is a number between 1 and 14 • *vlan_id* is a number between 3 and 4094 (inclusive). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management and chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Example:

To view chassis internal network information for the management module, while this management module is set at the persistent command environment, at the `system>` prompt, type

```
cin
```

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

```
system> cin
 -global -en off

Index 1
 -id 11
 -ip 11.1.1.1
 -en on

Index 2
 -id 12
 -ip 22.1.1.1
 -en on

Index 3
 not used

Index 4
 not used

Index 5
 not used

Index 6
 not used

Index 7
 not used
```

```
Index 8
 not used

Index 9
 not used

Index 10
 not used

Index 11
 not used

Index 12
 -id 123
 -ip 23.1.1.1
 -en on

Index 13
 not used

Index 14
 not used
system>
```

cinstatus command

This command displays a table listing the VLAN ID, the IP address, the MAC address, and the status of each chassis internal network (CIN) connection.

Table 20. cinstatus command

Function	What it does	Command	Valid targets
Display entries of the CIN status table	Reads entries of the CIN status table, five at a time. Each entry of the table returns: • CIN VLAN ID • CIN IP address • CIN MAC address • CIN status text	`cinstatus`	`-T system`
Display status of first five CIN entries	Displays the first five entries of the CIN status table.	`cinstatus -f`	`-T system`
Display entire CIN status table	Displays all the entries in the CIN status table.	`cinstatus -a`	`-T system`

Note: An asterisk * next to an IP address indicates a learned entry.

Example:

To display five entries of the CIN status table, while the BladeCenter unit is set as the persistent environment, at the `system>` prompt, type

```
cinstatus
```

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

```
system> cinstatus
    Note: * next to IP address indicates a learned entry

    VLAN IP Address        MAC Address        Status
    ---- ----------------  ------------------ --------------------
 1. 4094 0.0.0.1                             Not Operational
 2. 4094 0.0.0.2                             Not Operational
 3. 4    0.0.0.0                             Operational
 4. 4093 0.0.0.1                             Not Operational
 5. 4094 0.0.0.0                             Operational

 Last entry reached
system>
```

clear command

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

The command must always include the `-cnfg` or `-config` option.

Table 21. clear command

Function	What it does	Command	Valid targets
Restore default configuration of primary management module and keep logs	Restores the default configuration of the primary management module, retaining log information; then, resets the management module. No results are returned from this command because it resets the management module. When you restore the management-module configuration, the Ethernet configuration method is set to a value of dthens. After the management module resets, this causes the management module to try dhcp configuration and then default to the static IP configuration, which might cause the management module to remain offline for longer than normal. See the "ifconfig command" on page 171 for information.	`clear -cnfg` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration and chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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 -cnfg` This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration and I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.

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

```
clear -cnfg
```

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

clearlog command

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

Table 22. 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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis log management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Clear advanced management-module audit or system event log	Clears the management-module audit event log, the system event log, or both, and displays a message confirming that the specified event log was cleared. **Notes:** • Audit log events are created by the actions of users. • If the *log_type* is not specified, this command will clear both logs. • Although system events and audit events are stored internally in separate log files, they are presented to the user as a single log that can be filtered.	`clearlog -l` *log_type* where *log_type* is `audit` or `system`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis log management See "Commands and user authority" on page 8 for additional information.	`-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 -l audit
```

The following example shows the information that is returned:

```
system:mm[1]> clearlog -l audit
OK
system:mm[1]>
```

clock command

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

Table 23. clock command

Function	What it does	Command	Valid targets
Display advanced management module clock information	Displays the following information for the advanced 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 advanced management module date	Sets the date for the advanced 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. This command can only be run by users who have the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set advanced management module time	Sets the time for the advanced 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 23. clock command (continued)

Function	What it does	Command	Valid targets
Set advanced management module clock GMT offset	Sets the time for the advanced 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 23. clock command (continued)

Function	What it does	Command	Valid targets
Set advanced 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. This command can only be run by users who have the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	

Table 23. clock command (continued)

Function	What it does	Command	Valid targets
Set advanced management module clock daylight-savings time mode	Sets the daylight-savings time mode for the advanced 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-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 advanced management module or blade server and the location and contact name for the advanced management module.

Table 24. 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 advanced management module names can only contain alphanumeric characters, hyphens, pound signs, underscores, and periods.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for management module)
		• Blade configuration (for blade server)
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system:mm[x]`
			`-T system:blade[x]`
			
			where *x* is the primary management-module or a blade server bay number.

Table 24. config command (continued)

Function	What it does	Command	Valid targets
Set location of management module	Sets the location of the primary advanced management module.	`config -loc "location"` where *"location"* is up to 47 characters in length and contained within double-quotes. Advanced management module locations can contain any character other than "<" and ">". This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set contact name for advanced management module	Sets the contact name for the primary advanced management module.	`config -contact "contact_name"` where *"contact_name"* is up to 47 characters in length and contained within double-quotes. Advanced management module contact names can contain any character other than "<" and ">". This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 24. config command (continued)

Function	What it does	Command	Valid targets
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 Systems 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 Systems 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 advanced management module.	`config -uuid "unique_id"` where *"unique_id"* is 32 hexadecimal digits and is contained within double-quotes. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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 Systems 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 advanced management module.	`config -tm "type_model"` where *"type_model"* is up to seven characters in length and contained within double-quotes. Advanced management module type / model designators can contain any character other than "<" and ">". This command can only be run by users who have the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 24. 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 Systems 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 advanced management module.	`config -sn "serial_number"` where *"serial_number"* is up to seven characters in length and contained within double-quotes. Advanced management module serial numbers can contain any character other than "<" and ">". This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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 25. console command

Function	What it does	Command	Valid targets
Create SOL session with blade server	Creates an SOL connection to the specified blade server. **Note:** The advanced management module supports a persistent SOL connection that remains intact until you escape from the SOL console, or another user uses the override option to take over your SOL console. A persistent command, if dropped, automatically attempts to reconnect.	`console` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-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. **Note:** The advanced management module supports combing this is option with the -l option to override an existing session, and not reconnect if the connection drops.	`console -o` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade server bay number.
Create non-persistent SOL session with blade server	Creates an SOL connection to the specified blade server for users who do not want to use a persistent session. **Note:** This option can be combined with the -o option to override an existing session, and not reconnect if the connection drops.	`console -l` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-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 by a DHCP server to the primary management module external network interface, blade server management network interfaces, and I/O module DHCPv6 server.

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

Table 26. dhcpinfo command

Function	What it does	Command	Valid targets
Display Ethernet channel 0 DHCP configuration for management module	If the IP configuration for management module 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* • -server6 *IPv6_dhcp_ip_address* • -i6 *IPv6_address* • -d6 *IPv6_domainname* • -dns61 *IPv6_primary_dns_ip_address* • -dns62 *IPv6_secondary_dns_ip_address* • -dns63 *IPv6_tertiary_dns_ip_1address*	`dhcpinfo -eth0`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display management network DHCP configuration for blade server	If the IPv6 configuration for the specified blade server management network Ethernet channel is assigned by a DHCP server, the IPv6 IP address is displayed. If the IP configuration for the specified blade server management network Ethernet channel is *not* assigned by a DHCP server, an error message is displayed.	`dhcpinfo -ethx` where *x* is the blade server management network channel number to display.	`-T system:blade[x]` where *x* is the blade server bay number.
Display DHCP configuration for I/O module	If the IPv6 configuration for the specified I/O module is assigned by a DHCP server, the IPv6 IP address is displayed. If the IPv6 configuration for the I/O module is *not* assigned by a DHCP server, an error message is displayed.	`dhcpinfo`	`-T system:switch[x]` where *x* is the I/O-module bay number.

Example: To display the DHCP server assigned network settings that do not support IPv6 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]>
```

To display the DHCP server assigned network settings that support IPv6 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
DHCP is disabled
-server6 FE80:0000:0000:0000:0202:55FF:FE21:0F23
-i6 2000:1013:0000:0000:DDDD:CCCC:D7C8:F925
-d6 datacentertech.net
-dns61 2000:1013:0000:0000:0000:0000:0100:0100
-dns62 2000:1013:0000:0000:0000:0000:0100:0101
-dns63 2000:1013:0000:0000:0000:0000:0100:0102
system:mm[1]>
```

displaylog command

This command displays management-module event log entries.

Note: Event descriptions and suggested user actions for items shown by the displaylog command can be viewed using the "eventinfo command" on page 138.

Table 27. 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.
Display log entries with Event ID	Displays log entries with Event ID.	`displaylog -e`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display log entries with their call-home flag	Displays log entries with their call-home flag.	`displaylog -c`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display all management-module event log entries	Displays all entries in the management module event log.	`displaylog -a`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display all event log filters	Displays all filters that can be used to control management module event log output.	`displaylog -filters`	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 27. displaylog (display management-module event log) command (continued)

Function	What it does	Command	Valid targets
Display event log entries filtered by date	Displays management module event log information that meets the specified date filter criteria. **Note:** • This command displays the first five most recent entries in the management-module event log that meet the specified filter criteria. Adding the -a option to the command displays all entries that meet the specified filter criteria. • If the filter criteria entered does not match the criteria previously specified, this resets the counter and displays the first five most recent log entries that match the specified filter criteria. • The index number displayed for each filtered log entry might not match the index number shown for the same log entry displayed in an unfiltered list.	`displaylog -date` *date_filter* where *date_filter* is a pipe (`|`) separated list of date filters in mm/dd/yy format.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display event log entries filtered by severity level	Displays management module event log information that meets the specified severity level filter criteria. **Note:** • This command displays the first five most recent entries in the management-module event log that meet the specified filter criteria. Adding the -a option to the command displays all entries that meet the specified filter criteria. • If the filter criteria entered does not match the criteria previously specified, this resets the counter and displays the first five most recent log entries that match the specified filter criteria. • The index number displayed for each filtered log entry might not match the index number shown for the same log entry displayed in an unfiltered list.	`displaylog -sev` *severity_filter* where *severity_filter* is a pipe (`|`) separated list of severity filters: • `I` (information) • `E` (error) • `W` (warning)	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display event log entries filtered by source	Displays management module log information that stored in the audit log.	`displaylog -src Audit`	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 27. displaylog (display management-module event log) command (continued)

Function	What it does	Command	Valid targets
Display event log entries filtered by every flag except the one specified	Displays management module log information that is stored in logs other than the specified log. **Note:** • This command displays the first five most recent entries in the management-module event log that meet the specified filter criteria. Adding the -a option to the command displays all entries that meet the specified filter criteria. • If the filter criteria entered does not match the criteria previously specified, this resets the counter and displays the first five most recent log entries that match the specified filter criteria. • The index number displayed for each filtered log entry might not match the index number shown for the same log entry displayed in an unfiltered list.	`displaylog -src !`*filter_out* where *filter_out* is the category of event log entries that is not to be displayed. Use the `displaylog -filters` command to discover excludable event log categories.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display audit log entries filtered by source	Displays management module audit log information that meets the specified source filter criteria. **Note:** • This command displays the first five most recent entries in the management-module event log that meet the specified filter criteria. Adding the -a option to the command displays all entries that meet the specified filter criteria. • If the filter criteria entered does not match the criteria previously specified, this resets the counter and displays the first five most recent log entries that match the specified filter criteria. • The index number displayed for each filtered log entry might not match the index number shown for the same log entry displayed in an unfiltered list.	`displaylog -src` *source_filter* where *source_filter* is a pipe (`|`) separated list of source filters. To specify a range of blade servers as the source, use a hyphen (`-`), as follows: `Blade_01-08`.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 27. displaylog (display management-module event log) command (continued)

Function	What it does	Command	Valid targets
Display log entries filtered by call-home flag	Displays log entries that meet the specified call-home events filter criteria. **Note:** • This command displays the five most recent entries in the management-module event log that meet the specified filter criteria. Adding the -a option to the command displays all entries that meet the specified filter criteria. • If the filter criteria entered does not match the criteria previously specified, this resets the counter and displays the first five most recent log entries that match the specified filter criteria. • The index number displayed for each filtered log entry might not match the index number shown for the same log entry displayed in an unfiltered list.	`displaylog -ch` *option* where *option* are: • `C` (call home) • `N` (no call home)	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display the state of the log state event option	Displays the state (enabled or disabled) of the log state event option, which generates an event when the event log becomes 75% or 100% full.	`displaylog -lse`	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable monitoring of event log state	Enables or disables the monitoring of the event log state to generate an event when the log becomes 75% or 100% full. **Note:** The displaylog -lse command must be run exclusive of other log-reading command options (-f, -a, -filters, -date, -sev, - src, -i, and -l).	`displaylog -lse` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis log management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Save event log to TFTP server	Saves the event log with the specified filename to the specified TFTP server. **Note:** The -i and -l command options must be run together and exclusive of other command options.	`displaylog -i` *ip_address* `-l` *filename* where: • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the event log is being saved. • *filename* is the name of the event log file.	`-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>
```

displaysd command

This command captures and displays service information.

Service information for the management modules includes BladeCenter VPD, the management-module event log, connection status, and self-test results. If multiple user interface sessions issue the displaysd command, the commands will be processed in the order that they are received. Some types of service information are displayed for only the primary management module.

Table 28. displaysd command

Function	What it does	Command	Valid targets
Capture and display service information	Capture and display service information on page from the primary or standby management module.	`displaysd`	`-T system:mm[x]` where *x* is the primary or standby management-module bay number.
Display management module connection and self-test status	Displays connection status and latest self-test results for the primary management module.	`displaysd -mmstat`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Save service information to TFTP server	Saves service information from primary management module with the specified filename to the specified TFTP server. **Note:** The -save and -i command options must be run together.	`displaysd -save` *filename* `-i` *ipaddress* where: • *filename* is the location where service information will be saved. The filename should use a .tgz extension to allow support personnel to identify the file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display all blade server SRC records	Displays a list of the most recent (up to 32) SRCs for the specified blade server. **Note:** SRC information is available for only those blade servers that support this feature.	`displaysd -src list`	`-T system:blade[x]` where *x* is the blade serverbay number.
Display specific blade server SRC record	Displays a specific SRC, based on the specified record number, for the specified blade server. **Note:** SRC information is available for only those blade servers that support this feature.	`displaysd -src` *index* where *index* is the SRC record number to display, between 1 and 32.	`-T system:blade[x]` where *x* is the blade serverbay number.

Example: To capture and display service information from the management module in bay 1, while the chassis is set as the persistent command environment, at the system> prompt, type

```
displaysd -T system:mm[1]
```

To capture service information from the management module in bay 1 and save it to a file named sdc.tgz on a TFTP server with a IP address of 9.67.22.176, while the chassis is set as the persistent command environment, at the system> prompt, type

```
displaysd -T system:mm[1] -save sdc.tgz -i 9.67.22.176
```

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

```
system> displaysd -T system:mm[1]
SPAPP Capture Available
Time: 10/04/2005 21:47:43
UUID: Not Available
•
•
•
system> displaysd -T system:mm[1] -save sdc.tgz -i 9.67.22.176
OK
system>
```

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

dns command

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

Table 29. 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 *IPv4_first_ip_address* • -i2 *IPv4_second_ip_address* • -i3 *IPv4_third_ip_address* • -i61 *IPv6_first_ip_address* • -i62 *IPv6_second_ip_address* • -i63 *IPv6_third_ip_address* • -ddns *dynamic_DNS_state* (enabled/disabled) • -p *DNS_server_priority* (ipv4/ipv6)	`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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Dynamic DNS - enable / disable	Enables or disables dynamic DNS for the management module.	`dns -ddns state` where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 29. dns command (continued)

Function	What it does	Command	Valid targets
DNS first IPv4 IP address - set	Sets the first IPv4 IP address.	`dns -i1` *ip_address* where *ip_address* is the first IP address in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
DNS second IPv4 IP address - set	Sets the second IPv4 IP address.	`dns -i2` *ip_address* where *ip_address* is the second IP address in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
DNS third IPv4 IP address - set	Sets the third IPv4 IP address.	`dns -i3` *ip_address* where *ip_address* is the third IP address in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 29. dns command (continued)

Function	What it does	Command	Valid targets
DNS first IPv6 IP address - set	Sets the first IPv6 IP address.	`dns -i61` *ip_address* where *ip_address* is the first IP address in IPv6 format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
DNS second IPv6 IP address - set	Sets the second IPv6 IP address.	`dns -i62` *ip_address* where *ip_address* is the second IP address in IPv6 format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
DNS third IPv6 IP address - set	Sets the third IPv6 IP address.	`dns -i63` *ip_address* where *ip_address* is the third IP address in IPv6 format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 29. dns command (continued)

Function	What it does	Command	Valid targets
DNS server priority - set	Sets the DNS server priority for the management module to IPv4 or IPv6..	`dns -p` *priority* where *priority* is `ipv4` or `ipv6`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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 that does not have IPv6 support, 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]>
```

To display the DNS status of a primary management module that supports IPv6, 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 this command:

```
system:mm[1]> dns
Enabled
Enabled
-i1 192.168.70.230
-i2 0.0.0.0
-i3 0.0.0.0
-i61 2002:1013::211:25ff:fec3:227d
-i62 ::
-i63 ::
-ddns disabled
-p ipv4
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 6 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 30. 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*]:exp[*y*]
Blade server management card	system:blade[*x*]:mgmtcrd
Blade server microprocessor	system:blade[*x*]:cpu[*y*]
Blade server storage expansion unit	system:blade[*x*]:be[*y*]
Blade server high-speed expansion card	system:blade[*x*]:hsec[*y*]
Blade server memory	system:blade[*x*]:memory[*y*]
Blade server mezzanine for double-width form factor	system:blade[*x*]:sb
Blade server concurrent KVM feature card	system:blade[*x*]:ckvm
I/O (switch) module	system:switch[*x*]
Power module	system:power[*x*]
Blower	system:blower[*x*]
Media tray	system:mt[*x*]
Media tray battery backup unit	system:mt[*x*]:bbu[*y*]
Alarm panel (BladeCenter HT only)	system:tap
Multiplexer expansion module (BladeCenter HT only)	system:mux[*x*]
Network clock module (BladeCenter HT only)	system:ncc[*x*]
Storage module (BladeCenter S unit only)	system:storage[*x*]
Storage module disk drive (BladeCenter S unit only)	system:storage[*x*]:disk[*y*]

Table 31. env (environment) command

Function	What it does	Command	Valid targets

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

Set management module as command target	Sets the management module as the persistent target for commands during the current session.	`env -T system:mm[x]` where *x* is the bay (1 or 2) that identifies the management module.	The env command can be directed to any installed device, in this case `-T system:mm[x]` where *x* is the management-module bay number.
Set blade server as command target	Sets the specified blade server as the persistent target for commands during the current session.	`env -T system:blade[x]` where *x* is the blade bay that identifies the blade server. A blade server that occupies more than one blade bay is identified by the lowest bay number that it occupies.	The env command can be directed to any installed device, in this case `-T system:blade[x]` where *x* is the blade bay that identifies the blade server.

Table 31. env (environment) command (continued)

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

Table 31. 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[x]` where *x* is the media-tray bay where the media tray is installed.	The env command can be directed to any installed device, in this case `-T system:mt[x]` where *x* is the media-tray bay where the media tray is installed.
Set media tray battery backup unit as command target	Sets the specified battery backup unit on the specified media tray as the persistent target for commands during the current session.	`env -T system:mt[x]:bbu[y]` where *x* is the media tray on which the battery backup unit is installed. where *y* is the battery backup unit number:	The env command can be directed to any installed device, in this case `-T system:mt[x]:bbu[y]` where *x* is the media tray on which the battery backup unit is installed. where *y* is the battery backup unit number:

Table 31. env (environment) command (continued)

Function	What it does	Command	Valid targets
Set alarm panel as command target (BladeCenter HT units only)	Sets the alarm panel as the persistent target for commands during the current session.	`env -T system:tap`	The env command can be directed to any installed device, in this case `-T system:tap`
Set multiplexer expansion module as command target (BladeCenter HT units only)	Sets the multiplexer expansion module as the persistent target for commands during the current session.	`env -T system:mux[`*x*`]` where *x* is the multiplexer expansion module number.	The env command can be directed to any installed device, in this case `-T system:mux[`*x*`]` where *x* is the multiplexer expansion module number.
Set network clock module as command target (BladeCenter HT units only)	Sets the network clock module as the persistent target for commands during the current session.	`env -T system:ncc[`*x*`]` where *x* is the network clock module number.	The env command can be directed to any installed device, in this case `-T system:ncc[`*x*`]` where *x* is the network clock module number.
Set storage module as command target (BladeCenter S units only)	Sets the storage module as the persistent target for commands during the current session.	`env -T system:storage[`*x*`]` where *x* is the storage-module bay where the storage module is installed.	The env command can be directed to any installed device, in this case `-T system:storage[`*x*`]` where *x* is the storage-module bay where the storage module is installed.
Set storage module disk drive as command target (BladeCenter S units only)	Sets the specified disk drive in the specified storage module as the persistent target for commands during the current session.	`env -T system:storage[`*x*`]:disk[`*y*`]` where *x* is the storage module on which the disk drive is installed. where *y* is the disk drive number:	The env command can be directed to any installed device, in this case `-T system:storage[`*x*`]:disk[`*y*`]` where *x* is the storage module on which the disk drive is installed. where *y* is the disk drive number:

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]
```

ethoverusb command

This command sets and displays the setting for the Ethernet-over-USB command interface of a blade server service processor, for blade servers that support this feature.

Table 32. ethoverusb command

Function	What it does	Command	Valid targets
Display blade server Ethernet-over-USB setting	Displays the Ethernet-over-USB command interface setting for the service processor of the specified blade server. **Note:** This command will execute only on blade servers that support an Ethernet-over-USB command interface for the service processor.	`ethoverusb`	`-T system:blade[x]` where *x* is the blade server bay number.
Set blade server Ethernet-over-USB setting	Enables or disables the Ethernet-over-USB command interface setting for the service processor of the specified blade server. **Note:** This command will execute only on blade servers that support an Ethernet-over-USB command interface for the service processor.	`ethoverusb -s` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade server bay number.

Example: To view the Ethernet-over-USB command interface setting for the service processor of the blade server in bay 2, while this blade server is set as the persistent command environment, at the `system:blade[2]>` prompt, type

```
ethoverusb
```

To disable the Ethernet-over-USB command interface setting for the service processor of the blade server in bay 2, while this blade server is set as the persistent command environment, at the `system:blade[2]>` prompt, type

```
ethoverusb -s disabled
```

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

```
system:blade[2]> ethoverusb
enabled
system:blade[2]> ethoverusb -s disabled
OK
system:blade[2]> ethoverusb
disabled
system:blade[2]>
```

eventinfo command

This command displays advanced management module event information and suggested user actions. See the *BladeCenter Advanced Management Module Messages Guide* for a complete list of all non-device specific events and recommended actions, sorted by event ID. Device specific event information is in the documentation for the device.

Table 33. eventinfo command

Function	What it does	Command	Valid targets
Display event description and user action	Displays the event description and suggested user action for the specified event ID.	`eventinfo -`*id* where *id* is the event ID displayed from the "displaylog command" on page 119. Event IDs are of the form 0x*nnnnnnnn*, where *nnnnnnnn* is a hexadecimal number that identifies the specific event (the 0x prefix is not entered). Leading zeros need not be entered when using the `eventinfo` command: in this example, specifying an event ID of 00104204, or 104204 would return the same result.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display event description	Displays the event description for the specified event ID.	`eventinfo -`*id* `-d` where *id* is the event ID displayed from the "displaylog command" on page 119. Event IDs are of the form 0x*nnnnnnnn*, where *nnnnnnnn* is a hexadecimal number that identifies the specific event (the 0x prefix is not entered). Leading zeros need not be entered when using the `eventinfo` command: in this example, specifying an event ID of 00104204, or 104204 would return the same result.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 33. eventinfo command (continued)

Function	What it does	Command	Valid targets
Display event user action	Displays the suggested user action for the specified event ID.	`eventinfo -id -u` where *id* is the event ID displayed from the "displaylog command" on page 119. Event IDs are of the form 0x*nnnnnnnn*, where *nnnnnnnn* is a hexadecimal number that identifies the specific event (the 0x prefix is not entered). Leading zeros need not be entered when using the `eventinfo` command: in this example, specifying an event ID of 00104204, or 104204 would return the same result.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example: To view the event description and suggested user action for an event with an ID of 0x00104204, while the BladeCenter unit is set as the persistent command environment, at the `system:>` prompt, type

```
eventinfo -T mm[1] -00104204
```

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

```
system> eventinfo -T mm[1] -00104204
Event Description:
The primary advanced management module was reset.
Recommended Action:
Information only; no action is required.
system>
```

events command

This command manages the Call Home events exclusion list for the advanced management module.

Table 34. events command

Function	What it does	Command	Valid targets
Display Call Home events list and free space	Displays a list of Call Home event IDs that will not be reported by the Call Home feature, and how many more events can be added to this Call Home events exclusion list. This Call Home exclusion list allows a maximum of 20 events.	`events -che` This command can only be run by users who have one or more of the following command authorities: • 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 See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Add a Call Home event to the Call Home Exclusion list	Adds a Call Home event to the Call Home exclusion list. Events on this list are specified by an event ID, and are not included in the Call Home reports. **Note:** The Service Advisor terms and conditions must first be accepted, or the Automated FTP/TFTP Report of Service Data must be enabled before using this command.	`events -che -add` *event_ID* where *event_ID* is an eight-digit hexadecimal number with an optional prefix of 0x or 0X. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 34. events command (continued)

Function	What it does	Command	Valid targets
Remove a Call Home event from the Call Home Exclusion list	Removes a Call Home event from the Call Home exclusion list. Events removed from this list are included in the Call Home reports. **Note:** The Service Advisor terms and conditions must first be accepted, or the Automated FTP/TFTP Report of Service Data must be enabled before using this command.	`events -che -rm` *event_ID* where *event_ID* is • an eight-digit hexadecimal number with an optional prefix of 0x or 0X to remove a single Call Home event • `all` to remove all the Call Home events from the exclusion list This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example: To view the Call Home exclusion list and the number of remaining events can be added to the list, while the BladeCenter unit is set as the persistent command environment, at the `system:>` prompt, type

```
events -T mm[1] -che
```

To add Call Home event number 0x00020003 to the Call Home exclusion list, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
events -T mm[1] -che -add 0x00020003
```

To remove Call Home event number 0x00020001 from the Call Home exclusion list, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
events -T mm[1] -che -rm 0x00020001
```

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

```
system> events -T mm[1] -che
A maximum of 20 events can be added to this exclusion list, currently
18 more events can be added.
Call Home Exclusion List is illustrated as follows:
Index        Event ID
 1           0x00020001
 2           0x00020002
system> events -T mm[1] -che -add 0x00020003
OK
system> events -T mm[1] -che
A maximum of 20 events can be added to this exclusion list, currently
17 more events can be added.
Call Home Exclusion List is illustrated as follows:
Index        Event ID
 1           0x00020001
 2           0x00020002
```

```
 3           0x00020003
system> events -T mm[1] -che -rm 0x00020001
OK
system> events -T mm[1] -che
A maximum of 20 events can be added to this exclusion list, currently
18 more events can be added.
Call Home Exclusion List is illustrated as follows:
Index        Event ID
 1           0x00020002
 2           0x00020003
system>
```

exit command

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

Table 35. 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
```

feature command

This command manages licensing for advanced features for the advanced management module.

Table 36. feature command

Function	What it does	Command	Valid targets
Display feature list and license status	Displays a list of advanced features for the management module and their licensing status.	`feature`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Add a feature license	Adds a license for a management module advanced feature. Features on this list are specified using the feature index number that appears at the left of the feature list.	`feature -index -add -key lisc_key` where: • *index* is the number for the feature at the left of the feature list displayed by the `feature` command. • *lisc_key* is the 7-character part number of the feature. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Remove a feature license	Removes a license for a management module advanced feature. Features on this list are specified using the feature index number that appears at the left of the feature list.	`feature -index -remove` where *index* is the number for the feature at the left of the feature list displayed by the `feature` command. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 36. feature command (continued)

Function	What it does	Command	Valid targets
Import datacenter feature licenses	Import a datacenter feature licensing file for use by the BladeCenter unit. The file name to import must specify a qualified location for the licensing file that indicates the protocol to be used. For example, tftp://192.168.0.1/license.csv	`feature -apply` *file_location* where *file_location* is a qualified location for the license file of up to 256 characters in length that indicates the protocol to be used (tftp, ftp, ftps, http, or https) and contains any character except the percent sign (%) or double-quote (⌂). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Export datacenter feature licenses	Export a BladeCenter feature licensing file for use by other BladeCenter units in the datacenter. The file name to export must specify a qualified location for the licensing file that indicates the protocol to be used. For example, tftp://192.168.0.1/license.csv **Note:** While the licensing file is exporting, a string of periods will display on the screen to indicate progress; a new period being added every three seconds.	`feature -retrieve` *file_location* where *file_location* is a qualified location for the license file of up to 256 characters in length that indicates the protocol to be used (tftp, ftp, ftps, http, or https) and contains any character except the percent sign (%) or double-quote (⌂). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example: To view the feature list, while the BladeCenter unit is set as the persistent command environment, at the `system:>` prompt, type

```
feature -T mm[1]
```

To remove the license for the first feature in the list, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
feature -T mm[1] -1 -remove
```

To export a licensing file to the location tftp://10.11.20.23/IBMtest.csv, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
feature -retrieve -T mm[1] tftp://10.11.20.23/IBMtest.csv
```

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

```
system> feature -T mm[1]
1. IBM BladeCenter Open Fabric Manager
-serial 2304369
License Status: Active
system> feature -T mm[1] -1 -remove
OK
system> feature -T mm[1]
1. IBM BladeCenter Open Fabric Manager
License Status: No License
system> feature -retrieve -T mm[1] tftp://10.11.20.23/IBMtest.csv
.................
OK
system>
```

files command

This command manages files uploaded to the advanced management module.

Table 37. files command

Function	What it does	Command	Valid targets
Display file list and free space	Displays a list of files and space remaining in the advanced management module file system.	`files`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Delete file	Deletes a file from the advanced management module file system. **Note:** This command can only be used to delete files: it will not delete directories.	`files -d filename` where *filename* is a valid, existing filename of less than 256 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration • Chassis configuration • Blade administration • Blade configuration • I/O module administration • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example: To view the files and remaining space in the management module file system, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
files
```

To delete the file `tftproot/tftp_file.pkt` from the management module file system, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
files -d tftproot/tftp_file.pkt
```

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

```
system:mm[1]> files
     12288 Thu Jan 05 13:28:23 2006 lost+found/
      1024 Thu Jul 06 19:32:51 2006 tftproot/
      1024 Thu Jul 06 19:34:15 2006 tftproot/manu/
      1024 Thu Jul 06 19:34:15 2006 tftproot/manu/manu2/
         0 Sat Aug 19 09:22:02 2006 tftproot/tftp_file.pkt
         0 Sun Oct 01 07:57:19 2006 tftproot/.Do_not_delete_this_directory
         0 Tue Dec 15 11:07:19 2009 test
         0 Thu Apr 13 23:45:40 2006 bob.pkt
      1024 Tue Feb 02 15:29:17 2010 pubkeys/
       426 Tue Feb 02 15:29:17 2010 pubkeys/ssh_key.pub
      5652 Fri May 12 00:56:36 2006 asm.cfg
Total space:   73108480 bytes
Used:             24576 bytes
Available:     73083904 bytes
system:mm[1]> files -d tftproot/tftp_file.pkt
OK
system:mm[1]>
```

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 power redundancy loss and limiting fan noise during thermal events.

Note: For scripting purposes, the -qm and -os fuelg options for management modules other than the advanced management module are supported by the advanced management module.

Table 38. fuelg command

Function	What it does	Command	Valid targets
Display power domain status overview	Displays health status, total power usage, total dc power available, total ac power in use, thermal response (acoustic mode) settings, total thermal output in BTU/hour, and the polling intervals used for trending for all power domains. **Note:** For the BladeCenter S unit, output will indicate whether the chassis is running in 220 V ac or 110 V ac mode.	`fuelg`	`-T system`
Display blade server power status overview	Displays the power management and capping setting (on/off) and power management capability for the specified blade server. Depending on the power management capability of the specified blade server, the following information will also display: • CPU duty cycles • Effective and maximum CPU speeds • Power capping value (minimum and maximum) • Maximum, minimum, and average power levels • Time when above data was captured • Power saver mode status (on, off)	`fuelg`	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Display I/O module power status	Displays the maximum, minimum, and average power information for the specified I/O module.	`fuelg`	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.
Display blower power status and temperature	Displays the maximum power, minimum power, average power, and current temperature information for the specified blower module.	`fuelg`	`-T system:blower[`*x*`]` where *x* is the blower bay number.
Display media tray temperature	Displays the current temperature for the specified media tray.	`fuelg`	`-T system:mt[`*x*`]` where *x* is the media tray number.

Table 38. fuelg command (continued)

Function	What it does	Command	Valid targets
Display detailed power domain status	Displays detailed status and usage information for the specified power domains, including the policy setting for that domain, the maximum power limit, and the power in use. The valid states for components in the domain are: • * - blade server might throttle • C - communication error • D - discovering • Hib - hibernate • NP - module is not present • SB - standby • T - throttled • U - unable to power up **Note:** For the BladeCenter S, output will indicate whether the chassis is running in 220 V ac or 110 V ac mode.	`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. **Note:** The BladeCenter S unit has only one power domain. Use either `pd` or `pd1` to specify the power domain for the BladeCenter S unit.	`-T system`

Table 38. fuelg command (continued)

Function	What it does	Command	Valid targets
Set power domain redundancy loss policy	Sets how the BladeCenter unit responds to a condition that could cause a loss of redundant pow **Note:** For the BladeCenter S, output will indicate whether the chassis is running in 220 V or 110 V ac mode.er.	`fuelg` *domain* `-pm` *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: – `nonred` (default) allows loss of redundancy. – `redwoperf` prevents components from turning on that will cause loss of power redundancy. – `redwperf` power throttles components to maintain power redundancy and prevents components from turning on that will cause loss of power redundancy. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
Display power trending for specified time period and power domain	Displays power trending information for the selected time interval and selected power domain for the BladeCenter unit.	`fuelg` *domain* `-pt` *period* where: • *domain* is: – `pd1` for power domain 1. – `pd2` for power domain 2. – If no *domain* is specified, the *period* is applied to all power domains. • *period* is 1, 6, 12, or 24 hours.	`-T system`

Table 38. fuelg command (continued)

Function	What it does	Command	Valid targets

Display power trending for specified time period	Displays power trending information for the selected time interval for the specified command target.	`fuelg -pt` *period*
		
		where *period* is 1, 6, 12, or 24 hours.
			`-T system`
			`-T system:blade[`*x*`]`
			`-T system:switch[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the blade server, I/O module, or blower bay number.

Set power polling interval	Sets the amount of time between thermal and power samples that are taken to build trending data.	`fuelg -int` *interval* where *interval* is between 10 and 60 minutes, inclusive, in 5-minute increments. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Display thermal trending for specified time period	Displays thermal trending information for the selected time interval for the specified command target.	`fuelg -tt` *period*
		
		where *period* is 1, 6, 12, or 24 hours.
			`-T system:mt[`*x*`]`
			`-T system:blower[`*x*`]`
			
			where *x* is the blade server or blower bay number.

Table 38. fuelg command (continued)

Function	What it does	Command	Valid targets
Thermal event response (acoustic mode)	Sets the acoustic mode of BladeCenter-unit blowers response to thermal events.	`fuelg -am` *setting* where the acoustic-mode *setting* of: • `off` (default) allows blowers to increase speed to provide additional cooling. • `on` keeps blowers at a fixed speed and power throttles BladeCenter components to reduce power consumption (only for BladeCenter components that support power throttling). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
Thermal event response (Telco environment)	Sets the Telco environment of the BladeCenter-unit blowers response to thermal events. **Note:** When the environment mode is set to nebs, the -am mode is automatically turned off.	`fuelg -e` *environment* where the thermal-event response *environment* of: • `nebs` allows blowers to increase speed to provide additional cooling. • `enterprise` allows acoustic mode. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 38. fuelg command (continued)

Function	What it does	Command	Valid targets
Set power capping value for blade server	Sets the power capping value for a specified blade server that support this feature. **Note:** A blade server must be turned on before you can set its power capping value.	`fuelg -pcap` *setting* where the power capping *setting* is a numeric value that falls within the range of power capping values displayed when running the `fuelg -T blade[x]` command on a blade server. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade-server bay number.
Power management and capping - enable or disable for blade server	Turns power management and capping for the specified blade server on or off. **Note:** A blade server must be turned on before you can enable power management and capping for it.	`fuelg -pme` *setting* where a *setting* of: • `off` (default) disables power management and capping for the blade server. • `on` enables power management and capping for the blade server. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade-server bay number.

Table 38. fuelg command (continued)

Function	What it does	Command	Valid targets
Static low power saver mode - enable or disable for blade server	Turns the static low power saver mode for the specified blade server on or off. **Notes:** • A blade server must be turned on before you can enable power saver mode for it. • Not all blade servers support the power saver mode.	`fuelg -ps` *setting* where a *setting* of: • `off` (default) disables power saver mode for the blade server. • `on` enables power saver mode for the blade server. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Dynamic power optimizer - enable or disable for blade server	Turns dynamic power optimizer for the specified blade server on or off. **Notes:** • A blade server must be turned on before you can enable dynamic power optimizer for it. • Not all blade servers support the dynamic power optimizer.	`fuelg -dps` *setting* where a *setting* of: • `off` (default) disables dynamic power optimizer for the blade server. • `on` enables dynamic power optimizer for the blade server. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.

Table 38. fuelg command (continued)

Function	What it does	Command	Valid targets
Favor performance over power - enable or disable for blade server	Turns the favor performance over power feature on or off for the specified blade server. **Notes:** • A blade server must be turned on before you can enable the favor performance over power feature for it. • Not all blade servers support the favor performance over power feature. • This feature can only be active if the dynamic power optimizer is enabled.	`fuelg -fpop` *setting* where a *setting* of: • `off` (default) disables favor performance over power for the blade server. • `on` enables favor performance over power for the blade server. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.

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 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
```

To view BladeCenter unit power trending information for the past 6 hours, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
fuelg -pt 6
```

To view the power status for the blade server in blade bay 1, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
fuelg -T blade[1]
```

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

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

Total DC Power Available:  8000
Total AC Power In Use:     1603 (+/- 16.0%)
Total Thermal Output:      5469 BTU/hour

Power Domain 1
--------------
Status: This power domain has mismatched power modules.
        Replace the power module.
Modules:
 Bay 1:   2880
```

```
 Bay 2:   3160
Power Management Policy: Basic Power Management
Power in Use:           1313 (+/- 16.0%)
Total Power:            4000
Allocated Power (Max):  1423
Remaining Power:        2577

Power Domain 2
--------------
Status: Power domain status is good.
Modules:
 Bay 3:   2880
 Bay 4:   2880
Power Management Policy: Basic Power Management
Power in Use:             73 (+/- 16.0%)
Total Power:            4000
Allocated Power (Max):  1082
Remaining Power:        2918

-am  on
-e enterprise
-int 10
```

```
system> fuelg pd1
Maximum Power Limit:  1450
Power In Use:          856

                                      Power  -- Allocated Power --
Bay(s)  Module                        State  Current   Max    Min
======  ============================  =====  =======  =====  =====
Chassis Components
        Midplane                       On         10     10     10
     1  Media Tray 1                   On         10     10     10
Chassis Cooling Devices
     1  Chassis Cooling Device 1       On         11     68     68
     2  Chassis Cooling Device 2       On         11     68     68
     3  Chassis Cooling Device 3       On         11     68     68
     4  Chassis Cooling Device 4       On         11     68     68
Power Module Cooling Devices
     1  PM Cooling Device 1            On         10     10     10
     2  PM Cooling Device 2            On         10     10     10
     3  PM Cooling Device 3            On         10     10     10
     4  PM Cooling Device 4 (NP)                   0     10     10
Storage
     1  Storage Module 1 (NP)                      0    120    120
     2  Storage Module 2               On          0    100    100
Management Module
     1  SN#YK168082H25F                On         25     25     25
I/O Modules
     1  Ethernet SM                    On         45     45     45
     2  Ethernet SM                    On         45     45     45
     3  I/O Module 3 (NP)                          0     45     45
     4  Server Conn Mod                On         45     45     45
Blades
     1  Maui A                         On        236    236    236
          (100%,100%,100%,100%)
     2  LewisA1-LS21 (T) (CA)          On         71     75     75
     3  Lucas_55 (T) (CA)              On         66     76     76
     4  Mongoose-2 (T) (CA)            On        108    127    121
     5  Crichton8 (T) (CA)             On         99    109    108
     6  Mongoose-3 (T) (CA)            On        142     34     34

Domain totals:
  Allocated Power                                 856   1414   1407

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"
```

```
      (CA) means "capped max power allocation"

-pm nonred

system> fuelg -pt 6
Date     Time     Avg Pwr
-------- -------- -------
07/17/07 08:09:44    2930
07/17/07 08:24:44    2926
07/17/07 08:39:48    2916
07/17/07 08:54:44    2906
07/17/07 09:09:44    2922
07/17/07 09:24:44    2926
07/17/07 09:39:44    2926
07/17/07 09:54:44    2926
07/17/07 10:09:44    2914
07/17/07 10:24:44    2928
07/17/07 10:39:48    2930
07/17/07 10:54:44    2914
07/17/07 11:09:43    2762
07/17/07 11:24:44    2924
07/17/07 11:39:44    2926
07/17/07 11:54:44    2932
07/17/07 12:09:44    2928
07/17/07 12:24:44    2922
07/17/07 12:39:43    2762
07/17/07 12:54:43    2772
07/17/07 13:09:43    2770
07/17/07 13:24:44    2766
07/17/07 13:39:44    2768
07/17/07 13:54:47    2926

system> fuelg -T blade[1]
-pme off
PM Capability: Dynamic Power Measurement with capping
Effective CPU Speed: 2955 MHz
Maximum CPU Speed: 3000 MHz
-pcap 190 (min: 174, max: 280)
Maximum Power:  235
Minimum Power:  199
Average Power:  235
Data captured at 07/17/07 13:59:05
system>
```

groups command

This command displays and configures Active Directory groups of the primary management module. This group information is used only when LDAP servers are enabled for authentication with local authorization.

Table 39. groups (Active Directory groups) command

Function	What it does	Command	Valid targets
Display all Active Directory groups	Displays all Active Directory groups, up to 16, configured for the BladeCenter unit.	`groups`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display specific Active Directory group	Displays information for the specified Active Directory group.	`groups -`*group_num* where *group_num* is a number from 1 to 16, inclusive, that identifies the Active Directory group.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Active Directory group name	Sets a name for the specified Active Directory group.	`groups -`*group_num* `-n` *group_name* where: • *group_num* is a number from 1 to 16, inclusive, that identifies the Active Directory group. • *group_name* is a alphanumeric string up to 63 characters in length that can include periods (.) and underscores (_). Each of the 16 group names must be unique. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 39. groups (Active Directory groups) command (continued)

Function	What it does	Command	Valid targets
Set Active Directory group authority level	Sets the authority level for the specified Active Directory group.	`groups -`*group_num* `-a` *group_authority* where: • *group_num* is a number from 1 to 16, inclusive, that identifies the Active Directory group. • *group_authority* uses the following syntax: – `operator` (Operator) – `rbs:`*levels*`:`*scope* 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 39. groups (Active Directory groups) command (continued)

Function	What it does	Command	Valid targets
Set Active Directory group authority level *(continued)*		where the *scope* is 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 1 for the Active Directory environment.) • 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) This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	
Delete Active Directory group	Delete the specified Active Directory group.	`groups -`*group_num* `-clear` where *group_num* is a number from 1 to 16, inclusive, that identifies the Active Directory group. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example: To create Active Directory group number 3 with a group name of group3 that 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

```
groups -3 -n group3 -a rbs:super:c1|b1-b14|s1-s4
```

To display information for group3, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
groups -3
```

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

```
system:mm[1]> groups -3 -n group3 -a rbs:super:c1|b1-b14|s1-s4
OK
system:mm[1]> groups -3
-n group3
-a Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Modules:1|2|3|4
system:mm[1]>
```

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 40. 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]`
			`-T system:storagex]` (for BladeCenter S units)
			where *x* is the primary management-module, blade server, I/O module, power module, blower bay, or storage 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 40. 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.

Display results with timestamp
 	
(BladeCenter E units only)
	Adds display of timestamp information to status command output.	`health -t`
		Note: The -t option must be used with the -f option.
			`-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 41. 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 advanced 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
    accseccfg -- View/edit account security config
  advfailover -- View/edit advanced failover mode
     alertcfg -- Displays/Configures the global remote alert settings
 alertentries -- View/edit remote alert recipients
      autoftp -- View/Edit auto ftp/tftp setting
      baydata -- View/edit Blade Bay Data string
         bofm -- Apply new BOFM configuration
         boot -- Boot target
    bootmode -- Boot mode
     bootseq -- View/edit the blade boot sequence settings
  buildidcfg -- View/Edit the Blade Firmware Build ID List
    chconfig -- View/edit Service Advisor Settings
       chlog -- Display Service Advisor Activity Log entires
    chmanual -- Manually generate call home request
         cin -- Displays/Configures Chassis Internal Network
   cinstatus -- Displays Status of Chassis Internal Network
       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
   displaysd -- Display service data
         dns -- View/edit DNS config
         env -- Set persistent command target
  ethoverusb -- View/edit the status of a blade SP's interface on Ethernet-over-USB
   eventinfo -- Display event description and user action
      events -- View/edit Events config
        exit -- Log off
     feature -- View/edit licensed features
       files -- Displays and deletes files stored on the AMM
       fuelg -- Power management
      groups -- View/edit Active Directory groups
      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
      iocomp -- View I/O compatibility for blades and switches
         kvm -- Controls the kvm owner
```

```
      ldapcfg -- View/edit LDAP config
          led -- Display and control Leds
         list -- Display installed targets
         mcad -- Displays and configures MCAD
    modactlog -- Displays module activity log
    monalerts -- Displays and configures monitored alerts
           mt -- Controls the media tray owner
          nat -- Display and configure NAT
          ntp -- View/edit NTP config
         ping -- Pings targeted switch module
     pmpolicy -- View/edit power management policy settings
      portcfg -- Serial port configuration
        ports -- Port configuration
        power -- Control target power
         rdoc -- Controls the remote DiskOnCard
         read -- Restore configuration from the chassis or a file
remotechassis -- Chassis discovered over the network
        reset -- Reset target
        scale -- Display and configure the settings of scalable complexes
       sddump -- Initiate service data dump
      sdemail -- Send service information using email
     security -- View/edit security config
      service -- Enable debugging by service personnel
     shutdown -- Shutdown target
          slp -- View/edit SLP parameters
         smtp -- View/edit SMTP config
         snmp -- View/edit SNMP config
          sol -- View SOL status and view/edit SOL config
       sshcfg -- View/edit SSH config
       sslcfg -- View/edit SSL config
       syslog -- View/edit syslog config
   tcpcmdmode -- View/edit TCP command mode config
    telnetcfg -- View/edit telnet config
        temps -- View temperatures
     trespass -- View/edit trespassing warning config
        uicfg -- View/edit user interface configuration
       update -- Update firmware from remote location
       uplink -- View/edit failover on network uplink loss config
        users -- View/edit user login profiles
        volts -- View voltages
        write -- Save configuration to chassis or a local file
      zonecfg -- Zone configuration for I/O modules

Type "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 42. 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 43. 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`
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration (for BladeCenter unit)
		• Blade configuration (for blade server)
		
		See "Commands and user authority" on page 8 for additional information.
			`-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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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 and installed options.

Table 44. ifconfig command

Function	What it does	Command	Valid targets
Display primary management module Ethernet channel 0 configuration	Displays the current configuration of Ethernet channel 0 for the primary management module. Possible return values are: • enabled • disabled • -i *static_ip_address* (dotted decimal IPv4 IP address format) • -g *gateway_address* (dotted decimal IPv4 IP address format) • -s *subnet_mask* (dotted decimal IPv4 IP address format) • -n *hostname* • -c *config_method* • -r *data_rate* • -d *duplex_mode* • -m *mtu* • -l *locally_administered_mac_addr* • -b *burnedin_mac_address* • -dn *domain_name* • -ipv6 *ipv6_state* • -ipv6static *static_ipv6_state* • -i6 *static_ip_address* (IPv6 format) • -p6 *address_prefix_length* • -g6 *gateway-default_route* • -dhcp6 *dhcpv6_state* • -sa6 *ipv6_stateless_autoconfig_state* If IPv6 is enabled, the link-local address *link_local_address* (for IPv6 connection) also displays. If IPv6 and stateless auto-configuration (-sa6) are both enabled, the Stateless auto-config IP Addresses / Prefix Length *address_table* (table listing auto-generated IPv6 addresses and their prefix lengths) also displays.	`ifconfig -eth0`	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Display standby management module Ethernet channel 0 configuration	Displays the current configuration of Ethernet channel 0 for the standby management module. **Note:** This option does not apply to the BladeCenter S unit.Possible return values are: • enabled • disabled • -i *static_ip_address* (dotted decimal IPv4 IP address format) • -g *gateway_address* (dotted decimal IPv4 IP address format) • -s *subnet_mask* (dotted decimal IPv4 IP address format) • -n *hostname* • -c *config_method* • -r *data_rate* • -d *duplex_mode* • -m *mtu* • -l *locally_administered_mac_addr* • -b *burnedin_mac_address* • -dn *domain_name* • -ipv6 *ipv6_state* • -ipv6static *static_ipv6_state* • -i6 *static_ip_address* (IPv6 format) • -p6 *address_prefix_length* • -g6 *gateway-default_route* • -dhcp6 *dhcpv6_state* • -sa6 *ipv6_stateless_autoconfig_state* If IPv6 is enabled, the link-local address *link_local_address* (for IPv6 connection) also displays. If IPv6 and stateless auto-configuration (-sa6) are both enabled, the Stateless auto-config IP Addresses / Prefix Length *address_table* (table listing auto-generated IPv6 addresses and their prefix lengths) also displays.	`ifconfig -eth0 -o`	`-T system:mm[x]` where *x* is the primary management-module bay number. **Note:** Even though this command displays information for the standby management module, it still must specify the primary management module as the command target.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set management module Ethernet channel 0 static IP address (IPv4)	Sets the IPv4 static IP address for Ethernet channel 0 for the management module. **Note:** Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth0 -i` *ip_address* where *ip_address* is the static IP address for Ethernet channel 0 in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 static IP address (IPv6)	Sets the IPv6 static IP address for Ethernet channel 0 for the management module.	`ifconfig -eth0 -i6` *ip_address* where *ip_address* is the static IP address for Ethernet channel 0 in IPv6 format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set standby management module Ethernet channel 0 static IP address (IPv4)	Sets the IPv4 static IP address for Ethernet channel 0 for the standby management module. **Note:** This option does not apply to the BladeCenter S unit.	`ifconfig -eth0 -o -i` *ip_address* where *ip_address* is the static IP address for Ethernet channel 0 in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number. **Note:** Even though this command displays information for the standby management module, it still must specify the primary management module as the command target.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set standby management module Ethernet channel 0 static IP address (IPv6)	Sets the IPv6 static IP address for Ethernet channel 0 for the standby management module. **Note:** This option does not apply to the BladeCenter S unit.	`ifconfig -eth0 -o -i6` *ip_address* where *ip_address* is the static IP address for Ethernet channel 0 in IPv6 format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number. **Note:** Even though this command displays information for the standby management module, it still must specify the primary management module as the command target.
Set management module Ethernet channel 0 gateway IP address (IPv4)	Sets the IPv4 gateway IP address for Ethernet channel 0 for the management module. **Note:** Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth0 -g` *ip_address* where *ip_address* is the gateway IP address for Ethernet channel 0 in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 gateway/default route (IPv6)	Sets the IPv6 gateway/default route for Ethernet channel 0 for the management module.	`ifconfig -eth0 -g6` *ip_address* where *ip_address* is the gateway/default route for Ethernet channel 0 in IPv6 format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set management module Ethernet channel 0 subnet mask (IPv4)	Sets the IPv4 subnet mask for Ethernet channel 0 for the management module. **Note:** Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth0 -s` *sub_mask* where *sub_mask* is the subnet mask for Ethernet channel 0 in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 hostname	Sets the host name for Ethernet channel 0 for the management module. **Note:** Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth0 -n` *hostname* where *hostname* is the host name for Ethernet channel 0. The hostname can be a string up to 63 characters in length that includes alphanumeric characters, hyphens, and underscores. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set standby management module Ethernet channel 0 hostname	Sets the host name for Ethernet channel 0 for the standby management module. **Note:** This option does not apply to the BladeCenter S unit.	`ifconfig -eth0 -o -n` *hostname* where *hostname* is the host name for Ethernet channel 0. The hostname can be a string up to 63 characters in length that includes alphanumeric characters, hyphens, and underscores. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number. **Note:** Even though this command displays information for the standby management module, it still must specify the primary management module as the command target.
Set management module Ethernet channel 0 configuration method	Sets the configuration method for Ethernet channel 0 for the management module. A value of `dthens` will try the DHCP configuration and default to the static IP configuration if DHCP is unsuccessful 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. • Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth0 -c` *config_method* where *config_method* is • `dhcp` • `static` • `dthens` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set management module Ethernet channel 0 data rate	Sets the data rate for Ethernet channel 0 for the management module.	`ifconfig -eth0 -r` *data_rate* where *data_rate* is • `auto` • `10` • `100` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 duplex mode	Sets the duplex mode for Ethernet channel 0 for the management module.	`ifconfig -eth0 -d` *duplex_mode* where *duplex_mode* is • `auto` • `half` • `full` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 0 MTU	Sets the MTU (maximum transmission unit) for Ethernet channel 0 for the management module.	`ifconfig -eth0 -m` *mtu* where *mtu* is between 60 and 1500, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set management module Ethernet channel 0 static MAC address (locally administered)	Sets the locally administered MAC address to the specified MAC address for Ethernet channel 0 for the management module. **Note:** Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth0 -l` *address* where *address* is the locally administered MAC address for Ethernet channel 0. The MAC address is 6 bytes in length, hexadecimal, separated by colons. The MAC address can not be a multicast address (the first byte must be even). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the standby management-module bay number.
Set standby management module Ethernet channel 0 static MAC address (locally administered)	Sets the locally administered MAC address to the specified MAC address for Ethernet channel 0 for the standby management module. **Note:** This option is not available on the BladeCenter S.	`ifconfig -eth0 -o -l` *address* where *address* is the locally administered MAC address for Ethernet channel 0. The MAC address is 6 bytes in length, hexadecimal, separated by colons. The MAC address can not be a multicast address (the first byte must be even). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number. **Note:** Even though this command displays information for the standby management module, it still must specify the primary management module as the command target.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set management module Ethernet channel 0 domain name	Sets the domain name for Ethernet channel 0 for Ethernet channel 0 for the management module. **Note:** Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth0 -dn` *domain* where *domain* is an alphanumeric string up to 127 characters in length. The domain name must contain at least one dot (.). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable IPv6 addressing for management module Ethernet channel 0	Enable or disable IPv6 addressing for Ethernet channel 0 for the management module.	`ifconfig -eth0 -ipv6` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable static IPv6 configuration for management module Ethernet channel 0	Enable or disable static IPv6 configuration for Ethernet channel 0 for the management module.	`ifconfig -eth0 -ipv6static` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set management module Ethernet channel 0 address prefix length	Sets the IPv6 address prefix length for Ethernet channel 0 for the management module.	`ifconfig -eth0 -p6` *length* where *length* is between 1 and 128 (inclusive). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable DHCPv6 for management module Ethernet channel 0	Enable or disable static DHCPv6 for Ethernet channel 0 for the management module.	`ifconfig -eth0 -dhcp6` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable IPv6 stateless auto-configuration for management module for Ethernet channel 0	Enable or disable IPv6 stateless auto-configuration for Ethernet channel 0 for the management module.	`ifconfig -eth0 -sa6` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Display primary management module Ethernet channel 1 configuration	Displays the current configuration of Ethernet channel 1 for the primary management module. Possible return values are: • up (enabled) • down (disabled) • -i *static_ip_address* (dotted decimal IPv4 IP address format) • -g *gateway_address* (dotted decimal IPv4 IP address format) • -s *subnet_mask* (dotted decimal IPv4 IP address format) • -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 management module Ethernet channel 1 static IP address (IPv4)	Sets the static IP address (IPv4) for Ethernet channel 1 for the management module. **Note:** Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth1 -i` *ip_address* where *ip_address* is the static IP address for Ethernet channel 1 in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 1 gateway IP address (IPv4)	Sets the gateway IP address (IPv4) for Ethernet channel 1 for the management module. **Note:** Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth1 -g` *ip_address* where *ip_address* is the gateway IP address for Ethernet channel 1 in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set management module Ethernet channel 1 subnet mask (IPv4)	Sets the subnet mask (IPv4) for Ethernet channel 1 for the management module. **Note:** Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth1 -s` *sub_mask* where *sub_mask* is the subnet mask for Ethernet channel 1 in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 1 data rate	Sets the data rate for Ethernet channel 1 for the management module.	`ifconfig -eth1 -r` *data_rate* where *data_rate* is • `auto` • `10` • `100` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 1 duplex mode	Sets the duplex mode for Ethernet channel 1 for the management module.	`ifconfig -eth1 -d` *duplex_mode* where *duplex_mode* is • `auto` • `half` • `full` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set management module Ethernet channel 1 MTU	Sets the MTU (maximum transmission unit) for Ethernet channel 1 for the management module.	`ifconfig -eth1 -m` *mtu* where *mtu* is between 60 and 1500, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set management module Ethernet channel 1 static MAC address (locally administered)	Sets the locally administered MAC address to the specified MAC address for Ethernet channel 1 for the management module. **Note:** Changes made to the IP configuration of the primary management module take effect after the next reset of the primary management module.	`ifconfig -eth1 -l` *address* where *address* is the locally administered MAC address for Ethernet channel 1. The MAC address is 6 bytes in length, hexadecimal, separated by colons. The MAC address can not be a multicast address (the first byte must be even). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the standby management-module bay number.
Enable management module Ethernet channel 1	Enables the Ethernet channel 1 interface for the management module.	`ifconfig -eth1 -up` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Disable management module Ethernet channel 1	Disables the Ethernet channel 1 interface for the management module.	`ifconfig -eth1 -down` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display cKVM and network configuration status for blade server	Displays the cKVM status and network status for the specified blade server. • Valid cKVM states include: – Enabled – Disabled • If the blade server supports network configuration, this command also displays the NIC numbers (such as -eth0 and -eth1), NIC states (up or down), and other NIC configuration information for the blade server and all network cards connected to the blade server.	`ifconfig`	`-T system:blade[x]` where *x* is the blade-server bay number.
Display network configuration information for network card	Displays the NIC number (such as -eth0 and -eth1), NIC state (up or down), and other NIC configuration information for the specified network card in the specified blade server.	`ifconfig -ethx` where *x* is the NIC number.	`-T system:blade[x]` where *x* is the blade-server bay number.
Set I/O module for blade server management traffic	Sets the I/O module that will be used to route management traffic for the specified blade server. **Note:** This command will run only if the target blade server supports manual configuration of its management network interface.	`ifconfig -eth1 -i IO_bay` where *IO_bay* is the bay number of the I/O module that should be used to route management traffic. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade-server bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Enable / disable cKVM feature for blade server	Enable or disable cKVM feature for the specified blade server. **Note:** The cKVM feature requires special hardware and is not available for all blade servers.	`ifconfig -ckvm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Set blade server Ethernet channel static IP address (IPv4)	Sets the IPv4 static IP address for the specified Ethernet channel of the specified blade server. **Note:** This command will run only if the target blade server supports manual configuration of its management network interface.	`ifconfig -eth`*x* `-i` *ip_address* where: • *x* is the NIC number. • *ip_address* is the static IP address for Ethernet channel *x* in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set blade server Ethernet channel static IP address (IPv6)	Sets the IPv6 static IP address for the specified Ethernet channel of the specified blade server. **Note:** • This command will run only if the target blade server supports manual IPv6 configuration of its management network interface. • A static IPv6 configuration ID is required for network interfaces that support more than one static configuation.	`ifconfig -eth`*x* `-i6` *ip_address* `-id` *id* where: • *x* is the NIC number. • *ip_address* is the static IP address for Ethernet channel *x* in IPv6 format. • *id* is the static IPv6 configuration ID. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Set blade server Ethernet channel gateway IP address (IPv4)	Sets the IPv4 gateway IP address for the specified Ethernet channel of the specified blade server. **Note:** This command will run only if the target blade server supports manual configuration of its management network interface.	`ifconfig -eth`*x* `-g` *ip_address* where: • *x* is the NIC number. • *ip_address* is the gateway IP address for Ethernet channel *x* in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set blade server Ethernet channel gateway/default route (IPv6)	Sets the IPv6 gateway/default route for the specified Ethernet channel of the specified blade server. **Note:** • This command will run only if the target blade server supports manual IPv6 configuration of its management network interface.. • A static IPv6 configuration ID is required for network interfaces that support more than one static configuation.	`ifconfig -eth`*x* `-g6` *ip_address* `-id` *id* where: • *x* is the NIC number. • *ip_address* is the gateway/default route for Ethernet channel *x* in IPv6 format. • *id* is the static IPv6 configuration ID. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Set blade server Ethernet channel subnet mask (IPv4)	Sets the IPv4 subnet mask for the specified Ethernet channel of the specified blade server. **Note:** This command will run only if the target blade server supports manual configuration of its management network interface.	`ifconfig -eth`*x* `-s` *sub_mask* where: • *x* is the NIC number. • *sub_mask* is the subnet mask for Ethernet channel *x* in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set blade server Ethernet channel configuration method	Sets the configuration method for the specified Ethernet channel of the specified blade server. A value of `dthens` will try the DHCP configuration and default to the static IP configuration if DHCP is unsuccessful after 2 minutes. **Note:** • This command will run only if the target blade server supports manual configuration of its management network interface. • If the DHCP setting is set to try the DHCP server and then use the static IP address, the NIC will use the static IP address when the DHCP server is not available during start up. When this occurs, the IP address might not be reachable if multiple devices were started with the same static IP address. • Blade servers based on the Power PC chip, including the JS12 and JS22, only support the static and DHCP options.	`ifconfig -eth`*x* `-c` *config_method* where: • *x* is the NIC number. • *config_method* is – `dhcp` – `static` – `dthens` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Set management module Ethernet channel VLAN ID	Sets the VLAN ID for the specified Ethernet channel of the specified blade server. **Note:** This command will run only if the target blade server supports manual configuration of its management network interface.	`ifconfig -eth`*x* `-v` *vlan_id* where: • *x* is the NIC number. • *vlan_id* is from 1 to 4095, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set state for blade server Ethernet channel VLAN ID	Enables or disables the VLAN ID for the specified Ethernet channel of the specified blade server. **Note:** This command will run only if the target blade server supports manual configuration of its management network interface.	`ifconfig -eth`*x* `-ve` *state* where: • *x* is the NIC number. • *state* is enable or disable. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Set blade server Ethernet channel hostname	Sets the host name for the specified Ethernet channel of the specified blade server. **Note:** This command will run only if the target blade server supports manual configuration of its management network interface.	`ifconfig -eth`*x* `-n` *hostname* where: • *x* is the NIC number. • *hostname* is the host name. The hostname can be a string up to 63 characters in length that includes alphanumeric characters, hyphens, and underscores. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Enable blade server Ethernet channel	Enables the specified Ethernet channel interface of the specified blade server. **Note:** This command will run only if the target blade server supports manual configuration of its management network interface.	`ifconfig -eth`*x* `-up` where *x* is the NIC number. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Disable blade server Ethernet channel	Disables the specified Ethernet channel interface of the specified blade server. **Note:** This command will run only if the target blade server supports manual configuration of its management network interface.	`ifconfig -eth`*x* `-down` where *x* is the NIC number. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Enable / disable IPv6 addressing for blade server	Enable or disable IPv6 addressing for the specified Ethernet channel interface of the specified blade server. **Note:** This command will run only if the target blade server supports manual IPv6 configuration of its management network interface.	`ifconfig -eth`*x* `-ipv6` *state* where: • *x* is the NIC number. • *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Set blade server address prefix length	Sets the IPv6 address prefix length for the specified Ethernet channel interface of the specified blade server. **Note:** • This command will run only if the target blade server supports manual IPv6 configuration of its management network interface. • A static IPv6 configuration ID is required for network interfaces that support more than one static configuation.	`ifconfig -eth`*x* `-p6` *length* `-id` *id* where: • *x* is the NIC number. • *length* is between 1 and 128 (inclusive). • *id* is the static IPv6 configuration ID. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Enable / disable DHCPv6 for blade server	Enable or disable static DHCPv6 for the specified Ethernet channel interface of the specified blade server. **Note:** This command will run only if the target blade server supports manual IPv6 configuration of its management network interface.	`ifconfig -eth`*x* `-dhcp6` *state* where: • *x* is the NIC number. • *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Enable / disable IPv6 stateless auto-configuration for blade server	Enable or disable IPv6 stateless auto-configuration for the specified Ethernet channel interface of the specified blade server. **Note:** This command will run only if the target blade server supports manual IPv6 configuration of its management network interface.	`ifconfig -eth`*x* `-sa6` *state* where: • *x* is the NIC number. • *state* is `enabled` or `disabled` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade-server bay number.
Set blade server ISMP static IP address (IPv4)	Sets the IPv4 static IP address for the integrated system management processor (ISMP) of the specified blade server. **Note:** This command will run only if the target blade server supports manual configuration of its management network interface.	`ifconfig -i` *ip_address* where *ip_address* is the static IP address for the blade server ISMP in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]:sp` where *x* is the blade-server bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Display network settings for BladeCenter unit	Displays network settings for the BladeCenter unit. Valid return values are: • -v *VLAN-id* • -maxv *enabled/disabled*	`ifconfig`	`-T system`
Enable / disable multiple video sessions for blade servers	Set state to allow only a single remote video session or allow up to four remote video sessions for each blade server.	`ifconfig -maxv` *state* where *state* is `enabled` (allow multiple video sessions) or `disabled` (allow only one video session). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
VLAN ID for BladeCenter unit	Sets the VLAN ID for the BladeCenter unit.	`ifconfig -v` *VLAN-id* where *VLAN-id* is from 1 to 4095, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
Set state for BladeCenter unit VLAN ID	Enables or disables the VLAN ID for the BladeCenter unit.	`ifconfig -ve` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Enable / disable global cKVM feature for BladeCenter unit	Enable or disable cKVM feature globally for the BladeCenter unit. (This is the same as running the `ifconfig -ckvm enable` command directed to each blade server.) **Note:** The cKVM feature requires special hardware and is not available for all blade servers.	`ifconfig -ckvm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
Display network settings for I/O module	Displays network settings for the specified I/O module. Valid return values are: • I/O-module type • -i *ip_address* (dotted decimal IPv4 IP address format) • -s *subnet_mask* (dotted decimal IPv4 IP address format) • -g *gateway_address* (dotted decimal IPv4 IP address format) • -em *ext_mgt_status* • -ep *ext_port_status* • -pm *enabled/disabled* (protected mode) • -pip *enabled/disabled* • -c *config_method* • -ipv6 *ipv6_state* • -ipv6static *static_ipv6_state* • -i6 *static_ip_address* (IPv6 format) • -p6 *address_prefix_length* (IPv6 format) • -g6 *gateway-default_route* (IPv6 format) • -dhcp6 *dhcpv6_state* • -sa6 *ipv6_stateless_autoconfig_state* If IPv6 is enabled, the link-local address *link_local_address* (for IPv6 connection) also displays. If IPv6 and stateless auto-configuration (-sa6) are both enabled, the Stateless auto-config IP Addresses / Prefix Length *address_table* (table listing auto-generated IPv6 addresses and their prefix lengths) also displays.	`ifconfig`	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set starting IP address for I/O module (IPv4)	Sets the IPv4 IP addresses for the specified I/O module.	`ifconfig -i` *ip_address* where *ip_address* is the IP address of the specified I/O module in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.
Set starting IP address for I/O module (IPv6)	Sets the IPv6 static IP address for the specified I/O module.	`ifconfig -i6` *ip_address* where *ip_address* is the static IP address for the specified I/O module in IPv6 format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.
Set I/O-module gateway IP address (IPv4)	Sets the gateway IPv4 IP address for the specified I/O module.	`ifconfig -g` *ip_address* where *ip_address* is the gateway IP address for the I/O module in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set I/O-module gateway IP address (IPv6)	Sets the IPv6 gateway/default route for the specified I/O module.	`ifconfig -g6 ip_address` where *ip_address* is the gateway IP address for the I/O module in IPv6 format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.
Keep new IP address configuration for I/O-module after reset	Retains a new IP address configuration after the specified I/O module is reset. **Note:** Make sure a valid New Static IP Configuration is entered for this I/O module so that when the module's factory defaults are restored, or when a reset is initiated by a source other than the management module, the New Static IP Configuration will be configured. In these cases management module communication with the I/O module will be preserved.	`ifconfig -pip enabled` This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.
Revert to old IP address configuration for I/O-module after reset	Reverts IP address to old configuration after the specified I/O module is reset. **Note:** The factory default IP configuration will become active when the I/O module is reset to factory defaults by either the management module or the I/O module. If an I/O module reset is initiated by a source other than the management module, then the previous IP configuration will be in affect. In both of these cases the management module will lose IP communications with the I/O module.	`ifconfig -pip disabled` This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set I/O-module subnet mask (IPv4)	Sets the IPv4 subnet mask for the specified I/O module.	`ifconfig -s` *sub_mask* where *sub_mask* is the subnet mask for the I/O module in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-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 the specified I/O module.	`ifconfig -em` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-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.	`ifconfig -ep` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Enable / disable protected mode for I/O module	Enables or disables protected mode for the specified I/O module.	`ifconfig -pm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.
Enable / disable IPv6 addressing for I/O module	Enable or disable IPv6 addressing for the specified I/O module.	`ifconfig -ipv6` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.
Enable / disable static IPv6 configuration for I/O module	Enable or disable static IPv6 configuration for the specified I/O module.	`ifconfig -ipv6static` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set I/O module address prefix length	Sets the IPv6 address prefix length for the specified I/O module.	`ifconfig -p6` *length* where *length* is between 1 and 128 (inclusive). This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.
Enable / disable DHCPv6 for I/O module	Enable or disable static DHCPv6 for the specified I/O module.	`ifconfig -dhcp6` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.
Enable / disable IPv6 stateless auto-configuration for I/O module	Enable or disable IPv6 stateless auto-configuration for the specified I/O module.	`ifconfig -sa6` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set IP addresses for RAID controller and SAS system (IPv4) (BladeCenter S units only)	Sets IPv4 IP addresses for RAID controller and SAS system.	`ifconfig -i` *ip_address_a* `-ir` *ip_address_b* where • *ip_address_a* is the IP address of the specified SAS system in dotted decimal IP address format. • *ip_address_b* is the IP address of the associated RAID controller in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the RAID controller bay number.
Set gateway IP addresses for RAID controller and SAS system (IPv4) (BladeCenter S units only)	Sets the IPv4 gateway IP addresses for RAID controller and SAS system.	`ifconfig -g` *ip_address_a* `-gr` *ip_address_b* where • *ip_address_a* is the gateway IP address of the specified SAS system in dotted decimal IP address format. • *ip_address_b* is the gateway IP address of the associated RAID controller in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the RAID controller bay number.

Table 44. ifconfig command (continued)

Function	What it does	Command	Valid targets
Set subnet masks for RAID controller and SAS system (IPv4) (BladeCenter S units only)	Sets the IPv4 subnet masks for the RAID controller and SAS system.	`ifconfig -s` *sub_mask_a* `-sr` *sub_mask_b* where • *sub_mask_a* is the subnet mask of the specified SAS system in dotted decimal IP address format. • *sub_mask_b* is the subnet mask of the associated RAID controller in dotted decimal IP address format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the RAID controller bay number.

Example:

To display the configuration for Ethernet channel 0, that does not support IPv6, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
ifconfig -eth0
```

To set the IPv4 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
```

To set the IPv4 IP addresses for the BladeCenter S SAS subsystem to 9.186.10.16 and the IPv4 IP address for the RAID controller to 9.186.10.17, while switch module 3 is set as the persistent command environment, at the `system:switch[3]>` prompt, type

```
ifconfig -i 9.186.10.16 -ir 9.186.10.17
```

To set the IPv4 gateway address for the BladeCenter S SAS subsystem to 9.186.10.1 and the IPv4 gateway address for the RAID controller to 9.186.11.1, while switch module 3 is set as the persistent command environment, at the system:switch[3]> prompt, type

```
ifconfig -g 9.186.10.1 -gr 9.186.11.1
```

The following example shows the information that is returned from these 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]>
```

```
system:switch[3]>ifconfig -i 9.186.10.16 -ir 9.186.10.17
OK
system:switch[3]>ifconfig -g 9.186.10.1 -gr 9.186.11.1
OK
system:mm[1]>
```

To display the configuration for Ethernet channel 0, that supports IPv6, while management module 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
ifconfig -eth0
```

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

```
system:mm[1]> ifconfig -eth0
Enabled
-i 10.13.3.230
-g 10.13.1.1
-s 255.255.0.0
-n primaryAMM
-c static
-r auto
-d auto
-m 1500
-l 00:00:00:00:00:00
-b 00:14:5E:DF:0F:CE
-dn primaryAMM.com
-ipv6 enabled
-ipv6static disabled
-i6 6::6
-p6 1
-g6 ::
-dhcp6 enabled
-sa6 enabled
Link-local address: fe80::214:5eff:fedf:fce
Stateless auto-config IP Addresses       Prefix Length
---------------------------------------  -------------
```

```
2000:1013::214:5eff:fedf:fce             64
2001:1013::214:5eff:fedf:fce             64
2002:1013::214:5eff:fedf:fce             64
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 45. 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]: exp[y]`
			`-T system:blade[x]: mgmtcrd`
			`-T system:blade[x]:sp`
			`-T system:blade[x]: be[y]`
			`-T system:blade[x]: be[y]:exp[z]`
			`-T system:blade[x]: be[y]:hsec[z]`
			`-T system:blade[x]:sb`
			`-T system:blade[x]: cpu[y]`
			`-T system:blade[x]: memory[y]`
			`-T system:blade[x]: hsec[y]`
			`-T system:blade[x]:ckvm`
			`-T system:switch[x]`
			`-T system:power[x]`
			`-T system:mt[x]`
			`-T system:mt[x]: bbu[y]`
			`-T system:storage[x]`
			`-T system:storage[x]: disk[y]`
			
			(continued on next page)

Table 45. info (configuration information) command (continued)

Function	What it does	Command	Valid targets
Display component information *(continued)*			where: • *x* is the management-module bay number, blade server bay number, I/O-module bay number, microprocessor number, power module bay number, media-tray bay number, storage bay number , or daughter-card number. • *y* or *z* is the: – blade server storage expansion unit number (be). – blade server I/O expansion card number (exp). – microprocessor number (CPU). – memory DIMM number. – high-speed expansion card number (hsec). – battery backup unit number (bbu). – disk drive number (disk).
Display management channel path information	Displays the management channel path information for the BladeCenter unit.	`info -path`	`-T system`
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`
Reload all component information	Forces reload of all VPD and MAC address information.	`info -reload all`	`-T system`

Notes:

1. The command target `-T system:blade[x]:exp[y]` is shown with a line break before the `:exp[y]`. When this command target is 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. For some targets, additional VPD information is available when using the advanced management module.
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 an advanced 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

Name: AMM_KP
Manufacturer: Not Available (Not Available)
Manufacturer ID: 288
Product ID: 1
Mach type/model: Management Module
Mach serial number: Not Available
Manuf date: 3005
Hardware rev: 51
Part no.: 26R099000000
FRU no.: 25R5777
FRU serial no.: 0J1U9E584130
CLEI: Not Available
AMM firmware
        Build ID:       BPET30U
        File name:      CNETCMUS.PKT
        Rel date:       08-09-07
        Rev:            30
AMM firmware (Flashed - pending restart)
        Build ID:       BPET30x
        File name:      CNETCMUS.PKT
        Rel date:       09-09-08
        Rev:            30
system:mm[1]>
```

iocomp command

This command displays the compatibility between all blade servers and their I/O modules. It can also display detailed interface information for an individual blade server or I/O module.

Table 46. iocomp command

Function	What it does	Command	Valid targets
Display compatibility between all blade servers and I/O modules	Displays I/O module compatibility information for all blade servers and I/O modules.	`iocomp`	`-T system`
Display blade server compatibility details	Displays detailed I/O module compatibility information for the specified blade server.	`iocomp`	`-T system:blade[`*x*`]` where *x* is the blade server bay number.
Display I/O module compatibility details	Displays detailed compatibility information for the specified I/O module.	`iocomp`	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Example: To view I/O module compatibility information for all blade servers and I/O modules, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
iocomp -T system
```

To view I/O module compatibility information for 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

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

To view I/O module compatibility information for the I/O module in bay 2, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
iocomp -T system:switch[2]
```

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

```
system:mm[1]> iocomp -T system
Blades
1    xPert1          OK
2    xPert2          OK
3    Development     OK
4    Marketing       OK
5    xpert3          OK
6    Sales           OK
7    xPert4          OK
9    xPert5          OK
11   Finance         OK
12   HR              OK
13   xPert6          OK
14   xPert7          OK

I/O Modules
1    OK
2    OK
3    OK
4    OK
```

```
system:mm[1]> iocomp -T system:blade[1]
  Bay     Power         Fabric Type       Fabric on Blade   Compt
-------  -------  ---------------------  ---------------  -------
 IOM 1   On       Ethernet Switch Module  Ethernet         OK
 IOM 2   On       Ethernet Switch Module  Ethernet         OK
system:mm[1]> iocomp -T system:switch[1]
   Bay       Power    Fabric Type      Compat
----------  -------  -------------  ----------
Blade 1     On       Ethernet        OK
Blade 2     On       Ethernet        OK
Blade 3     On       Ethernet        OK
Blade 4     On       Ethernet        OK
Blade 5     Off      Ethernet        OK
Blade 6     On       Ethernet        OK
Blade 7     On       Ethernet        OK
                     n/a             No Fabric
Blade 9     On       Ethernet        OK
                     Ethernet        OK
Blade 11    On       Ethernet        OK
Blade 12    On       Ethernet        OK
Blade 13    On       Ethernet        OK
Blade 14    On       Ethernet        OK
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 47. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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]>
```

ldapcfg command

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

Table 48. ldapcfg command

Function	What it does	Command	Valid targets
Display LDAP settings	Displays the LDAP settings for the management module.	`ldapcfg`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set LDAP security version	Sets version of LDAP security used by the management module. **Note:** • If the version is set to v1, the following values must also be set: – A group filter using the `-gf` command option. – A group search attribute using the `-gsa` command option. – A login permission attribute using the `-lpa` command option. • If the version is set to v2, the LDAP name must also be set using the `-t` command option.	`ldapcfg -v` *version* where *version* is: • `v1` for old user permission model • `v2` for the enhanced role-based security model This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 48. ldapcfg command (continued)

Function	What it does	Command	Valid targets
Set LDAP group filter	Sets the group filter for the management module that can be used for authentication during LDAP server login. **Note:** For a group filter to be used, LDAP security must be set to v1 using the `-v` command option.	`ldapcfg -gf "filter"` where *"filter"* is a quote-delimited string of up to 511 characters in length and consists of one or more group names. The colon (:) character is used to delimit multiple group names. Leading spaces and trailing spaces are ignored. Consecutive spaces are treated as a single space. The wildcard character (*) is not supported for security reasons. A group name can be specified as a full domain name or by using the common name (cn) portion. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set LDAP group search attribute	Sets the group search attribute that represents groups of user IDs stored on the LDAP server. On Active Directory servers, the group search attribute is typically set to "memberOf". On eDirectory servers, it is typically set to "groupMembership". In an OpenLDAP server environment, users are typically assigned to groups whose objectClass equals "PosixGroup". In this case, the group search attribute identifies members of a particular PosixGroup that is typically "memberUid". **Note:** For a group search attribute to be used, LDAP security must be set to v1 using the `-v` command option.	`ldapcfg -gsa "GSA"` where *"GSA"* is a quote-delimited alphanumeric string of up to 23 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 48. ldapcfg command (continued)

Function	What it does	Command	Valid targets
Set LDAP login permission attribute	Sets the login permission attribute that is used to determine retrieve user permissions on the LDAP server. **Note:** For a login permission attribute to be used, LDAP security must be set to v1 using the `-v` command option.	`ldapcfg -lpa` *"permission"* where *"permission"* is a quote-delimited alphanumeric string up to 23 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set LDAP name	Sets the LDAP name for the management module. **Note:** For an LDAP name to be used, LDAP security must be set to v2 using the `-v` command option.	`ldapcfg -t` *name* where *name* is an alphanumeric string up to 63 characters in length containing any character except for angle brackets (< and >) and spaces. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 48. ldapcfg command (continued)

Function	What it does	Command	Valid targets
Set LDAP server discovery method	Sets the method to use for discovering LDAP servers that provide user authentication. **Note:** • If the dns method is specified, the following values must also be set: – A domain name using the `-dn` command option. – A forest name using the `-fn` command option. • If the preconf method is specified, the following values must also be set: – An LDAP server hostname or IP address using the `-i1`, `-i2`, and `-i3` command options. – A port for each LDAP server hostname or IP address using the `-p1`, `-p2`, and `-p3` command options.	`ldapcfg -server` *method* where *method* is: • `dns` for dynamic discovery • `preconf` to use an LDAP server that was manually pre-configured This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set LDAP server domain name	Sets the search domain to use for Domain Controller (DC) dynamic discovery.	`ldapcfg -dn` *domain* where *domain* is an alphanumeric string up to 255 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set LDAP server forest name	Sets the forest name to use for Global Catalog (GC) dynamic discovery.	`ldapcfg -fn` *forestname* where *forestname* is an alphanumeric string up to 63 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 48. ldapcfg command (continued)

Function	What it does	Command	Valid targets
First LDAP server host name or IP address - set	Checks syntax and sets the first LDAP server host name or IP address to use for pre-configured LDAP server discovery. **Note:** A port for this LDAP server hostname or IP address must be set using the `-p1` command option.	`ldapcfg -i1` *hostname/ip_address* where *hostname/ip_address* is the first host name or IP address, up to 255 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Second LDAP server host name or IP address - set	Checks syntax and sets the second LDAP server host name or IP address to use for pre-configured LDAP server discovery. **Note:** A port for this LDAP server hostname or IP address must be set using the `-p2` command option.	`ldapcfg -i2` *hostname/ip_address* where *hostname/ip_address* is the second host name or IP address, up to 255 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Third LDAP server host name or IP address - set	Checks syntax and sets the third LDAP server host name or IP address to use for pre-configured LDAP server discovery. **Note:** A port for this LDAP server hostname or IP address must be set using the `-p3` command option.	`ldapcfg -i3` *hostname/ip_address* where *hostname/ip_address* is the third host name or IP address, up to 255 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 48. ldapcfg command (continued)

Function	What it does	Command	Valid targets
Fourth LDAP server host name or IP address - set	Checks syntax and sets the fourth LDAP server host name or IP address to use for pre-configured LDAP server discovery. **Note:** A port for this LDAP server hostname or IP address must be set using the `-p4` command option.	`ldapcfg -i4` *hostname/ip_address* where *hostname/ip_address* is the fourth host name or IP address, up to 255 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
First LDAP server port number - set	Sets the port number of the first LDAP server to use for pre-configured LDAP server discovery.	`ldapcfg -p1` *port* where *port* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Second LDAP server port number - set	Sets the port number of the second LDAP server to use for pre-configured LDAP server discovery.	`ldapcfg -p2` *port* where *port* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 48. ldapcfg command (continued)

Function	What it does	Command	Valid targets
Third LDAP server port number - set	Sets the port number of the third LDAP server to use for preconfigured LDAP server discovery.	`ldapcfg -p3 port` where *port* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Fourth LDAP server port number - set	Sets the port number of the fourth LDAP server to use for preconfigured LDAP server discovery.	`ldapcfg -p4 port` where *port* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set LDAP root distinguished name	Sets the root distinguished name for the root entry of the LDAP directory tree that is used as the base object for all searches.	`ldapcfg -rd "name"` where *"name"* is up to 255 characters in length and contained within double-quotes. Names can contain any character, including spaces. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 48. ldapcfg command (continued)

Function	What it does	Command	Valid targets
Set LDAP UID search attribute	Sets the UID search attribute that represents the user IDs stored on the LDAP server. On Active Directory servers, the UID search attribute is typically set to "sAMAccountName". On Novell eDirectory and OpenLDAP servers, it is typically set to "uid".	`ldapcfg -usa` *"UID"* where *"UID"* is up to 23 characters in length and contained within double-quotes. The UID can contain only letters, numbers, spaces, and the following characters: "-", "(", ")", "+", ",", ".", "/", ":", and"?". This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set LDAP server binding method	Sets the binding method for initial connection to the LDAP server. **Note:** • If the binding method is set to anon, a UID search attribute must be set using the `-usa` command option. • If the binding method is set to cc, the following values must also be set: – A UID search attribute using the `-usa` command option – A client distinguished name using the `-cd` command option. – A client password using the `-p` and `-cp` command options.	`ldapcfg -bm` *version* where *version* is: • `anon` for anonymous • `cc` for configured credentials • `lc` for login credentials This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set LDAP server to be used for authentication only	Enables the authentication mode to use the LDAP server for authentication only with local authorization. This automatically disables the authentication mode that uses the LDAP Server for both authentication and authorization. LDAP server authentication uses the settings configured by the "groups command" on page 159.	`ldapcfg -aom` *state* where *state* is `enabled` or `disabled` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 48. ldapcfg command (continued)

Function	What it does	Command	Valid targets
Set LDAP client distinguished name	Sets the client distinguished name (DN) for initial connection to the LDAP server. **Note:** A client password must also be set using the `-p` and `-cp` command options.	`ldapcfg -cd` *domain* where *domain* is an alphanumeric string up to 255 characters in length containing any character except for angle brackets (< and >) and spaces. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set LDAP client distinguished name password	Sets the client distinguished name password for initial connection to the LDAP server. **Note:** The passwords must be specified by both the `-p` and `-cp` command options and must match.	`ldapcfg -p` *password* where *password* is an alphanumeric string up to 15 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set (confirm) LDAP client distinguished name password	Sets, for confirmation purposes, the client distinguished name password for initial connection to the LDAP server. **Note:** The passwords must be specified by both the `-p` and `-cp` command options and must match.	`ldapcfg -cp` *password* where *password* is an alphanumeric string up to 15 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Note: The `-ds`, `-sd`, and `-sn` options for the `ldapcfg` command have been deleted and replaced by the `-dn` and `-fn` command options. To implement this transition,

the items specified for dynamic discovery have changed and must be modified to match the syntax required by the new command options.

Example:

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

```
ldapcfg
```

To enable the authentication mode to use the LDAP server for authentication only with local authorization, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
ldapcfg -aom enabled
```

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

```
system:mm[1]> ldapcfg
-server preconf
 Parameters for '-server dns' configuration:
   -dn
   -fn test_fn
 Parameters for '-server preconf' configuration:
   -i1
   -p1
   -i2
   -p2
   -i3
   -p3
   -i4 192.168.1.23
   -p4 11

Miscellaneous Parameters:
-rd 11
-usa
-bm cc
-aom enabled
 Parameters for '-bm cc' configuration:
   -cd

-v v1
 Parameters for '-v v1' configuration:
   -gf
   -gsa
   -lpa
 Parameters for '-v v2' configuration:
   -t
system:mm[1]> ldapcfg -aom enabled
OK
system:mm[1]>
```

led command

This command displays and sets the LED states for a specified command target, if this command target supports the LED.

Table 49. led command

Function	What it does	Command	Valid targets

Display various LED states	Displays various LED states. Values returned are:
	• status of all LEDs on the target blade and its subcomponents
	• status of info LED
	• status of location LED (on/off/blink)
	• status of the identification LED of the system for a specified number of seconds
		`led`	`-T system`
			`-T system:blade[x]`
			where *x* is the blade server number.

Display state for fanpack fault LED	Displays the state of the fan pack fault LED of the BladeCenter HT unit.	`led`	`-T system:power[x]` where *x* is the power module (fanpack) number.
Display state for blower fault LED	Displays the state of the blower fault LED of the BladeCenter HT unit.	`led`	`-T system:blower[x]` where *x* is the blower number.
Display front panel LED state for blade server	Displays the state of the front panel LEDs on the specified blade server.	`led`	`-T system:blade[x]` where *x* is the blade server number.
Display external port link status LED state for I/O module	Displays state of the external and internal port link status LEDs for the specified I/O module.	`led`	`-T system:switch[x]` where *x* is the I/O module (switch) bay number.

Display fault LED state
(for BladeCenter HT units only)
	Displays the state of the fault LED for the specified command target. Possible return values are:
	• The state of the requested LED is on
	• The state of the requested LED is off
		`led -e`	`-T system:tap`
			`-T system:ncc[x]`
			`-T system:mux[x]`
			`-T system:mt[x]`
			where *x* is the alarm panel module, network clock module, multiplexer expansion module, or media tray number.

Display safe-to-remove LED state
(for BladeCenter HT units only)
	Displays the state of the safe-to-remove LED, that is on the BladeCenter unit and some components, for the specified command target. Possible return values are:
	• on
	• off
		`led -r`	`-T system:tap`
			`-T system:ncc[x]`
			`-T system:mux[x]`
			where *x* is the alarm panel module, network clock module, or multiplexer expansion module.

Table 49. led command (continued)

Function	What it does	Command	Valid targets
Display LED state for blade server and all sub-components	Displays the state of all LEDs on the specified blade server and its subcomponents. Possible return values are: • on • off • blink	`led -l`	`-T system:blade[x]` where *x* is the blade server number.

Turn off information LED	Turns off the information LED, that is on the BladeCenter unit and some components, for the specified command target	`led -info off`
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis account management (for BladeCenter unit, network clock module, multiplexer expansion module, or media tray)
		• Chassis log management (for BladeCenter unit, network clock module, multiplexer expansion module, or media tray)
		• Chassis administration (for BladeCenter unit, network clock module, multiplexer expansion module, or media tray)
		• Chassis configuration (for BladeCenter unit, network clock module, multiplexer expansion module, or media tray)
		• Blade administration (for blade server)
		• Blade configuration (for blade server)
		• Blade remote presence (for blade server)
		See "Commands and user authority" on page 8 for additional information.
			`-T system`
			`-T system:blade[x]`
			`-T system:ncc[x]` (for BladeCenter HT units only)
			`-T system:mux[x]` (for BladeCenter HT units only)
			`-T system:mt[x]`
			where *x* is the blade server, network clock module, multiplexer expansion module, or media tray number.

Table 49. led command (continued)

Function	What it does	Command	Valid targets

Set location LED state	Sets the state of the location LED, that is on the BladeCenter unit and some blade servers, for the command target.	`led -loc` *state*
		
		where *state* is
		• `on`
		• `off`
		• `blink`
		
		Note: A *state* of `blink` can only be used for the `-T system` command target and for the blade servers.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis account management (for BladeCenter unit)
		• Chassis log management (for BladeCenter unit)
		• Chassis administration (for BladeCenter unit)
		• Chassis configuration (for BladeCenter unit)
		• Blade administration (for blade server)
		• Blade configuration (for blade server)
		• Blade remote presence (for blade server)
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system`
			`-T system:blade[`*x*`]`
			
			where *x* is the blade bay number.

Table 49. led command (continued)

Function	What it does	Command	Valid targets
Turn on location LED for specified period of time	Turns on the location LED, that is on the BladeCenter unit and some blade servers, for a specified period of time before turning it off automatically.	`led -loc on -d` *time* where *time* is the number of seconds the location LED will remain lit. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management • Chassis log management • Chassis administration • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Example: To display the failure LED status for the blade server in bay 1, while the BladeCenter HT unit is set as the persistent command environment, at the `system>` prompt, type

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

To display status of the front-panel LEDs for the blade server in bay 1, while the BladeCenter HT unit is set as the persistent command environment, at the `system>` prompt, type

```
led -T blade[1]
```

To display status of all LEDs for the blade server in bay 1, while the BladeCenter HT unit is set as the persistent command environment, at the `system>` prompt, type

```
led -l -T blade[1]
```

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

```
system> led -T blade[1]
hs21_345678
Error:           off
Information:     off
KVM:             off
MT:              off
Location:      blink
system> led -T blade[1] -l
Component           Label              State              Location
Processor1          CPU1               Off                System board
Processor2          CPU2               Off                System board
Blade1              Fault              Off                Front panel
Blade2              Information        Off                Front panel
Blade3              Location           Blink              Front panel
Blade4              Power              On                 Front panel
                    KVM                Off                Front panel
Blade5              Media Tray         Off                Front panel
```

```
Blade7          Over Temp       Off             System board
Blade8          N/A             Off             System board
Blade1          N/A             Off             System board
Storage1        DASD1           Off             System board
Memory1         DIMM1           Off             System board
Memory2         DIMM2           Off             System board
Memory3         DIMM3           Off             System board
Memory4         DIMM4           Off             System board
Memory5         DIMM5           Off             System board
Memory6         DIMM6           Off             System board
Memory7         DIMM7           Off             System board
Memory8         DIMM8           Off             System board
Panel1          N/A             Off             System board
Expansion1      N/A             Off             FRU
                N/A             Off             FRU
Expansion2      N/A             Off             FRU
                N/A             Off             FRU
                N/A             Off             FRU
                N/A             Off             FRU
Expansion3      N/A             Off             FRU
system>
```

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 50. 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 an advanced management module:

```
system> list -l a
system
        mm[1]     primary
        mm[2]     standby
        power[1]
        power[2]
        power[3]
        power[4]
        blower[1]
        blower[2]
        switch[1]
        switch[2]
        switch[3]
        switch[4]
        blade[1]  Accounting
                sp
                cpu[1]
                cpu[2]
        blade[2]  HR
                sp
                cpu[1]
                cpu[2]
        blade[3]  Development
                sp
```

```
                cpu[1]
        blade[4]  Marketing
                sp
                ckvm
                cpu[1]
                cpu[2]
        blade[5]  Sales
                sp
                cpu[1]
                cpu[2]
        blade[6]  TechSupport
                sp
                exp[2]
                cpu[1]
                cpu[3]
                cpu[4]
        mt[1]
system>
```

Note: The BladeCenter S unit supports one management module. The `list` command for this unit does not refer to primary and standby management modules.

mcad command

This command configures and displays the auto-discovery setting for the BladeCenter unit management channel.

Note: See the *BladeCenter Advanced Management Module User's Guide* for additional information about management channel auto discovery.

Table 51. mcad command

Function	What it does	Command	Valid targets
Display management channel auto-discovery status for BladeCenter unit	Displays the auto-discovery setting for the BladeCenter unit management channel. Valid states include: • Enabled • Disabled	`mcad`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable / disable management channel auto-discovery for BladeCenter unit	Enable or disable management channel auto-discovery for the BladeCenter unit.	`mcad -e state` where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

To display the auto-discovery setting for the BladeCenter unit management channel, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
mcad -T mm[1]
```

To enable management channel auto-discovery for the BladeCenter unit, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
mcad -T mm[1] -e enabled
```

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

```
system> mcad -T mm[1]
-e disabled
system> mcad -T mm[1] -e enabled
OK
system>
```

modactlog command

This command displays information about modules installed in all of the blade servers.

Table 52. modactlog command

Function	What it does	Command	Valid targets
Display blade server module information and activity	Displays a list of modules installed in all blade servers, along with their activity and VPD information.	`modactlog`	`-T system`

Example: To view the list of modules installed in all blade servers, along with their activity and VPD information, while the BladeCenter unit is set as the default command target, at the `system>` prompt, type

```
modactlog
```

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

```
system> modactlog
Bay  Name                          FRU Number   FRU Serial No Manuf. ID Action   Timestamp
---  ----------------------------  ------------ ------------- --------- -------  -------------------
14   Fibre Channel Expansion Card  59P6624      J1RJH3CY18N   SLRM      Added    15:51:18 02/09/2007
11   cKVM card                     13N0842      YK328064418F  IBM       Added    15:51:07 02/09/2007
system>
```

Note: The BladeCenter S unit will also display information about the Direct Serial Attach Module and the storage modules.

monalerts command

This command displays and configures alerts that are monitored by the advanced management module.

Important: The `monalertsleg` command is no longer supported by the advanced management module firmware. Legacy alert monitoring that uses the `monalertsleg` command must transition to use of the `monalerts` command. Existing legacy alert settings are automatically mapped to the new alert categories as part of the transition.

Table 53. monalerts command

Function	What it does	Command	Valid targets
Display monitored alert states	Displays the state of all alerts being monitored by the management module.	`monalerts`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set state for enhanced legacy alert categories	Enables enhanced legacy alert categories. • If enhanced legacy alert categories are enabled, alerts are configured using the `monalerts` command. • If enhanced legacy alert categories can not be disabled once they have been enabled.	`monalerts -ec` *state* where *state* is `enabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set monitoring state for all critical alerts	Enables or disables monitoring of all critical alerts.	`monalerts -ca` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 53. monalerts command (continued)

Function	What it does	Command	Valid targets
Set monitoring state for blade device critical alerts	Enables or disables monitoring of blade device critical alerts.	`monalerts -cb` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for I/O-module critical alerts	Enables or disables monitoring of I/O-module critical alerts.	`monalerts -ciom` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for storage-module critical alerts (BladeCenter S units only)	Enables or disables monitoring of storage-module critical alerts.	`monalerts -cstg` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 53. monalerts command (continued)

Function	What it does	Command	Valid targets
Set monitoring state for chassis or system management critical alerts	Enables or disables monitoring of chassis or system management critical alerts.	`monalerts -ccsm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for cooling device critical alerts	Enables or disables monitoring of cooling device critical alerts.	`monalerts -ccd` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for power module critical alerts	Enables or disables monitoring of power module critical alerts.	`monalerts -cpm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 53. monalerts command (continued)

Function	What it does	Command	Valid targets
Set monitoring state for all warning alerts	Enables or disables monitoring of all warning alerts.	`monalerts -wa` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for blade device warning alerts	Enables or disables monitoring of blade device warning alerts.	`monalerts -wb` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for I/O-module warning alerts	Enables or disables monitoring of I/O-module warning alerts.	`monalerts -wiom` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 53. monalerts command (continued)

Function	What it does	Command	Valid targets
Set monitoring state for storage-module warning alerts (BladeCenter S units only)	Enables or disables monitoring of storage-module warning alerts.	`monalerts -wstg` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for chassis or system management warning alerts	Enables or disables monitoring of chassis or system management warning alerts.	`monalerts -wcsm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for event log warning alerts	Enables or disables monitoring of event log warning alerts.	`monalerts -wel` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 53. monalerts command (continued)

Function	What it does	Command	Valid targets
Set monitoring state for cooling device warning alerts	Enables or disables monitoring of cooling device warning alerts.	`monalerts -wcd` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for power module warning alerts	Enables or disables monitoring of power module warning alerts.	`monalerts -wpm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for all informational alerts	Enables or disables monitoring of all informational alerts.	`monalerts -ia` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 53. monalerts command (continued)

Function	What it does	Command	Valid targets
Set monitoring state for blade device informational alerts	Enables or disables monitoring of blade device informational alerts.	`monalerts -ib` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for I/O-module informational alerts	Enables or disables monitoring of I/O-module informational alerts.	`monalerts -iiom` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for storage-module informational alerts (BladeCenter S units only)	Enables or disables monitoring of storage-module informational alerts.	`monalerts -istg` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 53. monalerts command (continued)

Function	What it does	Command	Valid targets
Set monitoring state for chassis or system management informational alerts	Enables or disables monitoring of chassis or system management informational alerts.	`monalerts -icsm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for power state informational alerts	Enables or disables monitoring of power state (on/off) informational alerts.	`monalerts -ipon` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for inventory change informational alerts	Enables or disables monitoring of inventory change (installed components) informational alerts.	`monalerts -iinv` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 53. monalerts command (continued)

Function	What it does	Command	Valid targets
Set monitoring state for event log informational alerts	Enables or disables monitoring of event log informational alerts.	`monalerts -iel` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for network change informational alerts	Enables or disables monitoring of network change informational alerts.	`monalerts -inc` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for user activity informational alerts	Enables or disables monitoring of user activity informational alerts.	`monalerts -iua` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 53. monalerts command (continued)

Function	What it does	Command	Valid targets
Set monitoring state for cooling device informational alerts	Enables or disables monitoring of cooling device informational alerts.	`monalerts -icd` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set monitoring state for power module informational alerts	Enables or disables monitoring of power module informational alerts.	`monalerts -ipm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example: To enable monitoring of all critical alerts and event log warning alerts and disable monitoring of all informational alerts, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
monalerts -ca enabled -wel enabled -ia disabled
```

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

```
system:mm[1]> monalerts -ca enabled -wel enabled -ia disabled
OK
system:mm[1]>
```

mt (media tray) command

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

Table 54. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 54. mt command (continued)

Function	What it does	Command	Valid targets
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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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]>
```

nat command

This command sets and displays the network address table (NAT) settings for the specified I/O module.

Notes:

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

Table 55. nat command

Function	What it does	Command	Valid targets
Display I/O-module network protocol settings	Displays the network port settings for the specified I/O module. Returned values include those in Table 56 on page 244.	`nat`	`-T system:switch[x]` where *x* is the I/O-module bay number.
Reset I/O-module network protocol settings	Resets all network address table settings for the specified I/O module to the default values. Default values are in Table 56 on page 244. You must activate any changes to the network protocol settings before they take effect.	`nat -reset` This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.
Activate I/O-module network protocol settings	Activates all network port settings for the specified I/O module, putting them into effect.	`nat -activate` This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.

Table 55. nat command (continued)

Function	What it does	Command	Valid targets
Set protocol name for row in I/O-module NAT table	Sets a protocol name for the specified row in the NAT table for the specified I/O module.	`nat -`*index* `-pn` *protocol_name* where: • *index* is a number from 1 to 10 that corresponds to a row in the NAT table. • *protocol_name* is a text string with a maximum length of 19 characters and no spaces. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.
Set protocol ID for row in NAT table	Sets a protocol ID for the specified row in the NAT table for the specified I/O module.	`nat -`*index* `-pi` *protocol_id* where: • *index* is a number from 1 to 10 that corresponds to a row in the NAT table. • *protocol_id* is TCP or UDP. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 55. nat command (continued)

Function	What it does	Command	Valid targets
Set internal port number for row in NAT table	Sets the internal port number for the specified row in the NAT table for the specified I/O module.	`nat -`*index* `-ip` *port_number* where: • *index* is a number from 1 to 10 that corresponds to a row in the NAT table. • *port_number* is between 1 and 65534, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.
Set external port number for row in NAT table	Sets the external port number for the specified row in the NAT table for the specified I/O module.	`nat -`*index* `-ep` *port_number* where: • *index* is a number from 1 to 10 that corresponds to a row in the NAT table. • *port_number* is between 1000 and 65534, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 55. nat command (continued)

Function	What it does	Command	Valid targets
Set state for row in NAT table	Enables or disables the specified row in the NAT table for the specified I/O module.	`nat -`*index* `-en` *state* where: • *index* is a number from 1 to 10 that corresponds to a row in the NAT table. • *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 56. Default NAT table values for nat command

Index	Protocol Name	Protocol ID	Internal Port	External Port	State
1	HTTP	TCP	80	1080	Enabled
2	TELNET	TCP	23	1023	Enabled
3	HTTPS	TCP	43	1043	Enabled
4	SSH	TCP	22	1022	Enabled
5	SNMP	UDP	161	1161	Enabled
6 through 10	Unset				

Example:

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

```
nat
```

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

```
system:switch[3]> nat
Index   Protocol Name   Protocol ID   Internal Port   External Port   Enabled
1       HTTP            TCP           80              1080            enabled
2       TELNET          TCP           23              1023            enabled
3       HTTPS           TCP           43              1043            enabled
4       SSH             TCP           22              1022            enabled
5       SNMP            UDP           161             1161            enabled
system:switch[3]>
```

ntp (network time protocol) command

This command configures and displays the management-module network time protocol (NTP) settings.

Table 57. ntp command

Function	What it does	Command	Valid targets
Display management module NTP settings	Displays the NTP settings for the specified I/O module. Possible return values are: • -en *state* (enabled, disabled) • -i *ipaddress/hostname* (IP address or hostname of the NTP server) • -f *update_frequency* (NTP update frequency, in minutes) • -v3en *state* (enabled, disabled) • -v3 *key_info* (NTP v3 authentication entry)	`ntp`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable / disable NTP	Enables or disables NTP for the management-module.	`ntp -en state` where *state* is enabled or disabled. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
NTP server IP address or hostname - set	Checks syntax and sets the IP address or hostname of the NTP server.	`ntp -i ipaddress/hostname` where *ipaddress/hostname* is the IP address or hostname of the NTP server. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 57. ntp command (continued)

Function	What it does	Command	Valid targets
NTP update frequency - set	Sets how often the management module clock is automatically updated by the NTP server.	`ntp -f` *time* where *time* is the NTP update frequency, in minutes with a maximum value of 45000. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
NTP - Enable / disable V3 authentication	Enables or disables V3 authentication between the management-module and the NTP server. **Note:** The NTP server authentication key must be set, using the ntp -v3 command option, before enabling V3 authentication.	`ntp -v3en` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
NTP server authentication key - set	Sets the v3 authentication key that the management module uses to access the NTP server. The authentication key contains the following values: • Key index: An NTP server can be configured with one or more key entries. The key index specifies which key the server expects the client to authenticate with. • Key type: The advanced management module supports only the MD5 key type. • Key: The key is an 8-character ASCII string.	`ntp -v3` *key_index key_type key* where: • *key_index* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. • *key_type* is `M` (MD5). • *key* is a 8-character ASCII string. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 57. ntp command (continued)

Function	What it does	Command	Valid targets
NTP clock- synchronize	Synchronizes the management-module clock with the NTP server. (You must configure a valid NTP server before you can synchronize.)	`ntp -synch` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

To display NTP settings for the management module, while management module 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
ntp
```

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

```
system:mm[2]> ntp
-en enabled
-i timeserver
-f 5
-v3en disabled
-v3 Not configured
NTP is disabled.
system:mm[2]>
```

ping command

This command tests the internal communication path between the advanced management module and a BladeCenter component by sending it a ping request.

Table 58. ping command

Function	What it does	Command	Valid targets
Display I/O module IP addresses	Displays a list of IP addresses for the specified I/O module.	`ping -i` This command can only be run by users who have one or more of the following command authorities: • Supervisor, • Operator (general operator, not chassis operator) • I/O module administration, • I/O module configuration • I/O module operator See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.
Ping IP address	Pings the specified IP address to test communication between it and the management module. **Note:** This command tests communication paths, including IP addresses outside of the BladeCenter unit.	`ping -i` *ip_address* where *ip_address* is the IP address for a component installed in the BladeCenter unit. All users can attempt to ping a specific IP address.	This command will attempt to ping the specified IP address, regardless of command target, including IP addresses outside of the BladeCenter unit.

Table 58. ping command (continued)

Function	What it does	Command	Valid targets
Ping I/O-module IP address	Pings the specified IP address of an I/O module to test communication.	`ping -i` *index* where *index* is the index number for the I/O-module IP address to ping. Use the `ping -i` command, with no arguments, to list available IP addresses and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor, • Operator (general operator, not chassis operator) • I/O module administration, • I/O module configuration • I/O module operator See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Example: To display list of IP addresses for the I/O module in bay 1, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
ping -i -T switch[1]
```

To ping the first IP address of the I/O module in bay 1 using an index number, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
ping -i 1 -T switch[1]
```

To ping the first IP address of the I/O module in bay 1 using an IP address, while the BladeCenter unit is set as the persistent command environment, at the `system>` prompt, type

```
ping -i 10.13.3.171
```

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

```
system> ping -i -T switch[1]
1. 10.13.3.171
2. FE80:0000:0000:0000:0218:B1FF:FE9F:9000
system> ping -i 1 -T switch[1]
Reply from 10.13.3.171: bytes=64 time=4.150ms
Reply from 10.13.3.171: bytes=64 time=0.392ms
Reply from 10.13.3.171: bytes=64 time=0.400ms
Reply from 10.13.3.171: bytes=64 time=0.389ms
system> ping -i 10.13.3.171
Reply from 10.13.3.171: bytes=64 time=0.418ms
Reply from 10.13.3.171: bytes=64 time=0.417ms
Reply from 10.13.3.171: bytes=64 time=0.362ms
Reply from 10.13.3.171: bytes=64 time=6.90ms
system>
```

pmpolicy command

This command displays and sets the power management policies for the BladeCenter unit.

Table 59. pmpolicy command

Function	What it does	Command	Valid targets
Display power management policy	Displays the current power management policy for all domains.	`pmpolicy`	`-T system`
Display power management policy for a BladeCenter S unit	Displays both the current and available power management policies for a BladeCenter S unit, that has a single power domain.	`pmpolicy` *domain* where *domain* is `pd`	`-T system`
Display power management policy for domain	Displays both the current and available power management policies for the specified power domain in a BladeCenter unit that supports two power domains.	`pmpolicy` *domain* where *domain* is: • `pd1` (power domain 1) • `pd2` (power domain 2)	`-T system`
Set power management policy for domain	Set power management policy for specified power domain.	`pmpolicy` *domain* `-pm` *policy* where *domain* is: • `pd1` (power domain 1) • `pd2` (power domain 2) where *policy* is: • `acred` (ac power source redundancy policy - BladeCenter S units only) • `acredov` (ac power source redundancy policy, with blade throttling - BladeCenter S units only) • `redwoperf` (power module redundancy, no oversubscription) • `redwperf` (power module redundancy with power throttling) • `nonred` (no power management policy) This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system`

Example:

To view the current policy and the available policies for a power domain 1, while the BladeCenter unit is set as the persistent command environment, at the system> prompt, type

```
pmpolicy pd1
```

The following example shows the output generated by this command.

```
system> pmpolicy pd1

Power Domain 1
--------------

*** Current Policy ***

Power Management Policy:
        Power Module Redundancy with Blade Throttling Allowed (redwperf)
Description:
        Very similar to Power Module Redundancy. This policy allows you to
        draw more total power; however, capable blades may be allowed to
        throttle down if one Power Module fails.
Power Supply Failure Limit:       1
Maximum Power Limit (Watts):   3380
Your Estimated Utilization:       5%

*** Available Policies ***

Power Management Policy:
        Power Module Redundancy (redwoperf)
Description:
        Intended for a single AC power source into the chassis where each
        Power Module is on its own dedicated circuit. Total allowed power
        draw is limited to one less than the number of Power Modules when
        more than one Power Module is present. One Power Module can fail
        without affecting blade operation. Multiple Power Module failures can
        cause the chassis to power off. Note that some blades may not be
        allowed to power on if doing so would exceed the policy power limit.
Power Supply Failure Limit:       1
Maximum Power Limit (Watts):   2880
Your Estimated Utilization:       6%

Power Management Policy:
        Basic Power Management (nonred)
Description:
        Total allowed power is higher than other policies and is limited only
        by the total power capacity of all the Power Modules up to the
        maximum of chassis power rating. This is the least conservative
        approach, since it does not provide any protection for AC power
        source or Power Module failure. If any single power supply fails,
        blade and/or chassis operation may be affected.
Power Supply Failure Limit:       0
Maximum Power Limit (Watts):   3520
Your Estimated Utilization:       5%

NOTE:
 Power Supply Failure Limit: This is the maximum number of power supplies
                             that can fail while still guaranteeing the
                             operation of the domain in the selected policy.
 Your Estimated Utilization: The estimated utilization is based on the maximum
                             power limit allowed in this policy and the current
                             aggregated power in use of all components in the
                             domain.

system>
```

portcfg command

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

Table 60. portcfg command

Function	What it does	Command	Valid targets
Display management-module serial port configuration	Displays the current configuration of the management-module serial port. Possible return values are: • -b *baud_rate* • -p *parity* • -s *stop_bits*	`portcfg -com1`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management-module serial port baud rate	Checks syntax and sets the baud (communications) rate of the management-module serial port.	`portcfg -com1 -b` *baud_rate* where *baud_rate* is 2400, 4800, 9600, 19200, 38400, or 57600. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management-module serial port parity	Checks syntax and sets the parity of the management-module serial port.	`portcfg -com1 -p` *parity* where *parity* is • `none` • `odd` • `even` • `mark` • `space` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 60. portcfg command (continued)

Function	What it does	Command	Valid targets
Set management-module serial port stop bits	Checks syntax and sets the number of stop bits for the management-module serial port.	`portcfg -com1 -s` *stop_bits* where *stop_bits* is 1 or 2. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

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

```
portcfg -com1
```

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

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

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

```
system:mm[1]> portcfg -com1
-b 2400
-p none
-s 1
system:mm[1]> portcfg -com1 -b 9600
These configuration changes will become active after the next reset of the MM.
system:mm[1]>
```

ports command

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

Note: Changes to the `-ftpdp`, `-ftpe`, `-ftpp`, `-httpp`, `-httpsp`, `-rpp`, `-smashse`, `-smashsp`, `-smashte`, `-smashtp`, `-snmp1ae`, `-snmp3ae`, `-snmpap`, `-snmpte`, `-snmptp`, `-sshe`, `-sshp`, `-tcme`, `-telnete`, `-telnetp`, `-telnett`, or `-tftpp` settings become active immediately. Changes to the remaining settings become active after the next reset of the advanced management module.

Table 61. ports command

Function	What it does	Command	Valid targets
Display network port settings	Displays the network port settings for the management module. Returned values are: • -ftpp *FTP_prt_num* • -ftpdp *FTP_data_prt_num* • -httpp *HTTP_prt_num* • -httpsp *HTTPS_prt_num* • -rpp *rpp_prt_num* • -slpp *SLP_prt_num* • -smashsp *secSMASH_SSH_prt_num* • -smashtp *SMASH_telnet_prt_num* • -snmpap *SNMP_agent_prt_num* • -snmptp *SNMP_traps_prt_num* • -sshp *SSH_prt_num* • -stcmp *secure_tcmp* • -tcmp *TCP_cmd_md_port* • -telnetp *_Telnet_prt_num* • -tftpp *TFTP_prt_num* • -ftpe *FTP_state* • -httpse *HTTPS_prt_state* • -kvme *KVM_state* • -ntpe *NTP_state* • -rde *rd_state* • -rdoce *rdoc_state* • -slpe *SLP_state*. • -smashse *sec_SMASH_SSH_state* • -smashte *SMASH_telnet_state* • -snmp1ae *SNMPv1_agent_state* • -snmp3ae *SNMPv3_agent_state* • -snmpte *SNMP_traps_state* • -sshe *SSH_prt_state* • -stcme *secure_TCP_cmd_mode* • -tcme *TCP_cmd_mode_state* • -telnete *Telnet_prt_state-* • -tftpe *TFTP_state* • -ftpt *FTP_timeout* • -tcmt *TCP_cmd_mode_timeout* • -telnett *Telnet_prt_timeout*	`ports`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display open management module ports	Displays the management module ports that are currently open.	`ports -open`	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Reset network port settings	Resets all network port settings for the management module to the default values. Default values are: • -ftpp: 21 • -ftpdp: 20 • -httpp: 80 • -httpsp: 443 • -rpp: 3900 • -slpp: 427 • -tcmp: 6090 • -smashtp: 50023 • -smashsp: 50022 • -snmpap: 161 • -snmptp: 162 • -sshp: 22 • -stcmp: 6091 • -telnetp: 23 • -tftpp: 69	`ports -reset` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set FTP port number	Sets the port number for the management module FTP port.	`ports -ftpp` *FTP_prt_num* where *FTP_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set FTP data port number	Sets the port number for the management module FTP data port.	`ports -ftpdp` *FTP_data_prt_num* where *FTP_data_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Set HTTP port number	Sets the port number for the management module HTTP port.	`ports -httpp` *HTTP_prt_num* where *HTTP_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set HTTPS port number	Sets the port number for the management module HTTPS port.	`ports -httpsp` *HTTPS_prt_num* where *HTTPS_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set Remote Presence port number	Sets the remote presence port number for the management module remote presence port.	`ports -rpp` *rpp_prt_num* where *rpp_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Set SLP port number	Sets the SLP port number.	`ports -slpp` *SLP_prt_num* where *SLP_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set SMASH Telnet port number	Sets the port number for the management module SMASH command-line processor over Telnet port.	`ports -smashtp` *SMASH_telnet_prt_num* where *SMASH_telnet_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Set SNMP agent port number	Sets the port number for the management module SNMP agent port.	`ports -snmpap` *SNMP_agent_prt_num* where *SNMP_agent_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set SNMP traps port number	Sets the port number for the management module SNMP traps port.	`ports -snmptp` *SNMP_traps_prt_num* where *SNMP_traps_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Set command mode port number	Sets the TCP command mode port number.	`ports -tcmp` *TCP_cmd_md_prt_num* where *TCP_cmd_md_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set secure command mode port number	Sets the secure TCP command mode port number.	`ports -stcmp` *secure_tcmp* where *secure_tcmp* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set SSH port number	Sets the port number for the management module SSH port.	`ports -sshp` *SSH_prt_num* where *SSH_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Set Telnet port number	Sets the port number for the management module Telnet port.	`ports -telnetp` *Telnet_prt_num* where *Telnet_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set TFTP port number	Sets the port number for the management module TFTP port.	`ports -tftpp` *TFTP_prt_num* where *TFTP_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable FTP	Enables or disables FTP for the management module.	`ports -ftpe` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Enable / disable HTTPS port	Enables or disables the management module HTTPS port.	`ports -httpse` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set KVM port state	Sets the KVM port state to on or off.	`ports -kvme` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable NTP	Enables or disables NTP for the management module.	`ports -ntpe` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Enable / disable RDE	Enables or disables remote disk for the management module.	`ports -rde` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable RDOCE	Enables or disables remote disk on card for the management module.	`ports -rdoce` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disables SLP	Enables or disables SLP for the management module.	`ports -slpe` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Enable / disable secure SMASH over SSH	Enables or disables the secure SMASH command-line processor over SSH for the management module.	`ports -smashse` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable SMASH over Telnet	Enables or disables SMASH command-line processor over Telnet for the management module.	`ports -smashte` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable SNMPv1 agent	Enables or disables the SNMPv1 agent for the management module.	`ports -snmp1ae` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Enable / disable SNMPv3 agent	Enables or disables the SNMPv3 agent for the management module.	`ports -snmp3ae` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable SNMP traps	Enables or disables the SNMP traps for the management module.	`ports -snmpte` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable SSH port	Enables or disables the management module SSH port.	`ports -sshe` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Enable / disable TCP command mode	Enables or disables the TCP command mode for the management module.	`ports -tcme` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set number of TCP command mode connections	Turns the TCP command mode on or off, or sets the maximum number of connections explicitly. **Note:** Any number of connections (1 through 20) displays a status of on. Zero connections displays a status of off.	`ports -tcme` *port_mode* where *port_mode* is `on` (1 connection), `off` (no connections), or a number between 0 and 20, inclusive, that indicates the maximum number of TCP session connections. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable secure TCP command mode	Enables or disables the secure TCP command mode for the management module.	`ports -stcme` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Set number of secure TCP command mode connections	Turns the secure TCP command mode on or off, or sets the maximum number of connections. **Notes:** • On a write operation, the maximum number of connections can be set explicitly (0-20), or it can be turned on (1 connection) or off (0 connections). • On a read operation, off means 0 connections, and on means 1 or more connections. • The total session count of TCM and STCM is limited to 20.	`ports -stcme` *port_mode* where *port_mode* is `on` (1 connection), `off` (no connections), or a number between 0 and 20, inclusive, that indicates the maximum number of TCP session connections. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable Telnet port	Enables or disables the management module Telnet port.	`ports -telnete` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable TFTP	Enables or disables TFTP for the management module.	`ports -tftpe` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Set FTP timeout	Sets the FTP timeout value for the management module.	`ports -ftpt` *timeout* where *timeout* is from 0 seconds (no timeout) to 4294295967 seconds, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set TCP command-mode timeout	Sets the TCP command-mode timeout value for the management module.	`ports -tcmt` *timeout* where *timeout* is from 0 seconds (no timeout) to 4294295967 seconds, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set Telnet port timeout	Sets the Telnet port timeout value for the management module.	`ports -telnett` *timeout* where *timeout* is from 0 seconds (no timeout) to 4294295967 seconds, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Display network port settings for I/O module	Displays the network port settings for the I/O module. These settings can include: • cable compatibility • cable length • cable type • data rate • label • port index • port media • port width • protocol • speed • speed setting • available speeds • state • state setting • type • vendor **Note:** Other device specific values might be returned.	`ports`	`-T system:switch[x]` where *x* is the I/O-module bay number.
Enable or disable port for I/O module	Enables or disables specified port on specified I/O module.	`ports -port_index -state state` where • *port_index* is from 1 to 65535, inclusive. • *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O module bay number.

Table 61. ports command (continued)

Function	What it does	Command	Valid targets
Sets speed of port for I/O module	Sets speed of specified port on I/O modules that support this feature.	`ports -`*port_index* `-speed` *speed_setting* where • *port_index* is from 1 to 65535, inclusive. • *speed_setting* specifies the port speed, in terms of: – *multiplier* – *units*, `m` or `g` for megabits or gigabits – *duplex mode*, `h` or `f` for half or full For example, `100mh` sets the port speed to 100 Mbps half-duplex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Example:

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

```
ports
```

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

```
ports -ftpe off
```

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

```
system:mm[1]> ports
-ftpp 21
-ftpdp 20
-httpp 80
-httpsp 443
-rpp 3900
-slpp 427
-smashsp 50022
-smashtp 50023
-snmpap 161
-snmptp 162
-sshp 22
```

```
-stcmp 6091
-tcmp 6090
-telnetp 23
-tftpp 69
-ftpe on
-httpse off
-kvme on
-ntpe off
-rde off
-rdoce on
-slpe on
-smashse on
-smashte on
-snmp1ae on
-snmp3ae on
-snmpte on
-sshe off
-stcme off
-tcme off
-telnete on
-tftpe off
-tcmt 0
-telnett 10000
-ftpt 300
system:mm[1]> ports -ftpe off
Changes to -sshe, -sshp, -smashse, -smashte, -smashsp, -telnete, -telnetp,
-telnett, -smashtp, -snmpte, -tcme, -tcmp, -tcmt, -stcme, -stcmp, -rpp,
-httpp,-httpse, -httpsp, -ftpe or -tftpe will become active immediately.
OK
system>
```

power command

This command turns on and turns off blade servers and I/O modules. For advanced management modules installed in BladeCenter HT units, it also turns on and turns off the alarm panel module and network clock module.

Table 62. power command

Function	What it does	Command	Valid targets

Power on	Turns on the specified command target.	`power -on`
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Blade administration (for blade server)
		• I/O module administration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system:blade[x]`
			`-T system:switch[x]`
			
			`-T system:tap` (BladeCenter HT units only)
			
			`-T system:ncc[x]` (BladeCenter HT units only)
			
			where *x* is the blade server, I/O-module bay, or network clock module number.

Power on to command console	Opens a command console with an SOL session when the specified blade server is turned on.	`power -on -c` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration and blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade server bay number.

Power off	Turns off the specified command target.	`power -off`
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Blade administration (for blade server)
		• I/O module administration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system:blade[x]`
			`-T system:switch[x]`
			
			`-T system:tap` (BladeCenter HT units only)
			
			`-T system:ncc[x]` (BladeCenter HT units only)
			
			where *x* is the blade server, I/O-module bay, or network clock module number.

Table 62. power command (continued)

Function	What it does	Command	Valid targets
Shutdown and power off blade server	Shuts down the operating system and turns off the specified blade server.	`power -softoff` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-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`
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Blade administration (for blade server)
		• I/O module administration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional information.
			`-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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration and blade remote presence See "Commands and user authority" on page 8 for additional information.	`-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.

Table 62. power command (continued)

Function	What it does	Command	Valid targets
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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 62. power command (continued)

Function	What it does	Command	Valid targets
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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade server bay number.
Set automatic power-on policy for BladeCenter unit	Sets the automatic power-on policy for the BladeCenter unit. Changes to the power-on policy setting take effect after the next cold start of the BladeCenter unit.	`power -ap` *policy* where *policy* is: • `restore`: all blade servers that were previously on will be powered on • `auto`: when power is applied to the BladeCenter unit, all blade servers will be powered on • `manual`: all blade servers will remain off until manually powered on This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system`
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.

Table 62. power command (continued)

Function	What it does	Command	Valid targets
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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.
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]>
```

rdoc command

This command displays volume information for remote disk-on-card local storage on the advanced management module. The command also allows you to mount, unmount, or map a file image to this device.

Table 63. rdoc command

Function	What it does	Command	Valid targets
Display advanced management module volume information	Displays the remote disk-on-card volume information for local storage on the advanced management module. Volume information returned includes: • Health condition • Size • Amount of free space	`rdoc`	`-T system:mm[x]` where *x* is the primary management module bay number.
Map file as advanced management module volume image	Maps the specified file as the active image for the remote disk-on-card local storage volume on the advanced management module.	`rdoc -map filename` where *filename* is the name of the file to be mapped as the active remote disk-on-card image. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management module bay number.
Mount advanced management module volume	Mounts the remote disk-on-card local storage volume on the advanced management module. **Note:** The advanced management module will only mount the first partition, if the volume has multiple partitions.	`rdoc -mount` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management module bay number.
Unmount advanced management module volume	Unmounts the remote disk-on-card local storage volume on the advanced management module.	`rdoc -unmount` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management module bay number.

Example: To display volume information for local storage on the advanced management module in bay 1, while this management module is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
rdoc
```

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

```
system:mm[1]> rdoc
Volume 0
Health: good
Volume Size: 73108480 (Bytes)
Free Size: 69120000 (Bytes)
system:mm[1]>
```

read command

This command restores the management-module configuration that was previously saved to the BladeCenter unit chassis or to a file.

Configurations are saved to the BladeCenter unit chassis or to a file using the "write command" on page 413.

Table 64. read command

Function	What it does	Command	Valid targets
Display management-module automatic configuration setting	Displays the automatic configuration setting (`-auto` command option) of the management module.	`read`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Restore management-module configuration from BladeCenter unit midplane	Restores the management-module configuration from an image that was previously saved to the BladeCenter unit midplane.	`read -config chassis` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Restore management-module configuration from file (no encryption)	Restores the management-module configuration from an image that was previously saved to a file while data encryption was not enabled for the BladeCenter unit.	`read -config file -l` *filename* `-i` *ip_address* where: • *filename* is the name of the configuration file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the configuration file is located. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 64. read command (continued)

Function	What it does	Command	Valid targets
Restore management-module configuration from file (encryption)	Restores the management-module configuration from an image that was previously saved to a file while data encryption was enabled for the BladeCenter unit. **Note:** When a configuration file was created with a pass-phrase (encryption enabled), if this configuration file is restored on the same management module, the pass-phrase entered during restoration is ignored.	`read -config file -l` *filename* `-i` *ip_address* `-p` *passphrase* where: • *filename* is the name of the configuration file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the configuration file is located. • *"passphrase"* is the quote-delimited pass-phrase that was used to save the original configuration file. Maximum pass-phrase length is 1600 characters. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable automatic management-module configuration	Enables automatic configuration of the management module, based on settings stored in the BladeCenter unit midplane, when the management module is installed. **Note:** The -auto option can only be used when the management-module configuration was stored to the BladeCenter unit midplane.	`read -config chassis -auto on` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 64. read command (continued)

Function	What it does	Command	Valid targets
Disable automatic management-module configuration	Disables automatic configuration of the management module, based on settings stored in the BladeCenter unit midplane, when the management module is installed.	`read -config chassis -auto off` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

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

```
read -config chassis
```

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

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

remacccfg command

This command displays and configures the remote presence access to one of the BladeCenter units from the chassis.

Table 65. remacccfg command

Function	What it does	Command	Valid targets
Display remote presence access	Displays the current settings for the remote presence access.	`remacccfg` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set remote presence disconnection mode	Sets the remote presence disconnection mode. **Notes:** • The current connected client cannot be disconnected if no mode is specified (nodisconnection as default). • If forcedisconnection or accessrequest is specified, the current connected client can be disconnected directly without any request or after getting a disconnection request and the disconnection is allowed.	`remacccfg -mode` *mode* where *mode* is nodisconnection, forcedisconnection, or accessrequest. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set session timeout interval	Sets the custom value for the remote presence session timeout. **Note:** If no value is specified, the default value of 60 minutes will be used.	`remacccfg -sto` *timeout* where *timeout* is from 1 to 30,000 minutes, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 65. remacccfg command (continued)

Function	What it does	Command	Valid targets
Set session request timeout interval	Sets the custom value for the remote presence session request timeout. **Note:** If no value is specified, the default value of 60 seconds will be used.	`remacccfg -srto` *timeout* where *timeout* is from 1 to 255 seconds, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set session request retry timeout interval	Sets the custom value for the remote presence session request retry timeout. **Note:** If no value is specified, the default value of 60 seconds will be used.	`remacccfg -srrto` *timeout* where *timeout* is from 1 to 255 seconds, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set session lost timeout interval	Sets the custom value for the remote presence session lost timeout. **Note:** If no value is specified, the default value of 10 minutes will be used.	`remacccfg -slto` *timeout* where *timeout* is from 1 to 255 minutes, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

remotechassis command

This command displays and manages the list of BladeCenter units that the management module discovers on the network.

Note: The advanced management module that runs the remotechassis command is also included in all lists.

Table 66. remotechassis command

Function	What it does	Command	Valid targets
Display complete list	Displays a list of all BladeCenter units that the management module discovers on the network. The list includes the following information about each BladeCenter unit: • Name • IP address • Status • Firmware level • Type • Serial number • FRU number • Chassis serial number • Chassis FRU number • Chassis machine-type model (MTM) • Chassis UUID	`remotechassis`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display list grouped by health status	Displays a list of names for BladeCenter units that the management module discovers on the network. The list is grouped by health status.	`remotechassis -health`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display list filtered by IP address	Displays a list of BladeCenter units that the management module discovers on the network, filtered by the specified IP address. The list includes the following information about each BladeCenter unit: • Name • IP address • Status • Firmware level • Type • Serial number • FRU number • Chassis serial number • Chassis FRU number • Chassis machine-type model (MTM) • Chassis UUID	`remotechassis -ip ip_address` where *ip_address* is an IP address pattern that uses the asterisk (*) as a wildcard (for example; 201.47.123.*).	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 66. remotechassis command (continued)

Function	What it does	Command	Valid targets
Display list filtered by name	Displays a list of BladeCenter units that the management module discovers on the network, filtered by the specified name. The list includes the following information about each BladeCenter unit: • Name • IP address • Status • Firmware level • Type • Serial number • FRU number • Chassis serial number • Chassis FRU number • Chassis machine-type model (MTM) • Chassis UUID	`remotechassis -name` *name* where *name* is a name pattern that uses the asterisk (*) as a wildcard (for example; WebServer*).	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Clear list	Clears the list of BladeCenter units that the management module discovered on the network.	`remotechassis -clear`	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

To list all BladeCenter units on the network with a name starting with "WebServer", while management module 1, that does not support IPv6, is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
remotechassis -name WebServer*
```

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

```
system:mm[1]> remotechassis -name WebServer*
Running chassis discovery...
-----------------------------------------------
Name:           WebServer001
IP:             145.48.204.212
Status:         normal
Firmware:       BPET25L,CNETMNUS.PKT,01-08-07,37,1
Type:           management-module
Serial:         0J1M9E585630
FRU:            25R5777
Chassis Serial: 23A2343
Chassis FRU:    25R5780R5780
Chassis MTM:    885222Z
Chassis UUID:   4E349451FA8011D9B10C89E0183AD13D
-----------------------------------------------
Name:           WebServer002
IP:             145.48.204.222
Status:         normal
Firmware:       BPET25L,CNETMNUS.PKT,01-08-07,37,1
Type:           management-module
Serial:         0J1M9E585656
FRU:            25R5777
Chassis Serial: 23A2356
Chassis FRU:    25R5780R5780
```

```
Chassis MTM:    885222Z
Chassis UUID:   4E325951FA8011D9B86C89E0183AD02D
-----------------------------------------------
system:mm[1]>
```

To list all BladeCenter units on the network with a name starting with "SYSTEM*", while management module 1, that supports IPv6, is set as the persistent command environment, at the system:mm[1]> prompt, type

```
remotechassis -name SYSTEM*
```

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

```
system:mm[1]> remotechassis -name SYSTEM*
Running chassis discovery...
-----------------------------------------------
Name:           SYSTEM
IP:             10.13.1.190
IPv6:           2002:1013::211:25ff:fec3:227c
                2001:1013::211:25ff:fec3:227c
                2000:1013::211:25ff:fec3:227c
                fe80::211:25ff:fec3:227c
                2000:1013::a1be:a348:7672:2def
                2000:1013::1:191
Status:         critical
Firmware:       BPET002,CNETMNUS.PKT,02-17-10,1
Type:           management-module
Serial:         YK118165A117
FRU:            39Y9661
Chassis Serial: KQWPLB9
Chassis FRU:    44X2302
Chassis MTM:    8852HC1
Chassis UUID:   E13112E1829448E29999DA2066681D89
-----------------------------------------------
Name:           SYSTEM
IP:             10.13.1.30
IPv6:           2000:1013::fc58:325c:c8b4:9c4c
                2000:1013::214:5eff:fed0:2e1c
                2000:1013::1:30
                fe80::5652:ff:fe69:d763
                2002:1013::211:25ff:fec3:8cfa
                2001:1013::211:25ff:fec3:8cfa
                2000:1013::211:25ff:fec3:8cfa
                fe80::211:25ff:fec3:8cfa
Status:         attention
Firmware:       BPET54A,CNETMNUS.PKT,02-17-10,84
Type:           management-module-telco
Serial:         YK118269Y115
FRU:            39Y9661
Chassis Serial: 23A0052
Chassis FRU:    42C3673
Chassis MTM:    87501RZ
Chassis UUID:   B5BAEC01A10B11DB9F3BC1BE8FFF3B3C
-----------------------------------------------
system:mm[1]>
```

reset command

This command resets blade servers, blade server integrated system management processors (service processors), I/O modules, or the primary management module. For advanced management modules installed in BladeCenter HT units, it also resets the multiplexer expansion module.

Table 67. reset command

Function	What it does	Command	Valid targets

Reset	Performs an immediate reset and restart of the specified device.	`reset`
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Blade administration (for blade server or blade server ISMP)
		• I/O module administration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system:blade[x]`
			`-T system:switch[x]`
			`-T system:blade[x]:sp`
			
			where *x* is the blade server or I/O-module bay number.

Reset primary management module	Performs an immediate reset and restart of the primary management module.	`reset` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Reset standby management module	Performs an immediate reset of the standby management module. **Note:** This option does not apply to the BladeCenter S unit.	`reset -standby` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number. **Note:** Even though this command resets the standby management module, it still must specify the primary management module as the command target.

Table 67. reset command (continued)

Function	What it does	Command	Valid targets
Reset blade server to command console	Opens a command console with an SOL session when the specified blade server is reset.	`reset -c` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration and blade remote presence See "Commands and user authority" on page 8 for additional information.	`-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 (stanfdby) 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. **Note:** This option does not apply to the BladeCenter S unit.	`reset -f` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` `-T system:mux[x]` (for advanced management modules in BladeCenter HT units only) where *x* is the primary management-module bay or multiplexer expansion module number.
Reset management module with forced failover	Resets the primary management module with failover to the standby management module. An error message is displayed if you try to force failover for a management module when a standby management module is not installed or if the firmware in the primary management module is updating. **Note:** This option does not apply to the BladeCenter S unit.	`reset -force` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration See "Commands and user authority" on page 8 for additional information.	`-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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.

Table 67. reset command (continued)

Function	What it does	Command	Valid targets
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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.
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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration and blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade server bay number.

Table 67. reset command (continued)

Function	What it does	Command	Valid targets
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 JS21 blade server, the command performs an immediate reset and restart of the specified JS21 blade server and clears all settings stored in non-volatile memory (NVRAM). • For all other blade servers, this option is not available.	`reset -clr` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration and blade remote presence See "Commands and user authority" on page 8 for additional information.	`-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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration and blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade server bay number.
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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration and blade remote presence See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade server bay number.

Table 67. reset command (continued)

Function	What it does	Command	Valid targets
Restart blade server and enter SMS menu	Performs an immediate reset and restart of the specified blade server and enters the System Management Services (SMS) firmware menu. **Note:** This option applies to all JS*xx* blade servers other than the JS20 blade server.	`reset -sms` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-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>
```

scale command

This command sets and displays the partition control and configuration settings for multiple blade servers or nodes in a scalable complex, for blade servers installed in the BladeCenter unit that support this feature.

Note:

- The scale command will execute only on blade servers that support scalable complexes.
- All blade servers in a scalable complex must be at the same firmware level. When scripting firmware updates for blade servers in a scalable complex, make sure that the `update` commands are included for each node in the complex.

Table 68. scale command

Function	What it does	Command	Valid targets
Display all scalable complex information	Displays all scalable complex information for the BladeCenter unit.	`scale`	`-T system`
Display information for specific scalable complex	Displays information for the specified scalable complex. **Note:** • The *complex_id* is found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -compid` *complex_id* where *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex.	`-T system`
Display information for specific node in a scalable complex	Displays information for a specific node in the scalable complex. **Note:** • The *complex_id* and *node_id* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -node` *node_id* `-compid` *complex_id* where : • *node_id* is the checksum or blade server bay number, of the node. • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex.	`-T system`
Display information for specific partition in a scalable complex	Displays information for a specific node in the scalable complex. **Note:** • The *complex_id* and *partition_id* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -compid` *complex_id* `-partition` *partition_id* where : • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. • *partition_id* is a partition identifier, assigned by the blade complex.	`-T system`

Table 68. scale command (continued)

Function	What it does	Command	Valid targets
Automatically create partition in scalable complex	Automatically creates a partition in the scalable complex. **Note:** • Creating a partition with nodes (blade servers) that are enabled for Blade Open Fabric Manager (BOFM) might cause loss of ports configured for Open Fabric Manager. • The *complex_id* is found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -auto -compid` *complex_id* where *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system`
Automatically create stand-alone partition in scalable complex	Automatically creates a stand-alone partition in the scalable complex. Single blade servers set up as a stand-alone partition will perform consistently if they are installed in another BladeCenter unit. **Note:** • Creating a partition with nodes (blade servers) that are enabled for Blade Open Fabric Manager (BOFM) might cause loss of ports configured for Open Fabric Manager. • The *complex_id* and *pri_node_chksum* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -auto` *pri_node_chksum* `-compid` *complex_id* where : • *pri_node_chksum* is a checksum that identifies the node where the partition is to be created. • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 68. scale command (continued)

Function	What it does	Command	Valid targets
Create stand-alone partition in scalable complex	Creates stand-alone partitions for specified blade servers or nodes in the scalable complex. Single blade servers set up as a stand-alone partition will perform consistently if they are installed in another BladeCenter unit. **Note:** • Creating a partition with nodes (blade servers) that are enabled for Blade Open Fabric Manager (BOFM) might cause loss of ports configured for Open Fabric Manager. • The comma-separated-value format of this command is primarily used to create stand-alone partitions, since these systems are not contiguous like blade-server systems. For blade-server systems, the command can accept a comma-separated-value list of blade server bay numbers, but these bay numbers must be contiguous. • The checksums, blade server bay numbers and *complex_id* are found by running the `scale` command with no options. • The namespace for a node checksum and blade server bay number should not overlap. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -create` *id_x*`,`*id_y* `-compid` *complex_id* where: • *id_x* and *id_y* are checksums or blade server bay numbers, separated by commas, that identify the node where the partition is to be created. The list can contain one or more comma-separated values. Both checksums and bay numbers can be used in the same list. • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See “Commands and user authority” on page 8 for additional information.	`-T system`

Table 68. scale command (continued)

Function	What it does	Command	Valid targets
Create partition in scalable complex	Creates partitions for specified blade servers in the scalable complex. **Note:** • Creating a partition with nodes (blade servers) that are enabled for Blade Open Fabric Manager (BOFM) might cause loss of ports configured for Open Fabric Manager. • For blade-server systems, a contiguous range of blade-server bays can be specified. • The blade server bay numbers and *complex_id* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -create` *start_bay*`-`*end_bay* `-compid` *complex_id* where: • *start_bay* and *end_bay* are blade server bay numbers, separated by a hyphen, that identify the range of blade server bays where partitions are to be created. The range can contain a single bay number. • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system`
Delete all partitions from scalable complex	Deletes all partitions in the scalable complex. **Note:** • All partitions must be powered off to delete them. • The blade server bay numbers and *complex_id* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -delete -compid` *complex_id* where *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 68. scale command (continued)

Function	What it does	Command	Valid targets
Delete partition from scalable complex	Deletes a specific partition in the scalable complex. **Note:** • A partition must be powered off to delete it. • The *complex_id* and *partition_id* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -delete -compid` *complex_id* `-partid` *partition_id* where : • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. • *partition_id* is a partition identifier, assigned by the blade complex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system`
Set partition mode to stand alone	Sets the mode for a specific partition in the scalable complex to standalone. A partition set to stand-alone mode operates as a single blade server system. Single blade servers set up as a stand-alone partition will perform consistently if they are installed in another BladeCenter unit. **Note:** • A partition must be powered off to change its mode. • The *complex_id* and *partition_id* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -mode standalone -compid` *complex_id* `-partid` *partition_id* where : • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. • *partition_id* is a partition identifier, assigned by the blade complex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 68. scale command (continued)

Function	What it does	Command	Valid targets
Set partition mode to partition	Sets the mode for a specific partition in the scalable complex to partition. **Note:** • A partition must be powered off to change its mode. • The *complex_id* and *partition_id* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -mode partition -compid` *complex_id* `-partid` *partition_id* where : • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. • *partition_id* is a partition identifier, assigned by the blade complex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system`
Power on partition in scalable complex	Turns on a specific partition in the scalable complex. **Note:** • The *complex_id* and *partition_id* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -on -compid` *complex_id* `-partid` *partition_id* where : • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. • *partition_id* is a partition identifier, assigned by the blade complex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 68. scale command (continued)

Function	What it does	Command	Valid targets
Power off partition in scalable complex	Turns off a specific partition in the scalable complex. **Note:** • The *complex_id* and *partition_id* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -off -compid` *complex_id* `-partid` *partition_id* where : • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. • *partition_id* is a partition identifier, assigned by the blade complex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system`
Power cycle partition in scalable complex	Cycles power for a specific partition in the scalable complex. If the partition is off, it will turn on. If the partition is on, it will turn off and then turn on. **Note:** • The *complex_id* and *partition_id* are found by running the `scale` command with no options. • The `-compid` command option is required for only blade-server systems that can have multiple scalable complexes defined in the same BladeCenter unit. This option does not need to be specified for stand-alone systems.	`scale -cycle -compid` *complex_id* `-partid` *partition_id* where : • *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the blade complex. • *partition_id* is a partition identifier, assigned by the blade complex. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system`

Example: To view all scalable complexes in the system, while the BladeCenter unit is set as the persistent command environment, at the system> prompt, type

```
scale
```

To power on a partition targeted by the complex ID "06EC" and the partition ID "1", while the BladeCenter unit is set as the persistent command environment, at the system> prompt, type

```
scale -on -compid 06EC -partid 1
```

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

```
system> scale

--- Complex ID: 06EC ---

Partition ID: 1
Assigned Nodes:
---------------

        Bay: 2
        Name: HX5 SDV #3
        Processors/Memory: 2 Intel Xeon/4 DIMMs 2GB
        Logical Node ID: 0
        Status: powered on
        Mode: partition
        Primary: Yes

        Bay: 3
        Name: HX5 SDV #4
        Processors/Memory: 2 Intel Xeon/4 DIMMs 2GB
        Logical Node ID: 1
        Status: powered on
        Mode: partition
        Primary: No

system> scale -on -compid 06EC -partid 1
Note: The power operation may take a few moments to complete.
OK
system>
```

sddump command

This command initiates a dump of service data from blade servers that support this function.

Table 69. sddump command

Function	What it does	Command	Valid targets
Dump service data	Dumps service data of the specified type from the specified blade server target. **Note:** Data dumps can be initiated, but are not collected, from the advanced management module.	`sddump -init` *type* where *type* is: • `sd` for a service data dump. • `sp` for a service processor data dump. • `pf` for a platform data dump. • `pt` for a partition data dump. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade server bay number.
Get service data	Collects and displays service data, from the last generated service-data dump, of the specified type from the specified blade server target.	`sddump -coll` *type* where *type* is: • `sd` to collect and display service data from last dump. • `sp` to collect and display service processor data from last dump. • `pf` to collect and display platform data from last dump. • `pt` to collect and display partition data from last dump. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[`*x*`]` where *x* is the blade server bay number.

Example: To initiate a data dump from the service processor of the blade server in bay 2, while this blade server is set as the persistent command environment, at the system:blade[2]> prompt, type

```
sddump -init sp
```

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

```
system:blade[2]> sddump -init sp
OK
system:blade[2]>
```

sdemail command

This command sends an email with the service information to the specified recipients.

Table 70. sdemail command

Function	What it does	Command	Valid targets
Send service information using email to specified recipients	Send an email with service information to the specified recipients. You assign a subject and an email address. When you run this command, it attaches the service log to the message.	`sdemail -subj "subject" -to address` where: • *"subject"* is a quote-delimited text string up to 119 characters in length. • *address* is the recipients email address. Multiple addresses separated with a comma can be entered (119 characters maximum). This command can only be run by users who have one or more of the following command authorities: • 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 See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management module bay number.

Example:

To send a service information email message, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
sdemail -to mail@cn.ibm.com -subj "Blade 8 Reboot"
```

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

```
system:mm[1]> sdemail -to mail@cn.ibm.com -subj "Blade 8 Reboot"
OK
```

security command

This command enables and displays the state of the data encryption feature for sensitive information stored in the advanced management module, such as passwords and keys.

Once enabled, the security feature can not be disabled without resetting all management module settings to their default configuration.

Table 71. security command

Function	What it does	Command	Valid targets
Display management module security setting	Displays the security setting for management module data encryption (on or off).	`security`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable data encryption for management module	Enables data encryption for the management module. **Attention:** If you enable data encryption, you can not disable it without resetting the management module to the default configuration.	`security -e` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

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

```
security -e
```

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

```
security
```

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

```
system:mm[1]> security -e
OK
system:mm[1]> security
-e on
system:mm[1]>
```

service command

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

Table 72. service command

Function	What it does	Command	Valid targets
Display service setting	Displays the service setting for technician debug of the advanced management module with a USB key (enable or disable).	`service`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable technician debug	Configure service setting to enable technician debug of the advanced management module with a USB key.	`service -enable` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Disable technician debug	Configure service setting to disable (default setting) technician debug of the advanced management module with a USB key.	`service -disable` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

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

```
service -enable
```

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

```
service
```

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

```
system:mm[1]> service -enable
OK
system:mm[1]> service
Debug with USB key: Enabled
system:mm[1]>
```

shutdown command

This command forces a blade server to shut down.

Table 73. shutdown command

Function	What it does	Command	Valid targets
Shutdown blade server	Forces a shutdown for the specified blade server.	`shutdown -f` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Blade administration See "Commands and user authority" on page 8 for additional information.	`-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 74. 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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

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

```
slp -t multicast
```

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

```
slp
```

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

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

smtp command

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

Table 75. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 75. smtp command (continued)

Function	What it does	Command	Valid targets
SMTP e-mail server domain name - set	Checks syntax and sets the SMTP e-mail server domain name.	`smtp -d` *domainname* where *domainname* is a valid domain name that meets the following criteria: • Alphanumeric string up to 63 characters in length. • Can contain dots (.), dashes (-), or underscores (_). • Must contain at least one dot. • No consecutive dots are allowed. • Quotes are not required. • Value can be cleared by setting it to an empty, double-quote limited string (""). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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 76. 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. **Note:** Before you can enable the SNMPv1 agent, the following must be specified: • management module contact name • management module location • at least one community name • at least one valid IP address for that community (see "config command" on page 111)	`snmp -a -state` where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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. **Note:** Before you can enable the SNMPv3 agent, the following must be specified: • management module contact name • management module location (see "config command" on page 111)	`snmp -a3 -state` where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 76. snmp command (continued)

Function	What it does	Command	Valid targets
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 1 first host name or IP address - set	Checks syntax and sets the first host name or IP address of community 1.	`snmp -c1i1` *hostname/ip_address* where *hostname/ip_address* is the first host name or IP address of community 1. • The first IP address of the first community can be set to 0.0.0.0 if the community access type is set to GET (for all management module types) or SET. • 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 76. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 76. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 1 second host name or IP address - set	Checks syntax and sets the second host name or IP address of community 1.	`snmp -c1i2` *hostname/ip_address* where *hostname/ip_address* is the second host name or IP address of community 1. • 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. snmp command (continued)

Function	What it does	Command	Valid targets
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SNMP community 2 first host name or IP address - set	Checks syntax and sets the first host name or IP address of community 2.	`snmp -c2i1` *hostname/ip_address* where *hostname/ip_address* is the first host name or IP address of community 2. • 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 2 second host name or IP address - set	Checks syntax and sets the second host name or IP address of community 2.	`snmp -c2i2` *hostname/ip_address* where *hostname/ip_address* is the second host name or IP address of community 2. • 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. snmp command (continued)

Function	What it does	Command	Valid targets
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
SNMP community 3 first host name or IP address - set	Checks syntax and sets the first host name or IP address of community 3.	`snmp -c3i1` *hostname/ip_address* where *hostname/ip_address* is the first host name or IP address of community 3. • 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. snmp command (continued)

Function	What it does	Command	Valid targets
SNMP community 3 second host name or IP address - set	Checks syntax and sets the second host name or IP address of community 3.	`snmp -c3i2` *hostname/ip_address* where *hostname/ip_address* is the second host name or IP address of community 3. • 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. snmp command (continued)

Function	What it does	Command	Valid targets
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 76. 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 website 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example: To view the SNMP configuration, while advanced 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 advanced 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 Enabled
-a3 Enabled
-t Enabled
-l Raleigh,NC
-cn Mr. Smith
-c1 public
-c1i1 9.44.146.157
-c1i2 9.44.147.24
-c1i3 9.49.165.217
-ca1 set
-c2 private
-c2i1 9.42.226.4
-c2i2
-c2i3
-ca2 get
-c3 test
```

```
-c3i1 9.44.247.64
-c3i2
-c3i3
-ca3 getsystem:mm[1]> snmp -a -on -t -on
system:mm[1]>
```

sol (serial over LAN) command

This command configures SOL functions and indicates SOL status.

Table 77. sol (serial over LAN) command

Function	What it does	Command	Valid targets

Display SOL status	Displays the SOL status for the targeted device:
	• When the command target is the primary management module, it displays the following values:
	– -status *on/off* (global SOL status)
	– -c *retry_count*
	– -e *CLI_key_sequence*
	– -i *retry_interval*
	– -r *reset_blade_key_seq*
	– -s *send_threshold*
	– -t *accumulate_timeout*
	– -v *VLAN_id*
	Note: For the advanced management module, the *VLAN_id* is identified as "VLAN ID".
	• When the command target is a blade server, it displays the following:
	– -status *enabled/disabled* (SOL status for the blade server)
	– Status of any SOL sessions for that blade server:
	- Not ready
	- Ready
	- Active
		`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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration • Blade configuration See “Commands and user authority” on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 77. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 77. sol (serial over LAN) command (continued)

Function	What it does	Command	Valid targets
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-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 enabled` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-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 enabled` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade server bay number.

Table 77. sol (serial over LAN) command (continued)

Function	What it does	Command	Valid targets
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 disabled` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-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 disabled` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:blade[x]` where *x* is the blade server bay number.

Table 77. sol (serial over LAN) command (continued)

Function	What it does	Command	Valid targets
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 77. sol (serial over LAN) command (continued)

Function	What it does	Command	Valid targets
Reset blade server key sequence - set	Sets the key sequence that will reset a blade server while a Telnet session in SOL mode.	`sol -r` *value* where *value* is the key sequence. In this sequence, a ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example: • `^[` (the carat symbol followed by a left bracket) means `Esc` • `^M` (the carat symbol followed by a capitol M) means carriage return. Refer to an ASCII-to-key conversion table for a complete listing of control-key sequences. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration • Blade configuration See "Commands and user authority" on page 8 for additional information.	`-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]>
```

sshcfg command

This command sets and displays the SSH status of the management module.

Table 78. sshcfg command

Function	What it does	Command	Valid targets
Display SSH status	Displays the SSH status of the management module. Returned values are: • -v1 off • -cstatus: state of CLI SSH server (enabled, disabled) • CLI SSH port number • -sstatus: state of SMASH SSH server (enabled, disabled) • SMASH SSH port number • ssh-dss fingerprint • ssh-rsa fingerprint • number of SSH public keys installed • number of locations available to store SSH keys **Note:** For scripting purposes, the "-v1 off" state is always displayed.	`sshcfg`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display RSA host key information	Displays RSA host key information for the management module.	`sshcfg -hk rsa`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display DSA host key information	Displays DSA host key information for the management module.	`sshcfg -hk dsa`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Generate host key	Generates a host key for the management module.	`sshcfg -hk gen` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 78. sshcfg command (continued)

Function	What it does	Command	Valid targets
Set state of CLI SSH server	Sets the state of the CLI SSH server for the management module.	`sshcfg -cstatus` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set state of SMASH SSH server	Sets the state of the SMASH SSH server for the management module.	`sshcfg -sstatus` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

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

```
sshcfg
```

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

```
system:mm[1]> sshcfg
-v1 off
-cstatus enabled
CLI SSH port 22
-sstatus disabled
SMASH SSH port 50024
ssh-dss 2048 bit fingerprint: 27:ee:bd:a9:27:28:d8:a5:93:03:3d:8e:77:d0:38:2c
ssh-rsa 2048 bit fingerprint: 66:c9:73:4f:18:11:02:10:f3:05:6e:d7:27:05:a5:01
2 SSH public keys installed
10 locations available to store SSH public keys
system:mm[1]>
```

sslcfg command

This command sets and displays the Secure Sockets Layer (SSL) status of the advanced management module.

Table 79. sslcfg command

Function	What it does	Command	Valid targets
Display management module SSL status	Displays the SSL status of the specified management module. This status includes information about SSL certificates.	`sslcfg`	`-T system:mm[x]` where *x* is the primary or standby management-module bay number.
Set SSL certificate handling for standby management module	Enables or disables use of an additional SSL certificate for the standby management module. If disabled, the standby management module uses the same SSL certificate as the primary management module. **Note:** An additional SSL certificate can only be configured when management module advanced failover is set to "swap" and the standby management module has a valid SSL certificate set up.	`sslcfg -ac` *state* where *state* is: • `on` to use an additional certificate • `off` to use the same certificate This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the standby management-module bay number.
Set SSL state for management module web server	Enables or disables SSL for the management module web server. **Note:** The SSL for the management module web server can only be enabled if a valid SSL certificate is set up.	`sslcfg -server` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary or standby management-module bay number.

Table 79. sslcfg command (continued)

Function	What it does	Command	Valid targets
Set SSL state for LDAP client	Enables or disables SSL for the LDAP client. **Note:** The SSL for the LDAP client can only be enabled if a valid SSL certificate is set up.	`sslcfg -client` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary or standby management-module bay number.

Table 79. sslcfg command (continued)

Function	What it does	Command	Valid targets
Generate self-signed certificate	Generates a self-signed certificate for the management module web server or the LDAP client. The following values must be set when generating a self-signed certificate: • Country using the `-c` command option. • State or province using the `-sp` command option. • City or locality using the `-cl` command option. • Organization name using the `-on` command option. • Management module host name using the `-hn` command option. **Note:** This host name must match the host name that is used by a web browser to connect to the management module. The following optional values can be set when generating a self-signed certificate: • Contact person using the `-cp` command option. • Email address of the contact person using the `-ea` command option. • Unit within a company or organization using the `-ou` command option. • Additional information such as a surname using the `-s` command option. • Additional information such as a given name using the `-gn` command option. • Additional information such as initials using the `-in` command option. • Additional information such as a distinguished name qualifier using the `-dq` command option.	`sslcfg -cert` *type* `-c` *country* `-sp` *"state"* `-cl` *"city"* `-on` *"org"* `-hn` *hostname* `-cp` *"name"* `-ea` *email* `-ou` *"org_unit"* `-s` *"surname"* `-gn` *"given_name"* `-in` *"initial"* `-dq` *"dn_qualifier"* where the following required options are: • *type* is: – `server` for a management module web server certificate. – `client` for an LDAP client certificate. • *country* is two-character alphabetic code for the country. • *"state"* is a state or province name of up to 60 characters in length. • *"city"* is a city or locality name of up to 50 characters in length. • *"org"* is an organization name of up to 60 characters in length. • *hostname* is a valid host name of up to 60 characters in length. where the following optional options are: • *"name"* is up to 60 characters in length. • *email* is a valid email address of up to 60 characters. • *"org_unit"* is up to 60 characters. • *"surname"* is up to 60 characters. • *"given_name"* is up to 60 characters. • *"initial"* is up to 20 characters. • *"dn_qualifier"* is up to 60 characters. *(continued on next page)*	`-T system:mm[`*x*`]` where *x* is the primary or standby management-module bay number.

Table 79. sslcfg command (continued)

Function	What it does	Command	Valid targets
Generate self-signed certificate *(continued)*		This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	

Table 79. sslcfg command (continued)

Function	What it does	Command	Valid targets
Generate CSR	Generates a certificate signing request (CSR) for the management module web server or the LDAP client. The following values must be set when generating a CSR: • Country using the `-c` command option. • State or province using the `-sp` command option. • City or locality using the `-cl` command option. • Organization name using the `-on` command option. • Management module host name using the `-hn` command option. **Note:** This host name must match the host name that is used by a web browser to connect to the management module. The following optional values can be set when generating a CSR: • Contact person using the `-cp` command option. • Email address of the contact person using the `-ea` command option. • Unit within a company or organization using the `-ou` command option. • Additional information such as a surname using the `-s` command option. • Additional information such as a given name using the `-gn` command option. • Additional information such as a initials using the `-in` command option. • Additional information such as a distinguished name qualifier using the `-dq` command option. • Additional information such as a CSR password using the `-cpwd` command option. *(continued on next page)*	`sslcfg -csr` *type* `-c` *country* `-sp` *"state"* `-cl` *"city"* `-on` *"org"* `-hn` *hostname* `-cp` *"name"* `-ea` *email* `-ou` *"org_unit"* `-s` *"surname"* `-gn` *"given_name"* `-in` *"initial"* `-dq` *"dn_qualifier"* `-cpwd` *password* `-un` *"un_name"* where the following required options are: • *type* is: – `server` for a management module web server CSR. – `client` for an LDAP client CSR. • *country* is two-character alphabetic code for the country. • *"state"* is a state or province name of up to 60 characters in length. • *"city"* is a city or locality name of up to 50 characters in length. • *"org"* is an organization name of up to 60 characters in length. • *hostname* is a valid host name of up to 60 characters in length. where the following optional options are: • *"name"* is up to 60 characters in length. • *email* is a valid email address of up to 60 characters. • *"org_unit"* is up to 60 characters. • *"surname"* is up to 60 characters. • *"given_name"* is up to 60 characters. *(continued on next page)*	`-T system:mm[`*x*`]` where *x* is the primary or standby management-module bay number.

Table 79. sslcfg command (continued)

Function	What it does	Command	Valid targets
Generate CSR *(continued)*	• Additional information such as an unstructured name qualifier using the `-un` command option.	• *"initial"* is up to 20 characters. • *"dn_qualifier"* is up to 60 characters. • *password* is between 6 and 30 characters. • *"un_name"* is up to 60 characters. **Note:** Arguments that must be quote-delimited are shown in quotation marks. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	
Download certificate file	Downloads the specified certificate file. The IP address of the TFTP server for downloading an SSL self-signed certificate or CSR must be set using the `-i` command. The file name for downloading an SSL self-signed certificate or CSR can be set using the `-l` command. If no file name is specified, the default file name for the file will be used.	`sslcfg -dnld -cert|-csr` *type* `-l` *filename* `-i` *ipaddress* where: • *type* is – `client` for an LDAP client – `server` for a management module web server • *filename* is a valid filename of up to 256 characters in length containing any character except the percent sign (%), forward-slash (/), or double-quote ("). • *ipaddress* is the IPv4 or IPv6 IP address of the TFTP server. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary or standby management-module bay number.

Table 79. sslcfg command (continued)

Function	What it does	Command	Valid targets
Import certificate file	Import (upload) the specified certificate file. The IP address of the TFTP server for uploading an SSL self-signed certificate must be set using the `-i` command. The file name for uploading an SSL self-signed certificate can be set using the `-l` command.	`sslcfg -upld -cert` *type* `-i` *ipaddress* `-l` *filename* where: • *type* is – `client` for an LDAP client – `server` for a management module web server • *ipaddress* is the IPv4 or IPv6 IP address of the TFTP server. • *filename* is a valid filename of up to 256 characters in length containing any character except the percent sign (%), forward-slash (/), or double-quote ("). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary or standby management-module bay number.

Table 79. sslcfg command (continued)

Function	What it does	Command	Valid targets
Import/download/ remove trusted certificate 1	Perform the specified operation on trusted certificate 1 for the SSL client. Valid operations are: • import (upload) • download • remove The IP address of the TFTP server for uploading or downloading a trusted certificate must be set using the `-i` command. The file name for uploading or downloading a trusted certificate can be set using the `-l` command.	`sslcfg -tc1` *operation* where *operation* is: • `import` • `download` • `remove` **Note:** The `-tc1` option must be used with the following options: • `-i` *ipaddress* • `-l` *filename* where: • *ipaddress* is the IPv4 or IPv6 IP address of the TFTP server. • *filename* is a valid filename of up to 256 characters in length containing any character except the percent sign (%), forward-slash (/), or double-quote ("). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary or standby management-module bay number.

Table 79. sslcfg command (continued)

Function	What it does	Command	Valid targets
Import/download/ remove trusted certificate 2	Perform the specified operation on trusted certificate 2 for the SSL client. Valid operations are: • import (upload) • download • remove The IP address of the TFTP server for uploading or downloading a trusted certificate must be set using the `-i` command. The file name for uploading or downloading a trusted certificate can be set using the `-l` command.	`sslcfg -tc2` *operation* where *operation* is: • `import` • `download` • `remove` **Note:** The `-tc2` option must be used with the following options: • `-i` *ipaddress* • `-l` *filename* where: • *ipaddress* is the IPv4 or IPv6 IP address of the TFTP server. • *filename* is a valid filename of up to 256 characters in length containing any character except the percent sign (%), forward-slash (/), or double-quote ("). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary or standby management-module bay number.

Table 79. sslcfg command (continued)

Function	What it does	Command	Valid targets
Import/download/ remove trusted certificate 3	Perform the specified operation on trusted certificate 3 for the SSL client. Valid operations are: • import (upload) • download • remove The IP address of the TFTP server for uploading or downloading a trusted certificate must be set using the `-i` command. The file name for uploading or downloading a trusted certificate can be set using the `-l` command. For importing a certificate "-l <filename>" is required.	`sslcfg -tc3` *operation* where *operation* is: • `import` • `download` • `remove` **Note:** The `-tc3` option must be used with the following options: • `-i` *ipaddress* • `-l` *filename* where: • *ipaddress* is the IPv4 or IPv6 IP address of the TFTP server. • *filename* is a valid filename of up to 256 characters in length containing any character except the percent sign (%), forward-slash (/), or double-quote ("). This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary or standby management-module bay number.

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

```
sslcfg
```

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

```
system:mm[1]> sslcfg
-server disabled
-client disabled
SSL Server Certificate status:
 A CA-signed certificate is installed
SSL Client Certificate status:
 No certificate has been generated
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
system:mm[1]>
```

syslog command

This command manages how the advanced management module handles transmission of event log messages to networked syslog event collectors.

Table 80. syslog command

Function	What it does	Command	Valid targets
Display syslog configuration	Displays the syslog event log transmission configuration of the advanced management module.	`syslog`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set syslog filter level	Set severity filtering levels for syslog event log transmission.	`syslog -sev` *level* where *level* is: • `i` selects error, warning, and informational logs • `w` selects error and warning logs • `e` selects error logs This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set syslog event log transmission state for collector 1	Enables or disables syslog event log transmission to collector 1.	`syslog -coll1` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 80. syslog command (continued)

Function	What it does	Command	Valid targets
Set syslog event log transmission state for collector 2	Enables or disables syslog event log transmission to collector 2.	`syslog -coll2` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
syslog event log collector 1 host name or IP address - set	Sets the host name or IP address for syslog event collector 1.	`syslog -i1` *hostname/ip_address* where *hostname/ip_address* is the collector 1 host name or IP address. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
syslog event log collector 2 host name or IP address - set	Sets the host name or IP address for syslog event collector 2.	`syslog -i2` *hostname/ip_address* where *hostname/ip_address* is the collector 2 host name or IP address. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 80. syslog command (continued)

Function	What it does	Command	Valid targets
syslog event log collector 1 port number - set	Sets the port number for syslog event collector 1.	syslog -p1 *port* where *port* is the collector 1 port number from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
syslog event log collector 2 port number - set	Sets the port number for syslog event collector 2.	`syslog -p2` *port* where *port* is the collector 2 port number from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 80. syslog command (continued)

Function	What it does	Command	Valid targets
Generate test message	Generates a test syslog message to test the configuration. **Note:** The -test command options must be run exclusive of other command options.	`syslog -test` This command can only be run by users who have one or more of the following command authorities: • 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 See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example: To view the syslog event log transmission configuration of the primary advanced management module in bay 1, while this management module is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
syslog
```

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

```
system:mm[1]> syslog
-sev 1
-coll1 enabled
-coll2 disabled
-i1 253.245.45.1
-i2
-p1 514
-p2 514
system:mm[1]>
```

tcpcmdmode command

This command displays and changes the timeout of the TCP command-mode sessions that are used by IBM Systems 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 81. tcpcmdmode command

Function	What it does	Command	Valid targets
Display TCP command-mode session status and timeout	Displays the secure and non-secure TCP command-mode session status (maximum number of sessions) and timeout.	`tcpcmdmode`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set TCP command-mode session timeout	Sets the secure and non-secure 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Disable TCP command-mode sessions	Disables TCP command-mode sessions that are used by IBM Systems Director software for out-of-band communication with the management module. This applies to both read and write operations.	`tcpcmdmode -status 0` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 81. tcpcmdmode command (continued)

Function	What it does	Command	Valid targets
Enable and set number of TCP command-mode sessions	Enables TCP command-mode and sets the maximum number of sessions that can be used by IBM Systems Director software for out-of-band communication with the management module. For read operations, all of the values from 1 to 20, inclusive, mean *enabled*. **Note:** The advanced management module supports a combined total of up to 20 secure and non-secure TCP command-mode sessions.	`tcpcmdmode -status` *number_sessions* where *number_sessions* is from 1 to 20, inclusive. (A value of 0 disables TCP command-mode sessions.) If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Disable secure TCP command-mode sessions	Disables secure TCP command-mode sessions that are used by IBM Systems Director software for out-of-band communication with the management module. This applies to both read and write operations.	`tcpcmdmode -sstatus 0` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable and set number of secure TCP command-mode sessions	Enables secure TCP command-mode and sets the maximum number of sessions that can be used by IBM Systems Director software for out-of-band communication with the management module. For read operations, all of the values from 1 to 20, inclusive, mean *enabled*. **Note:** The advanced management module supports a combined total of up to 20 secure and non-secure TCP command-mode sessions.	`tcpcmdmode -sstatus` *number_sessions* where *number_sessions* is from 1 to 20, inclusive. (A value of 0 disables secure TCP command-mode sessions.) If you enter a value outside this range, an error will be displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

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

```
tcpcmdmode -status 3
```

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

```
tcpcmdmode -sstatus 5
```

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 commands:

```
system:mm[1]> tcpcmdmode -status 3
OK
system:mm[1]> tcpcmdmode -sstatus 5
OK
system:mm[1]> tcpcmdmode -t 360
OK
system:mm[1]> tcpcmdmode
-status 3 connections
-sstatus 5 connections
-t 360 seconds
system:mm[1]>
```

telnetcfg (Telnet configuration) command

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

Table 82. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-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]>
```

temps command

This command displays actual temperatures and temperature threshold values for BladeCenter components.

Table 83. temps command

Function	What it does	Command	Valid targets

Display temperature values	Displays the current temperature and temperature threshold settings for the specified component:
	• The management module target displays the management module ambient temperature.
	• The blade server target displays the temperature values for components in the specified blade server, such as microprocessors and expansion modules.
	• The media tray target displays values for the temperature sensor in the media tray.
		`temps`	`-T system:mm[x]`
			`-T system:blade[x]`
			`-T system:mt`
			where *x* is the primary management-module or blade server bay number.

Example: To view the current temperature and temperature thresholds for the blade server in bay 3, while this blade server is set as the persistent command environment, at the `system:blade[3]>` prompt, type

```
temps
```

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

```
system:blade[3]> temps
                          Hard    Warning
Comp  Value  Warning  Shutdown   Reset
----  -----  -------  --------  -------
CPU1  38.00  85.00    95.00     78.00
CPU2  35.00  85.00    95.00     78.00
BEM   -----  -----    -----     -----
system:blade[3]>
```

trespass command

This command sets and displays the status and message for the advanced management module trespass feature that can display a warning message to users when they log in.

Table 84. trespass command

Function	What it does	Command	Valid targets
Display status of management module trespass feature	Displays status of the trespass feature for the management module. Possible return values are: • -twe (on or off) • -tw *warning_message* **Note:** The *warning_message* is shown only when the trespass feature is enabled (-twe on).	`trespass`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable / disable management module trespass feature	Enables or disables trespass feature for management module.	`trespass -twe` *state* where *state* is `on` or `off`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Set management module trespass message	Sets message that is displayed to users who log in to the management module when the trespass feature is enabled. **Note:** Setting a new *warning_message* permanently replaces the default warning message.	`trespass -tw` *"warning_message"* where *"warning_message"* is up to 1600 characters in length and enclosed in double-quotation marks. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 84. trespass command (continued)

Function	What it does	Command	Valid targets
Set management module trespass feature to default values	Sets trespass feature to default values: • -twe: off • -tw (warning message): WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of vendor/service contracts. The owner, or its agents , may monitor any activity or communication on the computer system or network. The owner, or its agents, may retrieve any information stored within the computer system or network. By accessing and using this computer system or network, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the computer system or network, including information stored locally or remotely on a hard drive or other media in use with this computer system or network.	`trespass -twd` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Example:

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

```
trespass -twe on
```

To set the trespass feature message to 'Authorized Access only', while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
trespass -tw "Authorized Access only"
```

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

```
trespass
```

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

```
system:mm[1]> trespass -twe on
OK
system:mm[1]> trespass -tw "Authorized Access only"
-tw OK
system:mm[1]> trespass
-twe on
-tw Authorized Access only
system:mm[1]>
```

uicfg command

This command displays and configures the management module user interface settings.

Table 85. uicfg command

Function	What it does	Command	Valid targets
Display management module user interface settings	Displays the user interface settings for the management module. Returned values indicate enabled or disabled status for the following interfaces: • -cli • -snmp • -tcm (TCP command mode) • -stcm (secure TCP command mode) • -web (web interface)	`uicfg`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable / disable command-line interface	Enables or disables the management module command-line interface (using Telnet or SSH).	`uicfg -cli` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Enable / disable SNMPv1 and SNMPv3	Enables or disables SNMPv1 and SNMPv3 connections to the management module.	`uicfg -snmp` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 85. uicfg command (continued)

Function	What it does	Command	Valid targets
Enable / disable TCP command mode	Enables or disables TCP command mode (used by IBM Systems Director) for the management module.	`uicfg -tcm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set number of TCP command mode connections	Enable or disable the TCP command mode, or sets the maximum number of connections explicitly. **Note:** Any number of connections (1 through 20) displays a status of enabled. Zero connections displays a status of disabled.	`uicfg -tcm` *port_mode* where *port_mode* is `enabled` (1 connection), `disabled` (no connections), or a number between 0 and 20, inclusive, that indicates the maximum number of non-secure TCP session connections. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable secure TCP command mode	Enables or disables secure TCP command mode (used by IBM Systems Director) for the management module.	`uicfg -stcm` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 85. uicfg command (continued)

Function	What it does	Command	Valid targets
Set number of secure TCP command mode connections	Enable or disable the secure TCP command mode, or sets the maximum number of connections explicitly. **Notes:** • On a write operation, the maximum number of connections can be set explicitly (0-20), or it can be enabled (1 connection) or disabled (0 connections). • On a read operation, disabled means 0 connections, and enabled means 1 or more connections. • The total session count of TCM and STCM is limited to 20.	`uicfg -stcm` *port_mode* where *port_mode* is `enabled` (1 connection), `disabled` (no connections), or a number between 0 and 20, inclusive, that indicates the maximum number of secure TCP session connections. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable / disable web interface	Enables or disables the management module web interface.	`uicfg -web` *state* where *state* is `enabled` or `disabled`. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

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

```
uicfg -stcm disabled
```

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

```
uicfg
```

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

```
system:mm[1]> uicfg -stcm disabled
Warning: Communication with IBM Systems Director via Secure TCP Command Mode
has been disabled.
OK
system:mm[1]> uicfg
-cli enabled (telnet only)
-snmp enabled
-stcm enabled
-tcm disabled
-web enabled
system:mm[1]>
```

update (update firmware) command

This command updates firmware using the uniform resource locator (URL) of a TFTP, FTP, HTTP, or HTTPS server and displays information about firmware installed in BladeCenter components.

Important:

- Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before you update the code.
- Scalable complexes in a BladeCenter unit require a consistent firmware level on all blade servers in a complex. When scripting firmware updates for blade servers in a scalable complex, make sure that the `update` commands are included for each node in the complex.

Table 86. 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 standby advanced management modules, the returned value will also indicate if a firmware update is in progress and the percentage that is complete.
	• 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 number, standby management-module number, blade server bay number, or I/O module bay number.

Table 86. update (update firmware) command (continued)

Function	What it does	Command	Valid targets

Update firmware using URL	Update firmware for the command target using a uniform resource locator (URL).
	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 (see "Commands and user authority" on page 8).
	Notes:
	• Updating to older firmware levels may cause loss of certain functionality
	• The JS22 or JS12 blade server firmware is too large to be updated using this command. See the *User's Guide* for your JS22 or JS12 blade server for information about updating firmware.
		`update -u` *U_R_L*
		
		where *U_R_L* is fully qualified uniform resource locator of a tftp, ftp, http, or https server where the firmware update image is located.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis administration (for management module)
		• Blade administration (for blade server)
		• I/O module administration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]:sp`
			`-T system:switch[`*x*`]`
			
			where *x* is the primary management-module, blade server bay number, or I/O-module bay number.

Update firmware and reboot	Update firmware and reboot the advanced management module to use new firmware if the update succeeds. **Important:** Command authority definitions might change between firmware versions. Make sure that the command authority level set for each user is correct after updating management-module firmware.	`update -u` *U_R_L* `-r` where *U_R_L* is fully qualified uniform resource locator of a tftp, ftp, http, or https server where the firmware update image is located. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis administration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module.

Table 86. 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.
	Notes:
	• Updating to older firmware levels may cause loss of certain functionality
	• The JS22 or JS12 blade server firmware is too large to be updated using this command. See the *User's Guide* for your JS22 or JS12 blade server for information about updating firmware.
		`update -u` *U_R_L* `-v`
		
		where *U_R_L* is fully qualified uniform resource locator of a tftp, ftp, http, or https server where the firmware update image is located.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis administration (for management module)
		• Blade administration (for blade server)
		• I/O module administration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]:sp`
			`-T system:switch[`*x*`]`
			
			where *x* is the primary management-module, blade server bay number, or I/O-module bay number.

Update I/O module firmware	Directly update I/O module firmware image. **Note:** Only some I/O modules have this capability.	`update -u` *U_R_L* `-img` *img_index* where: • *U_R_L* is fully qualified uniform resource locator of a tftp, ftp, http, or https server where the firmware update image is located. • *img_index* is the image index you are updating. Use the `update -a` command to list available images and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 86. update (update firmware) command (continued)

Function	What it does	Command	Valid targets
Update I/O module firmware (verbose)	Directly update I/O module firmware image, 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.	`update -u` *U_R_L* `-img` *img_index* `-v` where: • *U_R_L* is fully qualified uniform resource locator of a tftp, ftp, http, or https server where the firmware update image is located. • *img_index* is the image index to the I/O module firmware you are updating. Use the `update -a` command to list available images and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.
Activate I/O module firmware	Directly activate I/O module firmware image. **Note:** Only some I/O modules have this capability.	`update -activate` *img_index* where *img_index* is the image index you are activating. Use the `update -a` command to list available images and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 86. update (update firmware) command (continued)

Function	What it does	Command	Valid targets
Update and activate I/O module firmware	Directly update I/O module and activate the firmware image. **Notes:** • Only some I/O modules have this capability. • The activate option can be used with the other options. You can flash first, then activate the specified index. • The image index you activate can be different from the one you update.	`update -u` *U_R_L* `-img` *img_index* `-activate` *img_index* where: • *U_R_L* is fully qualified uniform resource locator of a tftp, ftp, http, or https server where the firmware update image is located. • *img_index* is the image index you are activating. Use the `update -a` command to list available images and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Table 86. update (update firmware) command (continued)

Function	What it does	Command	Valid targets

Update firmware
 	
(Obsolete command. See Note following table.)
	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` *filelocation*
		
		where:
		• *ip_address* is the IPv4 or IPv6 IP address of the TFTP server.
		• *filelocation* is the location of the firmware update file.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis administration (for management module)
		• Blade administration (for blade server)
		• I/O module administration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]:sp`
			`-T system:switch[`*x*`]`
			
			where *x* is the primary management-module, blade server bay number, or I/O (switch) module bay number.

Update firmware (verbose)
 	
(Obsolete command. See Note following table.)
	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` *filelocation* `-v`
		
		where:
		• *ip_address* is the IPv4 or IPv6 IP address of the TFTP server.
		• *filelocation* is the location of the firmware update file.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis administration (for management module)
		• Blade administration (for blade server)
		• I/O module administration (for I/O module)
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system:mm[`*x*`]`
			`-T system:blade[`*x*`]:sp`
			`-T system:switch[`*x*`]`
			
			where *x* is the primary management-module, blade server bay number, or I/O (switch) module bay number.

Table 86. update (update firmware) command (continued)

Function	What it does	Command	Valid targets
Update I/O module firmware *(Obsolete command. See Note following table.)*	Directly update I/O module firmware image. **Note:** Only some I/O modules have this capability.	`update -i` *ip_address* `-l` *filelocation* `-img` *img_index* where: • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server. • *filelocation* is the location of the firmware update file. • *img_index* is the image index you are updating. Use the `update -a` command to list available images and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O (switch) module bay number.

Table 86. update (update firmware) command (continued)

Function	What it does	Command	Valid targets
Update I/O module firmware (verbose) *(Obsolete command. See Note following table.)*	Directly update I/O module firmware image, 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. **Note:** Only some I/O modules have this capability.	`update -i` *ip_address* `-l` *filelocation* `-img` *img_index* `-v` where: • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server. • *filelocation* is the location of the firmware update file. • *img_index* is the image index to the I/O module firmware you are updating. Use the `update -a` command to list available images and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O (switch) module bay number.
Activate I/O module firmware *(Obsolete command. See Note following table.)*	Directly activate I/O module firmware image. **Note:** Only some I/O modules have this capability.	`update -activate` *img_index* where *img_index* is the image index you are activating. Use the `update -a` command to list available images and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O (switch) module bay number.

Table 86. update (update firmware) command (continued)

Function	What it does	Command	Valid targets
Update and activate I/O module firmware *(Obsolete command. See Note following table.)*	Directly update I/O module and activate the firmware image. **Notes:** • Only some I/O modules have this capability. • The activate option can be used with the other options. You can flash first, then activate the specified index. • The image index you activate can be different from the one you update.	`update -i` *ip_address* `-l` *filelocation* `-img` *img_index* `-activate` *img_index* where: • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server. • *filelocation* is the location of the firmware update file. • *img_index* is the image index you are activating. Use the `update -a` command to list available images and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module administration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[`*x*`]` where *x* is the I/O (switch) module bay number.

Note: The `-i` and `-l` options for the `update` command have been replaced by the `-u` command option. While the `-i` and `-l` options will remain active for a few releases before being removed, users are encouraged to transition to the `-u` option as soon as possible.

To accomplish this transition, the IP address and file location of the firmware update file or image, specified by the arguments to the `-i` and `-l` options, must be replaced by the `-u` option followed by an argument that specifies the fully qualified uniform resource locator (URL) of a tftp, ftp, http, or https server where the firmware update file or image is located.

Example: To update the advanced management module firmware from a TFTP server and reboot the advanced management module in management-module bay 1 after a successful update, type the following command at the `system:>` prompt. For this example, the IP address of the TFTP server is 9.37.177.215 and the firmware file containing the update is named CNETMNUS.pkt. The verbose mode and reboot flag are also specified.

```
update -u tftp://9.37.177.215/temp/CNETMNUS.pkt -T mm[1] -v -r
```

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

```
system> update -u tftp://9.37.177.215/temp/CNETMNUS.pkt -T mm[1] -v -r
100% transferred (100/100)
transfer completed successfully
flashing firmware to target device
Starting flash packet preparation.
Flash preparation - packet percent complete 4.
Flash preparation - packet percent complete 8.
Flash preparation - packet percent complete 12.
Flash preparation - packet percent complete 16.
Flash preparation - packet percent complete 20.
Flash preparation - packet percent complete 24.
Flash preparation - packet percent complete 28.
Flash preparation - packet percent complete 32.
Flash preparation - packet percent complete 36.
Flash preparation - packet percent complete 40.
Flash preparation - packet percent complete 44.
Flash preparation - packet percent complete 50.
Flash preparation - packet percent complete 54.
Flash preparation - packet percent complete 58.
Flash preparation - packet percent complete 62.
Flash preparation - packet percent complete 66.
Flash preparation - packet percent complete 70.
Flash preparation - packet percent complete 74.
Flash preparation - packet percent complete 78.
Flash preparation - packet percent complete 82.
Flash preparation - packet percent complete 86.
Flash preparation - packet percent complete 90.
Flash preparation - packet percent complete 94.
Flash preparation - packet percent complete 98.
Flash operation phase starting.
Flashing - packet percent complete 34.
Flashing - packet percent complete 50.
Flashing - packet percent complete 50.
Flashing - packet percent complete 50.
Flashing - packet percent complete 50.
Flashing - packet percent complete 50.
Flashing - packet percent complete 50.
Flashing - packet percent complete 50.
Flashing - packet percent complete 82.
Update of AMM Main Application firmware was successful.

The new firmware will become active after the next reset of the MM.

Rebooting AMM...
```

uplink (management module failover) command

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

Note: This command does not apply to the BladeCenter S unit.

Table 87. 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`
			`-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 -dps` *delay*
		where *delay* is from 10 to 172800 seconds, inclusive. If you enter a value outside this range, an error will be displayed.
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration
		See "Commands and user authority" on page 8 for additional information.
			`-T system`
			`-T system:mm[x]`
			where *x* is the primary management-module bay number.

Enable / disable physical uplink failover	Enables or disables failover to the standby management module if the external physical network interface of the primary management module fails.	`uplink -ep` *state*
		where *state* is `enabled` or `disabled`.
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration
		See "Commands and user authority" on page 8 for additional information.
			`-T system`
			`-T system:mm[x]`
			where *x* is the primary management-module bay number.

Table 87. uplink command (continued)

Function	What it does	Command	Valid targets

Set logical network uplink failover delay	Sets the amount of time between detection of a management-module logical uplink failure and failover to the standby management module.	`uplink -dls` *delay*
		
		where *delay* is from 60 to 172800 seconds, inclusive. If you enter a value outside this range, an error will be displayed.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system`
			`-T system:mm[`*x*`]`
			
			where *x* is the primary management-module bay number.

Enable / disable logical uplink failover	Enables or disables failover to the standby management module if the external logical network interface of the primary management module fails.
	
	You must enter a non-zero IP address (`-ip` command option) or IPv6 IP address (`-ip6` command option) for a device that the management module can access to check its logical network link before you can enable logical uplink failover.
		`uplink -el` *state*
		
		where *state* is `enabled` or `disabled`.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system`
			`-T system:mm[`*x*`]`
			
			where *x* is the primary management-module bay number.

Set IP address to check logical network uplink	Sets the IPv4 IP address of the device that the management module accesses to check its logical network link.	`uplink -ip` *ip_address*
		
		where *ip_address* is a valid IPv4 IP address. You must enter a non-zero IPv4 IP address, in dotted decimal IP address format, before you can enable logical uplink failover.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system`
			`-T system:mm[`*x*`]`
			
			where *x* is the primary management-module bay number.

Table 87. uplink command (continued)

Function	What it does	Command	Valid targets

Set IPv6 IP address to check logical network uplink	Sets the IPv6 IP address of the device that the management module accesses to check its logical network link.	`uplink -ip6` *ip_address*
		
		where *ip_address* is a valid IPv6 IP address. You must enter a non-zero IP address, in IPv6 format, before you can enable logical uplink failover.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system`
			`-T system:mm[`*x*`]`
			
			where *x* is the primary management-module bay number.

Set logical link loss alert and failover policy	Sets the alert and failover policy for logical link loss to check either the IPv4 IP address, the IPv6 IP address, or both of these IP addresses.
	Note: The `-alert` command option applies only when both the `-ip` and `-ip6` command options are set.
		`uplink -alert` *setting*
		
		where *setting* is:
		• `either` to check either the IPv4 IP address or the IPv6 IP address.
		• `both` to check both the IPv4 IP address and the IPv6 IP address.
		
		This command can only be run by users who have one or more of the following command authorities:
		• Supervisor
		• Chassis configuration
		
		See "Commands and user authority" on page 8 for additional information.
			`-T system`
			`-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 physical network interface of a primary management module fails, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
uplink -ep enabled
```

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 commands:

```
system:mm[1]> uplink -ep enabled
OK
system:mm[1]> uplink
Failover on network uplink loss is enabled for physical detection
Uplink delay for physical detection: 60 seconds

Failover on network uplink loss is enabled for logical detection
Uplink delay for logical detection: 1800 seconds
Destination IP for MM to check its logical link: 1.1.1.0
Destination IPv6 IP for MM to check its logical link: 1::2
Alert and failover if both IPv4 and IPv6 link checks fail
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 88. 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 • Current log in or log out state • Password compliance • State of account (active or inactive) • Number of SSH public keys installed for user	`users`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Display active users	Displays all users that are currently logged in to the management module. Returned values include: • User name • User IP address • Connection type (SNMPv1, SNMPv3, SSH, TCP command mode, Telnet, Web) • Session ID	`users -curr`	`-T system:mm[x]` where *x* is the primary management-module bay number.
Terminate user session	Terminates the specified user login session. **Note:** The session ID is found by running the `users -curr` command.	`users -ts` *sessionID* where *sessionID* is a number that corresponds to the user session ID. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Display single user profile	Displays the specified management-module user profile. Returned values are: • User name • Authority level • Context name • Authentication protocol • Privacy protocol • Access type • Hostname/IP address • Maximum simultaneous sessions allowed • Number of active sessions • Password compliance • Password expiration date • Account state • Number of SSH public keys installed for this user • Last time this user logged in	`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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Disable user account	Disable the specified management-module user account.	`users -`*user_number* `-disable` where *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management • Chassis administration • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Enable user profile	Enable a disabled management-module user account.	`users -`*user_number* -enable where *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management • Chassis administration • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Unlock user profile	Unlock a locked management-module user account.	`users -`*user_number* `-unlock` where *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management • Chassis administration • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. 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* -ms *max_sessions* 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 an 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) *(continued on next page)*	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Create user profile *(continued)*		• *context_name* is an alphanumeric string up to 31 characters in length that can include periods (.) and underscores (_). • *auth_protocol* choices are: – md5 – sha – none • *privacy_protocol* choices are: – des – aes – none • *privacy_pwd* is an alphanumeric string up to 31 characters in length that can include periods (.) and underscores (_). • *access_type* choices are: – get – set – trap • *ip_addr/hostname* is up to 63 characters in length. • *max_sessions* is a number from 0 to 20. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See “Commands and user authority” on page 8 for additional information.	

Table 88. 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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Change user password	Changes the user password in the specified management-module user profile. **Note:** Users can change their own password even if they do not have authority to manage accounts. The -op option is only used when changing your own password	`users -`*user_number* `-op` *old_password* `-p` *new_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. • *old_password* is the current password for the specified user. • *new_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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See “Commands and user authority” on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. 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 one of the following: – `operator` (read-only) – `rbs` (custom) The custom authority level parameter is specified using the following syntax: `rbs:`*levels*`:`*devices* where the *levels* are one or more of the following authority levels, separated by a vertical bar (`|`): • `super` (Supervisor) • `cam` (Chassis User Account Management) • `clm` (Chassis Log Management) • `co` (Chassis Operator) • `cc` (Chassis Configuration) • `ca` (Chassis Administration) • `bo` (Blade Operator) • `brp` (Blade Remote Present) • `bc` (Blade Configuration) • `ba` (Blade Administration) • `so` (I/O Module Operator) • `sc` (I/O Module Configuration) • `sa` (I/O Module Administration) *(continued on next page)*	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Set user authority level *(continued)*	**Notes:** • The LDAP authority levels are not supported by the management-module web interface. • To use the LDAP authority levels, make sure that the version of LDAP security used by the management module is set to v2 (enhanced role-based security model). See "ldapcfg command" on page 210 for information.	The *levels* can also include one or more of the following authority levels when using LDAP. • `brpv` (Blade Remote Presence View Video) • `brpk` (Blade Remote Presence KVM) • `brpr` (Blade Remote Presence Remote Drive Read) • `crpru` (Blade Remote Presence Remote Drive Read or Write) • `rps` (Remote Presence Supervisor) where the *devices* are one or more of the following devices, separated by a vertical bar (`|`). Ranges of devices are separated by a dash (`-`). • `c`*n* (Chassis *n*, where *n* is a valid chassis number. Use c1 for single-chassis environments.) • `b`*n* (Blade *n*, where *n* is a valid blade bay number in the chassis) • `s`*n* (I/O module *n*, where *n* is a valid I/O module bay number in the chassis) This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Set maximum number of simultaneous sessions for user	Sets the maximum number of simultaneous login sessions for the specified user.	`users -`*user_number* `-ms` *max-session* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *max-session* is a number from 0 to 20 that sets the maximum number of simultaneous sessions for the user. A value of 0 means that there is no session limit for the user. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. 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` – `none` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-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: – `aes` – `des` – `none` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Set privacy password for SNMPv3 user	Sets an SNMPv3 privacy password in the specified management-module user profile.	`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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set access type for SNMPv3 user	Sets an SNMPv3 access type for the specified management-module user profile. This command supports the following access types: • get: the user can query Management Information Base (MIB) objects and receive traps. • set: the user can query and set MIB objects and receive traps. • trap: the user can only receive traps.	`users -`*user_number* `-at` *access_type* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *access_type* is – `get` – `set` – `trap` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
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. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display SSH public key	Displays the entire specified SSH public key for the specified user in OpenSSH format. **Note:** The `-pk` and `-e` options must be used exclusive of all other `users` command options.	`users -`*user_number* `-pk -`*key_index* `-e` where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *key_index* identifies the key number from 1 to 12 to display. If the *-key_index* is `all`, then all keys for the user are displayed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Add SSH public key	Adds an SSH public key for the specified user. **Notes:** • The `-pk` and `-add` options must be used exclusive of all other `users` command options. • The SSH Public Key is added to the first available storage location. Each advanced management module can support up to 12 SSH public keys. • Each user is permitted a maximum of four SSH public keys, if the space is available.	`users -`*user_number* `-pk -add` *key* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *key* is a valid key in OpenSSH format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Add specific SSH public key	Adds a specific SSH public key for the specified user. **Note:** The `-pk` and `-add` options must be used exclusive of all other `users` command options.	`users -`*user_number* `-pk -`*key_index* `-add` *key* where: • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *key_index* identifies the key number from 1 to 12 to add. • *key* is a valid key in OpenSSH format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Remove SSH public key	Removes an SSH public key for the specified user. **Note:** The `-pk` and `-remove` options must be used exclusive of all other `users` command options.	`users -`*user_number* `-pk -`*key_index* `-remove` • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *key_index* identifies the key number from 1 to 12 to remove. If the *-key_index* is "all", then all keys for the user are removed. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Upload SSH public key	Uploads a new SSH public key.	`users -`*user_number* `-pk -upld -i` *ip_addr/hostname* `-l` *filename* • *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 IPv4 or IPv6 IP address or an alphanumeric hostname string up to 63 characters in length of the TFTP server. • *filename* is the filename of the key file. Keys must be in OpenSSH format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Replace SSH public key	Replaces an existing SSH public key.	`users -`*user_number* `-pk -`*key_index* `-upld -i` *ip_addr/hostname* `-l` *filename* • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *key_index* identifies the key number from 1 to 12 to replace. • *ip_addr/hostname* is a valid static IPv4 or IPv6 IP address or an alphanumeric hostname string up to 63 characters in length of the TFTP server. • *filename* is the filename of the key file. Keys must be in OpenSSH format. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Download SSH public key	Downloads a specific SSH public key to a TFTP server. **Note:** The `-pk` and `-dnld` options must be used exclusive of all other `users` command options.	`users -`*user_number* `-pk -`*key_index* `-dnld -i` *ip_addr/hostname* `-l` *filename* • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the `Display all user profiles` list. • *key_index* identifies the key number from 1 to 12 to upload. • *ip_addr/hostname* is a valid static IPv4 or IPv6 IP address or an alphanumeric hostname string up to 63 characters in length of the TFTP server. • *filename* is the filename of the key file. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Connect to SSH public key	Accept connections from SSH public key host.	`users -`*user_number* `-pk -`*key_index* `-af from=`*"list"* • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *key_index* identifies the key number from 1 to 12 to connect. • *"list"* is a comma-separate list of hostnames and IP addresses. The list is an alphanumeric string up to 511 characters in length that can include alphanumeric characters, commas, asterisks, question marks, exclamation points, periods, and hyphens. The string must be enclosed in double-quotes. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 88. users (management-module users) command (continued)

Function	What it does	Command	Valid targets
Comment SSH public key	Add comment to an SSH public key.	`users -`*user_number* `-pk -`*key_index* `-cm "`*comment*`"` • *user_number* is a number from 1 to 12 that corresponds to the user number assigned in the "Display all user profiles" list. • *key_index* identifies the key number from 1 to 12 to comment. • *"comment"* is up to 255 characters in length, enclosed in double-quotes. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis account management See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

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

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

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

To 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 commands:

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.

```
system:mm[1]> users -3 -n user3 -p passw0rd -a rbs:super:c1|b1-b14|s1-s4
-cn joe -ap md5 -pp des -ppw passw0rd -at get -I 192.168.70.129
OK

system:mm[1]> users
0 active session(s)
Password compliant
Account active
```

```
   Role:cam
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Modules:1|2|3|4|5|6|7|8|9|10
There are no SSH public keys installed for this user
2. kprevent
0 active session(s)
Password compliant
Account active
   Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Modules:1|2|3|4|5|6|7|8|9|10
There are no SSH public keys installed for this user
3. johnh
0 active session(s)
Password compliant
Account active
   Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Modules:1|2|3|4|5|6|7|8|9|10
There are no SSH public keys installed for this user
4. toms
1 active session(s)
Password compliant
Account active
   Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Modules:1|2|3|4|5|6|7|8|9|10
Number of SSH public keys installed for this user: 3
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]>
```

vlan command

This command configures and displays the VLAN (virtual local area network) settings of the management module.

Table 89. vlan command

Function	What it does	Command	Valid targets
Display VLAN settings	Displays the settings for V **Note:** The command issued by itself will display all entries, the global state, the commit timeout, and whether the current configuration has been committed.LAN.	`vlan` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Apply VLAN settings	Applies the configuration changes for VLAN. **Note:** Configuration changes must be committed before the commit timeout expires, otherwise the previous configuration will be restored.	`vlan -commit` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Apply VLAN settings timeout	Sets the custom value of the configuration changes timeout for VLAN.	`vlan -cto` *timeout* where *timeout* is from 1 to 255 minutes, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 89. vlan command (continued)

Function	What it does	Command	Valid targets
Set global VLAN state	Sets the global state of VLAN to enabled or disabled.	`vlan -state` *state* where *state* is • enabled • disabled This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set VLAN state	Sets the custom state of the non-fixed entry for VLAN. **Notes:** • *restart* is valid for non-fixed entries. • *default* is valid for every entry.	`vlan -vi` *vlan_entry_index* `-state` *state* where • *vlan_entry_index* is the VLAN entry's index. • *state* is – enabled – disabled – default – restart This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Delete global VLAN entry	Deletes all non-fixed VLAN entries.	`vlan -delete` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 89. vlan command (continued)

Function	What it does	Command	Valid targets
Delete VLAN entry	Deletes the specified VLAN entry.	`vlan -vi` *vlan_entry_index* `-delete` where *vlan_entry_index* is the VLAN entry's index. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Display VLAN entry	Displays the VLAN entry.	`vlan -vi` *vlan_entry_index* where *vlan_entry_index* is the VLAN entry's index. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Create VLAN entry	Creates the VLAN entry. **Notes:** • `-vi` and `-vid` must be set to create an entry. • `-state`, and `-n` are optional. • A default entry name is used if `-n` is not specified.	`vlan -vi` *vlan_entry_index* `-vid` *vlan_id* where • *vlan_entry_index* is the VLAN entry's index. • *vlan_id* is the number from 1 to 4,094, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 89. vlan command (continued)

Function	What it does	Command	Valid targets
Set VLAN ID	Sets the VLAN ID.	`vlan -vi` *vlan_entry_index* `-vid` *id* where • *vlan_entry_index* is the VLAN entry's index. • *id* is the number from 1 to 4,094, inclusive. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set remote presence access	Enables or disabled the remote presence access. **Note:** Before enabling the remote presence access, you have to disable it on whichever VLAN it is enabled on.	`vlan -vi` *vlan_entry_index* `-rp` *state* where • *vlan_entry_index* is the VLAN entry's index. • *state* is enabled or disabled. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 89. vlan command (continued)

Function	What it does	Command	Valid targets
Set SOL access	Enables or disabled the SOL access. **Note:** Before enabling the SOL access, you have to disable it on whichever VLAN it is enabled on.	`vlan -vi` *vlan_entry_index* `-sol` *state* where • *vlan_entry_index* is the VLAN entry's index. • *state* is enabled or disabled. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set VLAN tagging	Enables or disabled the VLAN tagging. **Note:** `vlan -tag` is only valid for the default entry.	`vlan -vi` *vlan_entry_index* `-tag` *state* where • *vlan_entry_index* is the VLAN entry's index. • *state* is enabled or disabled. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 89. vlan command (continued)

Function	What it does	Command	Valid targets
Set VLAN entry name	Sets the VLAN entry name.	`vlan -vi` *vlan_entry_index* `-n` *name* where • *vlan_entry_index* is the VLAN entry's index. • *name* is the quote-delimited VLAN entry name, of 1 to 31 characters in length. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set VLAN configuration	Sets the IPv4 configuration method for VLAN. **Note:** It is not applied to the fixed entry.	`vlan -vi` *vlan_entry_index* `-c` *method* where • *vlan_entry_index* is the VLAN entry's index. • *method* is static. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 89. vlan command (continued)

Function	What it does	Command	Valid targets
Set VLAN IP address (IPv4)	Sets the IPv4 address for VLAN. **Note:** It is not applied to the fixed entry.	`vlan -vi` *vlan_entry_index* `-i` *ip_address* where • *vlan_entry_index* is the VLAN entry's index. • *ip_address* is the IP address. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set VLAN subnet (IPv4)	Sets the IPv4 subnet for VLAN. **Note:** It is not applied to the fixed entry.	`vlan -vi` *vlan_entry_index* `-s` *subnet* where • *vlan_entry_index* is the VLAN entry's index. • *subnet* is the subnet. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 89. vlan command (continued)

Function	What it does	Command	Valid targets
Set VLAN gateway (IPv4)	Sets the IPv4 gateway for VLAN. **Note:** It is not applied to the fixed entry.	`vlan -vi` *vlan_entry_index* `-g` *gateway* where • *vlan_entry_index* is the VLAN entry's index. • *gateway* is the gateway. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.
Set VLAN subnet route	Sets the custom value of subnet route for VLAN. **Note:** It is not applied to the fixed entry.	`vlan -vi` *vlan_entry_index* `-sr`*x* *subnet_route* where • *vlan_entry_index* is the VLAN entry's index. • *x* is 1, 2, or 3. • *subnet_route* is the subnet route. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Table 89. vlan command (continued)

Function	What it does	Command	Valid targets
Set VLAN subnet mask	Sets the custom value of subnet mask for VLAN. **Note:** It is not applied to the fixed entry.	`vlan -vi` *vlan_entry_index* `-sm`*x* *subnet_mask* where • *vlan_entry_index* is the VLAN entry's index. • *x* is 1, 2, or 3. • *subnet_mask* is the subnet mask. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

To change the name of VLAN entry 2 to VLAN-2, while management module 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
vlan -vi 2 -n "VLAN-2"
```

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

```
vlan -commit
```

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

```
vlan
```

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

```
system:mm[1]> vlan -vi 2 -n "VLAN-2"
All changes must be committed within 2 minutes using -commit.
OK
system:mm[1]> vlan -commit
OK
system:mm[1]> vlan
-state disabled
-cto 2

Default entry
-vi 1
-n VLAN-1
-state enabled
-vid 1
-sol enabled
-rp enabled
-tag disabled
I/O module access enabled
```

```
IPv4 config method: static
IPv4 address: 9.72.217.71
IPv4 subnet: 255.255.248.0
IPv4 gateway: 9.72.216.1

-vi 2
-n VLAN-2
-state disabled
-vid 1000
-sol disabled
-rp disabled
Tagging: enabled
-c static
-i 0.0.0.0
-s 0.0.0.0
-g 0.0.0.0
-sr1 0.0.0.0
-sm1 0.0.0.0
-sr2 0.0.0.0
-sm2 0.0.0.0
-sr3 0.0.0.0
-sm3 0.0.0.0

The current configuration has been committed.
system:mm[1]>
```

volts command

This command displays actual voltages and voltage threshold values for BladeCenter components.

Table 90. volts command

Function	What it does	Command	Valid targets

Display voltage values	Displays the current voltage and voltage threshold settings for the specified component:
	• The management module target displays the voltage values for the BladeCenter unit.
	• The blade server target displays the internal voltage values for the specified blade server.
	
	Note: The voltage values that display will vary based on BladeCenter unit and blade server type.
		`volts`	`-T system:mm[x]`
			`-T system:blade[x]`
			
			where *x* is the primary management-module or blade server bay number.

Example: To view the current voltage and voltage thresholds for the blade server in bay 3, while this blade server is set as the persistent command environment, at the `system:blade[3]>` prompt, type

```
volts
```

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

```
system:blade[3]> volts
  Source      Value       Warning
-----------  -------  ----------------
1.8V Sense    +1.79    (+1.61,+1.97)
1.8VSB Sense  +1.83    (+1.61,+1.97)
12V Sense     +12.33   (+10.79,+13.21)
12VSB Sense   +12.30   (+10.74,+13.19)
3.3V Sense    +3.31    (+2.96,+3.62)
5V Sense      +5.06    (+4.39,+5.48)
system:blade[3]>
```

write command

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

Table 91. write command

Function	What it does	Command	Valid targets
Save management-module configuration to chassis	Saves an image of the management-module configuration to the BladeCenter unit chassis.	`write -config chassis` This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.
Save management-module configuration to file (no encryption)	Saves an image of the management-module configuration to a file while data encryption is not enabled for the BladeCenter unit.	`write -config file -l` *filename* `-i` *ip_address* where: • *filename* is the name of the configuration file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the configuration file is located. **Note:** If the `-l` *filename* option is not specified, the default filename of asm.cfg is used. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[x]` where *x* is the primary management-module bay number.

Table 91. write command (continued)

Function	What it does	Command	Valid targets
Save management-module configuration to file (encryption)	Saves an image of the management-module configuration to a file while data encryption is enabled for the BladeCenter unit. **Note:** When a configuration file is created with a pass-phrase (encryption enabled), if this configuration file is restored on the same management module, the pass-phrase entered during restoration is ignored.	`write -config file -l` *filename* `-i` *ip_address* `-p` *passphrase* where: • *filename* is the name of the configuration file. • *ip_address* is the IPv4 or IPv6 IP address of the TFTP server where the configuration file is located. • *passphrase* is a double-quote delimited pass-phrase that will be needed to restore the configuration file. Maximum pass-phrase length is 1600 characters. **Note:** If the `-l` *filename* option is not specified, the default filename of asm.cfg is used. This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 8 for additional information.	`-T system:mm[`*x*`]` where *x* is the primary management-module bay number.

Example:

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

```
write -config chassis
```

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

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

zonecfg command

This command sets and displays the serial attached SCSI (SAS) device information for BladeCenter components that is stored in I/O modules that support this feature.

Table 92. zonecfg command

Function	What it does	Command	Valid targets
Display SAS zone list	Displays a list of SAS device zones and their information that is stored in the specified I/O module.	`zonecfg`	`-T system:switch[x]` where *x* is the I/O-module bay number.
Activate SAS zone - single SAS switch	Activates a SAS zone, selected by index number, for the specified SAS switch module. **Note:** If the I/O module is not in an operating condition that allows a zone to be activated, the command returns an advisory message.	`zonecfg -activate` *zone* where *zone* is the index number for a valid zone. Use the `zonecfg` command, with no options, to list valid zones and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system:switch[x]` where *x* is the I/O-module bay number.
Activate SAS zone - all SAS switches	Activates a SAS zone, selected by index number, for all SAS switch modules. **Note:** If the I/O module is not in an operating condition that allows a zone to be activated, the command returns an advisory message.	`zonecfg -activate` *zone* where *zone* is the index number for a valid zone. Use the `zonecfg` command, with no options, on all I/O modules to determine the valid zones that are common to all SAS switch modules and their index numbers. This command can only be run by users who have one or more of the following command authorities: • Supervisor • I/O module configuration See "Commands and user authority" on page 8 for additional information.	`-T system`

Table 92. zonecfg command (continued)

Function	What it does	Command	Valid targets
Display SAS zone information	Displays information about a SAS zone, selected by index number, that is stored in the specified I/O module.	`zonecfg -view` *zone* where *zone* is the index number for a valid zone.	`-T system:switch[`*x*`]` where *x* is the I/O-module bay number.

Note: If you install both RAID SAS (RSS) and Non-RAID SAS (NSS) mass storage devices, you can only power on and manage the zone configuration for one at a time.

Example: To view the list of SAS zones stored in the I/O module in bay 1, while this I/O module is set as the persistent command environment, at the `system:switch[1]>` prompt, type

```
zonecfg
```

To activate SAS zone 5 for the I/O module in bay 1, while this I/O module is set as the persistent command environment, at the `system:switch[1]>` prompt, type

```
zonecfg –activate 5
```

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

```
system:switch[1]> zonecfg
Index: 3
Name: Name3
Description string for zone config 3
Status: Inactive
Type: Predefined
Date: <mm>

Index: 5
Name: Name5
Description string for zone config 5
Status: Inactive
Type: Configurable
Date: <mm>

Index: 2
Name: Name2
Description string for zone config 2
Status: Inactive
Type: Configurable
Date: <mm>

Index: 24
Name: Name24
Description string for zone config 24
Status: Active
Type: Configurable
Date: <mm>
system:switch[1]> zonecfg
Index: 3
Name: Name3
Description string for zone config 3
Status: Inactive
Type: Predefined
Date: <mm>

Index: 5
```

```
Name: Name5
Description string for zone config 5
Status: Pending
Type: Configurable
Date: <mm>

Index: 2
Name: Name2
Description string for zone config 2
Status: Inactive
Type: Configurable
Date: <mm>

Index: 24
Name: Name24
Description string for zone config 24
Status: Active
Type: Configurable
Date: <mm>
system:switch[1]> zonecfg –activate 5
OK
system:switch[1]>
```

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" on page 421
- "accseccfg command errors" on page 423
- "advfailover command errors" on page 424
- "alarm command errors" on page 425
- "alertcfg command errors" on page 426
- "alertentries command errors" on page 426
- "autoftp command errors" on page 427
- "baydata command errors" on page 427
- "bofm command errors" on page 428
- "boot command errors" on page 429
- "bootmode command errors" on page 429
- "bootseq command errors" on page 430
- "buildidcfg command errors" on page 430
- "chconfig command errors" on page 431
- "chlog command errors" on page 432
- "chmanual command errors" on page 433
- "cin command errors" on page 433
- "clear command errors" on page 435
- "clearlog command errors" on page 435
- "clock command errors" on page 435
- "config command errors" on page 436
- "console command errors" on page 437
- "dhcpinfo command errors" on page 438
- "displaylog command errors" on page 438
- "displaysd command errors" on page 439
- "dns command errors" on page 440
- "env command errors" on page 440
- "ethoverusb command errors" on page 440
- "eventinfo command errors" on page 441
- "events command errors" on page 441
- "exit command errors" on page 442
- "feature command errors" on page 442
- "files command errors" on page 444
- "fuelg command errors" on page 445
- "groups command errors" on page 448
- "health command errors" on page 448
- "help command errors" on page 449

- "history command errors" on page 449
- "identify command errors" on page 449
- "ifconfig command errors" on page 450
- "info command errors" on page 454
- "iocomp command errors" on page 455
- "kvm command errors" on page 455
- "ldapcfg command errors" on page 455
- "led command errors" on page 456
- "list command errors" on page 457
- "modactlog command errors" on page 457
- "monalerts command errors" on page 457
- "monalertsleg command errors" on page 458
- "mcad command errors" on page 457
- "mt command errors" on page 458
- "nat command errors" on page 458
- "ntp command errors" on page 459
- "ping command errors" on page 459
- "pmpolicy command errors" on page 460
- "portcfg command errors" on page 460
- "ports command errors" on page 460
- "power command errors" on page 462
- "rdoc command errors" on page 462
- "read command errors" on page 463
- "remacccfg command errors" on page 464
- "remotechassis command errors" on page 464
- "reset command errors" on page 465
- "scale command errors" on page 465
- "sddump command errors" on page 466
- "sdemail command errors" on page 467
- "security command errors" on page 467
- "service command errors" on page 467
- "shutdown command errors" on page 468
- "slp command errors" on page 468
- "smtp command errors" on page 468
- "snmp command errors" on page 469
- "sol command errors" on page 470
- "sshcfg command errors" on page 471
- "sslcfg command errors" on page 472
- "syslog command errors" on page 474
- "tcpcmdmode command errors" on page 475
- "telnetcfg command errors" on page 475
- "temps command errors" on page 476
- "thres command errors" on page 476
- "trespass command errors" on page 476
- "uicfg command errors" on page 477

- "update command errors" on page 478
- "uplink command errors" on page 480
- "users command errors" on page 481
- "vlan command errors" on page 485
- "volts command errors" on page 486
- "write command errors" on page 486
- "zonecfg command errors" on page 487

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 93. 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.

Table 93. Common errors (continued)

Error message	Definition
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.
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.

Table 93. Common errors (continued)

Error message	Definition
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.
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.

accseccfg command errors

This topic lists error messages for the accseccfg command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 94. accseccfg command errors

Error message	Definition
'Password required' is currently disabled.	A user without a password tries to change the security level to -high. User must have a password to perform this action.
'Password required' is currently enabled.	A user without a password tries to change the security level to -legacy. User must have a password to perform this action.
Reading account security level failed.	An error occurs while the management module is reading the security level.

Table 94. accseccfg command errors (continued)

Error message	Definition
Setting account defaults to high level failed.	An error occurs while the management module is setting the security level to -high.
Setting account defaults to legacy level failed.	An error occurs while the management module is setting the security level to -legacy.
The -high option cannot be used with other options.	The user tries to set the account security to high settings while changing individual option values.
The -legacy option cannot be used with other options.	The user tries to set the account security to legacy settings while changing individual option values.
The account inactivity disable time period must be greater than the account inactivity alert time period.	A user tries to set the account inactivity disable time period to be less than the account inactivity alert time period.
The argument for the option -dc is outside the valid range.	The user tries to set the -dc option to a value outside of its valid range.
The argument for the option -ia is outside the valid range.	The user tries to set the -ia option to a value outside of its valid range.
The argument for the option -id is outside the valid range.	The user tries to set the -id option to a value outside of its valid range.
The argument for the option -lf is outside the valid range.	The user tries to set the -lf option to a value outside of its valid range.
The argument for the option -lp is outside the valid range.	The user tries to set the -lp option to a value outside of its valid range.
The argument for the option -pe is outside the valid range.	The user tries to set the -pe option to a value outside of its valid range.
The argument for the option -rc is outside the valid range.	The user tries to set the -rc option to a value outside of its valid range.
The minimum password change interval must be less than the password expiration period (%d days or %d hours).	A user tries to set the -pc option to a value greater than the -pe option.
The password expiration period (%d days or %d hours) must be greater than the minimum password change interval.	A user tries to set the -pe option to a value less than the -pc option.
User must have a password to change the 'Password required' setting.	A user without a password tries to change the -pr option.

advfailover command errors

This topic lists error messages for the advfailover command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 95. advfailover command errors

Error message	Definition
Operation failed.	An error occurs while the management module is processing the command.
Operation not allowed, since the standby MM is not present.	The user tries to enable advanced failover when there is no standby management module installed in the BladeCenter unit.

Table 95. advfailover command errors (continued)

Error message	Definition
Unknown option: *option* where *option* identifies the illegal command option that was entered.	The user tries to enter an illegal command option.

alarm command errors

This topic lists error messages for the alarm command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 96. 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.
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.

alertcfg command errors

This topic lists errors for the alertcfg command.

There are no unique errors for the alertcfg command. See “Common errors” on page 421 for a list of error messages that apply to all commands.

alertentries command errors

This topic lists error messages for the alertentries command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 97. 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 (-).
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.

autoftp command errors

This topic lists errors for the autoftp command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 98. autoftp command errors

Error message	Definition
Autoftp is disabled, -i, -p, -u and -pw options are invalid.	A user tries to enter -i, -p, -u, or -pw options when the FTP/TFTP mode is set to disabled.
Invalid FTP/TFTP address.	A user tries to enter an FTP or TFTP address that is not valid.
Invalid input. Address must be less than 64 characters.	A user tries to enter an address that is 64 or more characters long.
Invalid input. Password must be less than 64 characters.	A user tries to enter a password that is 64 or more characters long.
Invalid input. Userid must be less than 64 characters.	A user tries to enter a user id that is 64 or more characters long.
Password must be enclosed in quotation marks. Displayed when the argument of option -p is not quote_delimited.	A user tries to enter a password without quotation marks.
Read autoftp configuration failed.	The management module was unable to read the autoftp configuration.
Read autoftp mode failed.	The management module was unable to read the autoftp mode status.
The mode is tftp, -u and -pw options are invalid.	A user tries to enter a user name or password when the mode is set to TFTP.
User Name must be enclosed in quotation marks.	A user tries to enter a user name without quotation marks.
When disabling autoftp, the -i, -p, -u and -pw options are invalid.	A user tries to enter -i, -p, -u, or -pw options when setting the FTP/TFTP mode to disabled in the same command.
When setting -m to tftp, the -u and -pw options are invalid.	A user tries to enter a user name or password when setting the FTP/TFTP mode to TFTP in the same command.

baydata command errors

This topic lists error messages for the baydata command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 99. baydata command errors

Error message	Definition
Error writing bay data to blade bay *bayNum*. where *bayNum* is the blade bay number.	An internal error occurs while the user is changing bay data for the specified blade server.
Invalid blade bay number	The command has an invalid bay number.

Table 99. baydata command errors (continued)

Error message	Definition
Invalid input. The bay data string must be less than the maximum number of characters allowed.	User enters bay data with -data option for a blade server that exceeds the maximum length of 60 characters.
The -clear and -data options cannot be used in the same command.	User issues a command with both -clear and -data options.
The bay data must be quote-delimited.	User enters bay data with -data option for a blade server without double quotation marks.
User not authorized to change bay data for bay number.	An unauthorized user issues a command to change bay data for the specified blade server.

bofm command errors

This topic lists errors for the bofm command.

Notes:

1. The BOFM command displays parsing errors and duplicate addresses that point to flaws in the comma-separated values (csv) configuration database file. The BladeCenter Open Fabric Manager is not a standard management module feature; it is offered and documented separately. See the *BladeCenter Open Fabric Manager Installation and Users Guide* for more detailed information.
2. If the number of advanced management module TCP command mode connections is zero, or if all available TCP command mode connections are in use, a connection failure message is generated by the BOFM feature. Make sure that the advanced management module TCP command mode connection limit is positive and that no more than the available number of connections are in use. See the *BladeCenter Open Fabric Manager Installation and Users Guide* for additional information.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 100. bofm command errors

Error message	Definition
Applying new configuration on MM failed.	An error occurs while the advanced management module is applying the BOFM configuration.
Confirming configuration change failed.	An error occurs while the advanced management module is confirming a configuration change.
File transfer failed.	An error occurs while transferring a file during file upload.
Getting BOFM status failed.	An error occurs while the advanced management module is getting BOFM status.
Getting duplicates failed.	An error occurs while the advanced management module is getting duplicates.
Getting parsing errors failed.	An error occurs while the advanced management module is getting parsing errors.
-i and -l are both required to upload a BOFM configuration file.	A user issues a command to apply BOFM configuration to the advanced management module without both -i and -l options.

Table 100. bofm command errors (continued)

Error message	Definition
Login failed.	Login fails while the management module is applying the BOFM configuration to the advanced management module.
Parsing errors.	An error occurs while the advanced management module is parsing the BOFM status.
Resetting BOFM configuration on MM failed.	An error occurs while the advanced management module is resetting the BOFM configuration.
Retrieving the file from TFTP server failed.	An error occurs while the advanced management module is retrieving the configuration file from a TFTP server.
Update Failed, there was a problem retrieving the file.	An error occurs while the advanced management module is uploading a file.

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 421 for a list of error messages that apply to all commands.

bootmode command errors

This topic lists errors for the bootmode command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 101. bootmode command errors

Error message	Definition
Boot mode not supported on blade[*x*] where *x* is the number of the blade-server bay.	The command is directed to a blade server that does not support the bootmode feature.
Error retrieving the boot mode of this blade.	The management module is unable read the boot mode of the blade server.
Set the blade boot mode to *option* failed where *option* is the selected boot mode.	The management module is unable to set the blade server boot mode to the specified value.

bootseq command errors

This topic lists error messages for the bootseq command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 102. bootseq command errors

Error message	Definition
Error writing boot sequence.	An error occurs while the management module is processing the command.
First device cannot be set to 'nodev'.	The user tries to set the first boot device to 'nodev'.
Invalid device for this blade or chassis.	The user tries to set a boot device to an invalid choice.
No duplicate settings are allowed.	The user tries to set multiple slots in the boot sequence to the same device.
Second device cannot be set to 'nodev' when third or fourth device is set.	The user tries to set the second boot device to 'nodev'.
Third device cannot be set to 'nodev' when fourth device is set.	The user tries to set the third boot device to 'nodev'.

buildidcfg command errors

This topic lists error messages for the buildidcfg command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 103. buildidcfg command errors

Error message	Definition
-create must be used exclusive of other options.	A user tries to create the blade firmware build ID list while using another command option. The `-create` command option must be run alone.
Adding an entry failed. Please check for duplicates or an invalid format.	An error occurs while adding an entry to the blade firmware build ID list.
Build ID must be enclosed in quotation marks.	A user tries to enter a blade firmware build ID without quotation marks.
Build revision must be enclosed in quotation marks.	A user tries to enter a blade firmware build revision without quotation marks.
Error creating the initial build ID list.	An error occurs while creating the blade firmware build ID list.
Error removing all the build ID entries.	An error occurs while removing all blade firmware build ID list entries.
Error removing build ID entry *identifier*. where the *identifier* identifies the build ID entry specified.	An error occurs while removing a blade firmware build ID list entry.
Importing list failed. Check for duplicates or an invalid format on line *line_number* where the *line_number* identifies the line number specified.	An error occurs during blade firmware build ID list import.
Machine type must be enclosed in quotation marks.	A user tries to enter a machine type without quotation marks.

Table 103. buildidcfg command errors (continued)

Error message	Definition
Manufacturer must be enclosed in quotation marks.	A user tries to enter a manufacturer name without quotation marks.
Modifying entry *identifier* failed. Please check for duplicates or an invalid format. where the *identifier* identifies the entry specified.	A user tries to modify an blade firmware build ID list entry with duplicate or wrong information.
No entries in the list.	The blade firmware build ID list is empty.
Operating error "export *identifier*" where the *identifier* identifies the information to export.	An error occurs during blade firmware build ID list information export.
Operating error "import *identifier*" where the *identifier* identifies the information to import.	An error occurs during blade firmware build ID list information import.
Some required options for the –ab command are missing.	A user tries to add a blade firmware build ID list entry, but does not include all of the required options.

chconfig command errors

This topic lists errors for the chconfig command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 104. chconfig command errors

Error message	Definition
Address must be enclosed in quotation marks.	A user tries to enter an address that is not enclosed in quotation marks
City must be enclosed in quotation marks.	A user tries to enter a city name that is not enclosed in quotation marks
IBM Support Center: invalid input. Please input 2 characters ISO country code for the IBM Support Center.	A user tries to enter a country code that is not valid.
Contact Company must be enclosed in quotation marks.	A user tries to enter a company name that is not enclosed in quotation marks
Contact Name must be enclosed in quotation marks.	A user tries to enter a contact name that is not enclosed in quotation marks
Email must be enclosed in quotation marks.	A user tries to enter an email that is not enclosed in quotation marks
Email: invalid input. Please make sure your input is not empty and within 30 characters.	A user tries to enter an email with a length that is not valid
Error to enable/disable Service Agent.	An error occurs while the advanced management module is enabling or disabling the service agent.
Error to enable Service Agent. You have not set all of the required contact Information fields yet.	A user tries to issue a command to enable a service agent that does not have the required contact information set.
HTTP Proxy is disabled now, you can not change proxy settings, please enable http proxy first.	A user tries to change proxy settings when the HTTP proxy is disabled.
Invalid HTTP Proxy location.	A user tries to enter a proxy address that is not a valid IP address or hostname
Invalid input. -loc should be less than 64 characters.	A user tries to enter a proxy address that is 64 or more characters long.

Table 104. chconfig command errors (continued)

Error message	Definition
Invalid input. -pw should be less than 16 characters.	A user tries to enter a proxy password that is 16 or more characters long.
Invalid input. Password may not contain angle brackets.	A user tries to enter a proxy password that contains "<" or "⌂>".
Invalid input. User Name must be less than 30 characters.	A user tries to enter a user name that is 30 or more characters long.
Invalid option argument for -li:	A user tries to use the -li option without the "view" or "accept" argument.
Terms and conditions is not accepted yet, please view and accept the terms and conditions first.	A user attempts to change the service advisor settings before accepting the terms and conditions.
The Terms and Conditions should be accepted first before using this command.	A user attempts to change the service manager settings before accepting the license agreement.
Phone number must be enclosed in quotation marks.	A user tries to enter a phone number that is not enclosed in quotation marks
Phone number: invalid input. Please make sure your input is not empty and 5-30 characters.	A user tries to enter a phone number that is not valid
Postalcode must be enclosed in quotation marks.	A user tries to enter a postal code that is not enclosed in quotation marks.
Postalcode: invalid input. Please make sure your input is not empty and within 9 characters.	A user tries to enter a postal code is not valid in length.
State must be enclosed in quotation marks and has 2 or 3 characters.	A user tries to enter a state that is not enclosed in quotation marks, or is not two or three characters in length.

chlog command errors

This topic lists errors for the chlog command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 105. chlog command errors

Error message	Definition
-f must be used exclusive of other options.	The user tries to use the -f option at the same time as other options.
-s must be used exclusive of other options.	The user tries to use the -s option at the same time as other options.
A call home event with index *number* was not found. where *number* is the decimal number that specifies the serviceable activity log entry that the user is attempting to acknowledge or unacknowledge.	The management module was unable to find a specified call-home event activity log entry.
Error reading data for Terms and Conditions.	An error occurs while the management module is reading the terms and conditions information.
Fail to read Service Advisor Activity Log	The management module was unable to read the call-home event activity log.
Invalid syntax. Type 'chlog -h' for help.	A user fails to specify the parameter for the call-home activity log entry that they are attempting to acknowledge or unacknowledge.

Table 105. chlog command errors (continued)

Error message	Definition
Terms and Conditions not accepted yet.	The user attempts to view the call-home event activity log but has not yet accepted the Terms and Conditions.

chmanual command errors

This topic lists errors for the chmanual command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 106. chmanual command errors

Error message	Definition
-test must be used exclusive of other options	The user attempts to run this command with other options in addition to -test.
Error generating a manual Call Home	This command fails when the user attempts the manual call home operation.
Error generating a test Call Home	This command fails when the user attempts the test call home operation.
Invalid syntax. Type 'chmanual -h' for help.	The user attempts to use this command but uses improper syntax.
Problem description must be enclosed in quotation marks	The user attempts to run this command when the problem description is not enclosed in quotation marks.
Test Call Home should be operated on SYSTEM target	The user attempts to use this command when the command is not targeted on ‘system’ for test call home.
Terms and Conditions not accepted yet.	The user attempts to use this command but has not yet accepted the Terms and Conditions.
The Service Agent is disabled now, please enable it before calling 'chmanual'	The user attempts to use this command before the service advisor is enabled.

cin command errors

This topic lists error messages for the cin command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 107. cin command errors

Error message	Definition
-id cannot be the same as the blade management VLAN ID. Please try again.	A user tries to enter a command with a VLAN ID which is the same as the VLAN ID of the blade management.
-ip cannot be multicast. Please try again.	A user issues a command with an IP address which is the same as the IP address of the multicast.
-ip cannot be the same as the management module IP address. Please try again	A user tries to enter a command with an IP address which is the same as the IP address of the advanced management module.
An error occurred while changing CIN global status setting	An error occurs while user is changing CIN global status setting.
An error occurred while clearing CIN entry	An error occurs while the user is clearing a CIN entry.

Table 107. cin command errors (continued)

Error message	Definition
An error occurred while enabling/disabling CIN entry.	An error occurs while the user is enabling/disabling a CIN entry.
An error occurred while setting CIN entry.	An error occurs while configuring a CIN entry.
Both -id and -ip are required for adding a CIN entry.	A user tries to enter a command to add an entry without both -id and -ip options.
CIN blade pair TLV get failed	An error occurs while the management module is getting CIN blade server configuration parameters.
CIN global TLV get failed.	An error occurs while the management module is getting a CIN global configuration parameter.
CIN command failed.	An error occurs while the management module is executing a CIN command.
cin -*index* -en *state* cannot be used with other options. where • *index* identifies the cin index entry • *state* is on or off	The user tries to enter a command with the -en option with along with other options.
Duplicate CIN (-id, 0.0.0.0) pairs are not allowed. Please try again.	A user tries to enter a command with a duplicated -id/0.0.0.0 pair.
Duplicate -ip is not allowed. Please try again.	A user tries to enter a command with a duplicated IP address.
Internal error checking CIN entry.	An error occurs while the system checks user input for the CIN entry configuration.
Internal error getting CIN entry	An error occurs while the management module is getting CIN entry configuration parameters.
Invalid index parameter. Input must be numeric.	A user tries to enter a command with a non-numeric index.
Invalid index parameter. Input out of range.	A user tries to enter a command with an index which is out of range.
Invalid IP argument for an option. Enter 4 bytes separated by 3 dots.	A user tries to enter a command argument for IP address option which is invalid because it is too long, too short, or not numeric.
Invalid IP argument for an option. Too many bytes.	A user tries to enter a command with an invalid argument for IP address option which has more than four parts.
Invalid IP argument for an option. Too few bytes	A user tries to enter a command with an invalid argument for IP address option which has fewer than four parts.
Invalid IP argument for an option. Each byte has to be in the range (0-255).	A user tries to enter a command with an invalid argument for IP address option, each part of which is not in the range of 0-255.
Invalid option argument for -global -en:	A user issues a command with an invalid argument for -global -en option.
Invalid option argument for -en to enable an entry.	An error occurs while the user is enabling/disabling a CIN entry.

clear command errors

This topic lists error messages for the clear command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 108. 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 421 for a list of error messages that apply to all commands.

Table 109. 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 421 for a list of error messages that apply to all commands.

Table 110. 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.

Table 110. clock command errors (continued)

Error message	Definition
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 421 for a list of error messages that apply to all commands.

Table 111. config command errors

Error message	Definition
Arguments containing spaces must be enclosed in quotation marks.	The user tries to enter an advanced management module Contact or Location without ending double quotes.
Contact must be enclosed in quotation marks.	The user tries to enter an advanced management module Contact without enclosing it in double quotes.
Invalid input. Contact may not contain angle brackets.	The user tries to enter an advanced management module Contact containing angle brackets ("<" and ">").
Invalid input. Location may not contain angle brackets.	The user tries to enter an advanced 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 advanced 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.

Table 111. config command errors (continued)

Error message	Definition
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 advanced management module Location without enclosing it in double quotes.
Reading SNMPv1/SNMPv3 status failed.	An internal errors occurs while the advanced 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 421 for a list of error messages that apply to all commands.

Table 112. 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.
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.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 113. dhcpinfo command errors

Error message	Definition
Advanced failover must be enabled before viewing the standby MM's DHCPv6 config.	A user tries to view the configuration of the standby management module when advanced failover is disabled.
Command cannot be issued to this type of Blade. Type env –h for help on changing targets.	A user issues the dhcpinfo command to a blade server that does not support IPv6.
DHCPv6 information is not available.	DHCPv6 is enabled, but the command target is not receiving any DHCPv6 settings.
DHCPv6 is disabled	The DHCPv6 assigned configuration can not be retrieved because DHCPv6 is disabled.
IPv6 is disabled	The DHCPv6 assigned config can not be retrieved because IPv6 is disabled.
This management network interface is not installed.	A user issues the dhcpinfo command to a blade server that does not support a management network interface.

displaylog command errors

This topic lists error messages for the displaylog command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 114. displaylog command errors

Error message	Definition
(There are no more entries in the event log.)	There are no more event log entries to display.
-f and -a cannot be used at the same time.	The user tries to use the -f and -a options in the same command.
-l and -i options must be used exclusive of the other options.	The user tries to issue a command with the -l and -i options at the same time as other options.
-lse option must be used exclusive of the other options	The user tries to set the -lse option at the same time as other options.
Both -l and -i options must be provided to save event log.	The user tries to issue a command to save the event log without -l and -i provided.
Cannot open file: *filename* where *filename* is the name of the file that was entered when the error occurred.	An error occurs while the management module is trying to open a file.
Duplicate date filter: *filter* where *filter* is the duplicate date filter that was entered.	The user tries to use duplicate date filters.
Duplicate call home filter: *filter* where *filter* is N or C.	The user tries to use duplicate call-home filters.

Table 114. displaylog command errors (continued)

Error message	Definition
Duplicate severity filter: *filter* where *filter* is the duplicate severity filter that was entered.	The user tries to use duplicate severity filters.
Duplicate source filter: *filter* where *filter* is the duplicate source filter that was entered.	The user tries to use duplicate source filters.
Invalid date filter: *filter* where *filter* is the invalid date filter that was entered.	The user tries to use an invalid date filter.
Invalid call home filter: *filter* where *filter* is the invalid filter that was entered.	The user tries to use an invalid call-home filter.
Invalid severity filter: *filter* where *filter* is the invalid severity filter that was entered.	The user tries to use an invalid severity filter.
Invalid source filter: *filter* where *filter* is the invalid source filter that was entered.	The user tries to use an invalid source filter.
Putting event log file *filename* to tftp server *ipaddress* failed where: • *filename* is the name of the log file • *ip_address* is the IP address of the TFTP server	An error occurs while the management module is trying to put the event log file to TFTP server.
Reading log entries failed.	An error occurs while the management module is reading log entries.

displaysd command errors

This topic lists error messages for the displaysd command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 115. displaysd command errors

Error message	Definition
-save and -i must both be specified when saving the service data.	A user tries to save the service data without specifying both the file name and IP address of the TFTP server.
Can not get the SRC's detail information.	The advanced management module fails to get the SRC detail information.
Error retrieving blade type.	The advanced management module fails to read the blade server type.
Error transferring file.	An unspecified TFTP error occurs.
No additional information for this SRC.	The advanced management module tries to get the detail information of a SRC which does not have detail information.
Read/write command error.	An error occurs while the management module is processing the command.
The format of the received data is wrong.	The advanced management module receives wrongly formatted data.

dns command errors

This topic lists error messages for the dns command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 116. 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.
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.
IPv6 configuration changes will not take effect until IPv6 is enabled.	A user attempts to configure the IPv6 DNS settings while IPv6 is disabled.
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 421 for a list of error messages that apply to all commands.

ethoverusb command errors

This topic lists errors for the ethoverusb command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 117. ethoverusb command errors

Error message	Definition
Blade SP's command interface on Ethernet-over-USB is not supported on blade *blade_number* where *blade_number* identifies the blade server.	The command is directed to a blade server that does not support Ethernet-over-USB.
Notice: This operation may take a short while to complete. Please view the status to determine when the operation has completed.	Confirmation message indicating that the command is processing and might take a short time to complete.

eventinfo command errors

This topic lists errors for the eventinfo command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 118. eventinfo command errors

Error message	Definition
Error reading eventinfo.	An error occurs when reading event information.
Invalid event ID.	A user attempts to enter an invalid event ID.

events command errors

This topic lists errors for the events command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 119. events command errors

Error message	Definition
-add and -rm should be used exclusively of each other.	A user attempts to issue a command with both options -add and -rm.
Call Home Exclusion List has reached its maximum size of *max* entries. No more events can be added to the list. where *max* is a decimal number.	A user attempts to add an entry while Call Home Exclusion List has reached its maximum size.
Error reading ftp/tftp of Service Data configuration.	An error occurs while the management module is reading the FTP/TFTP service data configuration.
Error reading data for Terms and Conditions.	An error occurs while the management module is reading the terms and conditions data.
Event *id* already exists in Call Home Exclusion List. where *id* is a hexadecimal number that identifies a call-home event.	A user attempts to add an entry which already exists in Call Home Exclusion List.
Event *id* does not exist in the Call Home Exclusion List. where *id* is a hexadecimal number that identifies a call-home event.	A user attempts to remove an entry which does not exist in Call Home Exclusion List.
Event *id* is invalid to be added into Call Home Exclusion List. where *id* is a hexadecimal number that identifies a call-home event.	A user attempts to add an entry with an invalid event id.
ftp/tftp of Service Data must be enabled before using this command.	A user attempts to issue an `events` command while the FTP/TFTP Report of Service Data is disabled
Read Call Home Exclusion List failed.	An error occurs while the management module is reading the Call Home Exclusion List.
The terms and conditions should be accepted first before using this command.	A user attempts to issue an `events` command before the terms and conditions have been accepted.

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 421 for a list of error messages that apply to all commands.

feature command errors

This topic lists errors for the feature command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 120. feature command errors

Error message	Definition
-add option requires -key option	The user tries to add a feature license without specifying the feature license key.
-key option must contain 7 alphanumeric characters	An invalid value was entered for the -key option.
Apply operation timed out	Applying a license file times out..
Error applying license file.	Applying a license file fails.
Error getting errors.	An error occurs while retrieving errors when applying a license file.
Error getting status.	An error occurs while getting status when applying or retrieving a license file.
Error parsing license file.	An error occurs while applying or retrieving a license file.
Error retrieving license file.	The license file fails to retrieve.
Error transferring license file.	The license file fails to transfer.
Failed to apply license to chassis *ip_address* where *ip_address* is the IP address for the BladeCenter unit on which the operation is being performed	An error occurs while applying a license file.
Failed to login to chassis *ip_address* where *ip_address* is the IP address for the BladeCenter unit on which the operation is being performed	An error occurs while applying a license file.
Failed to read license status	An error occur occurs while the advanced management module is reading the status of the feature license.
Failed to remove license for chassis *ip_address* where *ip_address* is the IP address for the BladeCenter unit on which the operation is being performed	An error occurs while applying a license file.
Failed to retrieve data for chassis *ip_address* where *ip_address* is the IP address for the BladeCenter unit on which the operation is being performed	An error occurs while applying a license file.
Failed to retrieve status for chassis *ip_address* where *ip_address* is the IP address for the BladeCenter unit on which the operation is being performed	An error occurs while applying a license file.
Failed to set license key	An error occur occurs while the advanced management module is setting the feature license key.

Table 120. feature command errors (continued)

Error message	Definition
Failed to validate chassis serial number	An error occur occurs while the advanced management module is validating the BladeCenter unit serial number. Make sure that the serial number is correct and retry the command.
Internal error.	An error occurs while retrieving a license file.
Internal error. Something was wrong with the file.	An error occurs while applying a license file.
Invalid error data returned	Error data is not valid.
Invalid license key	An error occur occurs while the advanced management module is validating the feature license key. Make sure that the license key is correct and retry the command.
line *number*: CSV read error. where *number* indicates the line in the license file that is in error.	An error occurs while applying a license file. Error location in license file is specified in the error message.
line *number*: File open error. where *number* indicates the line in the license file that is in error.	An error occurs while applying a license file. Error location in license file is specified in the error message.
line *number*: Incomplete line. where *number* indicates the line in the license file that is in error.	An error occurs while applying a license file. Error location in license file is specified in the error message.
line *number*: Invalid IP. where *number* indicates the line in the license file that is in error.	An error occurs while applying a license file. Error location in license file is specified in the error message.
line *number*: Line too long. where *number* indicates the line in the license file that is in error.	An error occurs while applying a license file. Error location in license file is specified in the error message.
line *number*: Unknown error: *code* where *number* indicates the line in the license file that is in error and *code* indicates the type of error.	An error occurs while applying a license file. Error location in license file is specified in the error message.
Remove license failed	An error occur occurs while the advanced management module is removing a feature license.
Unknown error for chassis *ip_address* where *ip_address* is the IP address for the BladeCenter unit on which the operation is being performed	Error type is unknown.
Unknown error type	Error type is unknown.

files command errors

This topic lists error messages for the files command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 121. files command errors

Error message	Definition
%, /, and \" are not allowed in the filename.	The user tries to enter a filename that is invalid.
Directory does not exist.	The user tries to enter a directory that does not exist.
Error deleting file *filename* where *filename* is the name of the file that was entered for deletion.	An error occurs while the management module is trying to delete a file.
Error deleting file *filename* where *filename* is the name of the file that was entered for deletion.	The user tries to delete a directory or delete a file that does not exist.
Error reading file list.	An error occurs while the management module is reading the directory file list.
Error reading file system space.	An error occurs while the management module is reading the file system space.
Error reading first file in dir *directory*. where *directory* is the name of the directory that was entered.	An error occurs while the management module is reading the first file in the directory.
File index out of sequence.	An error occurs while the management module is reading the index.
File list exhausted.	An error occurs while the management module is reading the file list.
File not found.	The specified file is not found.
Filename must be less than 256 characters	The user tries to enter a filename that is longer than 256 characters.
General, unknown error.	A command is rejected for unknown reasons.
Invalid command sent.	The user tries to enter an invalid command.
Invalid directory, filename.	The user tries to enter an invalid directory and filename.
Invalid file or directory name.	The user tries to enter an invalid directory or filename.
The directory name must be less than 256 characters.	A user tries to enter a directory name that is more than 256 characters in length.
Unknown caller id.	The caller ID is not recognized.
Unknown command.	The user tries to enter a command that is not recognized.
Unknown directory path.	The user tries to enter a directory path that is not recognized.

fuelg command errors

This topic lists error messages for the fuelg command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 122. 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.
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.
Effective CPU Speed not available.	An error occurs while the management module is reading the effective CPU Speed.
Error reading blade power management capability.	An error occurs while the management module is reading the blade server power management capability.
Error reading soft minimum.	An error occurs while the management module is reading the soft minimum value.
Error reading soft minimum, using guaranteed minimum instead.	An error occurs while the management module is reading the soft minimum value.
Error writing data for the option -pme Please make sure the blade is powered on	The user attempts to enable power management and capping for a blade server that is turned off.
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.

Table 122. fuelg command errors (continued)

Error message	Definition
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.
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.

Table 122. fuelg command errors (continued)

Error message	Definition
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.
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.

Table 122. fuelg command errors (continued)

Error message	Definition
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.

groups command errors

This topic lists errors for the groups command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 123. groups command errors

Error message	Definition
When creating a new group, a group name and authority level must be specified.	A user tries to create a new group without specifying a group name or authority level.

health command errors

This topic lists errors for the health command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 124. 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 421 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 421 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 421 for a list of error messages that apply to all commands.

Table 125. 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 125. 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 421 for a list of error messages that apply to all commands.

Table 126. ifconfig command errors

Error message	Definition
-em cannot be reconfigured while Stacking Mode is enabled on the AMM.	The user tries to issue a command with the -em option while Stacking Mode is enabled on the advanced management module.
-ep cannot be reconfigured while Stacking Mode is enabled on the AMM.	The user tries to issue a command with the -ep option while Stacking Mode is enabled on the advanced management module.
-ipv6static, -dhcp6, and -sa6 can't all be disabled.	A user attempts to issue a command that disables -ipv6static, -dhcp6, and -sa6 at the same time.
-*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.
-pip cannot be reconfigured while Stacking Mode is enabled on the AMM.	The user tries to issue a command with the -pip option while Stacking Mode is enabled on the advanced management 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.
Error converting the i6 address from string to bytes.	An error occurs while converting the i6 address from a string to bytes.
Enabling/Disabling new IP configuration failed.	An error occurs while the management module is enabling or disabling the new IP configuration.

Table 126. ifconfig command errors (continued)

Error message	Definition
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 data for Link-local address.	An error occurs while the management module is reading data for the link-local address.
Error reading data for Link-local address prefix length.	An error occurs while the management module is reading data for the link-local address prefix length.
Error reading data for Stateless auto-config IP Addresses.	An error occurs while the management module is reading the stateless auto-configuration IP address.
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).
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 blade cKVM status for blade *blade_number* failed. where *blade_number* identifies the blade server.	An error occurs while the management module is reading the cKVM status of targeted blade.
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.

Table 126. ifconfig command errors (continued)

Error message	Definition
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 (_).
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.

Table 126. ifconfig command errors (continued)

Error message	Definition
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).
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.
Option: -bsmp is not supported any more.	The user tries to direct the command to the -bsmp command target that is no longer supported.
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.
This target is no longer supported by the ifconfig command.	The user tries to direct the command to an invalid command target.
When setting –i6, -p6, or –g6, -id must be included.	A user tries to configure a blade server static IPv6 configuration and does not include the static configuration ID number.

info command errors

This topic lists error messages for the info command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 127. 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 version of cKVM *bay_number* failed. where the *bay_number* specifies the cKVM.	An error occurs while the management module is reading the firmware version of targeted cKVM.
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.
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.
Unable to read firmware VPD.	An error occurs while the management module is reading the firmware VPD.
Unable to read hardware VPD.	An error occurs while the management module is reading the hardware VPD.
Unknown device type.	The command is targeted to an unknown device type.

iocomp command errors

This topic lists errors for the iocomp command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 128. iocomp command errors

Error message	Definition
Error reading I/O Compatibility Detail for blade *blade_number* where *blade_number* identifies the blade server.	An error occurs while the management module is reading I/O compatibility for targeted blade server.
Error reading I/O Compatibility Detail for switch *bay_number* where the *bay_number* identifies the I/O module.	An error occurs while the management module is reading I/O compatibility for targeted I/O module.
ERROR!!! IOM *bay_number* reports incorrect width! sw_width = *sw_width* where • the *bay_number* identifies the I/O module • *sw_width* identifies the invalid width	An error occurs while the management module is reading I/O compatibility for targeted I/O module.
I/O Compatibility Detail or blade *blade_number*: unknown where *blade_number* identifies the blade server.	An error occurs while the management module is getting the width of the targeted blade server.

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 421 for a list of error messages that apply to all commands.

ldapcfg command errors

This topic lists error messages for the ldapcfg command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 129. ldapcfg command errors

Error message	Definition
A Client DN password is configured, client DN must be configured too.	The user tries to issue a command to remove the client DN setting with the client DN password configured.
AMM target name is limited to 63 characters.	A user tries to set an advanced management module target name that is longer than 63 characters.
Argument of option *-arguments* must be enclosed in quotation marks. where *arguments* is the name of the improperly entered arguments	The user tries to issue a command with arguments for the options that are not enclosed in quotation marks.
Arguments containing spaces must be enclosed in quotation marks.	The user tries to issue a command with arguments for options without ending double quotes.

Table 129. ldapcfg command errors (continued)

Error message	Definition
Both password and confirm password must be provided.	The user tries to issue a command without providing both the password and the confirm password.
Client DN password mismatch. Please reenter passwords.	The user tries to issue a command with both -p and -cp options, but their arguments do not match.
Client DN password mismatch. Please reenter passwords.	The user tries to issue a command with both -p and -cp options, but their arguments do not match.
If a Client DN password is configured, client DN must be configured too.	The user tries to issue a command to configure the client DN password while the client DN is not configured.
Invalid option argument for *-option*:*argument*. *format* where: • *option* identifies the option • *argument* identifies the invalid argument • *format* identifies the format of argument	The user tries to issue a command with invalid arguments for the options which do not conform to the format specified.
You are configuring Client DN password, but no Client DN. Please configure a Client DN.	The user tries to issue a command to set Client DN password while the Client DN is not configured.
You must configure a Search Domain given your selection of '*option*' for Domain Source. where *option* is sd or ltsd.	The user tries to issue a command for -ds *option* settings without the Source Domain configured.

led command errors

This topic lists errors for the led command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 130. led command errors

Error message	Definition
-d can only be used with the -loc on.	A user tries to issue a command to set the -d while the -loc setting is off.
Delay value must be less than *max*. where *max* is 60.	User input for the option -d exceeds the maximum.
Error getting LED status.	An error occurs while the management module is getting the system LED status.
Error reading system LED state.	An error occurs while the management module is reading the system LED state.
Error setting system LED.	An error occurs while the management module is configuring the system LED.
Invalid option argument for -loc.	A user tries to enter an invalid argument for the option -loc.
Error setting -loc for blade[slot]	An error occurs while setting location LED for the targeted blade.
-l can only be used by itself.	User issues a command with -l option inclusive of an argument or other options.
Error turning off information LED	An error occurs while the user is setting information LED to off.

Table 130. led command errors (continued)

Error message	Definition
The chassis location LED cannot be turned off at this time because one or more blades have their location LED active.	A user issues a command to turn off the chassis location LED under conditions when this is not allowed.

list command errors

This topic lists error messages for the list command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 131. 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.

mcad command errors

This topic lists error messages for the mcad command.

There are no unique errors for the mcad command. See "Common errors" on page 421 for a list of error messages that apply to all commands.

modactlog command errors

This topic lists errors for the modactlog command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 132. modactlog command errors

Error message	Definition
Unable to read the Module Activity Log.	No module activity log is found in the database.

monalerts command errors

This topic lists errors for the monalerts command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 133. monalerts command errors

Error message	Definition
-*option* must be used exclusive of its sub-options. where *option* is -ca, -wa, or -ia.	A user tries to issue a command with the -ca, -wa, or -ia option at the same time as its sub-options.
Invalid syntax. -ec is only allowed to be enabled.	A user tries to disable -ec (legacy alerts).
Note: If -ec is disabled, monalertsleg should be used.	A user tries to issue a monalerts command with the -ec disabled setting.

monalertsleg command errors

This topic lists errors for the monalertsleg command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Important: The `monalertsleg` command is no longer supported by the advanced management module firmware. Legacy alert monitoring that uses the `monalertsleg` command must transition to use of the `monalerts` command.

Table 134. monalertsleg command errors

Error message	Definition
Invalid syntax. -ec is only allowed to be enabled.	A user tries to disable -ec (legacy alerts).
Note: If -ec is enabled, monalerts should be used.	A user tries to issue a monalertsleg command with the *-ec enable* setting.

mt command errors

This topic lists errors for the mt command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 135. 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.

nat command errors

This topic lists error messages for the nat command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 136. nat command errors

Error message	Definition
Adding code authority failed.	A user tries to add code authority.
External port: Valid range is 1000 through 65534.	The user tries to set the external port number to a value outside of its valid range.
I/O Module is in protected mode and cannot be restored to its default configuration.	The user tries to restore the default configuration of an I/O module while it is in protected mode.
I/O Module is in Protected Mode and cannot change its NAT configuration.	The user tries to change the configuration of an I/O module while it is in protected mode.
Internal port: Valid range is 1 through 65534.	The user tries to set the internal port number to a value outside of its valid range.
NAT configuration is not supported on this IO module.	The user tries to direct a nat command to an I/O module that does not support the network address table.
The first two rules' protocol names cannot be changed.	The user tries to change the protocol names for HTTP or Telnet.

Table 136. nat command errors (continued)

Error message	Definition
When creating a new rule, all fields must be specified.	The user does not specify all the fields when attempting to make a new rule.
Invalid input. '-pn' must be less than *maximum_number* characters. where *maximum_number* is the maximum number of characters allowed for the protocol name.	The user tries to enter a protocol name with a string length of more than the maximum allowed.

ntp command errors

This topic lists error messages for the ntp command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 137. ntp command errors

Error message	Definition
Invalid value passed to -en flag. Valid values are enable/disable	The user input for the *-en* option is invalid.
Please set NTP server name or IP address before enabling NTP	The user tries to enable NTP before setting the server name or IP address.
Please set NTP server name or IP address before synchronizing the clock	The user tries to synchronize the clock before setting the NTP server name or IP address.
Please set NTP update frequency before enabling NTP	The user tries to enable NTP before setting the update frequency.
Please set NTP v3 authentication entry before enabling NTP authentication	The user tries to enable NTP authentication before configuring the v3 authentication.

ping command errors

This topic lists errors for the ping command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 138. ping command errors

Error message	Definition
Error reading IP address of switch *bay_number* where the *bay_number* designates the I/O module.	An error occurs while the management module is getting the current IP address of the targeted switch.
Error reading I/O Module's capabilities.	An error occurs while the management module is reading the I/O Module's capabilities.
Error reading I/O Module's second ip configuration.	An error occurs while the management module is reading the I/O Module's second ip configuration.
Error reading second IP address of I/O Module *bay_number* where the *bay_number* identifies the I/O module.	An error occurs while the management module is reading the second IP address of the I/O Module specified.

Table 138. ping command errors (continued)

Error message	Definition
The I/O module cannot be pinged while the IP config is protected.	The user tries to ping a protected member of an I/O module stack.

pmpolicy command errors

This topic lists errors for the pmpolicy command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 139. pmpolicy command errors

Error message	Definition
Error getting number of domains.	An error occurs while the advanced management module is getting the number of domains.
Getting current policy failed.	An error occurs while the advanced management module is getting the current policy for a domain.
Getting valid policies failed.	An error occurs while the advanced management module is getting the valid policies for power management.

portcfg command errors

This topic lists errors for the portcfg command.

There are no unique errors for the portcfg command. See "Common errors" on page 421 for a list of error messages that apply to all commands.

ports command errors

This topic lists error messages for the ports command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 140. ports command errors

Error message	Definition
A certificate must first be in place before SSL can be enabled.	The user tries to enable SSL before setting up a valid SSL certificate.
An SSH server key must first be in place before SSH can be enabled.	The user tries to enable SSH before setting up a valid SSH server key.
Duplicate port number entered.	The user tries to enter a command with a port number that is already in use.
Enabling SNMPv1 failed	The SNMPv1 configuration does not meet required criteria.
Enabling SNMPv3 failed	The SNMPv3 configuration does not meet required criteria.
Error: A community is configured without an IP address or host name. Please use 'snmp' command for snmp configuration.	Attempted to configure community without an IP address or host name.

Table 140. ports command errors (continued)

Error message	Definition
Error: A duplicate community name is configured. Please use ‘snmp' command for snmp configuration.	Attempted to configure a community name that was already defined.
Error: At least one configured community is required to enable SNMPv1. Please use ‘snmp' command for snmp configuration.	Attempted to enable SNMPv1 without configuring at least one community.
Error: IP address of 0.0.0.0, 0::0 is allowed only when the first community is configed as Get or Set access type. Please use ‘snmp' command for snmp configuration.	IP address of 0.0.0.0 or 0::0 is allowed only when the first community is configured as a GET or SET access type.
Error: System contact must be defined to enable SNMPv1. Please use ‘snmp' command for snmp configuration.	Attempted to enable SNMPv1 without defining a system contact.
Error: System location must be defined to enable SNMPv1. Please use ‘snmp' command for snmp configuration.	Attempted to enable SNMPv1 without defining a system location.
Error: System contact must be defined to enable SNMPv3. Please use ‘snmp' command for snmp configuration.	Attempted to enable SNMPv3 without defining a system contact.
Error: System location must be defined to enable SNMPv3. Please use ‘snmp' command for snmp configuration.	Attempted to enable SNMPv3 without defining a system location.
Error sanity checking of SNMP configuration.	An error occurs while the management module is checking the SNMP configuration.
Invalid parameter. The timeout must be between 0 and 4294967295 seconds.	The user tries to enter a timeout that is outside of the valid range.
Maximum connections can not exceed 20.	A user attempts to configure more than 20 connections.
No valid server certificate is in place for Secure TCP Command Mode. Use the sslcfg command to generate a certificate.	A user tries to change the state of stcm without a valid certificate in place.
Port number out of range.	A user tries to enter a port number that is outside of the valid range.
Resetting all ports to default values failed.	An error occurs while the management module is resetting all ports to their default values.
Secure SMASH CLP cannot be enabled without a valid SSH server key in place.	The user tries to enable the secure SMASH CLP before setting up a valid SSH server key.
The *-prior* option has been deprecated. Please use the -rpp option instead. where *prior* is kvmp, rdp, rdocp, or sdsp.	The user tries to enter a command with a deprecated option, such as -kvmp, -rdp, -rdocp, or -sdsp.
The total number of secure and legacy connections of TCP Command Mode cannot exceed 20	A user attempted to configure more than 20 TCP Command Mode connections.
This I/O module does not support port speed configuration.	The user tries to enter a command for a speed configuration which not supported by the targeted I/O module.
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.

power command errors

This topic lists error messages for the power command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 141. 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.
Powering on/off network clock failed.	An error occurs while the management module is powering the network clock on or off.
Powering on/off Telco Alarm Panel failed.	An error occurs while the management module is powering the Telco Alarm Panel 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.
The I/O Module is powering off.	The user tries to power on, power off, or restart a RAID SAS module which is in the process of powering off. (BladeCenter S only)

rdoc command errors

This topic lists error messages for the rdoc command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 142. rdoc command errors

Error message	Definition
Error getting rdoc status information.	An error occurred while retrieving status information.
Internal error. Please try again.	The command failed to execute.

read command errors

This topic lists error messages for the read command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 143. read command errors

Error message	Definition
Both the -i and -l options must be specified with the -config file.	The user does not specify both the -i and -l options when restoring configuration from a file.
Configuration restore from the chassis failed: i2c bus read error.	An error occurs while the management module is restoring the management module configuration from the BladeCenter unit midplane due to an i2c read error.
Configuration restore from the chassis failed: operation not supported.	An error occurs while the management module is restoring the management module configuration from the BladeCenter unit midplane due to a failed system check.
Configuration restore from the chassis failed: NVRAM compression error.	An error occurs while the management module is restoring the management module configuration from the BladeCenter unit midplane due to an EEPROM compression error.
Configuration restore from the chassis failed: unsupported midplane data format.	An error occurs while the management module is restoring the management module configuration from the BladeCenter unit midplane due to an unsupported EEPROM format.
Could not retrieve encryption data from the configuration file successfully.	The user tries to enter a passphrase that does not match the one that was used to create the backup configuration file.
Error writing autoread flag.	An error occurs while the management module is writing autoread flag.
File transfer failed.	An error occurs while transferring a file during file upload.
Firmware update is in progress. Try again later.	The user tries to restore the management module configuration from the BladeCenter unit midplane while the management module firmware is updating.
Please make sure you enter the correct passphrase for this configuration file.	The user tries to enter a passphrase that does not match the one that was used to create the backup configuration file.
Resource allocation failure! Memory allocation failed for configuration read.	An error occurs while the management module is allocating memory.
The -auto option can only be used with the -config chassis.	The user tries to set the -auto option when restoring the configuration from a file.
The -config option and a config source is required.	The user tries to issue a command to read configuration from a file without specifying both the -config option and config source.
The -config option is required.	The user does not include a required -config option for the command.
The -i, -l, and -p options can only be used with the -config file.	The user tries to specify a TFTP server and a configuration file when restoring the configuration from the BladeCenter unit midplane.
The passphrase is greater than 1600 characters.	The user tries to input a passphrase that exceeds the maximum length.

Table 143. read command errors (continued)

Error message	Definition
The passphrase must be quote-delimited.	The user tries to input a passphrase that is not quote-delimited.
There was a problem retrieving the file.	TFTP encounters an error when transferring the configuration file.
Update Failed, there was a problem retrieving the file.	An error occurs while the advanced management module is uploading a file.

remacccfg command errors

This topic lists error messages for the remacccfg command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

remotechassis command errors

This topic lists error messages for the remotechassis command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 144. remotechassis command errors

Error message	Definition
Clearing the internal discovered list of MM's failed.	An error occurs while the management module is clearing the internal discovered list of management modules.
Discovery cannot be run until SLP has been enabled.	The user tries to discover other BladeCenter units on the network when SLP is disabled.
Error running discovery.	An error occurs while the management module is running discovery.
Getting last discovery time failed.	An error occurs while the management module is reading last discovery time.
Getting the first entry of the internal discovered list of MM's failed.	An error occurs while the management module is reading the first entry of the internal discovered list of management modules.
Getting the internal discovered list of MM's failed.	An error occurs while the management module is reading the internal discovered list of management modules.
Unable to read SLP settings.	An error occurs while the management module is reading SLP settings.

reset command errors

This topic lists error messages for the reset command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 145. 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.
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.

scale command errors

This topic lists errors for the scale command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 146. scale command errors

Error message	Definition
Auto-create partition failed: *error_detail* where *error_detail* provides additional information about the error.	An error occurs while creating a partition.
Clearing complex failed: *error_detail* where *error_detail* provides additional information about the error.	An error occurs while clearing a complex.
Create a partition failed: *error_detail* where *error_detail* provides additional information about the error.	An error occurs while creating a partition.

Table 146. scale command errors (continued)

Error message	Definition
Deleting a partition failed: *error_detail* where *error_detail* provides additional information about the error.	An error occurs while deleting a partition.
Getting complex information failed: *error_detail* where *error_detail* provides additional information about the error.	An error occurs while gathering complex information.
Invalid node slot.	A user tries to enter a slot number for a node or blade server that is not valid. Make sure that the node information specified is valid.
Invalid range of node slots.	A user tries to enter a range of slot numbers for a node or blade server that is not valid. Make sure that the node information specified is valid.
Power controlling a partition failed: *error_detail* where *error_detail* provides additional information about the error.	An error occurs while changing the power state of a partition.
Setting mode failed: *error_detail* where *error_detail* provides additional information about the error.	An error occurs while changing the power state of a partition.

sddump command errors

This topic lists errors for the sddump command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 147. sddump command errors

Error message	Definition
Initiate data collection of *type* type not supported on blade[*x*] where *type* is the type of data requested and *x* is the number of the blade-server bay.	The management module is unable to collect the requested data from the specified blade server.
Initiate data collection type failed.	The management module is unable initiate data collection of the JS12 or JS22 blade server.

sdemail command errors

This topic lists errors for the sdemail command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 148. sdemail command errors

Error message	Definition
-to must be specified.	A user tries to send a service data email message without specifying the recipient.
Error sending service data email.	An error occurs when the management module tries to send a service data email message.
Invalid email address.	A user tries to enter an email address that is not valid.
Invalid input. Email address must be less than 120 characters.	A user tries to enter an email address that is 120 or more characters long.
Invalid syntax. Please type 'sdemail -h' for help.	A user enters the sdemail command without specifying the required options.
Subject must be enclosed in quotation marks.	A user tries to send a service data email message with a subject option that is not enclosed in quotation marks.

security command errors

This topic lists errors for the security command.

There are no unique errors for the security command. See “Common errors” on page 421 for a list of error messages that apply to all commands.

service command errors

This topic lists errors for the service command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 149. service command errors

Error message	Definition
Getting status of debug with USB key failed.	An error occurs while the management module is reading the status of debug with a USB key.

shutdown command errors

This topic lists errors for the shutdown command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 150. 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 421 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 421 for a list of error messages that apply to all commands.

Table 151. 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 421 for a list of error messages that apply to all commands.

Table 152. 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 421 for a list of error messages that apply to all commands.

Table 153. 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 153. 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.

sshcfg command errors

This topic lists errors for the sshcfg command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 154. sshcfg command errors

Error message	Definition
Getting CLI SSH port failed.	An error occurs while the management module is reading the CLI SSH port.
Getting DSA host key failed.	An error occurs while the management module is reading the DSA host key.
Getting host key size failed.	An error occurs while the management module is reading the host key size.
Getting installed key status failed.	An error occurs while the management module is reading the installed key status.
Getting number of SSH public keys installed failed.	An error occurs while the management module is reading the number of SSH public keys installed.
Getting SMASH SSH port failed.	An error occurs while the management module is reading the SMASH SSH port.
When displaying host keys, -hk must be used by itself.	The user tries to issue a command to display the host keys with option -hk.

sslcfg command errors

This topic lists errors for the sslcfg command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 155. sslcfg command errors

Error message	Definition
-dnld must be used with the -cert/-csr (server, client) as well as -i and optionally -l	A user tries to issue a download certificate or certificate signing request command without the -cert or -csr, and -i options.
-i must be provided to download a trusted certificate.	A user tries to issue a downloading trusted certificate command without the -i option.
-upld must be used with the -cert (server, client) as well as -i and -l	A user tries to issue an import certificate command without the -cert, -l and -i options.
Cannot open file: *filename* where *filename* is the name of the file that was entered for opening.	An error occurs while the management module is trying to open a file.
Cert generation for *server/client* failed where *server/client* specifies whether the certificate was being generated for a server or client.	An error occurs while the management module is generating a certificate for the server or client.
CLI map failed error = *error* where *error* specifies error.	An error occurs while the management module is mapping the file to memory.
Converting DER back to X509 format failed.	An error occurs while the management module is converting DER back to X509 format.
CSR generation for *server/client* failed where *server/client* specifies whether the certificate signing request was being generated for a server or client.	An error occurs while the management module is generating a certificate signing request for a server or client.
Downloading *Cert/CSR* to tftp server *argument* is failed where: • *Cert/CSR* specifies whether the user tried to download a certificate or certificate signing request. • *argument* identifies the IP address of the tftp server	An error occurs while the management module is downloading a certificate or certificate signing request to the tftp server for the SSL server or client.
Error: unknown application	An error occurs because an unknown certificate type is referred to.
Exporting *Cert/CSR* failed where *Cert/CSR* specifies whether the user tried to export a certificate or certificate signing request.	An error occurs while the management module is exporting a certificate or certificate signing request.
File transfer failed.	An error occurs while transferring a file during file upload.
Getting *filename* from tfpt server *argument* failed where: • *filename* identifies the name of the requested file • *argument* identifies the IP address of the tftp server	An error occurs while the management module is getting a file from the tftp server.

Table 155. sslcfg command errors (continued)

Error message	Definition
Getting certificate status of standby AMM failed.	An error occurs while the management module is reading the certificate status of the standby advanced management module.
Getting failover mode failed.	An error occurs while the management module is reading the failover mode.
Getting SSL Server/Client Certificate/CSR status failed.	An error occurs while the management module is reading the SSL server or client certificate or certificate signing request status.
Importing *certFileName* is failed where *certFileName* is the name of the certificate that was being imported.	An error occurs while the management module is importing a certificate.
Input length is greater than the maximum characters allowed.	A user tries to issue a command with an invalid argument for the option. The length of the input is greater than maximum.
Invalid IP arg for *-option: argument*. Each byte has to be in the range (0-255) where: • *option* identifies the command option • *argument* identifies the invalid IP address argument	A user tries to issue a command with an invalid argument for the IP Address option. One or more parts is not in the range of 0-255.
Invalid IP arg for *-option: argument*. Enter 4 bytes separated by 3 dots where: • *option* identifies the command option • *argument* identifies the invalid IP address argument	A user tries to issue a command with an invalid argument for the IP Address option. Invalid arguments could be too long, too short, or not numeric in all parts.
Invalid IP arg for *-option: argument*. Too few bytes where: • *option* identifies the command option • *argument* identifies the invalid IP address argument	A user tries to issue a command with an invalid argument for the IP Address option, an argument which has fewer than four parts.
Invalid IP arg for *-option: argument*. Too many bytes where: • *option* identifies the command option • *argument* identifies the invalid IP address argument	A user tries to issue a command with an invalid argument for the IP Address option, an argument which has more than four parts.
Invalid option for Cert generation: -cpwd	A user tries to issue a command with an invalid option -cpwd for certification generation.
Invalid option for Cert generation: -un	A user tries to issue a command with an invalid option -un for certification generation.
IPs Swaps is not configured.	A user tries to issue a command for the SSL configuration against the Standby Server target without the IPs Swaps configured.
Missing required options.	A user tries to issue a command for the SSL configuration without entering all the required options.
No *Cert/CSR* available. where *Cert/CSR* specifies whether the user specified a certificate or certificate signing request.	A user tries to issue a command to download a nonexistent certificate or certificate signing request.

Table 155. sslcfg command errors (continued)

Error message	Definition
No tc*index* available. where *index* is the number of the selected trusted certificate.	A user tries to issue a command to remove or download a nonexistent trusted certificate.
No valid client certificate is in place. Type 'sslcfg -h' for syntax help of the SSLclient Certificate generation command.	A user tries to issue a command to enable the SSL client without a valid client certificate in place.
No valid server certificate is in place. Type 'sslcfg -h' for syntax help of the SSL server Certificate generation command.	A user tries to issue a command to enable the SSL server without a valid server certificate in place.
No valid trusted certificate is in place. Type 'sslcfg -h' for syntax help of the SSL trusted Certificate importing command.	A user tries to issue a command to enable the SSL client without a valid trusted certificate in place.
Putting *filename* to tfpt server *ip_address* failed. where: • *filename* identifies the command option • *ip_address* identifies the IP address of the tftp server	An error occurs while the management module is putting a file to the tftp server.
Update Failed, there was a problem retrieving the file.	An error occurs while the advanced management module is uploading a file.
Writing X509 format certificate to file failed.	An error occurs while the management module is writing the X509 format certificate to File.

syslog command errors

This topic lists errors for the syslog command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 156. syslog command errors

Error message	Definition
Input length is greater than the maximum characters allowed.	A user tries to enter too many characters for an input field.
Invalid host name or ip address.	A user tries to enter an invalid hostname or ip address.
Port number out of range.	A user tries to enter an invalid port number.

tcpcmdmode command errors

This topic lists error messages for the tcpcmdmode command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 157. 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.
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 421 for a list of error messages that apply to all commands.

Table 158. 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.

Table 158. telnetcfg command errors (continued)

Error message	Definition
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.

temps command errors

This topic lists errors for the temps command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 159. temps command errors

Error message	Definition
Blade *blade_number*: Too many SDRs found. where *blade_number* identifies the blade server.	A database error occurs when too many SDRs are found.
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 the specified blade server.

thres command errors

This topic lists errors for the thres command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 160. threshold command errors

Error message	Definition
A duplicate option is found in the requested command.	The user tries to enter a duplicate argument.
Invalid threshold value.	The user tries to enter an invalid threshold value.
Unable to query the threshold request.	An error occurs during the query threshold request.
Unable to set the requested threshold.	An error occurs during the set threshold request.

trespass command errors

This topic lists error messages for the trespass command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 161. trespass command errors

Error message	Definition
twe must be enabled to modify the trespassing warning.	The user tries to issue a command to modify the trespassing warning without the *-twe enabled* setting.
The trespassing warning must be quote-delimited.	The user tries to enter a trespassing warning that is not enclosed in double-quotation marks.
The trespassing warning is greater than 1600 characters.	The user tries to enter a trespassing warning that is longer than 1600 characters.

uicfg command errors

The following table lists error messages for the uicfg command.

See “Common errors” on page 421 for a list of error messages that apply to all commands.

Table 162. uicfg command errors

Error message	Definition
Enabling SNMPv1/v3 failed.	The SNMPv1/v3 configuration does not meet required criteria. Possible configuration errors include: • A community is configured without an IP address or host name. • A duplicate community name is configured. • At least one configured community is required to enable SNMPv1. • IP address of 0.0.0.0 is allowed only for the first host name in the first community. • IP address of 0.0.0.0 is allowed only when the first community is configured as GET or SET access type. • System contact must be defined to enable SNMPv1/v3. • System location must be defined to enable SNMPv1/v3.
Error sanity checking of SNMP configuration.	An error occurs while the management module is sanity-checking the SNMP configuration.
Maximum connections can not exceed *maximum* where *maximum* designates the total number of permitted connections.	A user has 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 configure the Secure TCP Command Mode when a valid server certificate is not in place
Reading telnet/ssh/snmpv1/snmpv3 status failed.	An error occurs while the management module is reading the telnet, ssh, snmpv1, or snmpv3 status.
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.

update command errors

This topic lists error messages for the update command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 163. update command errors

Error message	Definition
-r must be used with -u to update firmware to AMM and automatically reboot AMM if firmware update succeeds.	A user tries to enter a command with the -r option to update firmware to a primary advanced management module, but fails to include the -u option.
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.
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.

Table 163. update command errors (continued)

Error message	Definition
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
Invalid syntax.	The user tries to execute a command without specifying a command option.
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.
Rebooting AMM failed.	An error occurs while the advanced management module is trying to reboot.
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.

Table 163. update command errors (continued)

Error message	Definition
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 421 for a list of error messages that apply to all commands.

Table 164. uplink command errors

Error message	Definition
-ip must be a valid IP address before enabling -el	A user tries to issue a command to enable the -el without a valid -ip setting.
A non-zero IP address must be set before enabling -el.	A user tries to enable -el while both -ip and -ip6 are zero.
At least one IP address must be non-zero when -el is enabled.	A user tries to set both -ip and -ip6 to zero while -el is enabled.
Error converting the IPv6 address from string to bytes.	An error occurs while converting the IPv6 address from a string to bytes.
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`.
No option argument for *option* where *option* is the command option for which no argument was specified.	A user tries to enter a command option without its required argument.
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.

Table 164. uplink command errors (continued)

Error message	Definition
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 421 for a list of error messages that apply to all commands.

Table 165. 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.
Deleting user failed.	An error occurs while the management module is deleting an user.
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.

Table 165. users command errors (continued)

Error message	Definition
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.
File transfer failed.	An error occurs while transferring a file during file upload.
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.
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.

Table 165. users command errors (continued)

Error message	Definition
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.
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.

Table 165. users command errors (continued)

Error message	Definition
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).
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.
Update Failed, there was a problem retrieving the file.	An error occurs while the advanced management module is uploading a file.

Table 165. users command errors (continued)

Error message	Definition
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.

vlan command errors

This topic lists error messages for the vlan command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 166. vlan command errors

Error message	Definition
Error reading vlan config.	An error occurs while the management module is reading the global VLAN settings.
Error reading vlan entry *index*. where *index* is the VLAN entry's index.	An error occurs while the management module is reading a VLAN entry's settings.
Name must be enclosed in quotation marks.	A user attempts to enter a name that does not have opening and closing quotation marks.
Invalid syntax. -commit must be used by itself.	A user issues a command with -commit option inclusive of an argument or other options.
Invalid syntax. -cto must be used by itself.	A user issues a command with -cto option inclusive of other options.
Invalid syntax. restart and default can only be used on individual, non-fixed entries.	A user attempts to use the restart or default on a fixed entry or global VLAN settings.
Invalid syntax. -delete must be used by itself, or in combination with -vi.	A user issues a command with -delete option inclusive of other options, except for -vi.
Error deleting vlan entry *index*. where *index* is the VLAN entry's index.	An error occurs while the management module is deleting a VLAN entry.
Invalid syntax. -state cannot be used on the fixed entry.	A user attempts to use -state on a fixed entry.
Invalid syntax. -c cannot be used on the fixed entry.	A user attempts to use -c on a fixed entry.
Invalid syntax. -i cannot be used on the fixed entry.	A user attempts to use -i on a fixed entry.
Invalid syntax. -g cannot be used on the fixed entry.	A user attempts to use -g on a fixed entry.
Invalid syntax. -s cannot be used on the fixed entry.	A user attempts to use -s on a fixed entry.
Invalid syntax. -sr1 cannot be used on the fixed entry.	A user attempts to use -sr1 on a fixed entry.
Invalid syntax. -sr2 cannot be used on the fixed entry.	A user attempts to use -sr2 on a fixed entry.
Invalid syntax. -sr3 cannot be used on the fixed entry.	A user attempts to use -sr3 on a fixed entry.
Invalid syntax. -sm1 cannot be used on the fixed entry.	A user attempts to use -sm1 on a fixed entry.
Invalid syntax. -sm2 cannot be used on the fixed entry.	A user attempts to use -sm2 on a fixed entry.
Invalid syntax. -sm3 cannot be used on the fixed entry.	A user attempts to use -sm3 on a fixed entry.
Invalid syntax. -tag cannot be used on non-default entries.	A user attempts to set the -tag option on a non-default entry.

Table 166. vlan command errors (continued)

Error message	Definition
Invalid syntax. -vid is needed to create a new entry.	A user attempts to create a new entry without specifying the -vid option.
Error writing -sol - currently assigned to another VLAN.	A user attempts to enable the -sol option on a VLAN entry without disabling it on another VLAN entry first.
Error writing -rp - currently assigned to another VLAN.	A user attempts to enable the -rp option on a VLAN entry without disabling it on another VLAN entry first.
Cannot enable VLAN - configuration incomplete.	A user attempts to enable a VLAN entry before configuring it completely.
Error writing -vid - the VLAN ID is a duplicate.	A duplicate VLAN ID is entered.
Error writing -i - the IP address is either a duplicate, or in the same subnet as another entry	A duplicate IP address is entered.

volts command errors

This topic lists errors for the volts command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 167. volts command errors

Error message	Definition
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 the targeted blade server.

write command errors

This topic lists error messages for the write command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 168. write command errors

Error message	Definition
Failed to save configuration settings to the chassis.	An error occurs while the management module is saving the management module configuration to the BladeCenter unit midplane.
Firmware update is in progress. Try again later.	A user tries to save the management module configuration to the BladeCenter unit midplane while the management module firmware is updating.
Getting security status failed.	An error occurs while the management module is reading the security status.
The -config option is required.	The user does not include a required -config option for the command.
The -i, -l, and -p options can only be used with the -config file.	The user tries to specify a TFTP server and a configuration file when saving the configuration to the BladeCenter unit midplane.
The -i option is required with the -config file.	A user tries to use the -i option with the -config chassis option.

Table 168. write command errors (continued)

Error message	Definition
The -p option is required when encryption is enabled.	The user tries to issue a command without the -p option while encryption is enabled.
Error creating file in memory.	The management module is unable to create the configuration file.
Error locking file.	The management module is unable to lock the configuration file.
Error opening file.	The management module is unable to open the configuration file.
Error transferring file.	The management module is unable to transfer the configuration file.
Error generating file.	The management module is unable to generate the configuration file.
Error allocating memory for file.	The management module is unable to allocate memory for the configuration file.
The passphrase is greater than 1600 characters.	The user input for the passphrase exceeds the maximum permitted length.
The passphrase must be quote-delimited.	The user input for the passphrase is not quote-delimited.

zonecfg command errors

This topic lists errors for the zonecfg command.

See "Common errors" on page 421 for a list of error messages that apply to all commands.

Table 169. zonecfg command errors

Error message	Definition
Activating zone configuration xxx on I/O module yyy failed.	The management module is unable activate the specified zone configuration on the specified I/O module.
Getting current active zone number failed.	An error occurs while the management module is reading the current active zone number.
Getting specified configuration of switch *slot* failed. where *slot* identifies the targeted I/O module.	An error occurs while the management module is reading the specified configuration of the targeted I/O module.
Getting zone configuration failed.	An error occurs while the management module is reading the zone configuration.
Invalid slot number for this command.	The I/O module is not in slot 3 or 4.
The index must be 32 or less.	The configuration index is bigger than 32.
Zone configuration not supported on this switch type.	The user tries to use this command on a non-SAS switch module.
The I/O Module is currently not powered on or in a fault state.	The user tries to show or activate a zone configuration for an RSS or NSS which is in the power-off state and a fault state.
Error retrieving data for I/O module *bay_number*. where *bay_number* identifies the targeted I/O module.	An error occurs while the management module is reading the data for the specified I/O module.

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.

Use this information to obtain additional information about IBM and IBM products, determine what to do if you experience a problem with your IBM system or optional device, and determine 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.

If you believe that you require IBM to perform warranty service on your IBM product, the IBM service technicians will be able to assist you more efficiently if you prepare before you call.

- 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.
- Check for updated firmware and operating-system device drivers for your IBM product. The IBM Warranty terms and conditions state that you, the owner of the IBM product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your IBM service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.ibm.com/systems/info/x86servers/serverproven/compat/us/ to make sure that the hardware and software is supported by your IBM product.
- Go to http://www.ibm.com/supportportal/ to check for information to help you solve the problem.
- Gather the following information to provide to IBM Support. This data will help IBM Support quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (IBM 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs
- Go to http://www.ibm.com/support/entry/portal/Open_service_request/ to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to IBM Support quickly and efficiently. IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

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/supportportal/.

Getting help and information from the World Wide Web

Up-to-date information about IBM products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about IBM systems, optional devices, services, and support is available at http://www.ibm.com/supportportal/. IBM System x information is at http://www.ibm.com/systems/x/. IBM BladeCenter information is at http://www.ibm.com/systems/bladecenter/. IBM IntelliStation information is at http://www.ibm.com/systems/intellistation/.

How to send DSA data to IBM

Use the IBM Enhanced Customer Data Repository to send diagnostic data to IBM.

Before you send diagnostic data to IBM, read the terms of use at http://www.ibm.com/de/support/ecurep/terms.html.

You can use any of the following methods to send diagnostic data to IBM:

- **Standard upload:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Standard upload with the system serial number:** http://www.ecurep.ibm.com/
- **Secure upload:** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Secure upload with the system serial number:** https://www.ecurep.ibm.com/

Creating a personalized support web page

You can create a personalized support web page by identifying IBM products that are of interest to you.

To create a personalized support web page, go to http://www.ibm.com/support/mynotifications/. From this personalized page, you can subscribe to weekly email

notifications about new technical documents, search for information and downloads, and access various administrative services.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with your IBM products.

For information about which products are supported by Support Line in your country or region, see http://www.ibm.com/services/supline/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 Business Partners** 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

Use this information to contact 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product, and use of those websites 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 of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies.

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 and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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.

Important notes

Processor speed indicates 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 can 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 that are available from IBM.

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

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as “total bytes written” (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. IBM is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

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 might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If IBM determines that the levels of particulates or gases in your environment have caused damage to the device, IBM may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 170. Limits for particulates and gases

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

1. ASHRAE 52.2-2008 - Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.
2. The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.
3. ANSI/ISA-71.04-1985. Environmental conditions for process measurement and control systems: Airborne contaminants. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Documentation format

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF files and want to request a web-based format or accessible PDF document for a publication, direct your mail to the following address:

Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

In the request, be sure to include the publication part number and title.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Telecommunication regulatory statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Federal Communications Commission (FCC) statement

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

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

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

Industry Canada Class A emission compliance statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

Australia and New Zealand Class A statement

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

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Germany Class A statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japan VCCI Class A statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Korea Communications Commission (KCC) statement

이 기기는 업무용(A급)으로 전자파적합기기로
서 판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для
снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission statement

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

Taiwan Class A compliance statement

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

Index

Special characters

! 168
? 166

A

accessibility features for this product 2
accessible documentation 496
account inactivity alert time
  set for management module 34
account inactivity disable time
  set for management module 35
account lockout period
  set for management module 36
account security commands 30
account security settings
  display for management module 30
  enable complex password for management module user authentication 33
  enable default administration password expiration for management module 34
  enable password change at first login to management module 36
  enable password required for management module 37
  set management module account inactivity alert time 34
  set management module account inactivity disable time 35
  set management module account lockout period 36
  set management module authentication logging timeout 32
  set management module CLI inactivity timeout 33
  set management module default to high 32
  set management module default to legacy 31
  set management module maximum LDAP sessions for user 36
  set management module maximum number of login failures 35
  set management module minimum number of different characters for password 34
  set management module password expiration time 37
  set management module password minimum change interval 37
  set management module password reuse cycle 38
  set management module user authentication method 33
  set management module web interface inactivity timeout 38
accseccfg 30
accseccfg *(continued)*
  options
    alt 32
    am 33
    cp, on 33
    ct 33
    dc 34
    de, on 34
    high 32
    ia 34
    ici 35
    id 35
    legacy 31
    lf 35
    lp 36
    mls 36
    pc, on 36
    pe 37
    pi 37
    pr, on 37
    rc 38
    wt 38
accseccfg command errors 423
accseccfg commands 30
  example 38
accumulate timeout
  set for SOL 332
acknowledge alarms
  alarm ID 46
  complete alarm key 46
  generator ID 45
  generator information 45
acknowledge call-home activity log entry
  management module 94
acoustic mode, disable 153
acoustic mode, enable 153
activate firmware
  I/O module 369, 373
  switch 369, 373
activate I/O module SAS zone 415
activate network protocol settings
  I/O module 241
activate SAS zone
  I/O module 415
Active Directory group, delete 161
Active Directory group, set authority level 160
Active Directory group, set name 159
Active Directory groups, display (all) 159
Active Directory groups, display (specific) 159
add Call Home events
  management module 140, 141
add feature license
  management module 144
add firmware build ID list entry
  blade server 81
add SSH public key 394
add SSH public key (specific) 394
additional SSL certificate
  disable for standby management module 339
  enable for standby management module 339
address
  IPv6 initial connection 15
  link local 15
address prefix length
  set for blade server 190
  set for channel 0 of management module 180
  set for I/O module 198
advanced failover settings
  disable network interface for standby management module 40
  display for management module 40
  enable network interface for standby management module and allow IP swap during failover 40
  enable network interface for standby management module and prevent IP swap during failover 41
advanced management module
  disable logical uplink failover 376
  enable logical uplink failover 376
  enable physical uplink failover 375
  logical uplink failover delay 376
  logical uplink failover IP address 376
  logical uplink failover IPv6 IP address 377
  network interface management commands 66
  physical uplink failover delay 375
  set logical link loss alert and failover policy 377
advfailover 40
  options
    ip. noswap 41
    ip. off 40
    ip. swap 40
advfailover command 40
  example 41
advfailover command errors 424
air filter
  set notification interval 42
  view notification interval 42
air filter notification 42
airfilter
  example 42
  management module 42
airfilter command
  0, 1, 3, 6 months 42
  notification interval 42
alarm
  acknowledge (alarm ID) 46
  acknowledge (complete alarm key) 46
  acknowledge (generator ID) 45
  acknowledge (generator information) 45

alarm *(continued)*
clear (alarm ID) 48
clear (complete alarm key) 48
clear (generator ID) 47
clear (generator information) 47
display (alarm ID) 44
display (all) 43
display (complete alarm key) 44
display (generator ID) 43
display (generator information) 44
display (power) 43
options
c, a 48
c, g 47
c, k 48
c, o 47
p 43
q 43
q, a 44
q, g 43
q, k 44
q, o 44
r, a 46
r, g 45
r, k 46
r, o 45
s, l 49
set 49
alarm command 43
alarm command errors 425
alarm commands
example 49
alarm panel
command target 135
alarm panel module
power off 272
power on 272
turn off 272
turn on 272
alert
test 58
alert categories (enhanced legacy)
disable 229
enable 229
alert notification method, set 57
alert recipient, create 54
alert recipient, delete 53
alert recipient, set email address 57
alert recipient, set hostname for alerts 58
alert recipient, set IP address for alerts 58
alert recipient, set name 55
alert recipient, set status 56
alert recipients, manage 53
alert state
display all 229
alert type, filter 56
alert type, set 56
alertcfg 51
options
dr 51
rl 51, 52
si 51
alertcfg command errors 426
alertcfg commands 51
example 52
alertentries 53
options
1 through 12 53
create (n, status, f, t, e, i) 54
del 53
e 57
f 56
i 58
n 55
status 56
t 57
test 58
alertentries command 53
alertentries command errors 426
alertentries commands
example 59
alerts
disable monitoring for all critical 229
disable monitoring for all informational 234
disable monitoring for all warning 232
disable monitoring for blade device critical 230
disable monitoring for blade device informational 235
disable monitoring for blade device warning 232
disable monitoring for chassis critical 231
disable monitoring for chassis informational 236
disable monitoring for chassis warning 233
disable monitoring for cooling device critical 231
disable monitoring for cooling device informational 238
disable monitoring for cooling device warning 234
disable monitoring for event log informational 237
disable monitoring for event log warning 233
disable monitoring for I/O module critical 230
disable monitoring for I/O module informational 235
disable monitoring for I/O module warning 232
disable monitoring for inventory change informational 236
disable monitoring for network change informational 237
disable monitoring for power module critical 231
disable monitoring for power module informational 238
disable monitoring for power module warning 234
disable monitoring for power state informational 236
disable monitoring for storage module critical 230
disable monitoring for storage module informational 235
alerts *(continued)*
disable monitoring for storage module warning 233
disable monitoring for system management critical 231
disable monitoring for system management informational 236
disable monitoring for system management warning 233
disable monitoring for user activity informational 237
display all states 229
enable monitoring for all critical 229
enable monitoring for all informational 234
enable monitoring for all warning 232
enable monitoring for blade device critical 230
enable monitoring for blade device informational 235
enable monitoring for blade device warning 232
enable monitoring for chassis critical 231
enable monitoring for chassis informational 236
enable monitoring for chassis warning 233
enable monitoring for cooling device critical 231
enable monitoring for cooling device informational 238
enable monitoring for cooling device warning 234
enable monitoring for event log informational 237
enable monitoring for event log warning 233
enable monitoring for I/O module critical 230
enable monitoring for I/O module informational 235
enable monitoring for I/O module warning 232
enable monitoring for inventory change informational 236
enable monitoring for network change informational 237
enable monitoring for power module critical 231
enable monitoring for power module informational 238
enable monitoring for power module warning 234
enable monitoring for power state informational 236
enable monitoring for storage module critical 230
enable monitoring for storage module informational 235
enable monitoring for storage module warning 233
enable monitoring for system management critical 231
enable monitoring for system management informational 236

alerts *(continued)*
enable monitoring for system management warning 233
enable monitoring for user activity informational 237
exclude service information with email alerts 51
include service information with email alerts 51
alerts, display 164
timestamp 164
algorithms, encryption 14
all information reload 204
assistance, getting 489
attributes, display for firmware 365
Australia Class A statement 497
authentication logging timeout
set for management module 32
authentication method
LDAP 217
authority, command 8
autoftp
options
desc 60
i 61
m 61
p 61
pw 61
u 61
autoftp command errors 427
autoftp commands 60
example 62
autoftp settings
call-home 60, 61
automatic configuration setting
display for management module 280
automatic power-on policy
set for BladeCenter unit 275

B

battery backup unit
command target 134
baud rate
set for serial port of management module 253
bay data
blade server 63
clear bay data 63
clear bay data for specific bay 64
display bay data 63
display bay data for specific bay 63
set bay data 64
set data definition to specific blade server 65
baydata 63
options
b bay_num 63
b bay_num -clear 64
b bay_num -data "data_definition" 65
clear 63
data "data_definition" 64
baydata command errors 427
baydata commands 63
example 65
binding method
LDAP 217
blade mezzanine
command target 133
blade server 185, 186
add firmware build ID list entry 81
all blade servers 78
bay data 63
boot 72
boot (to console) 72
collect service data 301
command target 132
config command 111, 114
example 114
create firmware build ID list 80
cycle power 72, 273
delete all entries from firmware build ID list 84
delete entry from firmware build ID list 85
dhcpinfo commands 117
disable cKVM 185
disable DHCPv6 191
disable Ethernet channel 190
disable IPv6 190
disable IPv6 stateless auto-configuration 191
display all SRC records 124
display bay data 63
display boot mode 74
display boot sequence 75
display cKVM status 184
display Ethernet-over-USB setting 137
display firmware build IDs 80
display management network DHCP configuration 117
display name 111
display network configuration status 184
display power state 273
display service data 301
display specific SRC record 124
display temperature 357
display voltage 412
dump service data 301
enable cKVM 185
enable DHCPv6 configuration 191
enable dynamic power optimizer 155
enable dynamic power optimizer, extended 156
enable Ethernet channel 189
enable IPv6 190
enable IPv6 stateless auto-configuration 191
enable local power control 275
enable power capping 154
enable power management 154
enable power saver mode 155
enable Wake on LAN 274
export firmware build ID list 86
get service data 301
import firmware build ID list 85
power off 272, 273
power on 272, 273
power on (to console) 272, 273
reset 72, 288
blade server *(continued)*
reset (clear NVRAM) 291
reset (enter SMS menu) 292
reset (run diagnostics with boot sequence) 291
reset (run diagnostics) 291
reset (to console) 72, 289
reset (with NMI) 290
set address prefix length 190
set as KVM owner 208
set as media tray owner 239
set boot mode 74
set boot sequence 76, 78
set Ethernet channel configuration method 188
set Ethernet channel gateway IP address (IPv4) 186
set Ethernet channel gateway/default route (IPv6) 187
set Ethernet channel hostname 189
set Ethernet channel subnet mask (IPv4) 187
set Ethernet channel VLAN ID 188
set Ethernet-over-USB setting 137
set I/O module for blade server management traffic 184
set IP address (IPv4) 185
set IP address (IPv6) 186
set name 111
set power capping 154
shutdown 273, 308
turn off 272, 273
turn on 272, 273
turn on (to console) 272, 273
update firmware build ID in firmware build ID list 83
update firmware build revision in firmware build ID list 84
update firmware type in firmware build ID list 83
update machine type in firmware build ID list 82
update manufacturer in firmware build ID list 82
blade server ISMP
set IP address (IPv4) 191
blade server module
display activity 228
display information 228
blade server power information display (overview) 149
blade server, display power trending 151, 152
blade servers
disable multiple video sessions 192
enable multiple video sessions 192
BladeCenter Open Fabric Manager
BladeCenter units 66
I/O modules 66
management module 66, 67, 68, 69, 70, 71
network interface management commands 66
NIC allocation 66
BladeCenter S 150
display
power management policies 251

BladeCenter T specific commands 29
BladeCenter unit
command target 132
configuring 20
disable global cKVM 193
disable management channel auto-discovery 227
display management channel auto-discovery status 227
display network settings 192
display serial number 111
display type/model 111
display uuid 111
enable global cKVM 193
enable management channel auto-discovery 227
set automatic power-on policy 275
set VLAN ID 192
BladeCenter units
clear list of discovered 286
display all discovered 285
display filtered by IP address 285
display filtered by name 286
display health for all discovered 285
blink location LED 169, 222
blower
command target 134
blower power information display 149
blower temperature display 149
blower, display power trending 151, 152
BMC
command target 133
bofm
options
l , i 66
l , i, d 67
l , i, d on 68
l , i, p off 70
l , i, p on 69
l , i, v 71
bofm command
example 71
bofm command errors 428
bofm commands 66
boot 72
blade server 72
options
c 72
p powercycle 72
p reset 72
boot (to console)
blade server 72
boot command errors 429
boot commands 72
example 73
boot mode
display for blade server 74
set for blade server 74
boot sequence
display for blade server 75
set for all blade servers 78
set for blade server 76
bootmode 74
options
p 74
bootmode command errors 429
bootmode commands 74
bootmode commands *(continued)*
example 74
bootseq 75
cd 76
floppy 76
hd0 76
hd1 76
hd2 76
hd3 76
hd4 76
hyper 76
iscsi 76
iscsicrt 76
legacy 76
nodev 76
nw 76
options
all 78
uefi 76
usbdisk 76
bootseq command errors 430
bootseq commands 75
example 79
buildidcfg 80
options
ab 81
create 80
db 84, 85
export 86
import 85
ub, ft 83
ub, id 83
ub, mfg 82
ub, mt 82
ub, rev 84
buildidcfg command errors 430
buildidcfg commands 80
example 86
built-in commands 27

C

call-home
autoftp settings 60, 61
problem description 95
test call home 96
call-home activity log
acknowledge call-home activity log entry for management module 94
display for management module 93
display FTP/TFTP server entries for management module 93
display IBM Support entries for management module 93
unacknowledge call-home activity log entry for management module 94
capture service information 124
certificate file (SSL CSR)
download 344
import 345
upload 345
certificate file (SSL self-signed certificate)
download 344
import 345
upload 345
change command environment 25, 131
change user password 387
chassis internal network command
cin 97
chassis internal network configuration 97
chassis internal network status 102
chassis internal network status command 102
chconfig 87
options
ca 89
cci 89
ce 89
cn 89
co 89
cph 89
cs 89
cz 89
li 87
loc 91
po 91
ps 91
pw 91
sa 88
sc 89
u 91
chconfig command errors 431
chconfig commands 87
example 91
China Class A electronic emission statement 499
chlog 93
options
ack 94
f 93
s 93
chlog command errors 432
chlog commands 93
example 94
chmanual
options
desc 95, 96
chmanual command errors 433
chmanual commands 95
example 96
cin 97
options
entry_index -ip ip_address 99
entry_index clear 98
entry_index en 98
entry_index id 99
global en 97
id 100
vlan_id -ip ip_address 99
CIN
turn all index entries on or off 98
cin all
options
clear 97
en state 98
cin command
chassis internal network 97
cin command errors 433
cin commands
example 100
cin configuration
Specify VLAN ID 100
CIN configuration 98

CIN configuration entries 97
CIN configuration entry
create 99
delete 98
disable 98
enable 98
Specify IP address 99
CIN configuration table
display for management module 97
CIN index entry
create 99
Specify IP address 99
CIN state
set for enable or disable 97
CIN status table entries 102
cinstatus 102
cinstatus command 102
cinstatus commands
example 102
cKVM
disable for blade server 185
disable globally for BladeCenter unit 193
enable for blade server 185
enable globally for BladeCenter unit 193
cKVM status
display for blade server 184
Class A electronic emission notice 496
clear
options
cnfg 103
clear alarms
alarm ID 48
complete alarm key 48
generator ID 47
generator information 47
clear CIN configuration
management module 97
clear command 103
clear command errors 435
clear commands
example 104
clear event log
management module 105
clear for management module 97
clear management module event log commands 105
example 105
clearlog
l 105
clearlog command errors 435
clearlog commands 105
example 105
CLI
exit codes for SSH 20
CLI inactivity timeout
set for management module 33
CLI key sequence
set for SOL 334
CLI SSH server
disable for management module 338
enable for management module 338
clock 106
options
d 106
dst 109
clock *(continued)*
options *(continued)*
g 107
t 106
clock command errors 435
clock commands 106
example 110
clock settings
display for management module 106
collect service data
blade server 301
command
health 163, 164
system physical configuration 225
command authority 8
command environment selecting 6
command history 168
command redirect 25, 131
command syntax 29
command target 25, 131
alarm panel 135
battery backup unit 134
blade mezzanine 133
blade server 132
BladeCenter unit 132
blower 134
BMC 133
disk drive 135
high-speed expansion card 133
I/O module 134
I/O-expansion card 133
integrated system management processor 133
management card 133
management module 132
media tray 134
memory 133
microprocessor 133
multiplexer expansion module 135
network clock module 135
power module 134
service processor 133
storage expansion unit 133
storage module 135
switch module 134
temporary 7
view 225
command target selection 6
command-line interface
enable for management module 361
errors 419
guidelines 5
case sensitivity 6
command history 6
data types 6
delimiters 6
help 6
options 5
output format 6
strings 6
introduction 1
starting 14
using 5, 25
command-line session configuration
display for management module 356
command-line timeout
set for management module 356
commands
accseccfg 30, 38
Active Directory, group authentication 159
advfailover 40, 41
airfilter 42
alarm 43, 49
alertcfg 51, 52
alertentries 53, 59
autoftp 60, 62
baydata 63, 65
bofm 66, 71
boot 72, 73
bootmode 74
bootseq 75, 79
buildidcfg 80, 86
built-in 27
chconfig 87, 91
chlog 93, 94
chmanual 95, 96
cin 100
cin command 97
cinstatus 102
cinstatus command 102
clear 103, 104
clear management module event log 105
clearlog 105
clock 106, 110
common 27
config 111, 114
configuration 27
console 115, 116
dhcpinfo 117, 118
discovery 28
display management module call-home events in events log 93
display management module event log 119, 123
displaylog 119, 123
displaysd 124, 125
dns 126, 129
environment 131, 136
ethoverusb 137
event log, clear for management module 105
event log, display for management module 93, 119, 123
eventinfo 138, 139
events 140, 141
examples
account security 38
accseccfg 38
advfailover 41
alarm 49, 223
alertcfg 52
alertentries 59
autoftp 62
baydata 65
blade server name 114
BladeCenter Open Fabric Management 71
bofm 71
boot 73
bootmode 74
bootseq 79
buildidcfg 86

commands *(continued)*
examples *(continued)*
chconfig 91
chlog 94
chmanual 96
cin 100
cinstatus 102
clear 104
clear management module event log 105
clearlog 105
clock 110
config 114
configure automated message settings 62
console 116
DHCP settings for management module 118
dhcpinfo 118
display automated message settings 62
display call-home owner 96
display KVM owner 209
display management module event log 123
display management module security 305
display media tray owner 240
display Service Advisor owner 91
display service information owner 303
displaylog 123
displaysd 125
DNS 129
env 136
environment 136
environment redirect 136
Ethernet network settings for management module 200
ethoverusb 137
eventinfo 139
events 141
exit 143
feature 146
files 147
fuelg 156
groups 162
health 164
help 166
history 168
I/O management 71
I/O module network protocol configuration 244
identify 170
ifconfig 200
info 205
iocomp 206
kvm 209
LDAP configuration for management module 219
ldapcfg 219
list 225
management module DHCP settings 118
management module DNS 129
management module Ethernet network settings 200
commands *(continued)*
examples *(continued)*
management module event log clear 105
management module event log display 123
management module LDAP configuration 219
management module name 114
management module network port configuration 270
management module restore configuration 282
management module save configuration 414
management module serial port settings 254
management module service 306
management module SLP configuration 309
management module SMTP settings 312
management module SNMP settings 328
management module SSH 338
management module telnet configuration 356
management module uplink failover 377
management module vlan 410
mcad 227
modactlog 228
monalerts 238
mt 240
name for blade server 114
name for management module 114
nat 244
network port configuration for management module 270
network protocol configuration for I/O module 244
ntp 247
ping 249
pmpolicy 252
portcfg 254
ports 270
power 277
rdoc 279
read 282
remotechassis 286
reset 292
restore configuration for management module 282
save configuration for management module 414
scale 300
sddump 302
sdemail 303
security 305
Serial Over LAN 335
serial port settings for management module 254
service 306
set call-home 96
set KVM owner 209
commands *(continued)*
examples *(continued)*
set management module security 305
set media tray owner 240
set Service Advisor 91
set service information 303
shutdown 308
slp 309
SLP configuration for management module 309
smtp 312
SMTP settings for management module 312
snmp 328
SNMP settings for management module 328
sol 335
SSH configuration for management module 338
sshcfg 338
sslcfg 348
syntax help 166
syslog 352
tcpcmdmode 355
telnetcfg 356
temps 357
trespass 359
uicfg 363
update 373
uplink 377
user account security 38
user interface configuration 363
users 400
vlan 410
vlan configuration for management module 410
volts 412
write 414
zonecfg 416
exit 143
feature 144, 146
files 147
fuelg 149, 156
group authentication, Active Directory 159
groups 159, 162
help 166
history 168
identify 169, 170
ifconfig 171, 200
info 203, 205
iocomp 206
kvm 208, 209
ldapcfg 210, 219
led 220, 223
LED 29
list 225
management module event log 28
management module failover 375, 377
mcad 227
memory 29
modactlog 228
monalerts 229, 238
monalertsleg 229
mt 239, 240

commands *(continued)*
nat 241, 244
ntp 245, 247
ping 248, 249
pmpolicy 251, 252
portcfg 253, 254
ports 255, 270
power 272, 277
power control 29
power management 29
power management policy 251
rdoc 278, 279
read 280, 282
remacccfg 283
remotechassis 285, 286
reset 288, 292
reset command 29
restore configuration 29
save configuration 29
scale 293, 300
sddump 301, 302
sdemail 303
security 305
Serial Over LAN 330, 335
service 306
session command 29
shutdown 308
slp 309
smtp 311, 312
snmp 314, 328
SOL 330, 335
sshcfg 337, 338
sslcfg 339, 348
syslog 349, 352
system management command 29
tcpcmdmode 353, 355
telnet configuration 356
telnetcfg 356
temps 357
trespass 358, 359
uicfg 361, 363
update 365, 373
uplink 375, 377
user interface configuration 361, 363
users 379, 400
vlan 402, 410
volts 412
write 413, 414
zonecfg 415, 416
comment SSH public key 400
commit
VLAN settings 402
commit timeout
VLAN settings 402
common commands 27
common errors 421
communicating with IBM Systems Director 353
communication
out-of-band 353
test I/O-module IP address 249
test IP address 248
test IP address (I/O-module) 249
communication rate
set for serial port of management module 253
compatibility
I/O module
display details for blade server 206
display details for I/O module 206
display for all components 206
component and reloading information 203
component information display 203
config 111
options
contact 112, 113, 114
loc 112
name 111
config command 111
example 114
config command errors 436
configuration
disable automatic for management module 282
enable automatic for management module 281
save for management module (to chassis) 413
view for management module 225
view tree for system 225
configuration (encryption)
save for management module (to file) 414
configuration (no encryption)
save for management module (to file) 413
configuration commands 27
configuration from file (encryption)
restore for management module 281
configuration from file (no encryption)
restore for management module 280
configuration from midplane
restore for management module 280
configuration information
display for network card 184
configuration method
set for channel 0 of management module 176
set for channel of blade server 188
configure LDAP command
example 219
configure network ports command
example 270
configure network protocols command
example 244
configure SLP command
example 309
confirm password
LDAP distinguished name 218
connect to SSH public key 399
console 115
create override SOL session 115
create SOL session 115
non-persistent session 115
options
l 115
o 115
persistent console 115
console command 115
console command errors 437
console commands
example 116
contact information
Service Advisor 89
contact information, Service Advisor
city 89
company 89
contact name 89
country 89
email address 89
phone number 89
postal code 89
state 89
street address 89
contact name
display for management module 111
set for management module 112, 113, 114
contamination, particulate and gaseous 495
create
VLAN entry 404
create alert recipient 54
create CIN configuration entry 99
create CIN index entry 99
create firmware build ID list
blade server 80
create override SOL session 115
create partition
scalable complex 296
create partition (automatically)
scalable complex 294
create SOL session 115
persistent console 115
create stand-alone partition
scalable complex 295
create stand-alone partition (automatically)
scalable complex 294
create user 383
creating a personalized support web page 490
critical alerts
disable monitoring for all 229
disable monitoring for blade device 230
disable monitoring for chassis 231
disable monitoring for cooling device 231
disable monitoring for I/O module 230
disable monitoring for power module 231
disable monitoring for storage module 230
disable monitoring for system management 231
enable monitoring for all 229
enable monitoring for blade device 230
enable monitoring for chassis 231
enable monitoring for cooling device 231
enable monitoring for I/O module 230
enable monitoring for power module 231

critical alerts *(continued)*
enable monitoring for storage module 230
enable monitoring for system management 231
CSR
generate for LDAP client 343
generate for management module web server 343
CSR (SSL)
download certificate file 344
import certificate file 345
upload certificate file 345
custom support web page 490
cycle power
blade server 72, 273
I/O module 273
switch module 273

D

data encryption
display management module setting 305
enable for management module 305
data rate
set for channel 0 of management module 177
set for channel 1 of management module 182
date
display for management module 106
set for management module 106
daylight-savings time mode
set for management module 109
daylight-savings time setting
display for management module 106
default IP address 15
delete
VLAN entry 403, 404
delete Active Directory group 161
delete alert recipient 53
delete all entries from firmware build ID list
blade server 84
delete all partitions
scalable complex 296
delete CIN configuration 98
delete entry from firmware build ID list
blade server 85
delete file
management module 147
delete partition
scalable complex 297
delete user 380
DHCP configuration
display for I/O module 117
DHCP settings for management module commands
example 118
dhcpinfo 117
options
eth0 117
dhcpinfo command errors 438
dhcpinfo commands 117
example 118
DHCPv6
disable for blade server 191
disable for I/O module 198
disable for management module 180
enable for blade server 191
enable for I/O module 198
enable for management module 180
disable
additional SSL certificate for standby management module 339
blade server Ethernet channel VLAN ID 189
BladeCenter unit VLAN ID 192
CLI SSH server for management module 338
enhanced legacy alert categories 229
logging of login events from same IP address 35
monitoring for all critical alerts 229
monitoring for all informational alerts 234
monitoring for all warning alerts 232
monitoring for blade device critical alerts 230
monitoring for blade device informational alerts 235
monitoring for blade device warning alerts 232
monitoring for chassis critical alerts 231
monitoring for chassis informational alerts 236
monitoring for chassis warning alerts 233
monitoring for cooling device critical alerts 231
monitoring for cooling device informational alerts 238
monitoring for cooling device warning alerts 234
monitoring for event log informational alerts 237
monitoring for event log warning alerts 233
monitoring for I/O module critical alerts 230
monitoring for I/O module informational alerts 235
monitoring for I/O module warning alerts 232
monitoring for inventory change informational alerts 236
monitoring for network change informational alerts 237
monitoring for power module critical alerts 231
monitoring for power module informational alerts 238
monitoring for power module warning alerts 234
monitoring for power state informational alerts 236
monitoring for storage module critical alerts 230
monitoring for storage module informational alerts 235
disable *(continued)*
monitoring for storage module warning alerts 233
monitoring for system management critical alerts 231
monitoring for system management informational alerts 236
monitoring for system management warning alerts 233
monitoring for user activity informational alerts 237
secure TCP command mode 354
Service Advisor 88
SMASH SSH server for management module 338
SSL for LDAP client 340
SSL for management module web server 339
syslog event log transmission for collector 1 349
syslog event log transmission for collector 2 350
TCP command mode 353
disable automatic configuration management module 282
disable CIN configuration entry 98
disable cKVM
blade server 185
disable DHCPv6
blade server 191
I/O module 198
management module 180
disable Ethernet channel
blade server 190
disable Ethernet channel 1
management module 184
disable global cKVM
BladeCenter unit 193
disable IPv6
blade server 190
I/O module 197
management module 179
disable IPv6 stateless auto-configuration
blade server 191
I/O module 198
management module 180
disable logical uplink failover
advanced management module 376
management module (advanced) 376
disable management channel auto-discovery
BladeCenter unit 227
disable multiple video sessions
blade servers 192
disable NAT table
I/O module 244
disable NEBS environment mode 153
disable network interface
management module (standby) 40
disable power domain acoustic mode 153
disable SOL
global 333
disable static IPv6 configuration
I/O module 197
management module 179

disable technician debug
management module 306
disable user 381
discovered BladeCenter units
clear list 286
display all 285
display filtered by IP address 285
display filtered by name 286
display health for all 285
discovery commands 28
disk drive 135
display
alert state 229
clock settings, management module 106
date, management module 106
daylight-savings time setting, management module 106
GMT offset, management module 106
management channel path information 204
power management policy
all domains 251
BladeCenter S 251
specified power domain 251
remote presence access 283
TCP command-mode session status 353
TCP command-mode session timeout 353
time, management module 106
VLAN entry 404
VLAN settings 402
display (reset counter) event log
management module 119
display active users 379
display activity
blade server module 228
display advanced failover settings
management module 40
display alarms
alarm ID 44
all 43
complete alarm key 44
generator ID 43
generator information 44
power 43
display alert properties (all recipients) 53
display alert properties (single recipient) 53
display alerts 164
timestamp 164
display all Active Directory groups 159
display all BladeCenter units on network 285
display all event log entries
management module 119
display all event log filters
management module 119
display all information
scalable complex 293
display all users 379
display automatic configuration setting
management module 280
display blade server power information overview 149
display blade server SRC record (specific) 124
display blade server SRC records (all) 124
display blower power information 149
display blower temperature 149
display boot mode
blade server 74
display call-home activity log
management module 93
display call-home event management module event log entries 93
display CIN configuration table 97
display cKVM status
blade server 184
display command-line session configuration
management module 356
display component information 203
display configuration information
network card 184
display contact name
management module 111
display DHCP configuration
I/O module 117
display DNS configuration
management module 126
display DSA host key information
management module 337
display entries of CIN status table 102
display Ethernet channel 0 configuration
management module (primary) 171
management module (standby) 172
display Ethernet channel 0 DHCP configuration
management module 117
display Ethernet channel 1 configuration
management module (primary) 181
display Ethernet-over-USB setting
blade server 137
display event description
management module 138
display event log
management module 119
display event log entries filtered by date
management module 120
display event log entries filtered by severity level
management module 120
display event log entries filtered by source
management module 120, 121
display event user action
management module 138, 139
display events list
management module 140
display failover configuration
management module 375
display features
management module 144
display file list
management module 147
display firmware attributes 365
display firmware build IDs
blade server 80
display free space
management module 140, 147
display FTP/TFTP server call-home activity log
management module 93
display global remote alert settings
management module 51
display health for BladeCenter units on network 285
display health status 163, 164
timestamp 164
display health status (tree) 163
display I/O module compatibility
all components 206
display I/O module compatibility details
blade server 206
I/O module 206
display I/O module power information 149
display I/O module SAS zone information 416
display I/O module SAS zone list 415
display IBM Support call-home activity log
management module 93
display information
blade server module 228
display IP addresses
I/O module 248
display KVM owner 208
display LDAP settings
management module 210
display LED state
blower fault 220
external port link status 220
fanpack fault 220
fault 220
for blade server and all sub-components 221
for blade server front panel 220
safe-to-remove 220
display licenses
management module 144
display location
management module 111
display log entries with call-home events
management module 119
display log entries with Event ID
management module 119
display management channel auto-discovery status
BladeCenter unit 227
display management module account security settings 30
display management module data encryption setting 305
display management module event log commands 119
example 123
display management module security 305
display management module status 124
display management network DHCP configuration
blade server 117
display media tray owner 239
display media tray temperature 149

display name
blade server 111
management module 111
display network configuration status
blade server 184
display network port settings
management module 255
switch 269
display network protocol settings
I/O module 241
display network settings
BladeCenter unit 192
I/O module 193
display node information
scalable complex 293
display NTP configuration
management module 245
display open ports
management module 255
display partition information
scalable complex 293
display POST status
I/O module 276
switch module 276
display power domain information details 150
display power domain information overview 149
display power state
blade server 273
I/O module 273
switch module 273
display power trending (blade server) 151, 152
display power trending (blower) 151, 152
display power trending (I/O module) 151, 152
display power trending (media tray) 152
display power trending (power domain) 151, 152
display power trending (system) 151, 152
display RSA host key information
management module 337
display SAS zone information
I/O module 416
display SAS zone list
I/O module 415
display serial number
BladeCenter unit 111
display serial port configuration
management module 253
display Service Advisor 87
display service data
blade server 301
display service data command 124
display service information 124
display service setting
management module 306
display single user 380
display SLP settings
management module 309
display SMTP server host name
management module 311
display SMTP server IP address
management module 311
display SNMP configuration
management module 314
display specific Active Directory groups 159
display specific complex information
scalable complex 293
display SSH public key 393
display SSH status
management module 337
display state
location LED 169
display state of -lse option
management module 122
Display status of first five CIN entries 102
display syslog configuration
management module 349
display telnet configuration
management module 356
display temperature
blade server 357
management module 357
media tray 357
display trespass feature status
management module 358
display type/model
BladeCenter unit 111
display uplink configuration
management module 375
display user interface settings
management module 361
display uuid
BladeCenter unit 111
display various LED states
LED states 220
display voltage
blade server 412
management module 412
displaylog 119
display log entries with call-home events 119
display log entries with Event ID 119
display state of -lse option 122
filter log entries by call-home events flag 122
options
-lse 122
a 119
c 119
ch 122
date 120
e 119
f 119
filters 119
i 122
i, l 122
l 122
l, i 122
lse 122
sev 120
src 120, 121
displaylog command errors 438
displaylog commands 119
example 123
displaysd 124
options
i 124
displaysd *(continued)*
options *(continued)*
i, save 124
mmstat 124
save 124
save, i 124
src 124
displaysd command errors 439
displaysd commands 124
example 125
distinguished name
LDAP client 218
distinguished name password
LDAP client 218
distinguished name password (confirm)
LDAP client 218
dns 126
options
-ddns 126
i1 127
i2 127
i3 127
i61 128
i62 128
i63 128
on 126
p 129
DNS
enable for management module 126
dns command errors 440
dns commands 126
example 129
DNS configuration
display for management module 126
DNS first IPv4 IP address
set for management module 127
DNS first IPv6 IP address
set for management module 128
DNS second IPv4 IP address
set for management module 127
DNS second IPv6 IP address
set for management module 128
DNS server priority
set for management module 129
DNS third IPv4 IP address
set for management module 127
DNS third IPv6 IP address
set for management module 128
documentation
using 490
documentation format 496
Domain Catalog discovery
set search domain 213
domain name
set for channel 0 of management module 179
set for management module LDAP server 213
download 346, 347, 348
download certificate file
SSL CSR 344
SSL self-signed certificate 344
download SSH public key 398
DSA host key information
display for management module 337
DSA, sending data to IBM 490

dump service data
blade server 301
duplex mode
set for channel 0 of management module 177
set for channel 1 of management module 182
dynamic DNS
enable for management module 126
dynamic power optimizer, enable for blade server 155
dynamic power optimizer, extended , enable for blade server 156

E

electronic emission Class A notice 496
Electronic emission notices 496
email alerts
exclude service information 51
include service information 51
enable
additional SSL certificate for standby management module 339
blade server Ethernet channel VLAN ID 189
BladeCenter unit VLAN ID 192
CLI SSH server for management module 338
enhanced legacy alert categories 229
monitoring for all critical alerts 229
monitoring for all informational alerts 234
monitoring for all warning alerts 232
monitoring for blade device critical alerts 230
monitoring for blade device informational alerts 235
monitoring for blade device warning alerts 232
monitoring for chassis critical alerts 231
monitoring for chassis informational alerts 236
monitoring for chassis warning alerts 233
monitoring for cooling device critical alerts 231
monitoring for cooling device informational alerts 238
monitoring for cooling device warning alerts 234
monitoring for event log informational alerts 237
monitoring for event log warning alerts 233
monitoring for I/O module critical alerts 230
monitoring for I/O module informational alerts 235
monitoring for I/O module warning alerts 232
monitoring for inventory change informational alerts 236
monitoring for logging of login events from same IP address 35
enable *(continued)*
monitoring for network change informational alerts 237
monitoring for power module critical alerts 231
monitoring for power module informational alerts 238
monitoring for power module warning alerts 234
monitoring for power state informational alerts 236
monitoring for storage module critical alerts 230
monitoring for storage module informational alerts 235
monitoring for storage module warning alerts 233
monitoring for system management critical alerts 231
monitoring for system management informational alerts 236
monitoring for system management warning alerts 233
monitoring for user activity informational alerts 237
secure TCP command mode 354
Service Advisor 88
SMASH SSH server for management module 338
SSL for LDAP client 340
SSL for management module web server 339
syslog event log transmission for collector 1 349
syslog event log transmission for collector 2 350
TCP command mode 354
enable automatic configuration
management module 281
enable CIN configuration entry 98
enable cKVM
blade server 185
enable command-line interface
management module 361
enable complex password for management module user authentication 33
enable data encryption
management module 305
enable default administration password expiration for management module 34
enable DHCPv6
blade server 191
I/O module 198
management module 180
enable DNS
management module 126
enable dynamic DNS
management module 126
enable dynamic power optimizer for blade server 155
enable dynamic power optimizer, extended, for blade server 156
enable Ethernet channel
blade server 189
enable Ethernet channel 1
management module 183
enable external management
I/O module 196
enable external ports
I/O module 196
enable fast POST
I/O module 275, 276
enable FTP
management module 261
enable global cKVM
BladeCenter unit 193
enable HTTPS port
management module 262
enable IPv6
blade server 190
I/O module 197
management module 179
enable IPv6 stateless auto-configuration
blade server 191
I/O module 198
management module 180
enable local KVM switching
globally 208
enable local media tray switching
globally 239
enable local power control
blade server 275
globally 274
enable logical uplink failover
advanced management module 376
management module (advanced) 376
enable management channel auto-discovery
BladeCenter unit 227
enable monitoring of event log state
management module 122
enable multiple video sessions
blade servers 192
enable NAT table
I/O module 244
enable NEBS environment mode 153
enable network interface and allow IP swap
management module (standby) 40
enable network interface and prevent IP swap
management module (standby) 41
enable NTP
management module 245, 262
enable password change at first login to management module 36
enable password required for management module 37
enable physical uplink failover
advanced management module 375
management module (advanced) 375
enable port
switch 269
enable power capping for blade server 154
enable power domain acoustic mode 153
enable power management for blade server 154, 155
enable power saver mode for blade server 155
enable protected mode
I/O module 197

enable RDE
management module 263
enable RDOCE
management module 263
enable remote media tray switching
globally 240
enable secure SMASH over SSH
management module 264
enable secure TCP command mode
management module 266, 362
enable security
management module 305
enable SLP
management module 263
enable SMASH over Telnet
management module 264
enable SNMP agent
management module (SNMPv1) 314
management module (SNMPv3) 314
enable SNMP traps
management module 265, 314
enable SNMPv1
management module 361
enable SNMPv1 agent
management module 264
enable SNMPv3
management module 361
enable SNMPv3 agent
management module 265
enable SOL
global 332
enable SSH port
management module 265
enable static IPv6 configuration
I/O module 197
management module 179
enable TCP command mode
management module 266, 362
enable technician debug
management module 306
enable Telnet port
management module 267
enable TFTP
management module 267
enable trespass feature
management module 358
enable user 381
enable V3 authentication for NTP
management module 246
enable Wake on LAN
blade server 274
globally 274
enable web interface
management module 363
encryption algorithms 14
end session 143
ending an SOL session 23, 115
enhanced legacy alert categories
disable 229
enable 229
entries of the CIN status table
display for management module 102
env 132, 133
options
bbu 134
be 133
blade 132
env *(continued)*
options *(continued)*
blower 134
ckvm 133
cpu 133
disk 135
exp 133
hsec 133
mgmtcrd 133
mt 134
mux 135
ncc 135
power 134
sb 133
sp 133
storage 135
switch 134
system (management module) 132
tap 135
env command errors 440
env commands
example 136
environment
alarm panel 135
blade mezzanine 133
blade server 132
BladeCenter unit 132
blower 134
BMC 133
disk drive 135
high-speed expansion card 133
I/O module 134
I/O-expansion card 133
integrated system management processor 133
management card 133
management module 132
media tray 134
memory 133
microprocessor 133
multiplexer expansion module 135
network clock module 135
power module 134
service processor 133
storage expansion unit 133
storage module 135
switch module 134
environment commands 131
example 136
errors
accseccfg command 423
advfailover command 424
alarm command 425
alertcfg command 426
alertentries command 426
autoftp command 427
baydata command 427
bofm command 428
boot command 429
bootmode command 429
bootseq command 430
buildidcfg command 430
chconfig command 431
chlog command 432
chmanual command 433
cin command 433
errors *(continued)*
clear command 435
clearlog command 435
clock command 435
command-line interface 419
common 421
config command 436
console command 437
dhcpinfo command 438
displaylog command 438
displaysd command 439
dns command 440
env command 440
ethoverusb command 440
eventinfo command 441
events command 441
exit command 442
feature command 442
files command 444
fuelg command 445
groups command 448
health command 448
help command 449
history command 449
identify command 449
ifconfig command 450
info command 454
iocomp command 455
kvm command 455
ldapcfg command 455
led command 456
list command 457
mcad command 457
modactlog command 457
monalerts command 457
monalertsleg command 458
mt command 458
nat command 458
ntp command 459
ping command 459
pmpolicy command 460
portcfg command 460
ports command 460
power command 462
rdoc command 462
read command 463
remacccfg command 464
remotechassis command 464
reset command 465
scale command 465
sddump command 466
sdemail command 467
security command 467
service command 467
shutdown command 468
slp command 468
smtp command 468
snmp command 469
sol command 470
sshcfg command 471
sslcfg command 472
syslog command 474
tcpcmdmode command 475
telnetcfg command 475
temps command 476
thres command 476
trespass command 476

errors *(continued)*
uicfg command 477
update command 478
uplink command 480
users command 481
vlan command 485
volts command 486
write command 486
zonecfg command 487
Ethernet
configuring remote connection 21
Ethernet channel
disable for blade server 190
enable for blade server 189
Ethernet channel 0 address prefix length
set for management module 180
Ethernet channel 0 configuration
display for management module (primary) 171
display for management module (standby) 172
Ethernet channel 0 configuration method
set for management module 176
Ethernet channel 0 data rate
set for management module 177
Ethernet channel 0 DHCP configuration
display for management module 117
Ethernet channel 0 domain name
set for management module 179
Ethernet channel 0 duplex mode
set for management module 177
Ethernet channel 0 gateway IP address (IPv4)
set for management module 174
Ethernet channel 0 gateway/default route (IPv6)
set for management module 174
Ethernet channel 0 hostname
set for management module 175
set for standby management module 176
Ethernet channel 0 MAC address
set for management module 178
set for standby management module 178
Ethernet channel 0 MTU
set for management module 177
Ethernet channel 0 static IP address (IPv4)
set for management module 173
set for standby management module 173
Ethernet channel 0 static IP address (IPv6)
set for management module 173
set for standby management module 174
Ethernet channel 0 subnet mask (IPv4)
set for management module 175
Ethernet channel 1
disable for management module 184
enable for management module 183
Ethernet channel 1 configuration
display for management module (primary) 181
Ethernet channel 1 data rate
set for management module 182
Ethernet channel 1 duplex mode
set for management module 182
Ethernet channel 1 gateway IP address (IPv4)
set for management module 181
Ethernet channel 1 MAC address
set for management module 183
Ethernet channel 1 MTU
set for management module 183
Ethernet channel 1 static IP address (IPv4)
set for management module 181
Ethernet channel 1 subnet mask (IPv4)
set for management module 182
Ethernet channel configuration method
set for blade server 188
Ethernet channel gateway IP address (IPv4)
set for blade server 186
Ethernet channel gateway/default route (IPv6)
set for blade server 187
Ethernet channel hostname
set for blade server 189
Ethernet channel static IP address (IPv4)
set for blade server 185
Ethernet channel static IP address (IPv6)
set for blade server 186
Ethernet channel subnet mask (IPv4)
set for blade server 187
Ethernet channel VLAN ID
set for blade server 188
Ethernet network settings for management module commands
example 200
Ethernet-over-USB setting
display for blade server 137
set for blade server 137
ethoverusb 137
options
s 137
ethoverusb command errors 440
ethoverusb commands 137
example 137
European Union EMC Directive conformance statement 497
event description
display 138
event log
clear for management module 105
display (reset counter) for management module 119
display all entries for management module 119
display all filters for management module 119
display entries for management module, filtered by date 120
display entries for management module, filtered by severity level 120
display entries for management module, filtered by source 120, 121
display for management module 119
enable monitoring of state 122
save to TFTP server 122
event log, clear for management module commands 105
event log, display for call-home event management module entries 93
event log, display for management module commands 119
event user action
display 138, 139
eventinfo 138, 139
eventinfo command errors 441
eventinfo commands 138
example 139
events 140
options
-add 140
-rm 141
events command errors 441
events commands 140
example 141
exit 143
exit codes (CLI)
Secure Shell server 20
exit command 143
exit command errors 442
exit commands
example 143
export datacenter feature licenses
management module 145
export firmware build ID list
blade server 86
external management
enable for I/O module 196
external ports
enable for I/O module 196

F

failover configuration
display for management module 375
fast POST
enable for I/O module 275, 276
FCC Class A notice 496
feature 144
options
-add 144
-apply 145
-remove 144
-retrieve 145
feature command errors 442
feature commands 144
example 146
feature license
add for management module 144
remove from management module 144
feature licenses
export for datacenter 145
import from datacenter 145
features
display for management module 144
files 147
options
d 147
files command errors 444
files commands 147
example 147
filter alert type 56

filter log entries by call-home events flag
management module 122
firmware
display attributes 365
update 366, 370
I/O module 367, 368, 369, 371, 372, 373
switch 367, 368, 369, 371, 372, 373
verbose 368, 372
update (verbose) 367, 370
firmware build ID
update in firmware build ID list 83
firmware build ID list
add entry for blade server 81
create for blade server 80
delete all entries 84
delete entry 85
export for blade server 86
import for blade server 85
update firmware build ID for blade server 83
update firmware build revision for blade server 84
update firmware type for blade server 83
update machine type for blade server 82
update manufacturer for blade server 82
firmware build IDs
display for blade server 80
firmware build revision
update in firmware build ID list 84
firmware requirements 2
firmware type
update in firmware build ID list 83
firmware update 365
flash location LED 169, 222
forest name
set for Global Catalog discovery 213
set for management module LDAP server 213
FTP
enable for management module 261
FTP data port number
set for management module 256
FTP port number
set for management module 256
FTP timeout
set for management module 268
fuelg 149, 150
options
am 153
dps 155
e 153
fpop 156
int 152
pcap 154
pm 151
pme 154, 155
pt 151, 152
tt 152
fuelg command errors 445
fuelg commands 149
example 156

G

gaseous contamination 495
gateway IP address (IPv4)
set for channel 0 of management module 174
set for channel 1 of management module 181
set for channel of blade server 186
set for I/O module 194, 199
gateway IP address (IPv6)
set for I/O module 195
gateway/default route (IPv6)
set for channel 0 of management module 174
set for channel of blade server 187
generate
CSR (LDAP client) 343
CSR (management module web server) 343
self-signed certificate (LDAP client) 341
self-signed certificate (management module web server) 341
generate host key
management module 337
generate syslog test message
management module 352
generate test alert 58
Germany Class A statement 497
get service data
blade server 301
getting help 490
global
enable local KVM switching 208
enable local media tray switching 239
enable local power control 274
enable remote media tray switching 240
enable Wake on LAN 274
Global Catalog discovery
set forest name 213
global disable
SOL 333
global enable
SOL 332
GMT offset
display for management module 106
set for management module 107
group filter
LDAP 211
group LDAP authentication, management module 159
group search attribute
LDAP 211
groups 159
options
a 160
clear 161
n 159
groups command 159
groups command errors 448
groups commands
example 162
guidelines
case sensitivity 6
command history 6
guidelines *(continued)*
data types 6
delimiters 6
help 6
options 5
output format 6
overview of 5
strings 6

H

hardware requirements 2
hardware service and support telephone numbers 491
health 163
display for all BladeCenter units on network 285
display status 163
display status (tree) 163
display status and alerts 164
display status and alerts with timestamp 164
options
f 164
l 163
t 164
health command 163, 164
example 164
health command errors 448
help 25, 166
getting 489
help command 166
help command errors 449
help commands
example 166
help, sending diagnostic data to IBM 490
help, World Wide Web 490
high-speed expansion card
command target 133
history 168
history command 168
history command errors 449
history commands
example 168
host key
generate for management module 337
host name
set for blade server 189
set for channel 0 of management module 175
set for channel 0 of standby management module 176
HTTP port number
set for management module 257
HTTP proxy setup
Service Advisor 91
HTTPS port
enable for management module 262
HTTPS port number
set for management module 257

I

I/O module
  activate network protocol settings 241
  activate SAS zone 415
  BladeCenter Open Fabric Manager 66
  bofm 66, 67, 68, 69, 70, 71
  bofm commands 66
  command target 134
  cycle power 273
  dhcpinfo commands 117
  disable DHCPv6 198
  disable IPv6 197
  disable IPv6 stateless auto-configuration 198
  disable NAT table 244
  disable static IPv6 configuration 197
  display DHCP configuration 117
  display IP addresses 248
  display network protocol settings 241
  display network settings 193
  display POST status 276
  display power state 273
  display SAS zone information 416
  display SAS zone list 415
  enable DHCPv6 configuration 198
  enable external management 196
  enable external ports 196
  enable fast POST 275, 276
  enable IPv6 197
  enable IPv6 stateless auto-configuration 198
  enable NAT table 244
  enable protected mode 197
  enable static IPv6 configuration 197
  I/O management commands 66
  keep new IP address configuration after reset 195
  nat command 241, 244
    example 244
  power off 272
  power on 272, 273
  reset 288
  reset (extended diagnostics) 290
  reset (full diagnostics) 290
  reset (standard diagnostics) 289
  reset configuration 103
  reset network protocol settings 241
  revert to old IP address configuration after reset 195
  set address prefix length 198
  set gateway IP address (IPv4) 194
  set gateway IP address (IPv6) 195
  set IP address (IPv4) 194
  set IP address (IPv6) 194
  set NAT external port number 243
  set NAT internal port number 243
  set NAT protocol ID 242
  set NAT protocol name 242
  set RAID IP address (IPv4) 199
  set subnet mask (IPv4) 196
  turn off 272
  turn on 273
I/O module compatibility
  display details for blade server 206
I/O module compatibility *(continued)*
  display details for I/O module 206
  display for all components 206
I/O module for blade server management traffic
  set for blade server 184
I/O module power information
  display 149
I/O module, display power
  trending 151, 152
I/O-expansion card
  command target 133
I/O-module IP address
  ping 249
  test communication 249
IBM Systems Director
  communication 353
IBM Taiwan product service 491
identify 169
  options
    s 169
    s, d 169
identify command 169
identify command errors 449
identify commands
  example 170
ifconfig 184, 192, 193
  options
    ckvm 185
    ckvm, enabled 193
    dhcp6 198
    em, enabled 196
    ep, enabled 196
    eth0 171
    eth0, c 176
    eth0, d 177
    eth0, dhcp6 180
    eth0, dn 179
    eth0, g 174
    eth0, g6 174
    eth0, i 173
    eth0, i6 173
    eth0, ipv6 179
    eth0, ipv6static 179
    eth0, l 178
    eth0, m 177
    eth0, n 175
    eth0, o 172
    eth0, o, i 173
    eth0, o, i6 174
    eth0, o, l 178
    eth0, o, n 176
    eth0, p6 180
    eth0, r 177
    eth0, s 175
    eth0, sa6 180
    eth1 181
    eth1, d 182
    eth1, down 184
    eth1, g 181
    eth1, i 181
    eth1, iom 184
    eth1, l 183
    eth1, m 183
    eth1, r 182
    eth1, s 182
    eth1, up 183
ifconfig *(continued)*
  options *(continued)*
    ethx 184
    ethx, c 188
    ethx, dhcp6 191
    ethx, down 190
    ethx, g 186
    ethx, g6 187
    ethx, i 185
    ethx, i6 186
    ethx, ipv6 190
    ethx, n 189
    ethx, p6 190
    ethx, s 187
    ethx, sa6 191
    ethx, up 189
    ethx, v 188
    ethx, ve 189
    g 194, 199
    g6 195
    i 191, 194, 199
    i6 194
    ipv6 197
    ipv6static 197
    ir 199
    maxv 192
    p6 198
    pip 195
    pm, enabled 197
    s 196, 200
    sa6 198
    v 192
    ve 192
ifconfig command errors 450
ifconfig commands 171
  example 200
import 346, 347, 348
import certificate file
  SSL CSR 345
  SSL self-signed certificate 345
import datacenter feature licenses
  management module 145
import firmware build ID list
  blade server 85
important notices 494
Industry Canada Class A emission compliance statement 497
info 203
  options
    path 204
    reload, all 204
    reload, fw 204
    reload, hw 204
    reload, mac 204
    reload, wwn 204
info command 203
info command errors 454
info commands
  example 205
information
  display for specific scalable complex 293
information (all)
  display for scalable complex 293
information about components and reloading components 203
information center 490

information display, blade server power (overview) 149
information display, blower power 149
information display, component 203
information display, I/O module power 149
information display, power domain (detailed) 150
information display, power domain (overview) 149
information LED
turn off 221
information reload, all 204
information reload, firmware 204
information reload, hardware 204
information reload, MAC addresses 204
information reload, WWN 204
informational alerts
disable monitoring for all 234
disable monitoring for blade device 235
disable monitoring for chassis 236
disable monitoring for cooling device 238
disable monitoring for event log 237
disable monitoring for I/O module 235
disable monitoring for inventory change 236
disable monitoring for network change 237
disable monitoring for power module 238
disable monitoring for power state 236
disable monitoring for storage module 235
disable monitoring for system management 236
disable monitoring for user activity 237
enable monitoring for all 234
enable monitoring for blade device 235
enable monitoring for chassis 236
enable monitoring for cooling device 238
enable monitoring for event log 237
enable monitoring for I/O module 235
enable monitoring for inventory change 236
enable monitoring for network change 237
enable monitoring for power module 238
enable monitoring for power state 236
enable monitoring for storage module 235
enable monitoring for system management 236
enable monitoring for user activity 237
integrated system management processor command target 133
iocomp 206
iocomp command errors 455
iocomp commands 206
example 206
IP address
CIN configuration entry 99
CIN index entry 99
display BladeCenter units on network filtered by 285
ping 248
test communication 248
IP address (I/O-module)
ping 249
test communication 249
IP address (IPv4)
set for blade server 185
set for blade server ISMP 191
set for I/O module 194
set for management module 173
set for standby management module 173
IP address (IPv6)
set for blade server 186
set for I/O module 194
set for management module 173
set for standby management module 174
IP address configuration
keep new after reset 195
revert to old after reset 195
IP address, default 15
IP addresses
display for I/O module 248
IPv6
disable for blade server 190
disable for I/O module 197
disable for management module 179
enable for blade server 190
enable for I/O module 197
enable for management module 179
IPv6 configuration (static)
disable for I/O module 197
disable for management module 179
enable for I/O module 197
enable for management module 179
IPv6 stateless auto-configuration
disable for blade server 191
disable for I/O module 198
disable for management module 180
enable for blade server 191
enable for I/O module 198
enable for management module 180
ISMP
reset 288

J

Japan VCCI Class A statement 498
Japan Voluntary Control Council for Interference Class A statement 498
JS20 blade server commands
reset (clear NVRAM) 291
reset (run diagnostics with boot sequence) 291
reset (run diagnostics) 291
reset (with NMI) 290
JSxx blade server commands
reset (enter SMS menu) 292

K

keep new IP address configuration after reset
I/O module 195
Korea Communications Commission statement 499
kvm 208
options
b 208
local 208
KVM
display owner 208
set owner 208
kvm command errors 455
kvm commands 208
example 209
KVM port
set state for management module 262

L

LDAP client
generate CSR 343
generate self-signed certificate 341
LDAP client distinguished name
set for management module 218
LDAP client distinguished name password
set for management module 218
LDAP client distinguished name password (confirm)
set for management module 218
LDAP group filter
set for management module 211
LDAP group search attribute
set for management module 211
LDAP login permission attribute
set for management module 212
LDAP name
set for management module 212
LDAP root distinguished name
set for management module 216
LDAP security version
set for management module 210
LDAP server (first) host name
set for management module 214
LDAP server (first) IP address
set for management module 214
LDAP server (first) port number
set for management module 215
LDAP server (fourth) host name
set for management module 215
LDAP server (fourth) IP address
set for management module 215
LDAP server (fourth) port number
set for management module 216
LDAP server (second) host name
set for management module 214
LDAP server (second) IP address
set for management module 214
LDAP server (second) port number
set for management module 215
LDAP server (third) host name
set for management module 214

LDAP server (third) IP address
set for management module 214
LDAP server (third) port number
set for management module 216
LDAP server authentication method
set for management module 217
LDAP server binding method
set for management module 217
LDAP server discovery method
set for management module 213
LDAP server domain name
set for management module 213
LDAP server forest name
set for management module 213
LDAP settings
display for management module 210
LDAP UID search attribute
set for management module 217
ldapcfg 210
options
aom 217
bm 217
cd 218
cp 218
dn 213
fn 213
gf 211
gsa 211
i1 214
i2 214
i3 214
i4 215
lpa 212
p 218
p1 215
p2 215
p3 216
p4 216
rd 216
server 213
t 212
usa 217
v 210
ldapcfg command 210
example 219
ldapcfg command errors 455
led 220
options
e 220
info 220
info off 221
l 220, 221
loc 220, 222
loc, d 223
r 220
LED (information)
turn off 221
LED (location), control 169
led command 220
led command errors 456
led commands
example 223
LED commands 29
LED state
display (blade server front panel) 220
LED state *(continued)*
display (external port link status) 220
display (fault) 220
display (for blade server and all sub-components) 221
display (safe-to-remove) 220
display (state for blower fault LED) 220
display (state for fanpack fault LED) 220
display various LED states 220
licenses
display for management module 144
light location LED 169, 222
time period 223
light location LED (BladeCenter unit)
time period 169
link local address 15
list 225
options
l 225
list command
example 225
list command errors 457
local KVM switching
enable globally 208
local media tray switching
enable globally 239
local power control
enable for blade server 275
enable globally 274
location
display for management module 111
set for management module 112
location LED
blink 169, 222
display state 169
flash 169, 222
light 169, 222
time period 223
light (BladeCenter unit)
time period 169
turn off 169, 222
location LED control 169
logging
disable for logging of login events from same IP address 35
enable for logging of login events from same IP address 35
logical link loss alert and failover policy
set for advanced management module 377
set for management module (advanced) 377
login permission attribute
LDAP 212

M

MAC address
set for channel 0 of management module 178
set for channel 0 of standby management module 178
set for channel 1 of management module 183
machine type
update in firmware build ID list 82
manage alert recipients 53
management card
command target 133
management channel auto-discovery
disable for BladeCenter unit 227
enable for BladeCenter unit 227
management channel auto-discovery status
display for BladeCenter unit 227
management channel path information
display 204
management module
account security commands 30, 66
accseccfg 30
accseccfg commands 30, 38
acknowledge call-home activity log entry 94
add Call Home events 140, 141
add feature license 144
add SSH public key 394
add SSH public key (specific) 394
advfailover command 40, 41
example 41
airfilter 42
autoftp commands 60, 62
bay data 63
bofm 66, 67, 68, 69, 70, 71
bofm commands 66, 71
cabling 12
change user password 387
chconfig commands 87, 91
chmanual commands 95, 96
cin commands 97
cinstatus commands 102
clear CIN configuration entries 97
clear event log 105
clear event log commands
example 105
command target 132
command-line session configuration 356
command-line timeout 356
comment SSH public key 400
config command 111, 114
example 114
configuring 21
connect to SSH public key 399
create alert recipient 54
create user 383
default IP address 15
delete Active Directory group 161
delete alert recipient 53
delete CIN configuration 98
delete file 147
delete user 380
DHCP settings commands
example 118
dhcpinfo commands 117, 118
direct connection 13
disable automatic configuration 282
disable CIN configuration entry 98
disable CLI SSH server 338
disable DHCPv6 180
disable Ethernet channel 1 184
disable IPv6 179

management module *(continued)*
disable IPv6 stateless auto-configuration 180
disable network interface for standby 40
disable SMASH SSH server 338
disable static IPv6 configuration 179
disable technician debug 306
disable user 381
display (reset counter) event log 119
display account security settings 30
display active users 379
display advanced failover settings 40
display alert properties (all recipients) 53
display alert properties (single recipient) 53
display all Active Directory groups 159
display all event log entries 119
display all event log filters 119
display all users 379
display automatic configuration setting 280
display call-home activity log 93
display CIN configuration table 97
display clock settings 106
display contact name 111
display date 106
display daylight-savings time setting 106
display DNS configuration 126
display DSA host key information 337
display entries of CIN status table 102
display Ethernet channel 0 DHCP configuration 117
display event description 138
display event log 119
display event log commands example 123
display event log entries filtered by date 120
display event log entries filtered by severity level 120
display event log entries filtered by source 120, 121
display event user action 138, 139
display events list 140
display features 144
display file list 147
display free space 140, 147
display FTP/TFTP server call-home activity log 93
display global remote alert settings 51
display GMT offset 106
display IBM Support call-home activity log 93
display LDAP settings 210
display licenses 144
display location 111
display log entries with call-home events 119
display log entries with Event ID 119
display name 111
management module *(continued)*
display network port settings 255
display NTP configuration 245
display open ports 255
display RSA host key information 337
display serial port configuration 253
display service setting 306
display single user 380
display SLP settings 309
display SMTP server host name 311
display SMTP server IP address 311
display SNMP configuration 314
display specific Active Directory groups 159
display SSH public key 393
display SSH status 337
display state of -lse option 122
display status 124
Display status of first five CIN entries 102
display syslog configuration 349
display temperature 357
display time 106
display trespass feature status 358
display user interface settings 361
display voltage 412
display volume information 278
dns commands 126, 129 example 129
download SSH public key 398
enable automatic configuration 281
enable CIN configuration entry 98
enable CLI SSH server 338
enable command-line interface 361
enable complex password 33
enable data encryption 305
enable default administration password expiration 34
enable DHCPv6 configuration 180
enable DNS 126
enable dynamic DNS 126
enable Ethernet channel 1 183
enable FTP 261
enable HTTPS port 262
enable IPv6 179
enable IPv6 stateless auto-configuration 180
enable monitoring of event log state 122
enable network interface for standby and allow IP swap 40
enable network interface for standby and prevent IP swap 41
enable NTP 245, 262
enable password change at first login 36
enable password required 37
enable RDE 263
enable RDOCE 263
enable secure SMASH over SSH 264
enable secure TCP command mode 266, 362
enable security 305
enable SLP 263
enable SMASH over Telnet 264
enable SMASH SSH server 338
management module *(continued)*
enable SNMP agent (SNMPv1) 314
enable SNMP agent (SNMPv3) 314
enable SNMP traps 265, 314
enable SNMPv1 361
enable SNMPv1 agent 264
enable SNMPv3 361
enable SNMPv3 agent 265
enable SSH port 265
enable static IPv6 configuration 179
enable TCP command mode 266, 362
enable technician debug 306
enable Telnet port 267
enable TFTP 267
enable trespass feature 358
enable user 381
enable V3 authentication for NTP 246
enable web interface 363
Ethernet network settings commands example 200
export datacenter feature licenses 145
failover configuration 375
filter alert type 56
filter log entries by call-home events flag 122
generate host key 337
generate syslog test message 352
IBM Systems Director communication 353
ifconfig commands 171, 200
import datacenter feature licenses 145
kvm commands 208, 209
ldapcfg command 210, 219 example 219
map image 278
mcad commands 227
mount volume 278
mt commands 239, 240
network connection 13
portcfg commands 253, 254
ports command 255, 270 example 270
read CIN status table entries 102
read command 280, 282 example 282
remacccfg command 283
remotechassis command 285, 286 example 286
remove feature license 144
remove SSH public key 395
replace SSH public key 397
reset (failover) 289
reset (force failover) 289
reset (primary) 288
reset (standby) 288
reset configuration (keep logs) 103
reset network port settings 256
restore configuration from file (encryption) 281
restore configuration from file (no encryption) 280
restore configuration from midplane 280
save configuration to chassis 413

management module *(continued)*
save configuration to file (encryption) 414
save configuration to file (no encryption) 413
save event log to TFTP server 122
sdemail commands 303
security commands 30, 305
serial connection 14, 17
serial port settings commands example 254
service command example 306
service commands 306
set account inactivity alert time 34
set account inactivity disable time 35
set account lockout period 36
set account security default to high 32
set account security default to legacy 31
set Active Directory group authority level 160
set Active Directory group name 159
set alert notification method 57
set alert recipient email address 57
set alert recipient name 55
set alert recipient status 56
set alert type 56
set authentication logging timeout 32
set CIN state for global enable or disable 97
set CLI inactivity timeout 33
set contact name 112, 113, 114
set date 106
set daylight-savings time mode 109
set DNS first IPv4 IP address 127
set DNS first IPv6 IP address 128
set DNS second IPv4 IP address 127
set DNS second IPv6 IP address 128
set DNS server priority 129
set DNS third IPv4 IP address 127
set DNS third IPv6 IP address 128
set Ethernet channel 0 address prefix length 180
set Ethernet channel 0 configuration method 176
set Ethernet channel 0 data rate 177
set Ethernet channel 0 domain name 179
set Ethernet channel 0 duplex mode 177
set Ethernet channel 0 gateway IP address (IPv4) 174
set Ethernet channel 0 gateway/default route (IPv6) 174
set Ethernet channel 0 hostname 175
set Ethernet channel 0 MAC address 178
set Ethernet channel 0 MTU 177
set Ethernet channel 0 static IP address (IPv4) 173
set Ethernet channel 0 static IP address (IPv6) 173
set Ethernet channel 0 subnet mask (IPv4) 175
set Ethernet channel 1 data rate 182
management module *(continued)*
set Ethernet channel 1 duplex mode 182
set Ethernet channel 1 gateway IP address (IPv4) 181
set Ethernet channel 1 MAC address 183
set Ethernet channel 1 MTU 183
set Ethernet channel 1 static IP address (IPv4) 181
set Ethernet channel 1 subnet mask (IPv4) 182
set first LDAP server host name 214
set first LDAP server IP address 214
set first LDAP server port number 215
set fourth LDAP server host name 215
set fourth LDAP server IP address 215
set fourth LDAP server port number 216
set FTP data port number 256
set FTP port number 256
set FTP timeout 268
set GMT offset 107
set hostname for alerts 58
set HTTP port number 257
set HTTPS port number 257
set IP address (IPv4) 173
set IP address (IPv6) 173
set IP address for alerts 58
set LDAP client distinguished name 218
set LDAP client distinguished name password 218
set LDAP client distinguished name password (confirm) 218
set LDAP group filter 211
set LDAP group search attribute 211
set LDAP login permission attribute 212
set LDAP name 212
set LDAP root distinguished name 216
set LDAP security version 210
set LDAP server binding method 217
set LDAP server discovery method 213
set LDAP server domain name 213
set LDAP server for authentication only 217
set LDAP server forest name 213
set LDAP UID search attribute 217
set location 112
set maximum LDAP sessions for user 36
set maximum number of login failures 35
set maximum number of simultaneous sessions for user 390
set minimum number of different characters for password 34
set name 111
set NTP server hostname 245
set NTP server IP address 245
set NTP server key 246
management module *(continued)*
set NTP update frequency 246
set password expiration time 37
set password minimum change interval 37
set password reuse cycle 38
set privacy password (SNMPv3) 392
set Remote Presence port number 257
set second LDAP server host name 214
set second LDAP server IP address 214
set second LDAP server port number 215
set secure TCP command mode port number 260
set serial port baud rate 253
set serial port communication rate 253
set serial port parity 253
set serial port stop bits 254
set server host name 311
set server IP address 311
set SLP address type 309
set SLP multicast address 309
set SLP port number 258
set SMASH Telnet port number 258
set SMTP e-mail server domain name 312
set SNMP agent port number 259
set SNMP community 1 first host name 316
set SNMP community 1 first host name - get 318
set SNMP community 1 first host name to set 317
set SNMP community 1 IP address (first host) 316
set SNMP community 1 IP address (first host) to get 318
set SNMP community 1 IP address (first host) to set 317
set SNMP community 1 IP address (second host) 319
set SNMP community 1 IP address (third host) 320
set SNMP community 1 name 315
set SNMP community 1 second host name 319
set SNMP community 1 third host name 320
set SNMP community 1 view type (SNMPv3) 320
set SNMP community 2 first host name 321
set SNMP community 2 IP address (first host) 321
set SNMP community 2 IP address (second host) 322
set SNMP community 2 IP address (third host) 323
set SNMP community 2 name 321
set SNMP community 2 second host name 322
set SNMP community 2 third host name 323

management module *(continued)*
set SNMP community 2 view type (SNMPv3) 323
set SNMP community 3 first host name 324
set SNMP community 3 IP address (first host) 324
set SNMP community 3 IP address (second host) 325
set SNMP community 3 IP address (third host) 326
set SNMP community 3 name 324
set SNMP community 3 second host name 325
set SNMP community 3 third host name 326
set SNMP community 3 view type (SNMPv3) 326
set SNMP contact name 327
set SNMP location 328
set SNMP traps port number 259
set SSH port number 260
set state for KVM port 262
set syslog event log collector 1 IP address 350
set syslog event log collector 1 port number 351
set syslog event log collector 2 IP address 350
set syslog event log collector 2 port number 351
set syslog filter level 349
set TCP command mode port number 260
set TCP command-mode timeout 268
set Telnet port number 261
set Telnet port timeout 268
set TFTP port number 261
set third LDAP server host name 214
set third LDAP server IP address 214
set third LDAP server port number 216
set time 106
set trespass feature message 358
set trespass feature to default 359
set tsyslog event log collector 1 host name 350
set tsyslog event log collector 2 host name 350
set user access type (SNMPv3) 392
set user authentication method 33
set user authentication protocol (SNMPv3) 391
set user authority level 388
set user context name (SNMPv3) 390
set user hostname (SNMPv3 traps) 393
set user IP address (SNMPv3 traps) 393
set user name 385
set user password 386
set user privacy protocol (SNMPv3) 391
set web interface inactivity timeout 38
slp command 309
example 309
management module *(continued)*
smtp commands 311, 312
SMTP settings commands
example 312
snmp commands 314, 328
SNMP settings commands
example 328
SSH connection 18
sshcfg command 337, 338
example 338
SSL certificate status 339
SSL status 339
synchronize with NTP server 247
telnet configuration 356
telnet timeout 356
terminate user session 379
trespass command 358, 359
example 359
turn secure TCP command mode on or off 267, 363
turn TCP command mode on or off 266, 362
unacknowledge call-home activity log entry 94
unlock user 382
unmount volume 278
uplink configuration 375
upload SSH public key 396
view configuration 225
view power management policy 252
vlan command 402, 410
example 410
write command 413, 414
example 414
management module (advanced)
disable logical uplink failover 376
enable logical uplink failover 376
enable physical uplink failover 375
logical uplink failover delay 376
logical uplink failover IP address 376
logical uplink failover IPv6 IP address 377
physical uplink failover delay 375
set logical link loss alert and failover policy 377
management module (primary)
display Ethernet channel 0 configuration 171
display Ethernet channel 1 configuration 181
reset 288
management module (standby)
display Ethernet channel 0 configuration 172
reset 288
set Ethernet channel 0 hostname 176
set Ethernet channel 0 MAC address 178
set Ethernet channel 0 static IP address (IPv4) 173
set Ethernet channel 0 static IP address (IPv6) 174
set IP address (IPv4) 173
set IP address (IPv6) 174
management module air filter command 42
management module event log commands 28
management module failover commands 375
management module telnet configuration commands
example 356
management module uplink failover commands
example 377
management module web server
generate CSR 343
generate self-signed certificate 341
management module, group LDAP authentication 159
management module, user accounts 379
management network DHCP configuration
display for blade server 117
management-module firmware 2
manufacturer
update in firmware build ID list 82
map image
advanced management module volume 278
maximum LDAP sessions for user
set for management module 36
maximum number of login failures
set for management module 35
mcad 227
options
e 227
mcad command errors 457
mcad commands 227
example 227
media tray
command target 134
display owner 239
display temperature 357
set owner 239
media tray temperature display 149
media tray, display power trending 152
memory
command target 133
memory commands 29
microprocessor
command target 133
minimum number of different characters for password
set for management module 34
modactlog 228
modactlog command errors 457
modactlog commands 228
example 228
module (blade server)
display activity 228
display information 228
monalerts 229
options
ca 229
cb 230
ccd 231
ccsm 231
ciom 230, 233, 235
cpm 231
ec 229
ia 234

monalerts *(continued)*
options *(continued)*
ib 235
icd 238
icsm 236
iel 237
iinv 236
iiom 235
inc 237
ipm 238
ipon 236
iua 237
wa 232
wb 232
wcd 234
wcsm 233
wel 233
wiom 232
wpm 234
monalerts command errors 457
monalerts commands 229
example 238
monalertsleg command errors 458
monalertsleg commands 229
monitoring
disable for all critical alerts 229
disable for all informational alerts 234
disable for all warning alerts 232
disable for blade device critical alerts 230
disable for blade device informational alerts 235
disable for blade device warning alerts 232
disable for chassis critical alerts 231
disable for chassis informational alerts 236
disable for chassis warning alerts 233
disable for cooling device critical alerts 231
disable for cooling device informational alerts 238
disable for cooling device warning alerts 234
disable for event log informational alerts 237
disable for event log warning alerts 233
disable for I/O module critical alerts 230
disable for I/O module informational alerts 235
disable for I/O module warning alerts 232
disable for inventory change informational alerts 236
disable for network change informational alerts 237
disable for power module critical alerts 231
disable for power module informational alerts 238
disable for power module warning alerts 234
disable for power state informational alerts 236
monitoring *(continued)*
disable for storage module critical alerts 230
disable for storage module informational alerts 235
disable for storage module warning alerts 233
disable for system management critical alerts 231
disable for system management informational alerts 236
disable for system management warning alerts 233
disable for user activity informational alerts 237
enable for all critical alerts 229
enable for all informational alerts 234
enable for all warning alerts 232
enable for blade device critical alerts 230
enable for blade device informational alerts 235
enable for blade device warning alerts 232
enable for chassis critical alerts 231
enable for chassis informational alerts 236
enable for chassis warning alerts 233
enable for cooling device critical alerts 231
enable for cooling device informational alerts 238
enable for cooling device warning alerts 234
enable for event log informational alerts 237
enable for event log warning alerts 233
enable for I/O module critical alerts 230
enable for I/O module informational alerts 235
enable for I/O module warning alerts 232
enable for inventory change informational alerts 236
enable for network change informational alerts 237
enable for power module critical alerts 231
enable for power module informational alerts 238
enable for power module warning alerts 234
enable for power state informational alerts 236
enable for storage module critical alerts 230
enable for storage module informational alerts 235
enable for storage module warning alerts 233
enable for system management critical alerts 231
enable for system management informational alerts 236
monitoring *(continued)*
enable for system management warning alerts 233
enable for user activity informational alerts 237
mount volume
advanced management module 278
mt 239
options
b 239
local 239
remote 240
mt command errors 458
mt commands 239
example 240
MTU
set for channel 0 of management module 177
set for channel 1 of management module 183
multiple video sessions
disable for blade servers 192
enable for blade servers 192
multiplexer expansion module
command target 135
reset (failover) 289

N

name
display BladeCenter units on network filtered by 286
display for blade server 111
display for management module 111
set for blade server 111
set for management module 111
name (contact)
set for management module 112, 113, 114
nat 241
options
activate 241
en 244
ep 243
ip 243
pi 242
pn 242
reset 241
nat command 241
example 244
nat command errors 458
NAT external port number
set for I/O module 243
NAT internal port number
set for I/O module 243
NAT protocol ID
set for I/O module 242
NAT protocol name
set for I/O module 242
NAT table
disable for I/O module 244
enable for I/O module 244
NEBS, disable 153
network card
display configuration information 184

network clock module
command target 135
power off 272
power on 272
turn off 272
turn on 272
network configuration status
display for blade server 184
network interface
disable for standby management module 40
enable for standby management module and allow IP swap during failover 40
enable for standby management module and prevent IP swap during failover 41
network port settings
display for management module 255
display for switch 269
reset for management module 256
network protocol settings
activate for I/O module 241
display for I/O module 241
reset for I/O module 241
network settings
display for BladeCenter unit 192
display for I/O module 193
New Zealand Class A statement 497
node information
display for scalable complex 293
notes, important 494
notices 493
electronic emission 496
FCC, Class A 496
notification method, set for alerts 57
ntp 245
options
en, enabled 245
f 246
i 245
synch 247
v3 246
v3en, enabled 246
NTP
enable for management module 245, 262
ntp command 245
example 247
ntp command errors 459
NTP configuration
display for management module 245
NTP server
synchronize management module clock 247
NTP server hostname
set for management module 245
NTP server IP address
set for management module 245
NTP server key
set for management module 246
NTP update frequency
set for management module 246

O

online documentation 1
open ports
display for management module 255
options
a 102
f 102
out-of-band communication, IBM Systems Director 353
override persistent command environment 7

P

parity
set for serial port of management module 253
particulate contamination 495
partition
create for scalable complex 296
delete all from scalable complex 296
delete from scalable complex 297
power cycle in scalable complex 299
power off in scalable complex 299
power on in scalable complex 298
partition (automatic)
create for scalable complex 294
partition information
display for scalable complex 293
partition mode
set to partition for scalable complex 298
set to stand alone for scalable complex 297
password
change for user 387
LDAP distinguished name 218
password (confirm)
LDAP distinguished name 218
password expiration time
set for management module 37
password minimum change interval
set for management module 37
password reuse cycle
set for management module 38
path information
display for management channel 204
People's Republic of China Class A electronic emission statement 499
persistent command environment
override 7
persistent command target 6
ping
I/O-module IP address 249
IP address 248
IP address (I/O-module) 249
r 248, 249
ping command errors 459
ping commands 248
example 249
pmpolicy 251
options
pd 251
pdx 251
view for management module 252
pmpolicy command
example 252
pmpolicy command errors 460
polling interval, set for power trending 152
portcfg
options
com1 253
com1, b 253
com1, p 253
com1, s 254
portcfg command errors 460
portcfg commands 253
example 254
ports 255
options
-kvme, state 262
ftpdp 256
ftpe, on 261
ftpp 256
ftpt 268
httpp 257
httpse, on 262
httpsp 257
ntpe, on 262
open 255
rde, on 263
rdoce, on 263
reset 256
rpp 257
slpe , on 263
slpp 258
smashse, on 264
smashte, on 264
smashtp 258
snmp1ae, on 264
snmp3ae, on 265
snmpap 259
snmpte, on 265
snmptp 259
sshe, on 265
sshp 260
stcme, on 266
stcme, port mode 267
stcmp 260
tcme, on 266
tcme, port mode 266
tcmp 260
tcmt 268
telnete, on 267
telnetp 261
telnett 268
tftpe, on 267
tftpp 261
switch 269, 270
ports (open)
display for management module 255
ports command 255
example 270
ports command errors 460
POST status
display for I/O module 276
display for switch module 276
power
options
ap 275
cycle 273
cycle, c 273
fp 275, 276
local 274, 275

power *(continued)*
options *(continued)*
off 272
on 272
on, c 272
softoff 273
state 273
state, post 276
wol 274
power capping, enable for blade server 154
power capping, set for blade server 154
power command errors 462
power commands 272
example 277
power control commands 29
power cycle partition
scalable complex 299
power domain
disable acoustic mode 153
disable NEBS environment mode 153
enable acoustic mode 153
enable NEBS environment mode 153
power domain information display (detailed) 150
power domain information display (overview) 149
power domain redundancy loss policy, set 151
power domain, display power trending 151, 152
power management commands 29
power management policy
display
all 251
BladeCenter S policies 251
specified power domain policies 251
set
for specified power domain 251
power management, enable for blade server 154, 155
power module
command target 134
power off
alarm panel module 272
blade server 272, 273
I/O module 272
network clock module 272
switch module 272, 273
power off partition
scalable complex 299
power on
alarm panel module 272
blade server 272, 273
I/O module 272, 273
network clock module 272
switch module 272, 273
power on (to console)
blade server 272, 273
power on partition
scalable complex 298
power polling interval, set 152
power saver mode, enable for blade server 155
power state
display for blade server 273
power state *(continued)*
display for I/O module 273
display for switch module 273
power trending, display (blade server) 151, 152
power trending, display (blower) 151, 152
power trending, display (I/O module) 151, 152
power trending, display (power domain) 151, 152
power trending, display (system) 151, 152
primary management module 7
problem description
call-home 95
email 303
service information 303
product service, IBM Taiwan 491
protected mode
enable for I/O module 197

R

RAID controller
set gateway IP address (IPv4) 199
set subnet mask (IPv4) 200
RAID IP address (IPv4)
set for I/O module 199
RDE
enable for management module 263
rdoc 278
options
map 278
mount 278
unmount 278
rdoc command errors 462
rdoc commands 278
example 279
RDOCE
enable for management module 263
read 280
options
config 280
config, auto, off 282
config, auto, on 281
config, l , i 280
config, l , i, p 281
read CIN configuration status table entries 102
read CIN status table entries for management module 102
read command 280
example 282
read command errors 463
redirect command 25, 131
redundancy loss policy, power domain (set) 151
reload all information 204
reload firmware information 204
reload hardware information 204
reload MAC address information 204
reload MAC addresses information 204
reload WNN information 204
remacccfg 283
mode 283
slto 284
remacccfg *(continued)*
srrto 284
srto 284
sto 283
remacccfg command 283
remacccfg command errors 464
remote alert
set retry interval 51
set retry limit 52
remote media tray switching
enable globally 240
remote presence access
display 283
set 405
remote presence disconnection mode
set 283
Remote Presence port number
set for management module 257
remotechassis 285
options
clear 286
health 285
ip 285
name 286
remotechassis command 285
example 286
remotechassis command errors 464
remove 346, 347, 348
remove feature license
management module 144
remove SSH public key 395
replace SSH public key 397
required, firmware 2
required, hardware 2
reset 288
blade server 72, 288
I/O module 288
ISMP 288
management module (primary) 288
management module (standby) 288
options
c 289
clr 291
ddg 291
dg 291
exd 290
f 289
force 289
full 290
sft 290
sms 292
standby 288
std 289
service processor 288
switch module 288
reset (clear NVRAM)
blade server 291
reset (enter SMS menu)
blade server 292
reset (extended diagnostics)
I/O module 290
switch module 290
reset (failover)
management module 289
multiplexer expansion module 289
reset (force failover)
management module 289

reset (full diagnostics)
I/O module 290
switch module 290
reset (run diagnostics with boot sequence)
blade server 291
reset (run diagnostics)
blade server 291
reset (standard diagnostics)
I/O module 289
switch module 289
reset (to console)
blade server 72, 289
reset (with NMI)
blade server 290
reset blase server key sequence
set for SOL 335
reset command 29
reset command errors 465
reset commands 288
example 292
reset configuration
I/O module 103
switch module 103
reset configuration (keep logs)
management module 103
reset default configuration 103
reset network port settings
management module 256
reset network protocol settings
I/O module 241
responding to thermal events 153
restore configuration
management module (from file with encryption) 281
management module (from file with no encryption) 280
management module (from midplane) 280
restore configuration commands 29
restore management module configuration command
example 282
retry count
set for SOL 331
retry interval
set for remote alerts 51
set for SOL 330
retry limit
set for remote alerts 52
retry number
set for remote alerts 51
revert to old IP address configuration after reset
I/O module 195
RSA host key information
display for management module 337
Russia Class A electromagnetic interference statement 499
Russia Electromagnetic Interference (EMI) Class A statement 499

S

SAS system
set gateway IP address (IPv4) 199
set subnet mask (IPv4) 200
SAS zone
activate for I/O module 415
SAS zone information
display for I/O module 416
SAS zone list
display for I/O module 415
save configuration commands 29
save configuration to chassis
management module 413
save configuration to file (encryption)
management module 414
save configuration to file (no encryption)
management module 413
save event log to TFTP server
management module 122
save management module configuration command
example 414
save service information
save to TFTP server 124
scalable complex
create partition 296
create partition (automatically) 294
create stand-alone partition 295
create stand-alone partition (automatically) 294
delete all partitions 296
delete partition 297
display all information 293
display node information 293
display partition information 293
display specific complex information 293
power cycle partition 299
power off partition 299
power on partition 298
set partition mode to partition 298
set partition mode to stand alone 297
scale 293
options
auto 294
compid 293
compid, partition 293
create 295, 296
cycle 299
delete 296, 297
mode 297, 298
node 293
off 299
on 298
scale command errors 465
scale commands 293
example 300
sddump
options
coll 301
init 301
sddump command errors 466
sddump commands 301
example 302
sdemail
options
subj 303
to 303
sdemail command errors 467
sdemail commands 303
example 303
search domain
set for Domain Catalog discovery 213
secure command-line interface 14
Secure Shell connection clients 14
secure shell server
disabling 19
Secure Shell server
exit codes (CLI) 20
using 18
secure SMASH
enabling 19
secure SMASH over SSH
enable for management module 264
secure TCP command mode
disable 354
enable 354
enable for management module 266, 362
set number of sessions 354
turn secure TCP command mode on or off for the management module 267, 363
secure TCP command mode port number
set for management module 260
security 14, 305
display management module account settings 30
display management module setting 305
enable complex password for management module user authentication 33
enable default administration password expiration for management module 34
enable for management module 305
enable password change at first login to management module 36
enable password required for management module 37
options
e 305
set management module account default to high 32
set management module account default to legacy 31
set management module account inactivity alert time 34
set management module account inactivity disable time 35
set management module account lockout period 36
set management module authentication logging timeout 32
set management module CLI inactivity timeout 33
set management module maximum LDAP sessions for user 36
set management module maximum number of login failures 35
set management module minimum number of different characters for password 34
set management module password expiration time 37

security *(continued)*
set management module password minimum change interval 37
set management module password reuse cycle 38
set management module user authentication method 33
set management module web interface inactivity timeout 38
security command errors 467
security commands 305
account security 30
example 305
selecting command environment 6
selecting command target 6
self-signed certificate
generate for LDAP client 341
generate for management module web server 341
self-signed certificate (SSL)
download certificate file 344
import certificate file 345
upload certificate file 345
send threshold
set for SOL 331
sending diagnostic data to IBM 490
Serial Over LAN 22
Serial Over LAN commands 330
example 335
serial port baud rate
set for management module 253
serial port communication rate
set for management module 253
serial port configuration
display for management module 253
serial port parity
set for management module 253
serial port settings for management module commands
example 254
serial port stop bits
set for management module 254
server host name
set for management module 311
server IP address
set for management module 311
service 306
options
disable 306
enable 306
Service Advisor
contact information 89
disable 88
display owner 87
enable 88
HTTP proxy setup 91
service and support
before you call 489
hardware 491
software 491
service command
example 306
service command errors 467
service commands 306
service data
collect for blade server 301
display command 124
service data *(continued)*
display for blade server 301
dump from blade server 301
get for blade server 301
service information
capture 124
display 124
email 303
exclude from email alerts 51
include with email alerts 51
problem description 303
save to TFTP server 124
service processor
command target 133
reset 288
service setting
display for management module 306
session command 29
session lost timeout interval
set 284
session request retry timeout interval
set 284
session request timeout interval
set 284
session timeout interval
set 283
set
date, management module 106
daylight-savings time mode, management module 109
GMT offset, management module 107
power management policy specified power domain 251
remote presence access 405
remote presence disconnection mode 283
session lost timeout interval 284
session request retry timeout interval 284
session request timeout interval 284
session timeout interval 283
sol access 406
TCP command-mode session timeout 353
time, management module 106
VLAN configuration 407
VLAN entry name 407
VLAN gateway 409
VLAN ID 405
VLAN IP address 408
VLAN subnet 408
VLAN subnet mask 410
VLAN subnet route 409
VLAN tagging 406
set accumulate timeout
SOL 332
set Active Directory group authority level 160
set Active Directory group name 159
set address prefix length
blade server 190
I/O module 198
set alarm 49
set alert notification method 57
set alert recipient email address 57
set alert recipient name 55
set alert recipient status 56
set alert type 56
set automatic power-on policy
BladeCenter unit 275
set boot mode
blade server 74
set CIN state for disable
management module 97
set CIN state for enable
management module 97
set CLI key sequence
SOL 334
set command-line timeout
management module 356
set contact name
management module 112, 113, 114
set DNS first IPv4 IP address
management module 127
set DNS first IPv6 IP address
management module 128
set DNS second IPv4 IP address
management module 127
set DNS second IPv6 IP address
management module 128
set DNS server priority
management module 129
set DNS third IPv4 IP address
management module 127
set DNS third IPv6 IP address
management module 128
set Ethernet channel 0 address prefix length
management module 180
set Ethernet channel 0 configuration method
management module 176
set Ethernet channel 0 data rate
management module 177
set Ethernet channel 0 domain name
management module 179
set Ethernet channel 0 duplex mode
management module 177
set Ethernet channel 0 gateway IP address (IPv4)
management module 174
set Ethernet channel 0 gateway/default route (IPv6)
management module 174
set Ethernet channel 0 hostname
management module 175
standby management module 176
set Ethernet channel 0 MAC address
management module 178
standby management module 178
set Ethernet channel 0 MTU
management module 177
set Ethernet channel 0 static IP address (IPv4)
management module 173
standby management module 173
set Ethernet channel 0 static IP address (IPv6)
management module 173
standby management module 174
set Ethernet channel 0 subnet mask (IPv4)
management module 175

set Ethernet channel 1 data rate
management module 182
set Ethernet channel 1 duplex mode
management module 182
set Ethernet channel 1 gateway IP address (IPv4)
management module 181
set Ethernet channel 1 MAC address
management module 183
set Ethernet channel 1 MTU
management module 183
set Ethernet channel 1 static IP address (IPv4)
management module 181
set Ethernet channel 1 subnet mask (IPv4)
management module 182
set Ethernet channel configuration method
blade server 188
set Ethernet channel gateway IP address (IPv4)
blade server 186
set Ethernet channel gateway/default route (IPv6)
blade server 187
set Ethernet channel hostname
blade server 189
set Ethernet channel static IP address (IPv4)
blade server 185
set Ethernet channel static IP address (IPv6)
blade server 186
set Ethernet channel subnet mask (IPv4)
blade server 187
set Ethernet channel VLAN ID
blade server 188
set Ethernet-over-USB setting
blade server 137
set first LDAP server host name
management module 214
set first LDAP server IP address
management module 214
set first LDAP server port number
management module 215
set fourth LDAP server host name
management module 215
set fourth LDAP server IP address
management module 215
set fourth LDAP server port number
management module 216
set FTP data port number
management module 256
set FTP port number
management module 256
set FTP timeout
management module 268
set gateway IP address (IPv4)
I/O module 194
RAID controller 199
SAS system 199
set gateway IP address (IPv6)
I/O module 195
set hostname for alerts 58
set HTTP port number
management module 257
set HTTPS port number
management module 257
set I/O module for blade server management traffic
blade server 184
set IP address (IPv4)
blade server 185
blade server ISMP 191
I/O module 194
management module 173
standby management module 173
set IP address (IPv6)
blade server 186
I/O module 194
management module 173
standby management module 174
set IP address for alerts 58
set KVM owner 208
set LDAP client distinguished name
management module 218
set LDAP client distinguished name password
management module 218
set LDAP client distinguished name password (confirm)
management module 218
set LDAP group filter
management module 211
set LDAP group search attribute
management module 211
set LDAP login permission attribute
management module 212
set LDAP name
management module 212
set LDAP security version
management module 210
set LDAP server binding method
management module 217
set LDAP server discovery method
management module 213
set LDAP server domain name
management module 213
set LDAP server for authentication only
management module 217
set LDAP server forest name
management module 213
set LDAP server root distinguished name
management module 216
set LDAP UID search attribute
management module 217
set location
management module 112
set logical link loss alert and failover policy
advanced management module 377
management module (advanced) 377
set logical uplink failover delay
advanced management module 376
management module (advanced) 376
set logical uplink failover IP address
advanced management module 376
management module (advanced) 376
set logical uplink failover IPv6 IP address
advanced management module 377
management module (advanced) 377
set management module account inactivity alert time 34
set management module account inactivity disable time 35
set management module account lockout period 36
set management module account security default
high 32
legacy 31
set management module authentication logging timeout 32
set management module CLI inactivity timeout 33
set management module maximum LDAP sessions for user 36
set management module maximum number of login failures 35
set management module minimum number of different characters for password 34
set management module password expiration time 37
set management module password minimum change interval 37
set management module password reuse cycle 38
set management module user authentication method 33
set management module web interface inactivity timeout 38
set maximum number of simultaneous sessions for user 390
set media tray owner 239
set name
blade server 111
management module 111
set NAT external port number
I/O module 243
set NAT internal port number
I/O module 243
set NAT protocol ID
I/O module 242
set NAT protocol name
I/O module 242
set NTP server hostname
management module 245
set NTP server IP address
management module 245
set NTP server key
management module 246
set NTP update frequency
management module 246
set number of sessions
secure TCP command mode 354
TCP command mode 354
set partition mode to partition
scalable complex 298
set partition mode to stand alone
scalable complex 297
set physical uplink failover delay
advanced management module 375
management module (advanced) 375
set port speed
switch 270
set power capping for blade server 154
set power domain redundancy loss policy 151
set power polling interval 152

set privacy password (SNMPv3) 392
set Remote Presence port number
management module 257
set reset blase server key sequence
SOL 335
set retry count
SOL 331
set retry interval 51
SOL 330
set retry limit
remote alerts 52
set retry number 51
remote alerts 51
set SAS controller IP address (IPv4)
I/O module 199
set second LDAP server host name
management module 214
set second LDAP server IP address
management module 214
set second LDAP server port number
management module 215
set secure TCP command mode port number
management module 260
set send threshold
SOL 331
set serial port baud rate
management module 253
set serial port communication rate
management module 253
set serial port parity
management module 253
set serial port stop bits
management module 254
set server host name
management module 311
set server IP address
management module 311
set SLP address type
management module 309
set SLP multicast address
management module 309
set SLP port number
management module 258
set SMASH Telnet port number
management module 258
set SMTP e-mail server domain name
management module 312
set SNMP agent port number
management module 259
set SNMP community 1 first host name
management module 316
set SNMP community 1 first host name -get
management module 318
set SNMP community 1 first host name to set
management module 317
set SNMP community 1 IP address (first host)
management module 316
set SNMP community 1 IP address (first host) to get
management module 318
set SNMP community 1 IP address (first host) to set
management module 317
set SNMP community 1 IP address (second host)
management module 319
set SNMP community 1 IP address (third host)
management module 320
set SNMP community 1 name
management module 315
set SNMP community 1 second host name
management module 319
set SNMP community 1 third host name
management module 320
set SNMP community 1 view type (SNMPv3)
management module 320
set SNMP community 2 first host name
management module 321
set SNMP community 2 IP address (first host)
management module 321
set SNMP community 2 IP address (second host)
management module 322
set SNMP community 2 IP address (third host)
management module 323
set SNMP community 2 name
management module 321
set SNMP community 2 second host name
management module 322
set SNMP community 2 third host name
management module 323
set SNMP community 2 view type (SNMPv3)
management module 323
set SNMP community 3 first host name
management module 324
set SNMP community 3 IP address (first host)
management module 324
set SNMP community 3 IP address (second host)
management module 325
set SNMP community 3 IP address (third host)
management module 326
set SNMP community 3 name
management module 324
set SNMP community 3 second host name
management module 325
set SNMP community 3 third host name
management module 326
set SNMP community 3 view type (SNMPv3)
management module 326
set SNMP contact name
management module 327
set SNMP location
management module 328
set SNMP traps port number
management module 259
set SSH port number
management module 260
set state for KVM port
management module 262
set static IP address (IPv4)
blade server ISMP 191
set subnet mask (IPv4)
I/O module 196
RAID controller 200
SAS system 200
set syslog event log collector 1 host name
management module 350
set syslog event log collector 1 IP address
management module 350
set syslog event log collector 1 port number
management module 351
set syslog event log collector 2 host name
management module 350
set syslog event log collector 2 IP address
management module 350
set syslog event log collector 2 port number
management module 351
set syslog filter level
management module 349
set TCP command mode port number
management module 260
set TCP command-mode timeout
management module 268
set Telnet port number
management module 261
set Telnet port timeout
management module 268
set telnet timeout
management module 356
set TFTP port number
management module 261
set third LDAP server host name
management module 214
set third LDAP server IP address
management module 214
set third LDAP server port number
management module 216
set trespass feature message
management module 358
set trespass feature to default
management module 359
set user access type (SNMPv3) 392
set user authentication protocol (SNMPv3) 391
set user authority level 388
set user context name (SNMPv3) 390
set user hostname (SNMPv3 traps) 393
set user IP address (SNMPv3 traps) 393
set user name 385
set user password 386
set user privacy protocol (SNMPv3) 391
set VLAN ID
BladeCenter unit 192
shutdown
blade server 273, 308
options
f 308
shutdown command errors 468
shutdown commands 308
example 308
simultaneous sessions
set maximum number for user 390

slp 309
options
i 309
t 309
SLP
enable for management module 263
SLP address type
set for management module 309
slp command 309
example 309
slp command errors 468
SLP multicast address
set for management module 309
SLP port number
set for management module 258
SLP settings
display for management module 309
SMASH (secure) over SSH
enable for management module 264
SMASH CLP
enabling 19
SMASH over Telnet
enable for management module 264
SMASH SSH server
disable for management module 338
enable for management module 338
SMASH Telnet port number
set for management module 258
smtp 311
options
d 312
s 311
smtp command errors 468
smtp commands 311
example 312
SMTP e-mail server domain name
set for management module 312
SMTP server host name
display for management module 311
SMTP server IP address
display for management module 311
SMTP settings for management module commands
example 312
snmp 314
options
-ca1 get -c1i1 0.0.0.0 318
-ca1 set -c1i1 0.0.0.0 317
a, on 314
a3, on 314
c1 315
c1i1 316
c1i2 319
c1i3 320
c2 321
c2i1 321
c2i2 322
c2i3 323
c3 324
c3i1 324
c3i2 325
c3i3 326
ca1 320
ca2 323
ca3 326
cn 327
l 328
snmp *(continued)*
options *(continued)*
t, on 314
SNMP agent
enable for management module (SNMPv1)
SNMPv1 314
enable for management module (SNMPv3)
SNMPv3 314
SNMP agent port number
set for management module 259
snmp command errors 469
snmp commands 314
example 328
SNMP community 1 first host name
set for management module 316
set to get for management module 318
SNMP community 1 first host name to set
set for management module 317
SNMP community 1 IP address (first host)
set for management module 316
SNMP community 1 IP address (first host) to get
set to get for management module 318
SNMP community 1 IP address (first host) to set
set for management module 317
SNMP community 1 IP address (second host)
set for management module 319
SNMP community 1 IP address (third host)
set for management module 320
SNMP community 1 name
set for management module 315
SNMP community 1 second host name
set for management module 319
SNMP community 1 third host name
set for management module 320
SNMP community 1 view type
set for management module (SNMPv3) 320
SNMP community 2 first host name
set for management module 321
SNMP community 2 IP address (first host)
set for management module 321
SNMP community 2 IP address (second host)
set for management module 322
SNMP community 2 IP address (third host)
set for management module 323
SNMP community 2 name
set for management module 321
SNMP community 2 second host name
set for management module 322
SNMP community 2 third host name
set for management module 323
SNMP community 2 view type
set for management module (SNMPv3) 323
SNMP community 3 first host name
set for management module 324
SNMP community 3 IP address (first host)
set for management module 324
SNMP community 3 IP address (second host)
set for management module 325
SNMP community 3 IP address (third host)
set for management module 326
SNMP community 3 name
set for management module 324
SNMP community 3 second host name
set for management module 325
SNMP community 3 third host name
set for management module 326
SNMP community 3 view type
set for management module (SNMPv3) 326
SNMP configuration
display for management module 314
SNMP contact name
set for management module 327
SNMP location
set for management module 328
SNMP settings for management module commands
example 328
SNMP traps
disable for management module 314
enable for management module 265, 314
SNMP traps port number
set for management module 259
SNMPv1
enable for management module 361
SNMPv1 agent
enable for management module 264
SNMPv3
community 1 view type 320
community 2 view type 323
community 3 view type 326
enable for management module 361
privacy password 392
trap receiver IP address or hostname 393
user access type 392
user authentication protocol 391
user context name 390
user privacy protocol 391
SNMPv3 agent
enable for management module 265
software service and support telephone numbers 491
sol 330
options
c 331
e 334
i 330
r 335
s 331
status 332, 333
t 332
SOL 22, 23, 115
global disable 333
global enable 332

SOL *(continued)*
set accumulate timeout 332
set CLI key sequence 334
set reset blase server key sequence 335
set retry count 331
set retry interval 330
set send threshold 331
status 330
sol access
set 406
sol command errors 470
sol commands
example 335
SOL commands 330
SOL session
ending 23, 115
starting 22
Specify IP address
CIN configuration entry 99
Specify VLAN ID
CIN configuration 100
SRC record
display specific for blade server 124
SRC records
display all for blade server 124
SSH
disabling 19
SSH clients 14
SSH connection 18
SSH port
enable for management module 265
SSH port number
set for management module 260
SSH public key add 394
SSH public key add (specific) 394
SSH public key comment 400
SSH public key connection 399
SSH public key display 393
SSH public key download 398
SSH public key remove 395
SSH public key replace 397
SSH public key upload 396
SSH status
display for management module 337
sshcfg 337
options
cstatus 338
hk, dsa 337
hk, gen 337
hk, rsa 337
sstatus 338
sshcfg command 337
example 338
sshcfg command errors 471
SSL
disable for LDAP client 340
enable for LDAP client 340
SSL certificate (additional)
disable for standby management module 339
enable for standby management module 339
SSL certificate status
management module 339
SSL CSR
download certificate file 344
SSL CSR *(continued)*
import certificate file 345
upload certificate file 345
SSL for LDAP client
disable 340
enable 340
SSL for management module web server
disable 339
enable 339
SSL for web server
disable for management module 339
enable for management module 339
SSL self-signed certificate
download certificate file 344
import certificate file 345
upload certificate file 345
SSL status
management module 339
SSL trusted certificate 1 346
download 346
import 346
remove 346
upload 346
SSL trusted certificate 2 347
download 347
import 347
remove 347
upload 347
SSL trusted certificate 3 348
download 348
import 348
remove 348
upload 348
sslcfg 339
options
ac 339
c 341, 343
cert 341
cl 341, 343
client 340
cp 341, 343
cpwd 343
csr 343
dnld 344
dq 341, 343
ea 341, 343
gn 341, 343
hn 341, 343
i 344, 345, 346, 347, 348
in 341, 343
l 344, 345, 346, 347, 348
on 341, 343
ou 341, 343
s 341, 343
server 339
sp 341, 343
tc1 346
tc2 347
tc3 348
un 343
upld 345
sslcfg command errors 472
sslcfg commands 339
example 348
stand-alone partition
create for scalable complex 295
stand-alone partition (automatic)
create for scalable complex 294
standby management module
disable additional SSL certificate 339
enable additional SSL certificate 339
set Ethernet channel 0 hostname 176
set Ethernet channel 0 MAC address 178
set Ethernet channel 0 static IP address (IPv4) 173
set Ethernet channel 0 static IP address (IPv6) 174
set IP address (IPv4) 173
set IP address (IPv6) 174
standby management modules 7
starting a session using SSH 18
starting a session using Telnet 16
starting an SOL session 22
starting command-line interface 14
state
VLAN 403
static IP address (IPv4)
set for blade server ISMP 191
set for channel 0 of management module 173
set for channel 0 of standby management module 173
set for channel 1 of management module 181
set for channel of blade server 185
static IP address (IPv6)
set for channel 0 of management module 173
set for channel 0 of standby management module 174
set for channel of blade server 186
static IPv6 configuration
disable for I/O module 197
disable for management module 179
enable for I/O module 197
enable for management module 179
status
display for management module 124
SOL 330
stop bits
set for serial port of management module 254
storage expansion unit
command target 133
storage module
command target 135
subnet mask (IPv4)
set for channel 0 of management module 175
set for channel 1 of management module 182
set for channel of blade server 187
set for I/O module 196
set for RAID controller 200
set for SAS system 200
support web page, custom 490
switch
display network port settings 269
enable port 269
set port speed 270
switch module
command target 134

switch module *(continued)*
cycle power 273
display POST status 276
display power state 273
power off 272, 273
power on 272, 273
reset 288
reset (extended diagnostics) 290
reset (full diagnostics) 290
reset (standard diagnostics) 289
reset configuration 103
turn off 272, 273
turn on 272, 273
synchronize clock with NTP server
management module 247
syntax help 166
syntax help commands
example 166
syslog 349
options
coll1 349
coll2 350
i1 350
i2 350
p1 351
p2 351
sev 349
test 352
syslog command errors 474
syslog commands 349
example 352
syslog configuration
display for management module 349
syslog event log collector 1 host name
set for management module 350
syslog event log collector 1 IP address
set for management module 350
syslog event log collector 1 port number
set for management module 351
syslog event log collector 2 host name
set for management module 350
syslog event log collector 2 IP address
set for management module 350
syslog event log collector 2 port number
set for management module 351
syslog event log transmission for collector 1
disable 349
disable for management module 349
enable 349
enable for management module 349
syslog event log transmission for collector 2
disable 350
disable for management module 350
enable 350
enable for management module 350
syslog filter level
set for management module 349
syslog test message
generate for management module 352
system
view configuration tree 225
system management command 29
system physical configuration command 225
system power management policy command 251
system, display power trending 151, 152

T

Taiwan Class A compliance statement 499
target 25, 131
TCP command mode
disable 353
enable 354
enable for management module 266, 362
set number of sessions 354
turn TCP command mode on or off for the management module 266, 362
TCP command mode port number
set for management module 260
TCP command-mode session status
display 353
TCP command-mode session timeout
display 353
set 353
TCP command-mode timeout
set for management module 268
tcpcmdmode 353
options
status, 0 353, 354
status, 1 to 20 354
t 353
tcpcmdmode command errors 475
tcpcmdmode commands 353
example 355
technician debug
disable for management module 306
enable for management module 306
Telco environment 153
telecommunication regulatory statement 496
telnet configuration
display for management module 356
telnet configuration commands 356
Telnet connection 14, 16
Telnet port
enable for management module 267
Telnet port number
set for management module 261
Telnet port timeout
set for management module 268
telnet timeout
set for management module 356
telnetcfg 356
options
t 356
telnetcfg command errors 475
telnetcfg commands 356
example 356
temperature
display for blade server 357
display for management module 357
display for media tray 357
temperature display, blower 149
temperature display, media tray 149
temporary command target 7
temps 357
temps command errors 476
temps commands 357
example 357
terminate 379
terminate session 143
terminate user session
management module 379
test alert
generate 58
test call home
call-home 96
test communication
I/O-module IP address 249
IP address 248
IP address (I/O-module) 249
TFTP
enable for management module 267
TFTP port number
set for management module 261
thermal event response 153
thermal trending, display (blower) 152
thermal trending, display (media tray) 152
thres command errors 476
time
display for management module 106
set for management module 106
trademarks 493
trespass 358
options
tw 358
twd 359
twe 358
trespass command 358
example 359
trespass command errors 476
trespass feature
enable for management module 358
trespass feature default
set for management module 359
trespass feature message
set for management module 358
trespass feature status
display for management module 358
trusted certificate 1 (SSL)
download 346
import 346
remove 346
upload 346
trusted certificate 2 (SSL)
download 347
import 347
remove 347
upload 347
trusted certificate 3 (SSL)
download 348
import 348
remove 348
upload 348
turn all CIN index entries on or off 98
turn off
alarm panel module 272
blade server 272, 273
I/O module 272
network clock module 272
switch module 272, 273

turn off LED
information 221
turn off location LED 169, 222
turn on
alarm panel module 272
blade server 272, 273
I/O module 272, 273
network clock module 272
switch module 272, 273
turn on (to console)
blade server 272, 273
turn secure TCP command mode on or off
management module 267, 363
turn TCP command mode on or off
management module 266, 362

U

uicfg 361
options
cli, enabled 361
snmp, enabled 361
stcm, enabled 362
stcm, port mode 363
tcm, enabled 362
tcm, port mode 362
web, enabled 363
uicfg command errors 477
uicfg commands 361
example 363
unacknowledge call-home activity log entry
management module 94
United States electronic emission Class A notice 496
United States FCC Class A notice 496
unlock user 382
unmount volume
advanced management module 278
update
options
a 365
activate 368
i, l 370
i, l, img 371, 372
i, l, img, activate 372, 373
i, n 370
u 366
u, img 367, 368
u, img, activate 369
u, r 366
u, v 367
update command 365
update command errors 478
update commands
example 373
update firmware 365, 366, 370
I/O module 367, 368, 369, 371, 372, 373
switch 367, 368, 369, 371, 372, 373
verbose 368, 372
update firmware (verbose) 367, 370
update firmware build ID in firmware build ID list
blade server 83
update firmware build revision in firmware build ID list
blade server 84
update firmware type in firmware build ID list
blade server 83
update machine type in firmware build ID list
blade server 82
update manufacturer in firmware build ID list
blade server 82
uplink 375
options
alert 377
dls 376
dps 375
el, enabled 376
ep, enabled 375
ip 376
ip6 377
uplink command errors 480
uplink commands 375
example 377
uplink configuration
display for management module 375
uplink failover (logical)
disable for advanced management module 376
disable for management module (advanced) 376
enable for advanced management module 376
enable for management module (advanced) 376
uplink failover (physical)
enable for advanced management module 375
enable for management module (advanced) 375
uplink failover delay (logical)
set for advanced management module 376
set for management module (advanced) 376
uplink failover delay (physical)
set for advanced management module 375
set for management module (advanced) 375
uplink failover IP address (logical)
set for advanced management module 376
set for management module (advanced) 376
uplink failover IPv6 IP address (logical)
set for advanced management module 377
set for management module (advanced) 377
upload 346, 347, 348
upload certificate file
SSL CSR 345
SSL self-signed certificate 345
upload SSH public key 396
user authentication method
enable complex password 33
user authentication method *(continued)*
set for management module 33
user interface configuration 361
example 363
user interface settings
display for management module 361
user session 379
users 379
options
1 through 12 380
a 388
ap 391
at 392
clear 380
cn 390
create (n, p, a, cn, ap, pp, ppw, at, i) 383
curr 379
disable 381
enable 381
i 393
ms 390
n 385
op 387
p 386
pk, add 394
pk, af 399
pk, cm 400
pk, dnld 398
pk, e 393
pk, remove 395
pk, upld 396, 397
pp 391
ppw 392
ts 379
unlock 382
users command 379
users command errors 481
users commands
example 400
users, change password 387
users, create 383
users, delete 380
users, disable 381
users, display (active) 379
users, display (all) 379
users, display (single) 380
users, enable 381
users, management module 379
users, set access type (SNMPv3) 392
users, set authentication protocol (SNMPv3) 391
users, set authority level 388
users, set context name (SNMPv3) 390
users, set hostname (SNMPv3 traps) 393
users, set IP address (SNMPv3 traps) 393
users, set maximum number of simultaneous sessions 390
users, set name 385
users, set password 386
users, set privacy password (SNMPv3) 392
users, set privacy protocol (SNMPv3) 391
users, unlock 382

using
Secure Shell server 18
using the command-line interface 5

V

V3 authentication for NTP
enable for management module 246
view command target 225
vlan 402
c 407
commit 402
cto 402
delete 403, 404
g 409
i 408
n 407
rp 405
s 408
smx 410
sol 406
srx 409
state 403
tag 406
vi 404
vid 405
VLAN
state 403
vlan command 402
example 410
vlan command errors 485
VLAN configuration
set 407
VLAN entry
create 404
delete 403, 404
display 404
VLAN entry name
set 407
VLAN gateway
set 409
VLAN ID
CIN configuration 100
disable for blade server Ethernet channel 189
disable for BladeCenter unit 192
enable for blade server Ethernet channel 189
enable for BladeCenter unit 192
set 405
set for BladeCenter unit 192
set for channel of blade server 188
VLAN IP address
set 408
VLAN settings
commit 402
commit timeout 402
display 402
VLAN subnet
set 408
VLAN subnet mask
set 410
VLAN subnet route
set 409
VLAN tagging
set 406
voltage
display for blade server 412
display for management module 412
volts 412
volts command errors 486
volts commands 412
example 412
volume information
display for management module 278

W

Wake on LAN
enable for blade server 274
enable globally 274
warning alerts
disable monitoring for all 232
disable monitoring for blade device 232
disable monitoring for chassis 233
disable monitoring for cooling device 234
disable monitoring for event log 233
disable monitoring for I/O module 232
disable monitoring for power module 234
disable monitoring for storage module 233
disable monitoring for system management 233
enable monitoring for all 232
enable monitoring for blade device 232
enable monitoring for chassis 233
enable monitoring for cooling device 234
enable monitoring for event log 233
enable monitoring for I/O module 232
enable monitoring for power module 234
enable monitoring for storage module 233
enable monitoring for system management 233
web interface
enable for management module 363
web interface inactivity timeout
set for management module 38
WNN information reload 204
write
options
config 413
config, l ,i 413, 414
write command 413
example 414
write command errors 486

Z

zonecfg 415
options
activate 415
view 416
zonecfg command errors 487
zonecfg commands 415
example 416

Part Number: 00V9902

Printed in USA

(1P) P/N: 00V9902