lenovo

Flex System FC3171 8 Gb SAN Switch Command Line Interface User's Guide

lenovo

Flex System FC3171 8 Gb SAN Switch Command Line Interface User's Guide

Note: Before using this information and the product it supports, read the general information in "Notices" on page 391.

First Edition, April 2015

Contents

Chapter 1. Lenovo Flex System FC3171 8 Gb SAN Switch

The Lenovo Flex System FC3171 8 Gb SAN Switch is a full-fabric Fibre Channel module that can be converted to a pass-thru module when configured in transparent mode.

This *Command Line Interface User's Guide* contains the following instructions and information about managing the switch using the command line interface (CLI):

- Command line interface usage, which includes logging into the switch, opening and closing and Admin session, entering commands, getting help, setting page breaks, creating a support file, and downloading and uploading files
- User account configuration, which includes, displaying user account information, creating user accounts, and modifying user accounts and passwords
- Network and fabric configuration, which includes displaying the Fibre Channel and Ethernet network configuration, configuring the Ethernet port, configuring system parameters, verifying Fibre Channel and network connections, and managing IP security
- Connection security configuration, which includes managing and displaying SSL and SSH services, and creating an SSL security certificate
- Device security configuration, which includes displaying, configuring, modifying, and resetting the security database
- Server authentication configuration, which includes displaying and configuring server parameters on the switch
- Event log configuration, which includes starting and stopping event logging, displaying the event log, managing the event log configuration, clearing the event log, logging into a remote host, and creating and downloading a log file
- Call Home configuration, which includes Call Home concepts, configuring the Call Home service, managing the Call Home database, testing a Call Home profile, testing a Call Home profile, changing SMTP servers, clearing the Call Home message queue, and resetting the Call Home database
- Simple Network Management Protocol configuration
- Alphabetical listing and description of each command
- Mapping port locations and software numbering

Related documentation

This *Command Line Interface user's guide* contains instructions for configuring and managing the switch or pass-thru module using the CLI. It also lists and describes all of the CLI commands.

The product documentation for your specific Lenovo Flex System network switch, pass-thru module, or chassis might contain additional, more-detailed troubleshooting information. For the most up-to-date product documentation for all of your Lenovo Flex System products, go to the IBM Flex System Information Center at
http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp.

The following documentation contains important, useful information to help you with the setup, installation, configuration, operation, and troubleshooting processes for these devices. This documentation is preloaded on the Lenovo Flex System Manager and is also available at http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp:

- Lenovo Flex System network device *User's Guides*

  These documents contain detailed information about installing, configuring, updating, and troubleshooting specific Lenovo Flex System network devices, which include network switches, pass-thru modules, and adapters.

- *Lenovo Flex System Enterprise Chassis Installation and Service Guide*

  This document contains information about setting up, configuring, and troubleshooting the Lenovo Flex System Enterprise Chassis and its components

- *Lenovo Flex System Chassis Management Module Command Line Interface Reference Guide*

  This document explains how to use the Chassis Management Module command-line interface (CLI) to directly access management functions. The command-line interface also provides access to the text-console command prompt on each compute node through a Serial over LAN (SOL) connection.

- *Lenovo Flex System Chassis Management Module User's Guide*

  This document explains how to use the Chassis Management Module user interface to manage chassis components.

- *Lenovo Flex System Manager System Management Guide*

  This document explains how to use the Lenovo Flex System Manager user interface to manage chassis components.

- Lenovo Flex System compute node *Installation and Service Guides*

  Each type of compute node has a customized *Installation and User's Guide*.

- Lenovo *Notices for Network Devices* CD

  This CD ships with networking products (adapters, switches, and pass-thru modules). It contains license documentation and the following documents:

- *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru Installation and User's Guide*

  This document explains the operation and installation of the Lenovo Flex System FC3171 8 Gb SAN Switch and Pass-thru.

- *Lenovo Flex System FC3171 8 Gb SAN Switch Command Line Interface User's Guide*

  This document explains how to manage the switch using the CLI.

- *Lenovo Flex System FC3171 8 Gb SAN Switch QuickTools User's Guide*

  This document explains how to manage the switch using the QuickTools application.

- *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru CIM Agent Reference Guide*

  This document explains how the Common Interface Model (CIM) Agent functions as an implementation of the Storage Management Initiative (SMI)-Specification 1.1.

- *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru Event Message Guide*

  This document lists and explains the event messages for the Lenovo Flex System FC3171 8 Gb SAN Switch and Pass-thru.

- *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru Simple Network Management Protocol Reference Guide*

  This document explains how to use the Simple Network Management Protocol (SNMP) to manage and monitor the Lenovo Flex System FC3171 8 Gb SAN Switch and Pass-thru.

The updated Lenovo Flex System documentation is available on the April 2015 Manager and from the IBM Flex System Information Center at http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp.

Notices and statements in this document

The caution and danger statements in this document are also in the multilingual *Safety Information* document, which is on the *Documentation* CD. Each statement is numbered for reference to the corresponding statement in the *Safety Information* document.

The following notices and statements are used in this document:

- **Note:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage might occur.
- **Caution:** These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.
- **Danger:** These statements indicate situations that can be potentially lethal or hazardous to you. A danger statement is placed just before the description of a potentially lethal or hazardous procedure step or situation.

Chapter 2. Command line interface usage

You can use the CLI through an SSH interface to perform a variety of fabric and switch management tasks. The CLI is accessible through the following methods:

- Using your server management interface
- From a command-line window on a connected network management workstation
- From a command line window on a workstation connected to the switch Ethernet port
- From a command line window on a workstation connected to the switch serial port

Notes:
Before you configure your switch, be sure that the management modules in your server unit or workstations are properly configured. In addition, to accessing and managing your switch from an external environment, you might need to enable certain features, such as the external ports and external management over all ports. For more detailed information about configuring your management module, see your server Installation Guide.

This chapter describes the following tasks:

- Logging in to the switch
- Opening and closing an Admin session
- Entering commands
- Getting help
- Setting page breaks
- Creating a support file
- Downloading and uploading files

Notes:
Throughout this document, references in text to commands and keywords use initial capitalization for clarity. Actual command and keyword entries are case insensitive.

Logging in to the switch

To log in to a switch, complete the following steps:

1. Open an SSH session and provide a switch bay IP address. For information about Lenovo Flex System switch bay IP addresses, see the *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru Installation and User's Guide.*
   - For a Windows® platform, use an SSH client such as PuTTY.
   - For a Linux® platform, type `ssh USERID@xxx.xxx.xxx.xxx`, where *xxx.xxx.xxx.xxx* is the switch bay IP address.
2. Press Enter.

   A command-prompt window opens.
3. At the login prompt, type the management-module user name (Windows only). At the password prompt, type the management-module password. The user name 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 that the sixth character in `PASSW0RD` is the number zero (0), not the letter O.).

   The Command Line Interface Shell window opens.
4. Type `admin start` and press Enter to obtain administrator privileges.
5. Normally, the date and time are set by the CMM through the Network Time Protocol (NTP). However, as an option, you can set the date and time of the switch by typing `date [MMDDhhmmCCYY]` where:

   [MM] is the month

   [DD] is the day

   [hh] is the hour in 24-hour format

   [mm] is the minute

   [CC] is the century identifier

   [YY] is the last two numbers of the year

   For example, the format for 28 November 28 2011 8:46 p.m. is date 112820462011.

   Press Enter.
6. Type `admin end` and press Enter to exit from the administrator operating mode and return to the standard operating mode.

This user account provides full access to the switch and its configuration. After planning your fabric management needs and creating your own user accounts, consider changing the password for this account. for more information about authority levels, see "Access authority" on page 149. For information about creating user accounts, see the "User" command on page 363.

A switch supports a combined maximum of 19 logins or sessions reserved as follows:

- Four logins or sessions for internal applications such as management server and SNMP
- Nine high priority SSH/Telnet sessions
- Six logins or sessions for QuickTools logins, Application Programming Interface (API) inband and out-of-band logins, and SSH/Telnet logins. Additional logins will be refused.

Opening and closing an Admin session

The command line interface performs monitoring and configuration tasks. Commands that perform monitoring tasks are available to all user accounts. Commands that perform configuration tasks are available only after entering the Admin Start command to open an Admin session. A user account must have Admin authority to enter the Admin Start command.

The following is an example of how to open and close an Admin session:

```
IBM8Gb #> admin start
IBM8Gb (admin) #>
.
.
.
IBM8Gb (admin) #> admin end
```

Entering commands

The command-line completion feature simplifies entering and repeating commands. Table 1 describes the command-line completion keystrokes.

Table 1. Command-line completion

Keystroke	Effect
Tab	Completes the command line. Enter at least one character and press the tab key to complete the command line. If more than one possibility exists, press the Tab key again to display all possibilities.
Up Arrow	Scrolls backward through the list of previously entered commands.
Down Arrow	Scrolls forward through the list of previously entered commands.
Control-A	Moves the cursor to the beginning of the command line
Control-E	Moves the cursor to the end of the command line.
Control-U	Clears the command line.

Getting help

To display help for a command, enter the Help command followed by the command. The following is an example of the help that is available for the Config Edit command.

```
IBM8Gb #> help config edit
config edit [CONFIG_NAME]
This command initiates a configuration session and places the current session
into config edit mode.
If CONFIG_NAME is given and it exists, it gets edited; otherwise, it gets
created.  If it is not given, the currently active configuration is edited.

Admin mode is required for this command.

  Usage: config edit [CONFIG_NAME]
```

Setting page breaks

Some display commands deliver so much information to the screen that it scrolls off too quickly to read it. You can limit the display to 20 lines by turning on page breaks. By default, page breaks are turned off. The following is an example of how to turn page breaks on and how it affects the display.

```
IBM8Gb #> set pagebreak on
IBM8Gb #> help
                                General Help
                                ------------

admin           ADMIN_OPTIONS
config          CONFIG_OPTIONS
create          CREATE_OPTIONS
date            [MMDDhhmmCCYY]
exit
feature         FEATURE_OPTIONS
firmware        install
hardreset
help            HELP_OPTIONS
history
hotreset
image           IMAGE_OPTIONS
logout
passwd          [USER_ACCT_NAME]
ping            IP_ADDR
ps
quit
reset           RESET_OPTIONS
set             SET_OPTIONS
show            SHOW_OPTIONS
shutdown
test            TEST_OPTIONS

        Press any key for more help or 'q' to end this list...
uptime
user            USER_OPTIONS
whoami
```

Creating a support file

If you contact technical support about a problem with your switch, they may request that you create and send a support file. This support file contains all of the switch configuration information that can be helpful in diagnosing the problem. The Create Support command creates the support file (dump_support.tgz) on the switch. If your workstation has an sFTP server, you can proceed with the command prompts to send the file from the switch to a remote host. Otherwise, you can use sFTP to download the support file from the switch to your workstation.

Notes:

The sFTP switch service is enabled by default, and the FTP and TFTP services are disabled. If you intend to use FTP or TFTP, you must first enable the service. For more information about switch services, see "Managing switch services" on page 50.

The following example creates a support file and sends it to a remote host.

```
IBM8Gb #> create support

  This may take several seconds...

Log Msg: [Wed Nov 02 14:06:47.341 CDT 2011][C][8400.003B][Switch][Creating
the support file - this will take several seconds]
command result: Passed.

Transfer the dump support file to another machine? (y/n) : y
ftp or sftp [ftp]: sftp
Enter address of ftp server (IPv4 or IPv6) : 10.20.108.130
Login name: root
Enter a valid remote directory path.
:
Would you like to continue downloading support file? (y/n) : y
Enter host password for user 'root':
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  870k    0     0  100  870k      0   595k  0:00:01  0:00:01 --:--:--  595k
Transfer the dump support file to another machine? (y/n) : n
```

If your workstation does not have an sFTP server, enter the Create Support command to create the support file, and use sFTP to download the support file from the switch to your workstation as shown in the following example:

```
IBM8Gb #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): n
```

To download the support file from the switch to the workstation, do the following:

1. Open a terminal window and move to the directory where you want to download the support file.
2. Enter the sFTP command and the switch IP address or symbolic name.

   ```
   >sftp images@ip_address
   ```

3. When prompted for a user and password, enter the FTP account name and password (images, images).

   ```
   Password: images
   ```

4. Set binary mode and use the Get command to download the file (dump_support.tgz).

   ```
   sftp>get dump_support.tgz
       Fetching /dump_support.tgz to dump_support.tgz
       /dump_support.tgz                100%  137KB 136.8KB/s   00:00
   sftp> quit
   ```

Downloading and uploading files

There are several files that reside on the switch that you can download to the workstation for examination or for safekeeping. These files include the following:

- Backup configuration file (configdata)
- Event log files (`logfile`)
- Audit log files (`audit.log`)
- Support files (`dump_support.tgz`)

You can upload firmware image files or backup configuration files to the switch to reinstall firmware or restore a corrupted configuration.

- For information about uploading and installing firmware file, see “Installing firmware” on page 58.
- For information about uploading and restoring a switch configuration, see “Back up and restore a switch configuration” on page 53.
- For information about creating and uploading an event log file or a n audit log file, see “Creating and downloading an event log file” on page 124.
- For information about creating and uploading a support file, see “Creating a support file” on page 9.

The switch uses sFTP to exchange files between the switch and the workstation. If your workstation does not have an sFTP server, use an sFTP client such as PuTTY.

Notes:

The sFTP switch service is enabled by default, and the FTP and TFTP services are disabled. If you intend to use FTP or TFTP, you must first enable the service. For more information about switch services, see “Managing switch services” on page 50.

Chapter 3. User account configuration

User accounts and their respective passwords are the first line of switch security. A user account consists of an account name, an authority level, and an expiration date. Switches come from the factory with certain user accounts defined for special purposes. Table 2 describes these accounts, their passwords, and their purposes. These accounts cannot be deleted from the switch.

Table 2. Factory user accounts

User account name	Password	Purpose
USERID	PASSW0RD[1]	The administrator account provides access to the SSH/Telnet server for managing the switch. USERID is the only account name that has permission to create and modify other user accounts. To secure your USERID user account, be sure to change the password for this account. The user account and password are case sensitive.
images	images	This user account provides access to a Secure File Transfer Protocol (sFTP) server or a File Transfer Protocol (FTP) server for exchanging files between the switch and the workstation.
snmpadmin1	admin1pass	This user account provides secure access to devices for SNMPv3 through a combination of packet authentication and encryption over the network.

[1] The sixth character in the initial default password character is a zero, not the letter O.

This chapter describes the following user account configuration tasks:

- Displaying user account information
- Creating user accounts
- Modifying user accounts and passwords

Displaying user account information

You can display all user accounts defined on the switch (User Accounts command) or just those user accounts that are logged on (User List or Show Users command).

The following example displays all user accounts defined on the switch. Account information includes account name, authority, and expiration date.

```
IBM8Gb (admin) #> user accounts

  Current list of user accounts
  -----------------------------
  images       (admin authority = False, never expires)
  admin        (admin authority = True , never expires)
  USERID       (admin authority = True , never expires)
  user1        (admin authority = True , never expires)
  user2        (admin authority = False, expires in < 50 days)
  user3        (admin authority = True , expires in < 100 days)
```

The following example displays user accounts that are logged on to the switch:

```
IBM8Gb (admin) #> user list

  User             cim@OB-session1
  Client           cim
  Logged in Since  day month date time year

  User             snmp@IB-session2
  Client           Unknown
  Logged in Since  day month date time year

  User             snmp@OB-session3
  Client           Unknown
  Logged in Since  day month date time year

  User             admin@OB-session8
  Client           10.33.21.27
  Logged in Since  day month date time year
```

Creating user accounts

A user account consists of an account name, an authority level, and an expiration date. The account name can be up to 15 characters and must begin with an alphanumeric character. The authority level grants admin authority (true) or denies it (false). The expiration date sets the date when the user account expires. Only the USERID user account can create user accounts.

The following example creates a new user account named *user1* with admin authority that expires in 100 days.

```
IBM8Gb (admin) #> user add
    Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (8-20 chars)  : *******

please confirm account password: *******

set account expiration in days (0-2000, 0=never): [0] 100

should this account have admin authority? (y/n): [n] y

OK to add user account 'user1' with admin authority
and to expire in 100 days?

Please confirm (y/n): [n] y
```

Modifying user accounts and passwords

Only the USERID account can modify a user account, delete a user account, or change the password of another user account. However, all user accounts can change their own passwords. The User command modifies and deletes user accounts. The Passwd command changes passwords.

The following example removes the expiration date and admin authority for the user account named user1.

```
IBM8Gb (admin) #> user edit

      Press 'q' and the ENTER key to abort this command.

  account name (1-15 chars)      : user1
  set account expiration in days (0-2000, 0=never): [0]
  should this account have admin authority? (y/n): [n]

  OK to modify user account 'user1' with no admin authority
  and to expire in 0 days?

  Please confirm (y/n): [n]
```

The following example deletes the user account named user3.

```
IBM8Gb (admin) #> user delete user3

  The user account will be deleted.  Please confirm (y/n): [n] y
```

In the following example, the `USERID` account changes the password for the user account named user2.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> passwd user2

      Press 'q' and the ENTER key to abort this command.

  account OLD password               : ********
  account NEW password (8-20 chars)  : ********

  please confirm account NEW password: ********
  password has been changed.
```

Chapter 4. Network and fabric configuration

Network configuration consists of the IP parameters that identify the switch in the network and provide for IP security. This chapter describes the following network configuration tasks:

- Displaying the Ethernet network configuration
- Displaying name server information
- Configuring the Ethernet port
- Verifying a switch in the network
- Verifying and tracing Fibre Channel connections
- Managing IP security

Displaying the Ethernet network configuration

The Show Fabric command displays IP addresses for all switches in the fabric, as shown in the following example:

```
IBM8Gb #> show fabric
  Domain           *133(0x85)
  WWN              10:00:00:c0:dd:0d:53:91
  SymbolicName     IBM8Gb
  HostName         <undefined>
  EthIPv4Address   10.20.116.133
  EthIPv6Address   <undefine>

  * indicates principal switch
```

The Show Setup System command displays the entire switch network configuration, which includes the following:

- IP configurations
- DNS server configuration

To display specific information, add the corresponding keyword. For example, to display DNS configuration information, enter the Show Setup System DNS command:

```
IBM8Gb #> show setup system dns

System Information
  ------------------
  DNSClientEnabled        False
  DNSLocalHostname        <undefined>
  DNSServerDiscovery      Static
  DNSServer1Address       <undefined>
  DNSServer2Address       <undefined>
  DNSServer3Address       <undefined>
  DNSSearchListDiscovery  Static
  DNSSearchList1          <undefined>
  DNSSearchList2          <undefined>
  DNSSearchList3          <undefined>
  DNSSearchList4          <undefined>
  DNSSearchList5          <undefined>
```

Displaying name server information

The Show NS command displays the list of WWNs in fabric as shown in the following example:

```
IBM8Gb #> show ns all
  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   1 (0x1)   010100 N    3   21:00:00:09:6b:36:32:d7 20:00:00:09:6b:36:32:d7
  2   1 (0x1)   010200 N    3   21:01:00:e0:8b:a5:a9:6e 20:01:00:e0:8b:a5:a9:6e
  3   1 (0x1)   010300 N    2,3 10:00:00:00:c9:56:49:cb 20:00:00:00:c9:56:49:cb
  4   1 (0x1)   010900 N    3   21:01:00:e0:8b:a0:ff:35 20:01:00:e0:8b:a0:ff:35
  5   1 (0x1)   010a00 N    3   21:01:00:e0:8b:a5:16:6f 20:01:00:e0:8b:a5:16:6f
  6   1 (0x1)   010b00 N    3   21:01:00:e0:8b:a5:f3:70 20:01:00:e0:8b:a5:f3:70
  7   1 (0x1)   010c00 N    3   21:01:00:e0:8b:a5:31:6f 20:01:00:e0:8b:a5:31:6f

  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   99 (0x63) 630000 N    2,3 20:00:00:c0:dd:0d:2b:54 10:00:00:c0:dd:0d:2b:54
  2   99 (0x63) 630001 N    2,3 10:00:00:00:c9:56:49:ca 20:00:00:00:c9:56:49:ca
  3   99 (0x63) 630002 N    3   21:00:00:09:6b:36:32:d6 20:00:00:09:6b:36:32:d6
  4   99 (0x63) 630004 N    3   21:00:00:e0:8b:85:16:6f 20:00:00:e0:8b:85:16:6f
  5   99 (0x63) 630008 N    3   21:00:00:e0:8b:85:f3:70 20:00:00:e0:8b:85:f3:70
  6   99 (0x63) 63000f N    3   21:00:00:e0:8b:85:a9:6e 20:00:00:e0:8b:85:a9:6e
  7   99 (0x63) 630010 N    3   21:00:00:e0:8b:85:31:6f 20:00:00:e0:8b:85:31:6f
  8   99 (0x63) 630017 N    3   21:00:00:e0:8b:80:ff:35 20:00:00:e0:8b:80:ff:35
  9   99 (0x63) 630800 N    3   20:02:00:a0:b8:0f:7f:9f 20:02:00:a0:b8:0f:7f:9e
  10  99 (0x63) 630900 N    3   20:03:00:a0:b8:0f:7f:9f 20:02:00:a0:b8:0f:7f:9e
```

Configuring the Ethernet port

Use the Set Setup System command in an Admin session to configure the Ethernet port and other network parameters. You can configure all of the following parameters in one session, or you can configure specific parameters by adding the corresponding keyword:

- IPv4 configuration
- IPv6 configuration
- DNS server configuration

IPv4 configuration

The switch supports IPv4, which includes the following:

- Network discovery method
- IP address
- Subnet mask
- IP gateway address

The network discovery method determines how the switch acquires its IP address. The IP address can come from the IP address that resides on the switch or from a server. The switch IP address can be changed only with the CLI or with QuickTools. The switch supports network discovery from the following server types:

- Bootstrap Protocol (BootP)
- Reverse Address Resolution Protocol (RARP)
- Dynamic Host Configuration Protocol (DHCP)

To configure the IP version 4 parameters, enter the Set Setup System Ipv4 command:

```
IBM8Gb (admin) #> set setup system ipv4

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    EthIPv4NetworkEnable    True
    EthIPv4NetworkDiscovery Static
    EthIPv4NetworkAddress   10.20.116.133
    EthIPv4NetworkMask      255.255.255.0
    EthIPv4GatewayAddress   10.20.116.1

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    EthIPv4NetworkEnable    (True / False)                      :
    EthIPv4NetworkDiscovery (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp) :
    EthIPv4NetworkAddress   (dot-notated IP Address)            : 10:20:30:40
    EthIPv4NetworkMask      (dot-notated IP Address)            : 255.0.0.0
    EthIPv4GatewayAddress   (dot-notated IPv4 Address)          : 10.20.30.254

  Do you want to save and activate this system setup? (y/n): [n] y
```

IPv6 configuration

The switch supports IPv6, which includes the following:

- Network discovery method
- IP address
- IP gateway address

The network discovery method determines how the switch acquires its IP address. The IP address can come from the IP address (static) that resides on the switch, from a DHCP server, or it can be learned from a router through the Neighbor Discovery Protocol (NDP). The switch IP address can be changed only with the CLI or with QuickTools.

To configure the IPv6 parameters, enter the Set Setup System Ipv6 command:

```
IBM8Gb (admin) #> set setup system ipv6

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    EthIPv6NetworkEnable    False
    EthIPv6Discovery        Static
    EthIPv6NetworkAddress   <undefined>
    EthIPv6GatewayAddress   <undefined>

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    EthIPv6NetworkEnable    (True / False)                    :
    EthIPv6Discovery        (1=Static, 2=Dhcpv6, 3=Ndp)       :
    EthIPv6NetworkAddress   (IPv6 Address/Mask Length format) :
    EthIPv6GatewayAddress   (IPv6 Address)                    :

  Do you want to save and activate this system setup? (y/n): [n]
```

DNS server configuration

A DNS server manages the host names for a fabric. Host names enable you to specify servers and switches by a meaningful name rather than an IP address. To configure a DNS server, enter the Set Setup System Dns command in an Admin session as shown in the following example:

```
IBM8Gb (admin) #> set setup system dns

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    DNSClientEnabled        False
    DNSLocalHostname        <undefined>
    DNSServerDiscovery      Static
    DNSServer1Address       <undefined>
    DNSServer2Address       <undefined>
    DNSServer3Address       <undefined>
    DNSSearchListDiscovery  Static
    DNSSearchList1          <undefined>
    DNSSearchList2          <undefined>
    DNSSearchList3          <undefined>
    DNSSearchList4          <undefined>
    DNSSearchList5          <undefined>

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    DNSClientEnabled        (True / False)               :
    DNSLocalHostname        (hostname)                   :
    DNSServerDiscovery      (1=Static, 2=Dhcp, 3=Dhcpv6) :
    DNSServer1Address       (IPv4, or IPv6 Address)      :
    DNSServer2Address       (IPv4, or IPv6 Address)      :
    DNSServer3Address       (IPv4, or IPv6 Address)      :
    DNSSearchListDiscovery  (1=Static, 2=Dhcp, 3=Dhcpv6) :
    DNSSearchList1          (domain name)                :
    DNSSearchList2          (domain name)                :
    DNSSearchList3          (domain name)                :
    DNSSearchList4          (domain name)                :
    DNSSearchList5          (domain name)                :

  Do you want to save and activate this system setup? (y/n): [n]
```

Verifying a switch in the network

You can verify that a switch is communicating in the network using the Ping command. The following example successfully tests the network for a switch with IP address 10.20.11.57.

```
IBM8Gb #> ping 10.20.11.57
  Ping command issued. Waiting for response...
IBM8Gb #>
  Response successfully received from 10.20.11.57.
```

If the switch was unreachable, you would see the following display.

```
IBM8Gb #> ping 10.20.11.57
  Ping command issued. Waiting for response...
  No response from 10.20.11.57. Unreachable.
```

Verifying and tracing Fibre Channel connections

You can verify Fibre Channel connections between the switch and the fabric as well as display routing information. Enter the Fcping command to verify a Fibre Channel connection to a switch or a device as shown in the following example. The target device can be defined as a Fibre Channel address or a WWN.

```
IBM8Gb #> fcping 970400 count 3
28 bytes from local switch to 0x970400 time = 10 usec
28 bytes from local switch to 0x970400 time = 11 usec
28 bytes from local switch to 0x970400 time = 119 usec
```

The following is an example of a connection failure:

```
IBM8Gb #> fcping 0x113344 count 3
     28 bytes from local switch to 0x113344 failed
```

Enter the Fctrace command to display Fibre Channel routing information between two devices as shown in the following example. The devices can be defined as Fibre Channel addresses or WWNs.

```
IBM8Gb#> fctrace 970400 970e00 hops 5

  36 bytes from 0x970400 to 0x970e00, 5 hops max

  Domain  Ingress Port WWN         Port  Egress Port WWN          Port
  ------  ----------------         ----  ---------------          ----
  97      20:04:00:c0:dd:02:cc:2e  4     20:0e:00:c0:dd:02:cc:2e  14
  97      20:0e:00:c0:dd:02:cc:2e  14    20:04:00:c0:dd:02:cc:2e  4
```

Managing IP security

To modify IP security, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time through the CLI, QuickTools, or another management application. You must also open an Ipsec Edit session with the Ipsec Edit command. The Ipsec Edit session provides access to the Ipsec, Ipsec Association, Ipsec Policy, Ike Peer, and Ike Policy commands with which you make modifications to the IP security IP security and Internet key exchange (IKE) configurations.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec)#> ipsec . . .
IBM8Gb (admin-ipsec)#> ipsec policy . . .
IBM8Gb (admin-ipsec)#> ipsec association. . .
IBM8Gb (admin-ipsec)#> ike peer . . .
IBM8Gb (admin-ipsec)#> ike policy . . .
```

When you are finished making changes, enter the Ipsec Save command to save and activate the changes and close the Ipsec Edit session. Changes take effect immediately.

```
IBM8Gb (admin-ipsec)#> ipsec save
```

To close the Ipsec Edit session without saving changes, enter the Ipsec Cancel command.

```
IBM8Gb (admin-ipsec)#> ipsec cancel
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

To remove all IP security policies and associations, enter the Reset Ipsec command.

```
IBM8Gb (admin) #> reset ipsec
```

The following sections present IP security concepts and management tasks:

- IP security concepts
- Displaying IP security information
- Managing the security policy database
- Managing the security association database
- Managing IKE peers
- Managing IKE policies
- Resetting the IP security configuration

IP security concepts

Attention:
IP security configurations can be complex: it is possible to unintentionally configure policies and associations that isolate a switch from all communication.

IP security provides encryption-based security for IPv4 and IP6 communications between devices through the use of security policies and associations. The Internet key exchange (IKE) protocol automates the creation of IP security associations on the switch and connected devices and the sharing of encryption keys through the configuration of IKE peers and policies. The security association database comprises all IP security associations. The security policy database comprises all IP security policies. The IKE database comprises all IKE policies and peers. The EncryptionMode service can be set to apply stronger encryption requirements affecting IP security, IKE, and PKI.

Legacy and Strict security

The EncryptionMode service (Legacy or Strict) determines which encryption algorithms, key lengths, and Diffie-Hellman groups can be applied to IP security associations, IKE peers, IKE policies, PKI keys, and certificates. Legacy mode uses encryption algorithms with a strength of 80 bits or greater, and keys with a length of 1,024 or greater. Strict mode uses encryption algorithms with a strength of 112 bits or greater, and keys with a length of 2,048 or greater. Strict mode limits Diffie-Hellman groups to 14 and 24, excluding 1, 2, and 5. For more information about EncryptionMode, see Table 41.

At startup, the switch assesses the IP security, IKE configurations, PKI keys, and certificates against the Encryption Mode service. Under Strict mode, if these configurations use excluded encryption algorithms, key lengths, or Diffie-Hellman groups, the switch applies the configurations unchanged, but generates an alarm indicating the conflict. To resolve the alarm, you must reconfigure the associations, policies, and peers to comply with Strict mode limits.

Security policies and associations

A security policy defines the following parameters:

- Connection source and destination
- Data traffic direction: inbound or outbound
- Protocols for which to protect data traffic
- Security protocols; Authentication Header (AH) or Encapsulating Security Payload (ESP)
- Level of protection: IP security, discard, or none

Policies can define security for host-to-host and host-to-gateway connections; one policy for each direction. For example, to secure the connection between two hosts, you need two policies: one for outbound traffic from the source to the destination, and another for inbound traffic to the source from the destination. You can specify sources and destinations by IP addresses (version 4 or 6) or DNS host names. If a host name resolves to more than one IP address, the switch creates the necessary policies and associations. You can recognize these dynamic policies and associations because their names begin with *DynamicSP_* and *DynamicSA_* respectively.

A security association defines the encryption algorithm and encryption key (public key or secret) to apply when called by a security policy. A security policy may call several associations at different times, but each association is related to only one policy. The security association database is the set of all security associations.

You can apply IP security to all communication between two systems, or to selected protocols, such as ICMP, TCP, or UDP. Furthermore, instead of applying IP security, you can choose to discard all inbound or outbound traffic, or allow all traffic without encryption. Both the AH and ESP security protocols provide source authentication, ensure data integrity, and protect against replay.

IKE peers and policies

IKE is a protocol that automates the sharing of encryption keys and algorithms through the configuration of matching IP security associations on the switch and on the connected device (or peer). The peer configuration defines and configures the IKE security association connection through which the IKE protocol configures the IP security associations. The IKE policy defines the type of data traffic to secure between the switch and the peer, and how to encrypt that data. You must create the same IKE peer and IKE policy configurations on the switch and the peer device.

Public key infrastructure

Public key encryption requires a public key, a corresponding private key, and the necessary certificates to authenticate them. Public key infrastructure (PKI) provides support for the creation and management of public/private key pairs, signed certificates, and certificate authority (CA) certificates when using IKE. You can create a public/private key and combine it with one or more device identities to generate a certificate request. Submit the certificate request to a CA to obtain a signed certificate, which contains the authenticated public/private key pair. In addition to the signed certificate, you must also obtain a CA certificate to authenticate the CA. After downloading the signed certificate and a CA certificate to the switch and importing them into the PKI database, the signed certificate (which contains the authenticated public key) can then be used to complete the IKE peer configuration.

Displaying IP security information

You can display the following types of IP security information:

- Policy and association information
- Public key infrastructure information
- IKE peer and policy information
- IP security configuration history
- IP security configuration limits

Policy and association information

To display general or specific policy and association information, enter the Ipsec List command. The Ipsec List command does not require an Admin session nor an Ipsec Edit session. Within an Ipsec Edit session, the Ipsec Association List and Ipsec Policy List commands display the same information. You can display active, configured, and edited polices and associations:

- Active—policies and associations currently in use

- Configured—policies and associations that have been saved in the IP security database
- Edited—policies and associations that are being edited, but have not yet been saved

The following example displays all active policies and associations:

```
IBM8Gb #> ipsec list

  Active IPsec Information

  Security Association Database
  -----------------------------
  h2h-sh-sa
  h2h-hs-sa

  Security Policy Database
  ------------------------
  h2h-hs-sp
  h2h-sh-sp

  Summary
  -------
    Security Association Count:   2
    Security Policy Count:        2
```

IKE peer and policy information

To display general or specific peer and policy information, enter the Ike List command. The Ike List command does not require an Admin session nor an Ipsec Edit session. The Ike Peer List and Ike Policy List commands display the same information. You can display active, configured, and edited peers and polices:

- Active—peers and policies currently in use
- Configured—peers and policies that have been saved in the IKE database
- Edited—peers and policies that are being edited, but have not yet been saved

The following example displays all configured IKE peers and policies:

```
IBM8Gb #> ike list configured
  Configured (saved) IKE Information
  Peer                              Policy
  ------                            ----
  peer_1
                                    policy_1
                                    policy_2
  peer_2
                                    policy_3
  peer_3
                                    (no policies)
  (No peer)
                                    policy_4
Summary:
  Peer Count                        3
  Policy Count                      4
```

Public key infrastructure information

To display information in the PKI database about public/private key pairs, signed certificates, and certificate authorities, enter the following commands:

- Key List
- Certificate List Local
- Cert_Authority List

The following is an example of the Key List command for key1024:

```
IBM8Gb #> key list key1024
  Key key1024:
    private key with:
    pubkey:    RSA 1024 bits
    keyid:     49:80:4c:aa:d3:c3:bc:c7:f5:b1:41:34:ce:71:48:1d:b9:b3:d9:f9
    subjkey:   f4:b6:b9:27:25:7a:5a:69:a0:9e:cf:14:cd:3c:88:e9:d5:b1:aa:4a
```

The following is an example of the Key List command:

```
IBM8Gb #> key list
  Installed Keys:
    key2048
    key1024
  * indicates key has a matching local certificate
```

IP security configuration history

To display the IP security configuration history, enter the Ipsec History command to display a record of policy and association modifications as shown in the following example:

```
IBM8Gb #> ipsec history

  IPsec Database History
  ----------------------
  ConfigurationLastEditedBy      johndoe@OB-session5
  ConfigurationLastEditedOn      Sat Mar  8 07:14:36 2008
  Active Database Checksum       00000144
  Inactive Database Checksum     00000385
```

History information includes the following:

- Time of the most recent activation and the user account that performed it
- Time of the most recent modification to the IP security configuration and the user account that made it
- Checksum for the active and inactive databases

IP security configuration limits

To display a summary of the objects in the IP security configuration and their maximum limit, enter the Ipsec Limits command, as shown in the following example:

```
IBM8Gb #> ipsec limits

  Configured (saved) IPsec Information

  IPsec Attribute            Maximum  Current
  ---------------            -------  -------
  MaxConfiguredSAs               512        0
  MaxConfiguredSPs               128        0
```

In an Ipsec Edit session, the Ipsec Limits command displays the number of both configured associations and policies, plus those created in the edit session but not yet saved.

Managing the security policy database

The security policy database is made up of user-defined policies and dynamic policies (policies created by the switch). In addition to creating a policy, you can delete, modify, rename, and copy user-defined policies. Dynamic policies can only be copied. The following sections provide instructions for:

- Creating a policy
- Deleting a policy
- Modifying a user-defined policy
- Renaming a user-defined policy
- Copying a policy

Creating a policy

To create a policy, enter the Ipsec Policy Create command, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec policy create h2h-sh-sp

  A list of attributes with formatting will follow.
  Enter a value or simply press the ENTER key to skip specifying a value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

  Value (press ENTER to not specify value, 'q' to quit):
    Description       (string value, 0-127 bytes)                    :  Host-to-host: switch->host
   *SourceAddress     (hostname, IPv4, or IPv6 Address/[PrefixLength]):  fe80::2c0:ddff:fe03:d4c1
    SourcePort        (decimal value, 1-65535)                       :
   *DestinationAddress (hostname, IPv4, or IPv6 Address/[PrefixLength]):  fe80::250:daff:feb7:9d02
    DestinationPort   (decimal value, 1-65535)                       :
   *Protocol          (decimal value, or keyword)
                        Allowed keywords
                          icmp, icmp6, ip4, tcp, udp or any          :  any
   *Direction         (1=in, 2=out)                                  :  2
    Priority          (value, -2147483647 to +214783647)             :
   *Action            (1=discard, 2=none, 3=ipsec)                   :  3
    Mode              (1=transport, 2=tunnel)                 :  1
   *TunnelSource      (IPv4, or IPv6 Address)                 :  fe91::3d1:eecc:bf14:e5d2
   *TunnelDestination (IPv4, or IPv6 Address)                 :  fe91::361:ebcc:bfc8:0e13
   *ProtectionDesired (select one, transport-mode only)
                        1=ah   Authentication Header
                        2=esp  Encapsulating Security Payload
                        3=both                                       :  2
   *espRuleLevel      (1=default, 2=use, 3=require)                  :  3

  The security policy has been created.
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.
```

Deleting a policy

To delete a user-defined policy, enter the Ipsec Policy Delete command, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec policy delete policy_1
  The security policy will be deleted. Please confirm (y/n): [n] y

IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Modifying a user-defined policy

To modify an existing user-defined policy, enter the Ipsec Policy Edit command in an Admin session and an Ipsec Edit session as shown in the following example. An asterisk (*) indicates a required entry.

```
IBM8Gb (admin-ipsec) #> ipsec policy edit h2h-sh-sp
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current
  value.
  To remove a value for an optional attribute, use 'n'.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    Description             Host-to-host: switch->host
      .
      .
      .
    espRuleLevel            require

  New Value (press ENTER to not specify value, 'q' to quit, 'n' for none):
    Description (string value, 0-127 bytes)                    :
   *SourceAddress (IPv4, IPv6 or hostname/[PrefixLength])      :
    SourcePort (decimal value, 1-65535)                        :
   *DestinationAddress (IPv4, IPv6 or hostname/[PrefixLength]) :
    DestinationPort (decimal value, 1-65535)                   :
   *Protocol (decimal value, or keyword)
      Allowed keywords
         icmp, icmp6, ip4, tcp, udp or any                     : tcp
   *Direction (1=in, 2=out)                                    :
    Priority (value, -2147483647 to +2147483647)               :
   *Action (1=discard, 2=none, 3=ipsec)                        :
   *ProtectionDesired (select one, transport-mode only)
      1=ah Authentication Header
      2=esp Encapsulating Security Payload
      3=both :
   *ahRuleLevel (1=default, 2=use, 3=require)                  :
   *espRuleLevel (1=default, 2=use, 3=require)                 :

  The security policy has been edited.
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.

IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Renaming a user-defined policy

To rename a policy (policy_1), enter the Ipsec Policy Rename command as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec policy rename policy_1 policy_4

  The security policy will be renamed. Please confirm (y/n): [n] y

IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Copying a policy

You can copy both user-defined and dynamic policies. To copy a policy (policy_1), enter the Ipsec Policy Copy command as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec policy copy policy_1 policy_a
IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Managing the security association database

The security association database is made up of user-defined associations and dynamic associations (associations created by the switch). In addition to creating an association, you can delete, modify, rename, and copy user-defined associations. Dynamic associations can only be copied. The following sections provide instructions for:

- Creating an association
- Deleting an association
- Modifying a user-defined association
- Renaming a user-defined association
- Copying an association

Creating an association

To create an association, enter the Ipsec Association Create command, as shown in the following example. An asterisk (*) indicates a required entry. Shaded entries indicate options that are available only when EncryptionMode=Legacy. For more information about EncryptionMode, see Table 41.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec association create h2h-sh-sa

  A list of attributes with formatting will follow.
  Enter a value or simply press the ENTER key to skip specifying a value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

  Value (press ENTER to not specify value, 'q' to quit):
    Description        (string value, 0-127 bytes)           :  Host-to-host: switch->host
   *SourceAddress      (hostname, IPv4, or IPv6 Address)     :  fe80::2c0:ddff:fe03:d4c1
   *DestinationAddress (hostname, IPv4, or IPv6 Address)     :  fe80::250:daff:feb7:9d02
   *Protocol           (1=esp, 3=ah)                         :  1
   *SPI                (decimal value, 256-4294967295)       :  333
    Authentication     (select an authentication algorithm)
                          1=hmac-md5       (16 byte key)
                          2=hmac-sha1      (20 byte key)
                          3=hmac-sha256    (32 byte key)
                          4=aes-xcbc-mac   (16 byte key)
                       authentication algorithm choice       :  2
   *AuthenticationKey  (quoted string or raw hex bytes)      :  "12345678901234567890"
   *Encryption         (select an encryption algorithm)
                          2=3des-cbc       (24 byte key)
                          3=null           (0 byte key)
                          4=blowfish-cbc   (5-56 byte key)
                          5=aes-cbc        (16/24/32 byte key)
                          6=twofish-cbc    (16-32 byte key)
                       encryption algorithm choice           :  2
   *EncryptionKey      (quoted string or raw hex bytes)      :  "12345678901234567890123456789012"
    Mode               (1=transport, 2=tunnel)               :  1

  The security association has been created.
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.
```

Deleting an association

To delete a user-defined association, enter the Ipsec Association Delete command, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec association delete association_1

  The security association will be deleted. Please confirm (y/n): [n] y

IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Modifying a user-defined association

To modify an existing user-defined association, enter the Ipsec Association Edit command in an Admin session and an Ipsec Edit session as shown in the following example. An asterisk (*) indicates a required entry. Shaded entries indicate options that are available only when EncryptionMode = Legacy. For more information about EncryptionMode, see Table 41.

```
IBM8Gb (admin-ipsec) #> ipsec association edit h2h-sh-sa
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  To remove a value for an optional attribute, use 'n'.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
     Description         Host-to-host: switch->host
     .
     .
     EncryptionKey       12345678901234567890123 4

  New Value (press ENTER to not specify value, 'q' to quit, 'n' for none):
     Description         (string value, 0-127 bytes)         :
    *SourceAddress       (IPv4, IPv6 or hostname)            :
    *DestinationAddress  (IPv4, IPv6 or hostname)            :
    *Protocol            (1=esp, 3=ah)                       : ah
    *SPI                 (decimal value, 256-4294967295)     :
     Authentication      (select an authentication algorithm)
                            1=hmac-md5       (16 byte key)
                            2=hmac-sha1      (20 byte key)
                            3=hmac-sha256    (32 byte key)
                            4=aes-xcbc-mac   (16 byte key)
                         authentication algorithm choice     :
    *AuthenticationKey   (quotes string or raw hex bytes)    :
    *Encryption          (select an encryption algorithm)
                            2=3des-cbc (24 byte key)
                            3=null     (0 byte key)
                            4=blowfish-cbc (5-56 byte key)
                            5=aes-cbc (16/24/32 byte key)
                            6=twofish-cbc (32 byte key)
                          encryption algorithm choice        :
    *EncryptionKey        (quoted string or raw hex bytes)   :
     Mode                 (1=transport, 2=tunnel)            :

The security association has been edited.
This configuration must be saved with the 'ipsec save' command
before it can take effect, or to discard this configuration
use the 'ipsec cancel' command.

IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Renaming a user-defined association

To rename a user-defined association (association_1), enter the Ipsec Association Rename command, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec association rename association_1 association_4

  The security association will be renamed. Please confirm (y/n): [n] y

IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Copying an association

You can copy both user-defined and dynamic associations. To copy an association (association_1), enter the Ipsec Association Copy command, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec association copy association_1 association_a
IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Managing IKE peers

An IKE peer defines a peer device and configures the IKE security association through which the switch establishes the IP security associations defined by an IKE policy. The IKE database is made up of IKE peers and policies. In addition to creating an IKE peer, you can delete, modify, rename, and copy user-defined peers.

Creating an IKE peer

To create an IKE peer, enter the Ike Peer Create command, as shown in the following example. An asterisk (*) indicates a required entry. Shaded entries indicate options that are available only when EncryptionMode=Legacy. For more information about EncryptionMode, see Table 41.

```
IBM8Gb ># admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ike peer create peer_1

  A list of attributes with formatting will follow.
  Enter a value or simply press the ENTER key to skip specifying a value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

  Value (press ENTER to not specify value, 'q' to quit):
    Description      (string, max=127 chars, N=None)             :  Peer 1
   *Address          (hostname, IPv4, or IPv6 Address)           :  10.0.0.3
    Lifetime         (decimal value, 900-86400 seconds)          :  3600
   *Encryption       (select one or more encryption algorithms)
                          1=3des_cbc
                          2=aes_cbc_128
                          3=aes_cbc_192
                          4=aes_cbc_256                          :  1 4
   *Integrity        (select one or more integrity algorithms)
                          1=md5_96
                          2=sha1_96
                          3=sha2_256
                          4=aes_xcbc_96                          :  1 2 3
   *DHGroup          (select one or more Diffie-Hellman Groups)
                          1, 2, 5, 14, 24                        :  2 14
    Restrict         (True / False)                              :  True
   *Authentication   (1=secret, 2=public_key)                    :  1
   *Key              (quoted string or raw hex bytes)
                          maximum length for quoted string = 128
                          maximum length for raw hex bytes = 256
                         the raw hex length must be even        :  0x11223344

  The IKE peer has been created.
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.
IBM8Gb (admin-IPSEC) #> ipsec save
```

Deleting an IKE peer

To delete an IKE peer, enter the Ike Peer Delete command, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ike peer delete peer_1

  The IKE peer will be deleted. Please confirm (y/n): [n] y

IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Modifying an IKE peer

To modify an existing IKE peer, enter the Ike Peer Edit command in an Admin session and an Ipsec Edit session as shown in the following example. An asterisk (*) indicates a required entry. Shaded entries indicate options that are available only when EncryptionMode=Legacy. For more information about EncryptionMode, see Table 41.

```
IBM8Gb ># admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ike peer edit peer_1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Current Values:
    Description        Peer 1
    Address            10.0.0.3
    Lifetime           3600 (seconds)
    Encryption         3des_cbc aes_cbc_256
    Integrity          md5_96 sha1_96 sha2_256
    DHGroup            2 14
  Restrict           True
  Authentication     secret
  Key                0x1122334
New Value (press ENTER to not specify value, 'q' to quit, 'n' for none):
  Description      (string, max=127 chars, N=None)             :
  *Address         (hostname, IPv4, or IPv6 Address)           :  10.1.2.3
  Lifetime         (decimal value, 900-86400 seconds)          :
 *Encryption       (select one or more encryption algorithms)
                         1=3des_cbc
                         2=aes_cbc_128
                         3=aes_cbc_192
                         4=aes_cbc_256                         :
 *Integrity        (select one or more integrity algorithms)
                        1=md5_96
                        2=sha1_96
                        3=sha2_256
                        4=aes_xcbc_96                          :
 *DHGroup (select one or more Diffie-Hellman Groups)
                        1 , 2, 5, 14, 24                       :
  Restrict         (True / False)                              :  False
  Authentication   (1=secret)                                  :
 *Key              (quoted string or raw hex bytes)
                       maximum length for quoted string = 128
                       maximum length for raw hex bytes = 256
                       the raw hex length must be even :

The IKE peer has been edited.
This configuration must be saved with the 'ipsec save' command
before it can take effect, or to discard this configuration
use the 'ipsec cancel' command.
IBM8Gb (admin-IPSEC) #> ipsec save
```

Renaming an IKE peer

To rename an IKE peer (peer_1), enter the Ike Peer Rename command, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ike peer rename peer_1 peer_4

  The IKE peer will be renamed. Please confirm (y/n): [n] y

IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Copying an IKE peer

To copy an IKE peer (peer_1), enter the Ike Peer Copy command, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ike peer copy peer_1 peer_a
IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Managing IKE policies

An IKE policy defines and configures an IP security association between the switch and the peer device by which data traffic is selected and encrypted. The IKE database is made up of the IKE policies and peers. In addition to creating an IKE policy, you can delete, modify, rename, and copy user-defined policies.

Creating an IKE policy

To create an IKE policy, enter the Ike Policy Create command, as shown in the following example. An asterisk (*) indicates a required entry. Shaded entries indicate options that are available only when EncryptionMode=Legacy. For more information about EncryptionMode, see Table 41.

```
IBM8Gb (admin-ipsec) #> ike policy create policy_2
  A list of attributes with formatting will follow.
  Enter a value or simply press the ENTER key to skip specifying a value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

  Value (press ENTER to not specify value, 'q' to quit):
    Description        (string, max=127 chars, N=None)           :  Policy 2
   *Mode               (1=transport, 2=tunnel)                   :  1
   *LocalAddress       (IPv4, IPv6 Address or keyword 'All'      :  10.0.0.3
    LocalPort          (decimal value, 0-65535 or keyword 'All'  :  1234
    RemotePort         (decimal value, 0-65535 or keyword 'All'  :  0
   *Peer               (string, max=32 chars)                    :  peer_1
   *Protocol           (decimal value, 0-255, or keyword)
                          0=NotSpecified
                          Allowed keywords
                            icmp, icmp6, ip4, tcp, udp or any    :  udp
    Action             (1=ipsec)                                 :  1
    ProtectionDesired  (select one, transport-mode only)
                          1=esp  Encapsulating Security Payload  :  1
    LifetimeChild      (decimal value, 900-86400 seconds)        :  3600
    RekeyChild         (True / False)                            :  True
   *Encryption         (select one or more encryption algorithms)
                          1=3des_cbc
                          2=aes_cbc_128
                          3=aes_cbc_192
                          4=aes_cbc_256                          :  1
    Integrity          (select one or more integrity algorithms)
                          1=md5_96
                          2=sha1_96
                          3=sha2_256
                          4=aes_xcbc_96
                          or the keyword 'None'                  :  1 2 3
    DHGroup            (select one or more Diffie-Hellman Groups)
                          1, 2, 5, 14, 24 or the keyword 'None'  :  1 5
    Restrict           (True / False)                            :  True

  The IKE policy has been created.
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.
IBM8Gb (admin-ipsec) #> ipsec save
```

Deleting an IKE policy

To delete an IKE policy, enter the Ike Policy Delete command as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ike policy delete policy_1

  The IKE policy will be deleted. Please confirm (y/n): [n] y

IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Modifying an IKE policy

To modify an existing IKE policy, enter the Ike Policy Edit command in an Admin session and an Ipsec Edit session as shown in the following example. An asterisk (*) indicates a required entry. Shaded entries indicate options that are available only when EncryptionMode=Legacy. For more information about EncryptionMode, see Table 41.

```
IBM8Gb (admin-ipsec) #> ike policy edit policy_1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

  Current Values:
    Description         Policy 1
    Mode                tunnel
    LocalAddress        10.0.0.6
    LocalPort           456
    RemotePort          0 (All)
    Action              ipsec
    LifetimeChild       3600 (seconds)
    RekeyChild          True
    Restrict            False

  New Value (press ENTER to not specify value, 'q' to quit, 'n' for none):
    Description        (string, max=127 chars, N=None)           :  Policy 1a
   *Mode               (1=transport, 2=tunnel)                   :  1
   *LocalAddress       (IPv4, IPv6 Address or keyword 'All'      :
    LocalPort          (decimal value, 0-65535 or keyword 'All'  :
    RemotePort         (decimal value, 0-65535 or keyword 'All'  :
   *Peer               (string, max=32 chars)                    :  peer_2
   *Protocol           (decimal value, 0-255, or keyword)
                          0=NotSpecified
                          Allowed keywords
                            icmp, icmp6, ip4, tcp, udp or any    :  udp
    Action             (1=ipsec)                                 :  1
    ProtectionDesired  (select one, transport-mode only)
                          1=esp  Encapsulating Security Payload  :  1
    LifetimeChild      (decimal value, 900-86400 seconds)        :  2000
    RekeyChild         (True / False)                            :  true
   *Encryption         (select one or more encryption algorithms)
                           1=3des_cbc
                          2=aes_cbc_128
                          3=aes_cbc_192
                          4=aes_cbc_256                          :  1 3
    Integrity          (select one or more integrity algorithms)
                          1=md5_96
                          2=sha1_96
                          3=sha2_256
                          4=aes_xcbc_96
                          or the keyword 'None'                  :  1 3
    DHGroup            (select one or more Diffie-Hellman Groups)
                          1, 2, 5, 14, 24 or the keyword 'None'  :  2 5
    Restrict           (True / False)                            :  true

  The IKE policy has been edited.
```

```
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.
IBM8Gb (admin-IPSEC) #> ipsec save
```

Renaming an IKE policy

To rename an IKE policy (policy_1), enter the Ike Policy Rename command as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ike policy rename policy_1 policy_4
  The IKE policy will be renamed. Please confirm (y/n): [n] y

IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Copying an IKE policy

To copy an IKE policy (policy_1), enter the Ike Policy Copy command as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ike policy copy policy_1 policy_a
IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

Resetting the IP security configuration

Resetting the IP security configuration deletes all IP security policies, IP security associations, IKE peers, and IKE policies from the switch. There are two ways to do this. Within an Ipsec Edit session, enter the Ipsec Clear command, and then save the changes, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec clear
IBM8Gb (admin-ipsec) #> ipsec save
  The IPsec (and IKE) configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

The Reset Ipsec command deletes all polices, peers, and associations from the switch, but does not require an Ipsec Edit session.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> reset ipsec

The IPsec (and IKE) configuration will be reset and the default values
activated.
Please confirm (y/n): [n] y

Reset and activation in progress ....
```

Chapter 5. Switch configuration

Switch configuration consists of the following tasks:

- Displaying switch information
- Managing switch services
- Managing switch configurations
- Converting a full-fabric SAN switch to a pass-thru module
- Paging a switch
- Setting the date and time
- Resetting a switch
- Installing firmware
- Testing a switch
- Managing idle session timers

Displaying switch information

You can display the following types of switch information:

- Switch operational information
- System process information
- Elapsed time between resets
- Configuration information
- Hardware information
- Firmware information

Switch operational information

The Show Switch command displays a variety of module operational information, including the switch WWN, domain ID, firmware version, administrative state, and operational state, as shown in the following example:

```
IBM8Gb #> show switch
 Switch Information
 ------------------
 SymbolicName                       IBM8Gb
 SwitchWWN                          10:00:00:c0:dd:12:c8:b0
 BootVersion                        V1.12.5.108.0 (day mon date hh:mm:ss yyyy)
 CreditPool                         0
 DomainID                           110 (0x6e)
 FirstPortAddress                   6e0000
 FlashSize - MBytes                 256
 LogFilterLevel                     Info
 MaxPorts                           20
 NumberOfResets                     7
 ReasonForLastReset                 HotReset
 ActiveImageVersion - build date    V9.1.0.x.x (day mon date hh:mm:ss yyyy)
 PendingImageVersion - build date   V9.1.0.x.x (day mon date hh:mm:ss yyyy)
 ActiveConfiguration                default
 AdminState                         Online
 AdminModeActive                    False
 BeaconOnStatus                     False
 OperationalState                   Online
 PrincipalSwitchRole                False
 POSTFaultCode                      00000000
 POSTStatus                         Passed
 TestFaultCode                      00000000
 TestStatus                         NeverRun
 BoardTemp (1) - Degrees Celsius    26
 BoardTemp (2) - Degrees Celsius    25
 BoardTemp (3) - Degrees Celsius    34
 SwitchTemperatureStatus            Normal
```

System process information

The Ps command displays system process information to help you determine what processes are running and the CPU usage. The following example displays current system processes.

```
IBM8Gb #> ps
PID  PPID %CPU %MEM     TIME     ELAPSED COMMAND
286   260  0.0  9.0 00:00:00       55:52 cns
287   260  0.0  9.0 00:00:00       55:52 ens
288   260  0.0  9.0 00:00:00       55:52 dlog
289   260  0.4  9.3 00:00:14       55:52 ds
290   260  0.4 12.4 00:00:14       55:52 mgmtApp
291   260  0.0  9.0 00:00:00       55:52 sys2swlog
297   260  0.0  9.3 00:00:02       55:50 diagAgent
336   260  0.0  9.1 00:00:00       55:44 fc2
337   260  0.0  9.3 00:00:00       55:44 nserver
338   260  0.0  9.2 00:00:00       55:44 mserver
339   260  0.0  9.7 00:00:03       55:44 PortApp
340   260  0.0  9.3 00:00:00       55:44 qfsApp
341   260  0.0  9.3 00:00:00       55:44 eport
342   260  0.0  9.3 00:00:00       55:44 zoning
484   260  0.1  9.2 00:00:04       55:38 snmpservicepath
506   260  0.0  9.5 00:00:00       55:37 util
507   260  0.0  9.1 00:00:00       55:37 port_mon
508   260  0.0  9.1 00:00:00       55:37 diagExec
485   260  2.7  1.3 00:01:31       55:38 snmpd
486   260  0.8  1.2 00:00:28       55:38 snmpmain
```

The column titles are as follows:

- PID–Process identifier
- PPID–Parent process identifier
- %CPU–Percentage CPU usage
- TIME–Actual processing time
- ELAPSED–Elapsed time since the process started
- COMMAND–The command that initiated the process

Elapsed time between resets

The Uptime command displays the elapsed time since the switch was last reset and the reset method. A hot reset or non-disruptive firmware activation does not reset the elapsed time reported by this command. The following example displays the time since the last reset.

```
IBM8Gb #> uptime
  Elapsed up time  : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
  Reason last reset: NormalReset
```

Configuration information

The Show Config command displays a variety of configuration information at the port and switch levels. In addition to the basic switch configurations, the Show Config command displays parameters that control how data is maintained in the security and zoning databases. The Show Config command displays the following types of information:

- Switch configuration parameters
- Zoning configuration parameters
- Security configuration parameters

For information about displaying port configuration information, see "Displaying port information" on page 67.

Switch configuration parameters

Enter the Show Config Switch command to display the switch configuration parameters. These parameters determine the operational characteristics of the switch. For a description of these parameters, see Table 34.

```
IBM8Gb #> show config switch
 Configuration Name: default
 -------------------
  Switch Configuration Information
  --------------------------------
  TransparentMode       False
  AdminState            Online
  BroadcastEnabled      True
  InbandEnabled         True
  FDMIEnabled           True
  FDMIEntries           1000
  DefaultDomainID       19 (0x13)
  DomainIDLock          True
  SymbolicName          IBM8Gb
  PrincipalPriority     254
  ConfigDescription     Default Config
  ConfigLastSavedBy     admin@OB-session5
  ConfigLastSavedOn     day month date time year
  InteropMode           Standard
```

Zoning configuration parameters

Enter the Show Config Zoning command to display zoning configuration parameters. These parameters determine how zoning is applied to the switch. For a description of the zoning configuration parameters, see Table 36.

```
IBM8Gb #> show config zoning
 Configuration Name: default
  -------------------
  Zoning Configuration Information
  --------------------------------
  InteropAutoSave       True
  DefaultZone           Allow
  DiscardInactive       False
```

Security configuration parameters

Enter the Show Config Security command to display security configuration and port binding parameters. These parameters determine how security is applied to the switch. For a description of the switch security configuration parameters, see Table 32. For a description of the port binding parameter, see Table 33.

```
IBM8Gb #> show config security
  Configuration Name: default
  -------------------
  Switch Security Configuration Information
  -----------------------------------------
  FabricBindingEnabled  False
  AutoSave              True

  Port     Binding Status  WWN
  ----     --------------  ---
  0        False           No port binding entries found.
  15       False           No port binding entries found.
  16       False           No port binding entries found.
  17       False           No port binding entries found.
  18       False           No port binding entries found.
  19       False           No port binding entries found.
  1        False           No port binding entries found.
  2        False           No port binding entries found.
  3        False           No port binding entries found.
  4        False           No port binding entries found.
  5        False           No port binding entries found.
  6        False           No port binding entries found.
  7        False           No port binding entries found.
  8        False           No port binding entries found.
  9        False           No port binding entries found.
  10       False           No port binding entries found.
  11       False           No port binding entries found.
  12       False           No port binding entries found.
  13       False           No port binding entries found.
  14       False           No port binding entries found.
```

Hardware information

Use the Show Chassis, Show Power, Show Temp, and Show Voltage commands to display hardware status information. The Show Chassis command displays the status of the switch hardware including power supply, internal temperature, and Heartbeat LED status.

The following is an example of the Show Chassis command:

```
IBM8Gb #> show chassis

  Chassis Information
  -------------------
  BoardTemp (1) - Degrees Celsius   22
  BoardTemp (2) - Degrees Celsius   23
  BoardTemp (3) - Degrees Celsius   25
  PowerSupplyStatus (1)             Good
  HeartBeatCode                     1
  HeartBeatStatus                   Normal
```

The HeartBeatCode and HeartBeatStatus entries indicate the Power-on Self Test (POST) results revealed by the Heartbeat LED blink patterns. The result is normal operation or a blink pattern indicating a critical error as described in Table 3. For more information about the Heartbeat LED and its blink patterns, see your *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru Installation and User's Guide*.

Table 3. Heartbeat LED activity

HeartBeatCode–HeartBeatStatus	**Description**
1–Normal	One blink per second–Normal operation
2–AppDied	Two blink cluster–Internal firmware failure
3–PostFailed	Three blink cluster–Fatal POST error
4–CorruptFilesystem	Four blink cluster–Configuration file system error
5–Overheating	Five blink cluster– Over temperature

The Show Power command shows the status of the power sensors.

```
IBM8Gb: admin> show power

  Power Sensors:

  Sensor  Description       Value
  ------  ----------------  -------
       0  Current             46.84
       1  1-Second Avg        46.32
       2  30-Second Avg       46.25
```

The Show Temp command shows the status, current temperature, the high warning threshold, and the high alarm threshold for each of the internal temperature sensors. The following is an example of the Show Temp command:

```
IBM8Gb #> show temp
Temperature(C) Sensors:

  Sensor  Description          Status  Current  High Warn  High Alarm
  ------  -------------------  ------  -------  ---------  ----------
       0  BOARD                Normal       22         75          81
       1  DS1780               Normal       23        n/a         n/a
       2  MAX1617              Normal       24         75          80
       3  ASIC                 Normal       35        102         105
       4  LM75 0 (exhaust)     Normal       20         75          80
       5  LM75 1 (inlet)       Normal       24         75          80
```

The Show Voltage command shows the status, current voltage, low alarm threshold, and high alarm threshold for each of the internal voltage sensors. The following is an example of the Show Voltage command:

```
IBM8Gb #> show voltage

  Voltage Sensors:

  Sensor  Description  Status  Current  Low Alarm  High Alarm
  ------  -----------  ------  -------  ---------  ----------
       0  1.5V         Good       1.50       1.31        1.68
       1  1.25V        Good       1.24       1.00        1.50
       2  2.5V         Good       2.49       2.20        2.82
       3  3.3V         Good       3.31       2.99        3.62
       4  12V          Good      11.44      10.81       13.31
       5  1.2V         Good       1.23       1.04        1.38
       6  1.8V         Good       1.78       1.61        1.99
       7  1.8V_ANALOG  Good       1.78       1.58        2.02
       8  2.5V_ANALOG  Good       2.39       2.10        2.82
```

Firmware information

Enter the Show Version command to display a summary of switch identity information including the firmware version. The following is an example of the Show Version command:

```
IBM8Gb #> show version
      ****************************************************
      *                                                  *
      *       Command Line Interface SHell  (CLISH)      *
      *                                                  *
      ****************************************************

       SystemDescription   IBM Flex System FC3171 8Gb SAN Switch
       HostName            hsb5802-2
       EthIPv4NetworkAddr  10.20.125.47
       Eth1IPv4NetworkAddr 10.20.3.12
       EthIPv6NetworkAddr  fe80::2c0:ddff:fe01:6f27
       Eth1IPv6NetworkAddr fe80::2c0:ddff:fe01:6f28
       MACAddress          00:c0:dd:01:6f:27
       MAC1Address         00:c0:dd:01:6f:28
       SwitchUUID          20202020202020202020202020202020
       WorldWideName       10:00:00:c0:dd:01:6f:27
       SerialNumber        1029E00021
       SymbolicName        IBM8Gb
       ActiveSWVersion     V9.1.x.x.xxx
       ActiveTimestamp     day mon date hh:mm:ss yyyy
       POSTStatus          Passed
       LicensedExternalPorts 6
       LicensedInternalPorts 14
       SwitchMode          Full Fabric
```

Managing switch services

You can configure your switch to suit the demands of your environment by enabling or disabling a variety of switch services. You manage the switch services using the Show Setup Services and Set Setup Callhome commands. For a description of switch services, see Table 41.

Enter the Show Setup Services command to display the current switch service status, as shown in the following example:

```
IBM8Gb #> show setup services
  System Services Information
  -----------------------------------
  EncryptionMode                 Legacy
  TelnetEnabled                  False
  SSH/sFTPEnabled                True
  GUIMgmtEnabled                 False
  SSLEnabled                     True
  EmbeddedGUIEnabled (HTTP)      False
  EmbeddedGUIEnabled (HTTPs)     True
  NTPEnabled                     True
  CIMEnabled                     True
  FTPEnabled                     False
  MgmtServerEnabled              True
  CallHomeEnabled                True
  SLPEnabled                     True
```

Enter the Set Setup Services command within an Admin session to configure the switch services, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> set setup services

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PLEASE NOTE:
  -----------
  * Further configuration may be required after enabling a service.

  * If services are disabled, the connection to the switch may be lost.

  * When enabling SSL, please verify that the date/time settings
    on this switch and the workstation from where the SSL connection
    will be started match, and then a new certificate may need to be
    created to ensure a secure connection to this switch.

  EncryptionMode           (1=Legacy, 2=Strict) [Legacy ]
  TelnetEnabled                 (True / False)  [False  ]
  SSH/sFTPEnabled               (True / False)  [True   ]
  GUIMgmtEnabled                (True / False)  [False  ]
  SSLEnabled                    (True / False)  [True   ]
  EmbeddedGUIEnabled (HTTP)     (True / False)  [False  ]
  EmbeddedGUIEnabled (HTTPs)    (True / False)  [True   ]
  NTPEnabled                    (True / False)  [True   ]
  CIMEnabled                    (True / False)  [True   ]
  FTPEnabled                    (True / False)  [False  ]
  MgmtServerEnabled             (True / False)  [True   ]
  CallHomeEnabled               (True / False)  [True   ]
  SLPEnabled                    (True / False)  [True   ]

  Do you want to save and activate this services setup? (y/n): [n]
```

Managing switch configurations

The switch configuration determines the basic operational characteristics of the switch. A switch supports up to 10 configurations including the default configuration, named Default Config. The current switch operating characteristics are determined by the active configuration. Only one configuration can be active at one time.

Each switch configuration contains switch, port, port threshold alarm, and zoning configuration components. Managing switch configurations comprises the following tasks:

- Display a list of switch configurations
- Activate a switch configuration
- Copy a switch configuration
- Delete a switch configuration
- Modify a switch configuration
- Back up and restore a switch configuration

Display a list of switch configurations

Enter the Config List command to display the configurations stored on the switch as show in the following example. Notice that the Config List command does not require an Admin session.

```
IBM8Gb #> config list

  Current list of configurations
  ------------------------------
  default
  config_1
  config_2
```

Activate a switch configuration

Enter the Config Activate command to activate a switch configuration (config_1) as shown in the following example:

```
IBM8Gb (admin) config activate config_1
```

Copy a switch configuration

Enter the Config Copy command to create a copy of an existing configuration as shown in the following example:

```
IBM8Gb (admin) config copy config_1 config_2
```

Delete a switch configuration

Enter the Config Delete command to delete a configuration from the switch as shown in the following example. You cannot delete the active configuration nor the default configuration (Default Config).

```
IBM8Gb (admin) config delete config_2
```

Modify a switch configuration

To modify a switch configuration, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time through SSH, Telnet, QuickTools, or another management application. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name the active configuration is assumed.

The Config Edit session provides access to the Set Config commands with which you make modifications to the port, switch, port threshold alarm, or zoning configuration components as shown:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
   The config named default is being edited.
IBM8Gb (admin-config)#> set config port . . .
IBM8Gb (admin-config)#> set config switch . . .
IBM8Gb (admin-config)#> set config threshold . . .
IBM8Gb (admin-config)#> set config zoning . . .
```

The Config Save command saves the changes you made during the Config Edit session. In this case, changes to the configuration named *Default* are being saved to a new configuration named *config_10132003*. However, the new configuration does not take effect until you activate it with the Config Activate command:

```
IBM8Gb (admin-config)#> config save config_10132003
IBM8Gb (admin)#> config activate config_10132003
IBM8Gb (admin)#> admin end
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

The following is an example of the Set Config Switch command. For a description of the switch configuration parameters, see Table 34.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config switch

  A list of attributes with formatting and default values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  TransparentMode     (True / False)                          [False    ]
  AdminState          (1=Online, 2=Offline, 3=Diagnostics)    [Online   ]
  BroadcastEnabled    (True / False)                          [True     ]
  InbandEnabled       (True / False)                          [True     ]
  FDMIEnabled         (True / False)                          [True     ]
  FDMIEntries         (decimal value, 0-1000)                 [1000     ]
  DefaultDomainID     (decimal value, 1-239)                  [2        ]
  DomainIDLock        (True / False)                          [False    ]
  SymbolicName        (string, max=32 chars)                  [IBM8Gb   ]
  PrincipalPriority   (decimal value, 1-255)                  [254      ]
  ConfigDescription   (string, max=64 chars)              [Default Config]
```

To make temporary changes to the switch administrative state, enter the Set Switch State command.

Back up and restore a switch configuration

Successful management of switches and fabrics depends on the effective use of switch configurations. Backing up and restoring a configuration is useful to protect your work or for use as a template in configuring other switches. Backing up and restoring the switch configuration involves the following:

- Creating the backup file
- Downloading the configuration file
- Restoring the configuration file

Creating the backup file

The Config Backup command creates a file on the switch, named `configdata`. This file can be used to restore a switch configuration only from the command line interface; it cannot be used to restore a switch using QuickTools.

```
IBM8Gb #> config backup
```

The `configdata` file contains the following switch configuration information:

- All named switch configurations including port, switch, port threshold alarm, and zoning configurations components.
- All SNMP and network information defined with the Set Setup command.
- The zoning database includes all zone sets, zones, and aliases.
- The security database except the group primary and secondary secrets.

Downloading the configuration file

You use sFTP to download the `configdata` file to your workstation for safe keeping and to upload the file back to the switch for the restore function. To download the `configdata` file, open an sFTP session on the switch and login with the account name `images` and password `images`. Transfer the file in with the Get command as shown in the following example:

```
>sftp images@192.168.70.129
Connecting to 192.168.70.129...
   Password: images
   sftp>get configdata
       Fetching /configdata to configdata
       /configdata                 100%  137KB 136.8KB/s   00:00
sftp> quit
```

You should rename the `configdata` file on your workstation with the switch name and date, `config_switch_169_10112003`, for example.

Restoring the configuration file

The restore operation begins with the sFTP command to upload the configuration file from the workstation to the switch, then finishes with an SSH/Telnet session and the Config Restore command. To upload the configuration file, `config_switch_169_10112003` in this case, open an sFTP session with account name `images` and password `images`. Transfer the file with the Put command as shown:

```
>sftp images@192.168.70.129
Connecting to 192.168.70.129...
Password: images
sftp>put config_switch_169_10112003 configdata
    Uploading configdata-slot3 to /configdata
    configdata-slot3             100%  137KB 136.8KB/s   00:00
sftp>quit
```

The restore process replaces all configuration information on the switch and afterwards the switch is automatically reset. To restore the switch, open an SSH/Telnet session, then enter the Config Restore command from within an Admin session, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config restore
The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
  Alarm Msg: [day month date time year][A1005.0021][SM][Configuration is
being      restored -  this could take several minutes]
  Alarm Msg: [day month date time year][A1000.000A][SM][The switch will be
reset in 3 seconds due to a config restore]
IBM8Gb (admin) #>
  Alarm Msg: [day month date time year][A1000.0005][SM][The switch is being
reset]
```

Converting a full-fabric SAN switch to a pass-thru module

You can convert the Lenovo Flex System FC3171 8 Gb SAN Switch to a transparent pass-thru module by changing the TransparentMode parameter to True using the Set Config Switch command. Converting to a pass-thru module discards the current switch configuration. You can restore the switch to a full-fabric Lenovo Flex System FC3171 8 Gb SAN Switch by returning the TransparentMode parameter to False.

The pass-thru module concentrates multiple blade servers into the external ports. The external ports connect to Fibre Channel switches that support N-Port ID Virtualization (NPIV). The internal ports connect directly to server blades through the BladeCenter unit. The pass-thru module expands the fabric because, unlike a Fibre Channel switch, it does not count against the fabric domain ID limit.

Notes:

Converting the switch to a pass-thru module or back to a SAN switch also reboots the switch.

The following example changes the SAN Switch to a pass-thru module:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config switch

  A list of attributes with formatting and default values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  TransparentMode     (True / False)                        [False         ]
True
  AdminState          (1=Online, 2=Offline, 3=Diagnostics)   [Online        ]
  BroadcastEnabled    (True / False)                         [True          ]
  InbandEnabled       (True / False)                         [True          ]
  FDMIEnabled         (True / False)                         [True          ]
  FDMIEntries         (decimal value, 0-1000)                [1000          ]
  DefaultDomainID     (decimal value, 1-239)                 [2             ]
  DomainIDLock        (True / False)                         [False         ]
  SymbolicName        (string, max=32 chars)                 [IBM8Gb        ]
  PrincipalPriority   (decimal value, 1-255)                 [254           ]
  ConfigDescription   (string, max=64 chars)                 [Default Config]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.

IBM8Gb (admin) #> config save
IBM8Gb (admin) #> config activate
```

Paging a switch

To help you locate a particular switch, you can turn on the beacon feature with the Set Beacon command. This causes all port Logged-In LEDs to flash in unison. The following is an example of how to turn the beacon on and off.

```
IBM8Gb #> set beacon on
IBM8Gb $> set beacon off
```

Setting the date and time

The switch date and time can be set explicitly using the Date command or it can be set automatically through a Network Time Protocol (NTP) server. The Date command also displays the current time. Unlike the Date command, the NTP server also synchronizes the date and time on the switch with the date and time on the workstation. Synchronized date and time is required for Secure Socket Layer (SSL) connections.

To use an NTP server, you must enable the NTP client on the switch and specify an IP address for the NTP server.

Notes:

To set the date with the Date command, the NTP client must be disabled.

Enter the Date command to display the date and time, as shown in the following example:

```
IBM8Gb #> date
  Mon Apr 07 07:51:24 200x
```

Enter the Date command within an Admin session to set the date and time as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> date 013110152025
IBM8Gb (admin) #> date
  Fri Jan 31 10:15:03 UTC 2025
```

To configure the switch to use an NTP server, enter the Set Setup System Ntp command in an Admin session to enable the NTP client on the switch and to specify the NTP server IP address, as shown in the following example:

```
IBM8Gb #> show setup system ntp

  System Information
  ------------------
  NTPClientEnabled    True
  NTPServerDiscovery  Static
  NTPServerAddress    10.35.4.203
  NTPAuthEnabled      True
  NTPAuthKey          ********
  NTPAuthKeyIndex     1
```

Resetting a switch

Table 4 describes the methods for resetting a switch, the corresponding command, and the impact on the switch.

Table 4. Switch reset methods

Description	Hot Reset (Hotreset command)	Soft Reset (Reset Switch command)	Hard Reset (Hardreset Switch command)
Activates pending firmware	✔	✔	✔
Disrupts I/O traffic		✔	✔
QuickTools sessions reconnect afterwards	✔	✔	✔
Clears the event log	✔	✔	✔
Closes all management sessions	✔	✔	✔
Power-on self test			✔

Installing firmware

New firmware becomes available periodically on CD-ROM. Installing firmware on a switch involves the following steps:

1. Download the firmware image file to the switch.
2. Unpack the firmware image file.
3. Activate the new firmware. The activation can be disruptive or non-disruptive. For information about the conditions for a non-disruptive activation, see “Nondisruptive activation” on page 59.

The Firmware Install and the Image Install commands automate the firmware installation process and perform a disruptive activation as described in “One-step firmware installation” on page 60. To perform a nondisruptive activation, see “Custom firmware installation” on page 61.

Nondisruptive activation

You can load and activate new firmware on a switch disruptively or nondisruptively depending on the condition of the fabric and the commands you choose. If you attempt to perform a non-disruptive activation without satisfying the following conditions, the activation will fail. If the non-disruptive activation fails, you will usually be prompted to try again later. Otherwise, the switch will perform a disruptive activation.

- The current firmware version permits the installation and non-disruptive activation of 9.1 firmware. For information about previous compatible firmware versions, see the *Firmware Version 9.1 Release Notes*.
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, changing switch configurations, or installing firmware.
- No port on the switch is in the diagnostic state.
- No Zoning Edit sessions are open on the switch.
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.
- Install firmware on one switch at a time in the fabric. If you are installing firmware on one switch, wait 120 seconds after the activation is complete before installing firmware on a second switch.

Ports that are stable when the non-disruptive activation begins, then change states, will be reset. When the non-disruptive activation is complete, QuickTools sessions reconnect automatically. However, SSH and Telnet sessions must be restarted manually.

One-step firmware installation

The Firmware Install and Image Install commands download the firmware image file from an FTP, TFTP, or sFTP server to the switch, unpack the image file, and perform a disruptive activation in one step. You can also download from a URL.

Notes:

The sFTP switch service is enabled by default, and the FTP and TFTP services are disabled. If you intend to use FTP or TFTP, you must first enable the service. For more information about switch services, see "Managing switch services" on page 50.

The one-step installation process prompts you to enter the following:

- The file transfer protocol: FTP, TFTP, sFTP, or URL
- An account name and password on the remote host (FTP, sFTP)
- IP address of the remote host (FTP, TFTP, sFTP)
- Pathname for the firmware image file (FTP, TFTP, sFTP). For URL, enter a URL in the form http://, ftp://, or https://.

1. Enter the following commands to download the firmware from a remote host to the switch, install the firmware, then reset the switch to activate the firmware.

```
IBM8Gb #> admin start
IBM8Gb #> firmware install
  The switch will be reset. This process will cause a
  disruption to I/O traffic.
  Continuing with this action will terminate all management
  sessions,including any Telnet sessions. When the firmware
  activation is complete, you may log in to the switch again.
  Do you want to continue? [y/n]: y
  Press 'q' and the ENTER key to abort this command.
```

2. Enter your choice for the file transfer protocol with which to download the firmware image file.

```
FTP, TFTP, SFTP, or URL : sftp
```

3. In this example, enter your account name, the password, and the IP address of the remote host. When prompted for the source file name, enter the path for the firmware image file.

```
User Account    : johndoe
Password        : 888888888
IP Address      : 10.20.20.200
Source Filename : 9.1.0.xx_ipc
About to install image.  Do you want to continue? [y/n] y
```

4. When prompted to install the new firmware, enter Yes to continue or No to cancel. Entering Yes will disrupt traffic. This is the last opportunity to cancel.

```
About to install image. Do you want to continue? [y/n] y
Connected to 10.20.20.200 (10.20.20.200).
230 User johndoe logged in.
```

5. The firmware will now be downloaded from the remote host to the switch, installed, and activated.

Custom firmware installation

A custom firmware installation downloads the firmware image file from a remote host to the switch, unpacks the image file, and resets the switch in separate steps. This allows you to choose the type of reset and whether the activation will be disruptive (Reset Switch command) or nondisruptive (Hotreset command).

Notes:
The sFTP switch service is enabled by default, and the FTP and TFTP services are disabled. If you intend to use FTP or TFTP, you must first enable the service. For more information about switch services, see "Managing switch services" on page 50.

The following example illustrates a custom firmware installation with a nondisruptive activation.

1. Download the firmware image file from the workstation to the switch. Enter the Image Sftp command to download the firmware image file:

   ```
   IBM8Gb (admin) #> image sftp user_name ip_address filename
   ```

   - If the image file resides at a URL, you can enter the Image URL command to download the firmware image file:

     ```
     IBM8Gb (admin) #> image url http://xxxxx.xxxxx.com
     ```

   - If your workstation does not have an sFTP server, use an sFTP client such as PuTTY. The following example downloads the firmware image file from a Linux workstation to the switch:

     ```
     >sftp@ip_address or switchname
     Password: images
     sftp>put filename
         Uploading filename to /filename
         filename             100%  137KB 136.8KB/s   00:00
     sftp>quit
     ```

2. Display the list of firmware image files on the switch to confirm that the file was loaded.

   ```
   IBM8Gb #> admin start
   IBM8Gb (admin) $> image list
   ```

3. Unpack the firmware image file to install the new firmware in flash memory.

   ```
   IBM8Gb (admin) $> image unpack filename
   ```

4. Wait for the unpack to complete.

   ```
   Image unpack command result: Passed
   ```

5. A message will prompt you to reset the switch to activate the firmware. Use the Hotreset command to attempt a non-disruptive activation.

   ```
   IBM8Gb (admin) $> hotreset
   ```

Testing a switch

You can test all ports on a switch using the Test Switch command. There are three test types: online, offline, and connectivity. For information about testing individual ports, see "Testing a port" on page 81.

The following sections describe the test types, displaying test status, and cancelling a switch test:

- Online tests for switches
- Offline tests for switches
- Connectivity tests for switches
- Displaying switch test status
- Canceling a switch test

Online tests for switches

An online test is a non-disruptive test that exercises port-to-device connections for all ports that are online. The following is an example of an online test:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> test switch online

A list of attributes with formatting and current values will follow. Enter a
new value or simply press the ENTER key to accept the default value. If you
wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

LoopCount     (decimal value, 1-4294967295)   [100    ]
FrameSize     (decimal value, 40-2148)        [256    ]
DataPattern   (32-bit hex value or 'Default') [Default]
StopOnError   (True / False)                  [True   ]
LoopForever   (True / False)                  [False  ]

Do you want to start the test? (y/n) [n] y
```

Offline tests for switches

An offline test is a disruptive test that exercises all port connections for a switch in the diagnostics state. You must place the switch in the diagnostics state using the Set Switch State command before starting the test. There are two types of offline test: internal loopback and external loopback.

- An internal loopback test exercises all internal port connections.
- An external loopback test exercises all internal port and transceiver connections. A transceiver with a loopback plug is required for all ports.

The following example performs an offline internal loopback test on a switch:

```
IBM8Gb #> admin start
IBM8Gb (admin) #>set switch state diagnostics
IBM8Gb (admin) #> test switch offline internal

A list of attributes with formatting and current values will follow. Enter a
new value or simply press the ENTER key to accept the default value. If you
wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

LoopCount     (decimal value, 1-4294967295)   [100    ]
FrameSize     (decimal value, 40-2148)        [256    ]
DataPattern   (32-bit hex value or 'Default') [Default]
StopOnError   (True / False)                  [True   ]
LoopForever   (True / False)                  [False  ]

Do you want to start the test? (y/n) [n] y
```

Connectivity tests for switches

A connectivity test is a disruptive test that exercises all port and inter-port connections for a switch in the diagnostics state. You must place the switch in the diagnostics state using the Set Switch State command before starting the test. There are two types of connectivity test: internal loopback and external loopback.

- An internal loopback test exercises all internal port and inter-port connections.
- An external loopback test exercises all internal port, transceiver, and inter-port connections. A transceiver with a loopback plug is required for all ports.

The following example performs a connectivity internal test on a switch:

```
IBM8Gb #> admin start
IBM8Gb (admin) #>set switch state diagnostics
IBM8Gb (admin) #> test switch connectivity internal
A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  LoopCount     (decimal value, 1-4294967295)               [100    ]
  FrameSize     (decimal value, 40-2148)                    [256    ]
  DataPattern   (32-bit hex value or keyword 'Default')     [Default]
  StopOnError   (True / False)                              [True   ]
  LoopForever   (True / False)                              [False  ]

  Do you want to start the switch test? (y/n): [n] y
```

When the test is complete, remember to place the switch back online. The switch resets when it leaves the diagnostics state.

```
IBM8Gb (admin) #> set switch state online
```

Displaying switch test status

You can display the test status while the test is in progress by entering the Test Status Switch command as shown in the following example:

```
IBM8Gb (admin) #> test status switch

  Test    Test                  Test                Loop      Test
  Level   Type                  Status             Count  Failures
  -----   ----                  ------             -----  --------
  Switch  Online                Passed                 3         0

  Port    Test                  Test                Loop      Test
  Num     Type                  Status             Count  Failures
  ----    ----                  ------             -----  --------
  0       Online                Passed                 3         0
  15      Online                NeverRun               0         0
  16      Online                NeverRun               0         0
  17      Online                NeverRun               0         0
  18      Online                NeverRun               0         0
  19      Online                NeverRun               0         0
  1       Online                Passed                 3         0
  2       Online                Passed                 3         0
  3       Online                NeverRun               0         0
  4       Online                Passed                 3         0
  5       Online                NeverRun               0         0
  6       Online                NeverRun               0         0
  7       Online                NeverRun               0         0
  8       Online                NeverRun               0         0
  9       Online                NeverRun               0         0
  10      Online                Passed                 3         0
  11      Online                NeverRun               0         0
  12      Online                NeverRun               0         0
  13      Online                NeverRun               0         0
  14      Online                NeverRun               0         0
```

Canceling a switch test

To cancel a switch test that is in progress, enter the Test Cancel Switch command.

Managing idle session timers

You can limit the duration of idle login sessions and idle Admin sessions (Admin Start command). You can specify limits up to 1,440 minutes; specifying 0 means unlimited. Idle login sessions that exceed the limit are logged off (InactivityTimeout). An idle Admin session that exceeds the limit is ended, but the login session may be maintained (AdminTimeout). By default, no limit is enforced on idle login sessions; idle Admin sessions are ended after 10 minutes.

Enter the Show Setup System Timers command to display the idle login and Admin session configuration as shown in the following example:

```
IBM8Gb #> show setup system timers

  System Information
  ------------------
  AdminTimeout             10
  InactivityTimeout        0
```

Enter the Set Setup System Timers command to configure idle login and Admin session limits as shown in the following example:

```
IBM8Gb (admin) #> set setup system timers

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    AdminTimeout            30
    InactivityTimeout       0

  New Value (press ENTER to accept current value, 'q' to quit):
    AdminTimeout            (dec value 0-1440 minutes, 0=never) :
    InactivityTimeout       (dec value 0-1440 minutes, 0=never) :

  Do you want to save and activate this system setup? (y/n): [n]
```

Chapter 6. Port configuration

This chapter describes the following topics:

- Displaying port information
- Modifying port operating characteristics
- Mapping transparent fabric ports on a pass-thru module
- Port binding
- Resetting a port
- Configuring port threshold alarms
- Testing a port
- Extending port transmission distance

Displaying port information

You can display the following port information:

- Port configuration parameters
- Port operational information
- Port threshold alarm configuration parameters
- Port performance
- Transceiver information

Port configuration parameters

Enter the Show Config Port command to display the port configuration parameters. These parameters determine the operational characteristics of the port. See Table 31 for a description of these parameters.

The following example shows port configuration information for external port 0 on a full-fabric SAN switch.

```
IBM8Gb #> show config port 0

  Configuration Name: default
  ---------------------------

  Port Number: 0
  ------------
  AdminState         Online
  LinkSpeed          Auto
  PortType           GL
  SymbolicName       Port0
  ALFairness         False
  DeviceScanEnabled  True
  ForceOfflineRSCN   False
  ARB_FF             False
  InteropCredit      0
  ExtCredit          0
  FANEnabled         True
  AutoPerfTuning     False
  MSEnabled          True
  NoClose            False
  IOStreamGuard      Auto
  PDISCPingEnable    True
```

The following example displays port configuration information for internal port 1 on a full-fabric SAN switch.

```
IBM8Gb #> show config port 1

  Configuration Name: default
  ---------------------------

  Port Number: 1
  ------------
  AdminState         Online
  LinkSpeed          Auto
  PortType           F
  SymbolicName       Port1
  ALFairness         False
  DeviceScanEnabled  True
  ForceOfflineRSCN   False
  ARB_FF             False
  InteropCredit      0
  ExtCredit          0
  FANEnabled         True
  AutoPerfTuning     False
  MSEnabled          True
  NoClose            False
  IOStreamGuard      Disabled
  PDISCPingEnable    True
```

The following example shows port configuration information for external port 0 on a pass-thru module.

```
IBM8Gb #> show config port 0

  Configuration Name: default
  ---------------------------

  Port Number: 0
  ------------
  AdminState         Online
  LinkSpeed          Auto
  PortType           TF
  SymbolicName       Port0
```

The following example shows port configuration information for internal port 1 on a pass-thru module.

```
IBM8Gb #> show config port 1

  Configuration Name: default
  ---------------------------

  Port Number: 1
  ------------
  AdminState         Online
  LinkSpeed          Auto
  PortType           TH
  PrimaryTFPortMap   0
  BackupTFPortMap    15
  SymbolicName       Port1
```

Port operational information

Enter the Show Port command to display port operational information. The following example shows port operational information for external port 0 on a full-fabric module.

```
IBM8Gb #> show port 0
 Port Number: 0
  ------------
  AdminState         Online
  AsicNumber         0
  AsicPort           0
  ConfigType         GL
  EpIsoReason        NotApplicable
  IOStreamGuard      Disabled
  FabricWWN          00:00:00:00:00:00:00:00
  LinkSpeed          8Gb/s
  MaxCredit          16
  MediaPartNumber    FTLF8528P2BCV
  MediaRevision      A
  MediaSpeeds        2, 4, 8Gb/s
  MediaType          800-MX-SN-S
  MediaVendor        FINISAR CORP.
  MediaVendorID      00009065
  NeighborSwitcb     0000000000000000
  OperationalState   Online
  PerfTuningMode     Normal
  PortID             6f0000
  PortWWN            20:00:00:c0:dd:0d:8d:ab
  POSTFaultCode      00000000
  POSTStatus         Passed
  RunningType        E
  SupportedSpeeds    1, 2, 4, 8Gb/s
  SymbolicName       Port0
  SyncStatus         SyncAcquired
  TestFaultCode      00000000
  TestStatus         NeverRun
  UpstreamISL        False
  XmitterEnabled     True
                      Port Statistics

  ALInit             37                 LIP_F8_F7          0
  ALInitError        0                  LinkFailures       0
  BadFrames          0                  Login              3
  BBCR_FrameFailures 0                  Logout             2
  BBCR_RRDYFailures  0                  LongFramesIn       0
  Class2FramesIn     0                  LoopTimeouts       0
  Class2FramesOut    0                  LossOfSync         1
  Class2WordsIn      0                  LostFrames         0
  Class2WordsOut     0                  LostRRDYs          0
  Class3FramesIn     0                  PrimSeqErrors      0
  Class3FramesOut    0                  RxLinkResets       3
  Class3Toss         0                  RxOfflineSeq       2
  Class3WordsIn      0                  ShortFramesIn      0
  Class3WordsOut     0                  TotalErrors        0
  DecodeErrors       0                  TotalLinkResets    41
  EpConnects         3                  TotalLIPsRecvd     8
  FBusy              0                  TotalLIPsXmitd     39
  FlowErrors         0                  TotalOfflineSeq    40
  FReject            0                  TotalRxFrames      0
```

```
  InvalidCRC         0                  TotalRxWords       0
  InvalidDestAddr    0                  TotalTxFrames      0
  LIP_AL_PD_AL_PS    0                  TotalTxWords       0
  LIP_F7_AL_PS       0                  TxLinkResets       38
  LIP_F7_F7          8                  TxOfflineSeq       38
  LIP_F8_AL_PS       0
```

Port threshold alarm configuration parameters

Enter the Show Config Threshold command to display the port threshold alarm parameters. These parameters determine the error thresholds at which the switch issues alarms. See Table 35 for a description of these parameters.

```
IBM8Gb #> show config threshold
  Configuration Name: default
  ------------
  Threshold Configuration Information
  ----------------------------------
  ThresholdMonitoringEnabled      False
  CRCErrorsMonitoringEnabled      True
    RisingTrigger                 25
    FallingTrigger                1
    SampleWindow                  10
  DecodeErrorsMonitoringEnabled   True
    RisingTrigger                 25
    FallingTrigger                0
    SampleWindow                  10
  ISLMonitoringEnabled            True
    RisingTrigger                 2
    FallingTrigger                0
    SampleWindow                  10
  LoginMonitoringEnabled          True
    RisingTrigger                 5
    FallingTrigger                1
    SampleWindow                  10
  LogoutMonitoringEnabled         True
    RisingTrigger                 5
    FallingTrigger                1
    SampleWindow                  10
  LOSMonitoringEnabled            True
    RisingTrigger                 100
    FallingTrigger                5
    SampleWindow                  10
```

Port performance

Enter the Show Perf command to display port performance in terms of the volume of data transmitted, data received, or errors. You can display continuous live performance information for one or more ports, or an instantaneous summary. The following example displays an instantaneous summary in bytes and frames. Values are expressed in thousands (K) and millions (M) of bytes or frames per second.

```
IBM8Gb #> show perf
         Bytes/s    Bytes/s    Bytes/s    Frames/s   Frames/s   Frames/s
Port      (in)       (out)    (total)      (in)       (out)    (total)
----     -------    -------    -------    --------   --------   --------
Ext1:0   0          0          0          0          0          0
Ext2:15  49M        3M         52M        32K        2K         34K
Ext3:16  0          0          0          0          0          0
Ext4:17  0          0          0          0          0          0
Ext5:18  0          0          0          0          0          0
Ext6:19  0          0          0          0          0          0

Bay1    2M         23M        26M        1K         15K        17K
Bay2    0          0          0          0          0          0
Bay3    1M         25M        26M        972        16K        17K
Bay4    0          0          0          0          0          0
Bay5    0          0          0          0          0          0
Bay6    0          0          0          0          0          0
Bay7    0          0          0          0          0          0
Bay8    0          0          0          0          0          0
Bay9    0          0          0          0          0          0
Bay10   0          0          0          0          0          0
Bay11   0          0          0          0          0          0
Bay12   0          0          0          0          0          0
Bay13   0          0          0          0          0          0
Bay14   0          0          0          0          0          0
```

Transceiver information

Enter the Show Media command to display operational information about one or more transceivers as shown in the following example. For a description of the transceiver information in the Show Media display, see Table 52.

```
IBM8Gb #> show media 19
  Port Number: 19
  ------------
  MediaType             800-MX-SN-I
  MediaVendor           AVAGO
  MediaPartNumber       AFBR-57D5APZ
  MediaRevision         Q12
  MediaSerialNumber     AD0724E0569
  MediaSpeeds           2Gb/s, 4Gb/s 8Gb/s

                           Temp     Voltage     Tx Bias      Tx Pwr      Rx Pwr
                            (C)         (V)        (mA)        (mW)        (mW)
                      ----------- ----------- ----------- ----------- -----------
        Value              26.14        3.33        5.38       0.581       0.612
        Status            Normal      Normal      Normal      Normal      Normal
        HighAlarm          90.00        3.80        8.50       0.800       6.550
        HighWarning        85.00        3.63        8.50       0.700       1.100
        LowWarning        -10.00        2.97        2.00       0.100       0.049
        LowAlarm          -15.00        2.80        2.00       0.050       0.000
```

Modifying port operating characteristics

You can make permanent or temporary changes to port operating characteristics. You make permanent port configuration changes using the Set Config Port command. These changes are saved in the active configuration and are preserved across switch or port resets. The Set Port command makes temporary changes that apply until the next port or switch reset, or until you activate a configuration.

Notes:

- 8-Gbps SFPs do not support the 1-Gbps setting. Setting a port to 1-Gbps that has an 8-Gbps SFP cause the port to go down.
- Internal ports are set to 8-Gbps by default.

The following example permanently changes the administrative state for external port 0 on a full-fabric switch:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config port 0
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  0
  ------------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down)   [Online]
offline
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto)   [Auto  ]
  PortType         (GL / G / F / FL / Donor)                      [GL    ]
  SymPortName      (string, max=32 chars)                         [Port0 ]
  ALFairness       (True / False)                                 [False ]
  DeviceScanEnable (True / False)                                 [True  ]
  ForceOfflineRSCN (True / False)                                 [False ]
  ARB_FF           (True / False)                                 [False ]
  InteropCredit    (decimal value, 0-255)                         [0     ]
  ExtCredit        (dec value, increments of 15, non-loop only)   [0     ]
  FANEnable        (True / False)                                 [True  ]
  AutoPerfTuning   (True / False)                                 [False ]
  MFSEnable        (True / False)                                 [False ]
  MSEnable         (True / False)                                 [True  ]
  NoClose          (True / False)                                 [False ]
  IOStreamGuard    (Enable / Disable / Auto)                      [Auto  ]
  PDISCPingEnable  (True / False)                                 [True  ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
IBM8Gb (admin-config) #> config save
IBM8Gb (admin-config) #> config activate
```

The following example changes the administrative state for the internal port 1 on a full-fabric module:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config port 1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  1
  ------------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down)   [Online] offline
  LinkSpeed        (2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto)            [8Gb/s ]
  PortType         (F / Donor)                                    [F     ]
  SymPortName      (string, max=32 chars)                         [Port1 ]
  ALFairness       (True / False)                                 [False ]
  DeviceScanEnable (True / False)                                 [True  ]
  ForceOfflineRSCN (True / False)                                 [False ]
  ARB_FF           (True / False)                                 [False ]
  InteropCredit    (decimal value, 0-255)                         [0     ]
  ExtCredit        (dec value, increments of 15, non-loop only)   [0     ]
  FANEnable        (True / False)                                 [True  ]
  AutoPerfTuning   (True / False)                                 [False ]
  MFSEnable        (True / False)                                 [False ]
  MSEnable         (True / False)                                 [True  ]
  NoClose          (True / False)                                 [False ]
  IOStreamGuard    (Enable / Disable / Auto)                      [Auto  ]
  PDISCPingEnable  (True / False)                                 [True  ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
IBM8Gb (admin-config) #> config save
IBM8Gb (admin-config) #> config activate
```

You can configure external ports (0, 15, 16, 17, 18, 19) as a group based on port 0, or all internal ports (1–14) based on port 1 using the Set Config Ports command. The following example configures the external ports based on port 0 on a SAN switch and activates the configuration.

```
IBM8Gb #> admin start
IBM8Gb (admin) config edit
IBM8Gb (admin) #> set config ports external
  A list of attributes with formatting and current values for the port
  number or port type specified at the command line will follow.
  Each value that is changed will be set for ALL EXTERNAL PORTS.
  If you wish to terminate this process before reaching the end of the
  list press 'q' or 'Q' and the ENTER key to do so.

  Configuring all external ports (displaying values from port number:  0)
  ------------------------------------------------------------------

  AdminState      (1=Online, 2=Offline, 3=Diagnostics, 4=Down)     [Online]
  LinkSpeed       (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto)     [Auto ]
  PortType         (F / Donor)                                     [F     ]
  ALFairness       (True / False)                                  [False ]
  DeviceScanEnable (True / False)                                  [True  ]
  ForceOfflineRSCN (True / False)                                  [False ]
  ARB_FF           (True / False)                                  [False ]
  InteropCredit    (decimal value, 0-255)                          [0     ]
  ExtCredit        (dec value, increments of 15, non-loop only)    [0     ]
  FANEnable        (True / False)                                  [True  ]
  AutoPerfTuning   (True / False)                                  [False ]
  MFSEnable        (True / False)                                  [False ]
  MSEnable         (True / False)                                  [True  ]
  NoClose          (True / False)                                  [False ]
  IOStreamGuard    (Enable / Disable / Auto)                       [Auto  ]
  PDISCPingEnable  (True / False)                                  [True  ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command..

IBM8Gb (admin-config)#> config save
IBM8Gb (admin)#> config activate
IBM8Gb (admin)#> admin end
```

You can duplicate a specified port configuration on specified target ports using the clone config port command. The following example configures ports 15–19 based on port 0:

```
IBM8Gb #> admin start
IBM8Gb (admin) config edit
IBM8Gb (admin) #> clone config port 0 15-19
  Port 0 configuration will be cloned to ports 15 16 17 18 19
  Please confirm (y/n): [n] y
IBM8Gb (admin-config)#> config save
IBM8Gb (admin)#> config activate
IBM8Gb (admin)#> admin end
```

The following example temporarily changes the external port 0 administrative state to Down:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> set port 0 state down
```

Mapping transparent fabric ports on a pass-thru module

TF_Port mapping assigns one or more TF_Ports to pass traffic to and from a specified TH_Port. You can specify a primary mapping and a secondary mapping for each TH_Port. If all TF_Ports in the primary mapping fail, the secondary mapping is used. Table 5 describes the default primary and secondary mappings.

Table 5. Default primary and secondary port mappings

Primary mapping		**Secondary mapping**	
TH_Ports	TF_Ports	TH_Ports	TF_Ports
1, 2	0	1, 2	15
3, 4	15	3, 4	0
5, 6, 7	16	5, 6, 7	0
8, 9	17	8, 9	0
10, 11	18	10, 11	0
12, 13, 14	19	12, 13, 14	0

The following example creates a primary map and a backup map. This example assumes that ports 0, 15, 16, 17, 18, and 19 have been configured as TF_Ports.

- Primary map: TF_Ports 0, 15, 16 are mapped to all TH_Ports
- Backup map: TF_Ports 17, 18, and 19 are mapped to all TH_Ports

```
IBM8Gb #> admin start
IBM8Gb (admin) config edit
IBM8Gb (admin) #> set config ports internal
  A list of attributes with formatting and current values for the port
  number or port type specified at the command line will follow.
  Each value that is changed will be set for ALL INTERNAL PORTS.
  If you wish to terminate this process before reaching the end of the
  list press 'q' or 'Q' and the ENTER key to do so.

  Configuring all internal ports (displaying values from port number:  1)
  ----------------------------------------------------------------

  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online]
  LinkSpeed        (2=2Gb/s, 4=4Gb/s, A=Auto)                   [8Gb/s ]
  PrimaryTFPortMap (decimal value for port, N=no mapping)       [0     ] 0,15,16
  BackupTFPortMap  (decimal value for port, N=no mapping)       [15    ] 17,18,19

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.

IBM8Gb (admin-config)#> config save
IBM8Gb (admin)#> config activate
IBM8Gb (admin)#> admin end
```

Port binding

Port binding establishes up to 32 switches or devices that are permitted to log in to a particular port. Switches or devices that are not among the 32 are refused access to the port. Enter the Show Config Security Portbinding command to display the port binding configuration for all ports as shown in the following example.

```
IBM8Gb #> show config security portbinding

  Configuration Name: default
  -------------------

  Port     Binding Status  WWN
  ----     --------------  ---
  Ext1:0   False           No port binding entries found.
  Ext2:15  False           No port binding entries found.
  Ext3:16  False           No port binding entries found.
  Ext4:17  False           No port binding entries found.
  Ext5:18  False           No port binding entries found.
  Ext6:19  False           No port binding entries found.
  Bay1     False           No port binding entries found.
  Bay2     False           No port binding entries found.
  Bay3     False           No port binding entries found.
  Bay4     False           No port binding entries found.
  Bay5     False           No port binding entries found.
  Bay6     False           No port binding entries found.
  Bay7     False           No port binding entries found.
  Bay8     False           No port binding entries found.
  Bay9     False           No port binding entries found.
  Bay10    False           No port binding entries found.
  Bay11    False           No port binding entries found.
  Bay12    False           No port binding entries found.
  Bay13    False           No port binding entries found.
  Bay14    False           No port binding entries found.
```

Enter the Set Config Security Portbinding command to enable port binding for the selected port and to specify the world wide names of the authorized ports/devices. The following example enables port binding on port 0 and specifies two device world wide names.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config security port 0

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PortBindingEnabled (True / False)[False] true
  WWN                (N=None / WWN)[None ] 10:00:00:c0:dd:00:b9:f9
  WWN                (N=None / WWN)[None ] 10:00:00:c0:dd:00:b9:f8
  WWN                (N=None / WWN)[None ] n

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Resetting a port

Enter the Reset Port command to reinitialize one or more ports and to discard any temporary changes that have been made to the administrative state or link speed. The following example reinitializes port 15:

```
IBM8Gb #> reset port 15
```

Configuring port threshold alarms

The switch can monitor a set of port errors and generates alarms based on user-defined sample windows and thresholds. These port errors include the following:

- Cyclic Redundancy Check (CRC) errors
- Decode errors
- ISL connection count
- Device login errors
- Device logout errors
- Loss-of-signal errors

You make changes to the port threshold alarms by modifying the switch configuration as described in “Modify a switch configuration” on page 52. For a description of the port alarm threshold parameters, see Table 35.

The switch will down a port if an alarm condition is not cleared within three consecutive sampling windows (by default 30 seconds). Reset the port to bring it back online. An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling trigger.

Enter the Set Config Threshold command to enable and configure port threshold monitoring on the switch, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb  (admin) #> config edit
IBM8Gb (admin-config) #> set config threshold
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

ThresholdMonitoringEnabled     (True / False)              [False     ]
CRCErrorsMonitoringEnabled     (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
DecodeErrorsMonitoringEnabled  (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
ISLMonitoringEnabled           (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [2         ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
LoginMonitoringEnabled         (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
LogoutMonitoringEnabled        (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
 LOSMonitoringEnabled           (True / False)             [True      ]
  RisingTrigger                (decimal value, 1-1000)     [100       ]
  FallingTrigger               (decimal value, 0-1000)     [5         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

Finished configuring attributes.
This configuration must be saved (see config save command) and activated (see
config activate command) before it can take effect.
To discard this configuration use the config cancel command.
IBM8Gb (admin-config) #> config save
IBM8Gb (admin-config) #> config activate
```

Testing a port

You can perform an online or offline port test using the Test Port command. The following sections describe the test types, displaying test results, and canceling a test:

- Online tests for portsOnline tests for ports
- Offline tests for ports
- Display port test results
- Cancel a port test

Online tests for ports

An online test is a non-disruptive test that exercises the port, transceiver, and device connections. The port must be online and connected to a device. The following is an example of an online test:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> test port 1 online

A list of attributes with formatting and current values will follow. Enter a
new value or simply press the ENTER key to accept the default value. If you
wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

LoopCount     (decimal value, 1-4294967295)   [100      ]
FrameSize     (decimal value, 40-2148)        [256      ]
DataPattern   (32-bit hex value or 'Default') [Default  ]
StopOnError   (True / False)                  [True     ]
LoopForever   (True / False)                  [False    ]

Do you want to start the test? (y/n) [n] y

The test has been started.
A notification with the test result(s) will appear
on the screen when the test has completed.

IBM8Gb (admin) #>
  Test for port 1 Passed.
```

Offline tests for ports

An offline test is a disruptive test that exercises the port connections. You must place the port in the diagnostics state using the Set Port command before starting the test. There are two types of offline test: internal loopback and external loopback.

- An internal loopback test exercises the internal port connections.
- An external loopback test exercises the port and its transceiver. A transceiver with a loopback plug is required for the port.

The following example performs an offline test:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> set port 1 state diagnostics
IBM8Gb (admin) #> test port 1 offline internal

  A list of attributes with formatting and current values will follow. Enter
a new
  value or simply press the ENTER key to accept the default value. If you wish
to
  terminate this process before reaching the end of the list press 'q' or 'Q'
and
  the ENTER key to do so.

  LoopCount     (decimal value, 1-4294967295)   [100      ]
  FrameSize     (decimal value, 40-2148)        [256      ]
  DataPattern   (32-bit hex value or 'Default') [Default  ]
  StopOnError   (True / False)                  [True     ]
  LoopForever   (True / False)                  [False    ]

  Do you want to start the test? (y/n) [n] y

  The test has been started.
  A notification with the test result(s) will appear
  on the screen when the test has completed.

IBM8Gb (admin) #>
  Test for port 1 Passed.
When the test is complete, remember to place the port back online.
IBM8Gb (admin) #> set port 1 state online
```

When the test is complete, remember to place the port back online.

```
IBM8Gb (admin) #> set port 1 state online
```

Display port test results

You can display the test status while the test is in progress by entering the Test Status Port command as shown in the following example:

```
IBM8Gb (admin) #> test status port 1
Port               Test                Test               Loop      Test
Num      Port      Type                Status            Count  Failures
----     --------  ----                ------            -----  --------
1        1         Offline Internal    Passed               12         0
```

Cancel a port test

To cancel a port test that is in progress, enter the Test Cancel Port command.

Extending port transmission distance

You can extend the distance over which an external F_Port, G_Port, or E_Port can transmit by borrowing buffer credits from other ports. Each external and internal port is supported by a data buffer with a 16 credit capacity; that is, 16 maximum sized frames. For fibre optic cables, this capacity enables full bandwidth over the following approximate distances:

- 13 kilometers at 1-Gbps (0.6 credits/Km)
- 6 kilometers at 2-Gbps (1.2 credits/Km)
- 3 kilometers at 4-Gbps (2.4 credits/km)
- 1.5 kilometers at 8-Gbps (4.8 credits/km)

Beyond these distances, however, there is some loss of efficiency because the transmitting port must wait for an acknowledgement before sending the next frame.

Longer distances can be spanned at full bandwidth by extending credits to G_Ports, F_Ports, and E_Ports. Each external and internal port can donate 15 credits to a pool from which an external recipient port can borrow. Internal ports (1–14) cannot borrow credits. Donor ports are unable to carry traffic.

For example, you can configure an external recipient port to borrow 15 credits from one donor port. The external recipient port loses a credit in the process for a total of 30 credits (15+15=30). This will support communication over the following approximate distances:

- 50 Km at 1-Gbps (30÷0.6)
- 25 Km at 2-Gbps (30÷1.2)
- 12 Km at 4-Gbps (30÷2.4)
- 6 Km at 8-Gbps (30÷4.8)

Enter the Set Config Port command to borrow and allocate credits. The following example borrows credits from port 15 and allocates them to port 0:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config port
  A list of attributes with formatting and current values will follow. Enter
a new value or simply press the ENTER key to accept the current value. If you
wish to terminate this process before reaching the end of the attributes for
the port being processed, press 'q' or 'Q' and the ENTER key to do so. If you
wish to terminate the configuration process completely, press 'qq' or 'QQ' and
the ENTER key to so do.

  Configuring Port Number:  0
  ------------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online]
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto) [Auto  ]
  PortType         (GL / G / F / FL / Donor)                    [G     ]
  SymPortName      (string, max=32 chars)                       [Port1 ]
  ALFairness       (True / False)                               [False ]
  DeviceScanEnable (True / False)                               [True  ]
  ForceOfflineRSCN (True / False)                               [False ]
  ARB_FF           (True / False)                               [False ]
  InteropCredit    (decimal value, 0-255)                       [0     ]
  ExtCredit        (dec value, increments of 15, non-loop only) [0     ]  15
  FANEnable        (True / False)                               [True  ]  q

  Configuring Port Number:  15
  ------------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online]
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto) [Auto  ]
  PortType        (GL / G / F / FL / Donor)                   [GL    ]  donor
  SymPortName      (string, max=32 chars)                       [Port15]  qq

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
IBM8Gb (admin-config) #> config save
IBM8Gb (admin-config) #> config activate
```

Enter the Show Donor command to display the extended credit status for the switch as shown in the following example:

```
IBM8Gb #> show donor

          Config Ext Credit Max Credit Donated Donor Valid Groups to
  Port    Type   Requested  Available  to Port Group Extend Credit
  ----    ------ ---------- ---------- ------- ----- ---------------
  Ext1:0  G      15         30         None    0           0
  Ext2:15 Donor  0          0          None    0           0
  Ext3:16 GL     0          16         None    0           0
  Ext4:17 GL     0          16         None    0           0
  Ext5:18 GL     0          16         None    0           0
  Ext6:19 GL     0          16         None    0           0

  Bay1    F      0          16         None    0           0
  Bay2    F      0          16         None    0           0
  Bay3    F      0          16         None    0           0
  Bay4    F      0          16         None    0           0
  Bay5    F      0          16         None    0           0
  Bay6    F      0          16         None    0           0
  Bay7    F      0          16         None    0           0
  Bay8    F      0          16         None    0           0
  Bay9    F      0          16         None    0           0
  Bay10   F      0          16         None    0           0
  Bay11   F      0          16         None    0           0
  Bay12   F      0          16         None    0           0
  Bay13   F      0          16         None    0           0
  Bay14   F      0          16         None    0           0

  Donor Group  Credit Pool
  -----------  -----------
  0            0
```

Chapter 7. Zoning configuration

This chapter describes the following tasks:

- Displaying zoning database information
- Configuring the zoning database
- Modifying the zoning database
- Resetting the zoning database
- Removing inactive zone sets, zones, and aliases
- Managing zone sets
- Managing zones
- Managing aliases

Consider device access needs within the fabric. Access is controlled by the use of zoning. Some zoning strategies include the following:

- Separate devices by operating system.
- Separate devices that have no need to communicate with other devices in the fabric or have classified data.
- Separate devices into department, administrative, or other functional group.
- Reserve a path and its bandwidth from one port to another.

Zoning divides the fabric for purposes of controlling discovery and inbound traffic. A zone is a named group of ports or devices. Members of the same zone can communicate with each other and transmit outside the zone, but cannot receive inbound traffic from outside the zone. A port/device can be a member of up to eight zones whose combined membership does not exceed 64.

Zoning is hardware enforced on a switch port if the sum of the logged-in devices plus the devices zoned with devices on that port is 64 or less. If a port exceeds this sum, that port behaves as a soft zone member. The port continues to behave as a soft zone member until the sum of logged-in and zoned devices falls back to 64, and the port is reset.

A zone can be a component of more than one zone set. Several zone sets can be defined for a fabric, but only one zone set can be active at one time. The active zone set determines the current fabric zoning.

Displaying zoning database information

You can display the following information about the zoning database:

- Configured zone set information
- Active zone set information
- Zone set membership information
- Zone membership information
- Alias and alias membership information
- Zoning modification history
- Zoning database limits

Configured zone set information

The Zoneset List and the Zoning List commands display information about the all zone sets in the zoning database. Enter the Zoneset List command to display a list of the zone sets as shown in the following example:

```
IBM8Gb #> zoneset list

  Current List of ZoneSets
  ------------------------
  alpha
  beta
```

Enter the Zoning List command to display all zone sets, zones, and zone members in the zoning database as shown in the following example:

```
IBM8Gb #> zoning list

  Active (enforced) ZoneSet Information
  ZoneSet     Zone      ZoneMember
  -------------------------------
  wwn
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3

  Configured (saved in NVRAM) Zoning Information
  ZoneSet     Zone      ZoneMember
  -------------------------------
  wwn
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:16
```

Active zone set information

The Zoning Active and Zoneset Active commands display information about the active zone set. Enter the Zoning Active command to display component zones and zone members as shown in the following example:

```
IBM8Gb #> zoning active
Active (enforced) ZoneSet Information
  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3
```

Enter the Zoneset Active command to display the name of the active zone set and its activation history as shown in the following example:

```
IBM8Gb #> zoneset active

Active ZoneSet Information
--------------------------
  ActiveZoneSet    Beta
  LastActivatedBy  admin@OB-session6
  LastActivatedOn  day month date time year
```

Zone set membership information

The Zoneset Zones and Zone Zonesets commands display zone set membership information. Enter the Zoneset Zones command to display the member zones for a specified zone set as shown in the following example:

```
IBM8Gb #> zoneset zones ssss

  Current List of Zones for ZoneSet: ssss
  ---------------------------------
  zone1
  zone2
  zone3
```

Enter the Zone Zonesets command to display the zone sets for which a specified zone is a member as shown in the following example:

```
IBM8Gb #> zone zonesets zone1

  Current List of ZoneSets for Zone: zone1
  ---------------------------------
  zone_set_1
```

Zone membership information

Enter the Zone Members command to display the members for a specified zone as shown in the following example:

```
IBM8Gb #> zone members wwn_b0241f

  Current List of Members for Zone: wwn_b0241f
  ---------------------------------
  50:06:04:82:bf:d2:18:c2
  50:06:04:82:bf:d2:18:d2
  21:00:00:e0:8b:02:41:2f
```

Alias and alias membership information

The Alias List and Alias Members commands display information about aliases. Enter the Alias List command to display a list of all aliases as shown in the following example:

```
IBM8Gb #> alias list

  Current list of Zone Aliases
  ---------------------------
  alias1
  alias2
```

Enter the Alias Members command to display the membership for a specified alias as shown in the following example:

```
IBM8Gb #> alias members alias1

  Current list of members for Zone Alias: alias1
  ------------------------------------
  50:06:04:82:bf:d2:18:c4
  50:06:04:82:bf:d2:18:c5
  50:06:04:82:bf:d2:18:c6
```

Zoning modification history

Enter the Zoning History command to display a record of zoning modifications as shown in the following example:

```
IBM8Gb #> zoning history
  Active Database Information
  ---------------------------
  ZoneSetLastActivated/DeactivatedBy  Remote
  ZoneSetLastActivated/DeactivatedOn  day mon date hh:mm:ss yyyy
  Database Checksum                   00000000

  Inactive Database Information
  -----------------------------
  ConfigurationLastEditedBy           admin@OB-session17
  ConfigurationLastEditedOn           day mon date hh:mm:ss yyyy
  Database Checksum                   00000000
```

History information includes the following:

- Time of the most recent zone set activation or deactivation and the user account that performed it
- Time of the most recent modifications to the zoning database and the user account that made them.
- Checksum for the zoning database

Zoning database limits

Enter the Zoning Limits command to display a summary of the objects in the zoning database and their maximum limit as shown in the following example:

```
IBM8Gb #> zoning limits

  Zoning Attribute     Maximum   Current   [Zoning Name]
  ----------------     -------   -------   -------------
  MaxZoneSets          256       6
  MaxZones             2000      17
  MaxAliases           2500      1
  MaxTotalMembers      10000     166
  MaxZonesInZoneSets   2000      19
  MaxMembersPerZone    2000
                                 10        D_1_JBOD_1
                                 23        D_1_Photons
                                 9         D_2_JBOD1
                                 16        D_2_NewJBOD_2
                                 5         E1JBOD1
                                 5         E2JBOD2
                                 3         LinkResetZone
                                 3         LinkResetZone2
                                 8         NewJBOD1
                                 8         NewJBOD2
                                 24        Q_1Photon1
                                 8         Q_1_NewJBOD1
                                 13        Q_1_Photon_1
                                 21        Q_2_NewJBOD2
                                 3         ZoneAlias
                                 3         ZoneDomainPort
                                 4         ZoneFCAddr
  MaxMembersPerAlias   2000
                                 2         AliasInAZone
```

Configuring the zoning database

You can configure how the zoning database is applied to the switch and exchanged with the fabric through the zoning configuration parameters. The following zoning configuration parameters are available through the Set Config Zoning command. For more information about the zoning configuration parameters, see Table 36.

- InteropAutoSave–This parameter enables or disables the saving of changes to an active zone set in the switch's non-volatile memory.
- DefaultZone–This parameter enables or disables communication among ports/devices that are not defined in the active zone set.
- DiscardInactive–This parameter enables or disables the discarding of all zone sets except the active zone set.

If InteropAutoSave is False, you can revert zoning changes that have been received from another switch through the activation of a zone set, or merging of fabrics. Enter the Zoning Restore command to replace the volatile zoning database with the contents of the non-volatile zoning database.

To restore the zoning configuration to its factory values, enter the Reset Config or Reset Factory commands. Notice, however, that these commands also restore other aspects of the switch configuration.

To modify the zoning configuration, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time through SSH, Telnet, QuickTools, or another management application. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name, the active configuration is assumed.

The Config Edit session provides access to the Set Config Zoning command, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
   The config named default is being edited.
IBM8Gb (admin-config) #> set config zoning
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

  MergeAutoSave        (True / False)  [True ]
  DefaultZone          (Allow / Deny)  [Allow]
  DiscardInactive      (True / False)  [False]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.

IBM8Gb (admin-config)#> config save
IBM8Gb (admin)#> config activate
IBM8Gb (admin)#> admin end
```

Modifying the zoning database

To modify the zoning database, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time through SSH, Telnet, QuickTools, or another management application. You must also open a Zoning Edit session with the Zoning Edit command. The Zoning Edit session provides access to the Zoneset, Zone, Alias, and Zoning commands with which you make modifications to the zoning database.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning)#> zoneset . . .
IBM8Gb (admin-zoning)#> zone . . .
IBM8Gb (admin-zoning)#> alias . . .
IBM8Gb (admin-zoning)#> zoning . . .
```

When you are finished making changes, enter the Zoning Save command to save the changes and close the Zoning Edit session.

```
IBM8Gb (admin-zoning)#> zoning save
```

To close the Zoning Edit session without saving changes, enter the Zoning Cancel command.

```
IBM8Gb (admin-zoning)#> zoning cancel
```

Changes to the active zone set do not take effect until you activate it with the Zoneset Activate command. The active zone set is propagated throughout the fabric.

```
IBM8Gb (admin)#> zoneset activate zoneset_1
IBM8Gb (admin)#> admin end
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

To remove all zoning database objects (aliases, zones, and zone sets) and restore the zoning database to its factory state, enter the Reset Zoning command as shown in the following example:

```
IBM8Gb (admin) #> reset zoning
```

Resetting the zoning database

There are two ways to remove all aliases, zones, and zone sets from the zoning database:

- Enter the Zoning Clear command as shown in the following example:

  ```
  IBM8Gb #> admin start
  IBM8Gb (admin) #> zoning edit
  IBM8Gb (admin-zoning) #> zoning clear
  IBM8Gb (admin-zoning) #> zoning save
  ```

- Enter the Reset Zoning command as shown in the following example. The security configuration values (AutoSave, DefaultZone, and DiscardInactive) remain unchanged. This is the preferred method.

  ```
  IBM8Gb #> admin start
  IBM8Gb (admin) #> reset zoning
  ```

Removing inactive zone sets, zones, and aliases

Enter the Zoning Delete Orphans command to delete all objects from the zoning database except those in the active zone set.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning delete orphans
   This command will remove all zonesets, zones, and aliases
   that are not currently active.
Please confirm (y/n): [n] y
IBM8Gb (admin) #> zoning save
```

Managing zone sets

Managing zone sets consists of the following tasks:

- Create a zone set
- Delete a zone set
- Rename a zone set
- Copy a zone set
- Add zones to a zone set
- Remove zones from a zone set
- Activate a zone set
- Deactivate a zone set

All of these tasks except Activate a zone set and Deactivate a zone set require an Admin session and a Zoning Edit session.

Create a zone set

Enter the Zoneset Create command to create a new zone set, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zoneset create zoneset_1
IBM8Gb (admin-zoning) #>zoning save
```

Delete a zone set

Enter the Zoneset Delete command to delete a zone set, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zoneset delete zoneset_1
IBM8Gb (admin-zoning) #>zoning save
```

Rename a zone set

Enter the Zoneset Rename command to rename a zone set, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zoneset rename zoneset_old zoneset_new
IBM8Gb (admin-zoning) #>zoning save
```

Copy a zone set

Enter the Zoneset Copy command to copy a zone set and its contents to a new zone set, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zoneset copy zoneset_1 zoneset_2
IBM8Gb (admin-zoning) #>zoning save
```

Add zones to a zone set

Enter the Zoneset Add command to add a zone to a zone set, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zoneset add zoneset_1 zone_1 zone_2
```

Remove zones from a zone set

Enter the Zoneset Remove command to remove zones from a zone set, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zoneset remove zoneset_1 zone_1 zone_2
IBM8Gb (admin-zoning) #>zoning save
```

Activate a zone set

Enter the Zoneset Activate command to apply zoning to the fabric, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoneset activate zoneset_1
```

Deactivate a zone set

Enter the Zoneset Deactivate command to deactivate the active zone set and disable zoning in the fabric, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoneset deactivate
```

Managing zones

Managing zones consists of the following tasks:

- Create a zone
- Delete a zone
- Rename a zone
- Copy a zone
- Add members to a zone
- Remove members from a zone

All of these tasks require an Admin session and a Zoning Edit session.

Create a zone

Enter the Zone Create command to create a new zone, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zone create zone_1
IBM8Gb (admin-zoning) #> zoning save
```

Delete a zone

Enter the Zone Delete command to delete a zone (zone_1) from the zoning database, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zone delete zone_1
IBM8Gb (admin-zoning) #> zoning save
```

Rename a zone

Enter the Zone Rename command to rename zone_1 to zone_a, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zone rename zone_1 zone_a
IBM8Gb (admin-zoning) #> zoning save
```

Copy a zone

Enter the Zone Copy command to copy the contents of an existing zone (zone_1) to a new zone (zone_2), as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zone copy zone_1 zone_2
IBM8Gb (admin-zoning) #> zoning save
```

Add members to a zone

Enter the Zone Add command to add ports/devices to a zone (zone_1), as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zone add zone_1 alias_1 1,4 1,5
IBM8Gb (admin-zoning) #> zoning save
```

Remove members from a zone

Enter the Zone Remove command to remove ports/devices from a zone (zone_1), as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zone remove zone_1 alias_1 1,4 1,5
IBM8Gb (admin-zoning) #> zoning save
```

Managing aliases

Managing aliases consists of the following tasks:

- Create an alias
- Delete an alias
- Rename an alias
- Copy an alias
- Add members to an alias
- Remove members from an alias

All of these tasks require an Admin session and a Zoning Edit session.

Create an alias

Enter the Alias Create command to create a new alias as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> alias create alias_1
IBM8Gb (admin-zoning) #> zoning save
```

Delete an alias

Enter the Alias Delete command to delete alias_1 from the zoning database as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> alias delete alias_1
IBM8Gb (admin-zoning) #> zoning save
```

Rename an alias

Enter the Alias Rename command to rename alias_1 to alias_a as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> alias rename alias_1 alias_a
IBM8Gb (admin-zoning) #> zoning save
```

Copy an alias

Enter the Alias Copy command to copy alias_1 and its contents to alias_2 as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> alias copy alias_1 alias_2
IBM8Gb (admin-zoning) #> zoning save
```

Add members to an alias

Enter the Alias Add command to add ports/devices to alias_1 as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> alias add alias_1  1,4 1,5
IBM8Gb (admin-zoning) #> zoning save
```

Remove members from an alias

Enter the Alias Remove command to remove ports/devices from alias_1 as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> alias remove alias_1 1,4 1,5
IBM8Gb (admin-zoning) #> zoning save
```

Chapter 8. Connection security configuration

This chapter describes the following tasks:

- Managing SSL and SSH services
- Creating an SSL security certificate

The switch supports secure connections with SSH and switch management applications. The Secure SHell protocol (SSH) secures connections to the switch. The Secure Sockets Layer (SSL) protocol secures switch connections to the following management applications:

- QuickTools
- Application Programming Interface (API)
- Storage Management Initiative-Specification (SMI-S)

Managing SSL and SSH services

SSH/sFTP, SSL, and HTTPs services are enabled by default. All nonsecure service parameters, such as TelnetEnabled, FTPEnabled, GUIMgtEnabled, and EmbeddedGUIEnabled HTTP, are disabled by default.

The EncryptionMode service (Legacy or Strict) determines which encryption algorithms are applied to the secure protocols. Legacy mode uses encryption algorithms with a strength of 80 bits or greater. Strict mode uses encryption algorithms with a strength of 112 bits or greater. For more information about EncryptionMode, see Table 41.

Consider the following when using SSH/sFTP, SSL, and HTTPs services:

- To establish a secure connection, your workstation must use an SSH client.
- To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation (see “Setting the date and time” on page 57).
- The SSL service must be enabled to authenticate users through a RADIUS server (see “Configuring server authentication” on page 117).
- To disable SSL when using a user authentication RADIUS server, the RADIUS server authentication order must be local.
- Enabling SSL automatically creates a security certificate on the switch.

To display the SSL and SSH/sFTP service status, enter the Show Setup Services command:

```
IBM8Gb #> show setup services
  System Services Information
  -----------------------------------
  EncryptionMode                 Legacy
  TelnetEnabled                  False
  SSH/sFTPEnabled                True
  GUIMgmtEnabled                 False
  SSLEnabled                     True
  EmbeddedGUIEnabled (HTTP)      False
  EmbeddedGUIEnabled (HTTPs)     True
  NTPEnabled                     True
  CIMEnabled                     True
  FTPEnabled                     False
  MgmtServerEnabled              True
  CallHomeEnabled                True
  SLPEnabled                     True
```

To enable or disable the SSL and SSH/sFTP services, enter the Set Setup Services command. The following example disables the SSL service.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> set setup services

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PLEASE NOTE:
  -----------
  * Further configuration may be required after enabling a service.

  * If services are disabled, the connection to the switch may be lost.

  * When enabling SSL, please verify that the date/time settings
    on this switch and the workstation from where the SSL connection
    will be started match, and then a new certificate may need to be
    created to ensure a secure connection to this switch.

  EncryptionMode           (1=Legacy, 2=Strict) [Legacy]
  TelnetEnabled                 (True / False)  [False ]
  SSH/sFTPEnabled               (True / False)  [True  ]
  GUIMgmtEnabled                (True / False)  [False ]
  SSLEnabled                    (True / False)  [True  ] False
  EmbeddedGUIEnabled (HTTP)     (True / False)  [False ]
  EmbeddedGUIEnabled (HTTPs)    (True / False)  [True  ]
  NTPEnabled                    (True / False)  [True  ]
  CIMEnabled                    (True / False)  [True  ]
  FTPEnabled                    (True / False)  [False ]
  MgmtServerEnabled             (True / False)  [True  ]
  CallHomeEnabled               (True / False)  [True  ]
  SLPEnabled                    (True / False)  [True  ]

  Do you want to save and activate this services setup? (y/n): [y]
```

Creating an SSL security certificate

Enabling SSL automatically creates a security certificate on the switch. The security certificate is required to establish an SSL connection with a management application such as QuickTools. The certificate expires 1 January, 2038 00:00:00 UTC. Should the original certificate become invalid, enter the Create Certificate command to create a new one as shown in the following example:

```
IBM8Gb (admin) #> create certificate
  The current date and time is day mon date hh:mm:ss UTC yyyy.
  This is the time used to stamp onto the certificate.
  Is the date and time correct? (y/n): [n] y
  Certificate generation successful.
```

To ensure the creation of a valid certificate, be sure that the switch and the workstation time and date are the same (see “Setting the date and time” on page 57).

Chapter 9. Device security configuration

This chapter describes the following tasks:

- Displaying security database information
- Configuring the security database
- Modifying the security database
- Resetting the security database
- Managing security sets
- Managing groups

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or devices issuing management server commands.

Device security is defined through the use of security sets and groups. A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS). A security set is a set of up to three groups with no more than one of each group type. The security database is made up of all security sets on the switch.

In addition to authorization, the switch can be configured to require authentication to validate the identity of the connecting switch, device, or host. Authentication can be performed locally using the switch's security database, or remotely using an authentication server such as Microsoft® RADIUS.

Displaying security database information

You can display the following information about the security database:

- Configured security set information
- Active security set information
- Security set membership information
- Group membership information
- Security database modification history
- Security database limits

Configured security set information

The Securityset List and the Security List commands display information about the all security sets in the security database. Enter the Securityset List command to display a list of the security sets as shown in the following example:

```
IBM8Gb #> securityset list
Current list of SecuritySets
----------------------------
  alpha
  beta
```

Enter the Security List command to display all security sets, groups, and group members in the security database as shown in the following example:

```
IBM8Gb #> security list
  Active Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  No active securityset defined.

  Configured Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

Active security set information

The Security Active and Securityset Active commands display information about the active security set. Enter the Security Active command to display component groups and group members as shown in the following example:

```
IBM8Gb #> security active
  Active Security Information

  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

Enter the Securityset Active command to display the name of the active security set and its activation history as shown in the following example:

```
IBM8Gb #> securityset active
  Active SecuritySet Information
  ------------------------------
  ActiveSecuritySet alpha
  LastActivatedBy  Remote
  LastActivatedOn  day month date time year
```

Security set membership information

The Securityset Groups and Group Securitysets commands display security set membership information. Enter the Securityset Groups command to display the member groups for a specified security set as shown in the following example:

```
IBM8Gb #> securityset groups alpha
  Current list of Groups for SecuritySet: alpha
  -------------------------------------
  group1 (ISL)
  group2 (Port)
```

Enter the Group Securitysets command to display the security sets for which a specified group is a member as shown in the following example:

```
IBM8Gb #> group securitysets group_1

  Current list of SecuritySets for Group: group_1
  -------------------------------------
  SecuritySet_1
  SecuritySet_2
  SecuritySet_A
  SecuritySet_B
```

Group membership information

Enter the Group Members command to display the members for a specified group as shown in the following example:

```
IBM8Gb #> group members group_1
  Current list of members for Group: group_1
  --------------------------------
  10:00:00:c0:dd:00:71:ed
  10:00:00:c0:dd:00:72:45
  10:00:00:c0:dd:00:90:ef
  10:00:00:c0:dd:00:b8:b7
```

Security database modification history

Enter the Security History command to display a record of security database modifications as shown in the following example:

```
IBM8Gb #> security history
  Active Database Information
  ---------------------------
  SecuritySetLastActivated/DeactivatedBy  Remote
  SecuritySetLastActivated/DeactivatedOn  day month date time year
  Database Checksum                   00000000

  Inactive Database Information
  -----------------------------
  ConfigurationLastEditedBy           admin@IB-session11
  ConfigurationLastEditedOn           day month date time year
  Database Checksum                   00007558
```

History information includes the following:

- Time of the most recent security set activation or deactivation and the user account that performed it
- Time of the most recent modifications to the security database and the user account that made them
- Checksum for the security database

Security database limits

Enter the Security Limits command to display a summary of the objects in the security database and their maximum limit as shown in the following example:

```
IBM8Gb #> security limits
  Security Attribute   Maximum   Current   [Name]
  ------------------   -------   -------   ------
  MaxSecuritySets      4         1
  MaxGroups            16        2
  MaxTotalMembers      1000      19
  MaxMembersPerGroup   1000
                                 4         group1
                                 15        group2
```

Configuring the security database

You can configure how the security database is applied to the switch and exchanged with the fabric through the security configuration parameters. The following security configuration parameters are available through the Set Config Security command:

- AutoSave—This parameter enables or disables the saving of changes to an active security set in the switch's non-volatile security database.
- FabricBindingEnabled—This parameter enables or disables the configuration and enforcement of fabric binding on all switches in the fabric. Fabric binding associates switch worldwide names with a domain ID in the creation of ISL groups.

If AutoSave is False, you can revert device security changes that have been received from another switch through the activation of a security set, or merging of fabrics. Enter the Security Restore command to replace the volatile security database with the contents of the non-volatile security database.

To restore the security configuration to its factory values, you can enter the Reset Config or Reset Factory command. Notice, however, that these commands also restore other aspects of the switch configuration.

To modify the security configuration, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time either through SSH, Telnet, or QuickTools. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name, the active configuration is assumed. The Config Edit session provides access to the Set Config Security command as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config security
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  FabricBindingEnabled  (True / False)     [False]
  AutoSave              (True / False)     [True ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.

IBM8Gb (admin-config)#> config save
IBM8Gb (admin)#> config activate
IBM8Gb (admin)#> admin end
```

Modifying the security database

To modify the security database, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time either through SSH, Telnet, or QuickTools. You must also open a Security Edit session with the Security Edit command. The Security Edit session provides access to the Securityset, Group, and Security commands with which you make modifications to the security database.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> security edit
IBM8Gb (admin-security)#> securityset . . .
IBM8Gb (admin-security)#> group . . .
IBM8Gb (admin-security)#> security . . .
```

When you are finished making changes, enter the Security Save command to save the changes and close the Security Edit session.

```
IBM8Gb (admin-security)#> security save
```

To close the session without saving changes, enter the Security Cancel command.

```
IBM8Gb (admin-security)#> security cancel
```

Changes to the active security set do not take effect until you activate it with the Security Activate command. The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

```
IBM8Gb (admin)#> security activate
IBM8Gb (admin)#> admin end
```

Resetting the security database

There are two ways to remove all groups and security sets from the security database:

- Enter the Security Clear command as shown in the following example:

  ```
  IBM8Gb (admin-security) #> security clear
  All security information will be cleared.  Please confirm (y/n): [n] y
  IBM8Gb (admin-security) #> security save
  ```

- Enter the Reset Security command as shown in the following example. The security configuration values, autosave, and fabric binding remain unchanged.

  ```
  IBM8Gb (admin) #> reset security
  ```

Managing security sets

Managing security sets consists of the following tasks:

- Create a security set
- Delete a security set
- Rename a security set
- Copy a security set
- Add groups to a security set
- Remove groups from a security set
- Activate a security set
- Deactivate a security set

All of these tasks except Activate a security set and Deactivate a security set require a Security Edit session.

Create a security set

Enter the Securityset Create command to create a new security set, as shown in the following example:

```
IBM8Gb (admin-security) #> securityset create securityset_1
```

Delete a security set

Enter the Securityset Delete command to delete a security set, as shown in the following example:

```
IBM8Gb (admin-security) #> securityset delete securityset_1
```

Rename a security set

Enter the Securityset Rename command to rename a security set, as shown in the following example:

```
IBM8Gb (admin-security) #> securityset rename securityset_old securityset_new
```

Copy a security set

Enter the Securityset Copy command to copy a security set and its contents to a new security set, as shown in the following example:

```
IBM8Gb (admin-security) #> securityset copy securityset_1 securityset_2
```

Add groups to a security set

Enter the Securityset Add command to add a group to a security set, as shown in the following example:

```
IBM8Gb (admin-security) #> securityset add securityset_1 group_isl group_port
```

Remove groups from a security set

Enter the Securityset Remove command to remove groups from a security set, as shown in the following example:

```
IBM8Gb (admin-security) #> sescurityset remove securityset_1 group_isl
group_port
```

Activate a security set

Enter the Securityset Activate command to apply security to the fabric, as shown in the following example:

```
IBM8Gb (admin) #> securityset activate securityset_1
```

Deactivate a security set

Enter the Securityset Deactivate command to deactivate the active security set and disable security in the fabric, as shown in the following example:

```
IBM8Gb (admin) #> securityset deactivate
```

Managing groups

Managing groups consists of the following tasks:

- Create a group
- Delete a group
- Rename a group
- Copy a group
- Add members to a group
- Modify a group member
- Remove members from a group

All of these tasks require an Admin session and a Security Edit session.

Create a group

Creating a group involves specifying a group name and a group type. There are three types of groups:

- ISL group–secures connected switches
- Port group–secures connected devices
- MS group–secures management server commands

Enter the Group Create command to create a new port group, as shown in the following example:

```
IBM8Gb (admin-security) #> group create group_port port
```

Delete a group

Enter the Group Delete command to delete group_port from the security database, as shown in the following example:

```
IBM8Gb (admin-security) #> group delete group_port
```

Rename a group

Enter the Group Rename command to rename group_port to port_1, as shown in the following example:

```
IBM8Gb (admin-security) #> group rename group_port port_1
```

Copy a group

Enter the Group Copy command to copy the contents of an existing group (group_port) to a new group (port_1), as shown in the following example:

```
IBM8Gb (admin-security) #> group copy group_port port_1
```

Add members to a group

Adding a member to a group involves specifying a group, the member worldwide name, and the member attributes. The member attributes define the authentication method, encryption method, secrets, and fabric binding, depending on the group type.

- For ISL member attributes, see Table 7.
- For Port member attributes, see Table 8.
- For MS member attributes, see Table 9.

Enter the Group Add command to add a member to a group, as shown in the following example:

```
IBM8Gb (admin-security) #> group add group_1
  A list of attributes with formatting and default values will follow
  Enter a new value or simply press the ENTER key to accept the current value
  with exception of the Group Member WWN field which is mandatory.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Group Name       group_1
  Group Type       ISL
  Member          (WWN)                        [00:00:00:00:00:00:00:00] 10:00:00:c0:dd:00:90:a3
  Authentication  (None / Chap)                    [None                   ]chap
  PrimaryHash     (MD5 / SHA-1)                    [MD5                    ]
  PrimarySecret   (32 hex or 16 ASCII char value)  [                       ]0123456789abcdef
  SecondaryHash   (MD5 / SHA-1 / None)             [None                   ]
  SecondarySecret (40 hex or 20 ASCII char value)  [                       ]
  Binding         (domain ID 1-239, 0=None)        [0                      ]

  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

Modify a group member

Modifying a group member involves changing the member attributes. The member attributes define the authentication method, encryption methods, secrets, and fabric binding, depending on the group type.

- For ISL member attributes, see Table 7.
- For Port member attributes, see Table 8.
- For MS member attributes, see Table 9.

Enter the Group Edit command to change the attributes of a group member, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> security edit
IBM8Gb (admin-security) #> group edit G1 10:00:00:c0:dd:00:90:a3
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Group Name        g1
  Group Type        ISL
  Group Member      10:00:00:c0:dd:00:90:a3
  Authentication    (None / Chap)                   [None]  chap
  PrimaryHash       (MD5 / SHA-1)                   [MD5 ]  sha-1
  PrimarySecret     (40 hex or 20 ASCII char value) [    ]
12345678901234567890
  SecondaryHash     (MD5 / SHA-1 / None)            [None]  md5
  SecondarySecret   (32 hex or 16 ASCII char value) [    ]  1234567890123456
  Binding           (domain ID 1-239, 0=None)       [3   ]

  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

Remove members from a group

Enter the Group Remove command to remove a member from a group, as shown in the following example:

```
IBM8Gb (admin-security) #> group remove group_1 10:00:00:c0:dd:00:90:a3
```

Chapter 10. Server authentication configuration

Authentication can be performed locally using the switch's security database, or remotely using a Remote Dial-In User Service (RADIUS) server, such as Microsoft RADIUS, or a lightweight director access protocol (LDAP) server. With a RADIUS or LDAP server, the security database for the entire fabric resides on the server. In this way, you can manage the security database centrally, rather than on each switch. You can configure up to five RADIUS servers and up to four LDAP servers.

You can configure server authentication for just the switch or both the switch and the initiator device if the device supports authentication. When using a server authentication, every switch in the fabric must have a network connection. A RADIUS or LDAP server can also be configured to authenticate user accounts. For information about user accounts, see Chapter 3, "User account configuration" on page 13. A secure connection is required to authenticate user logins with a RADIUS or LDAP server. For information about secure connections, see Chapter 8, "Connection security configuration" on page 101.

Notes:

The Lenovo Flex System FC3171 8 Gb SAN Switch uses secure LDAP (LDAP over SSL–LDAPS) to connect to the configured LDAP servers, regardless of the LDAP server's port number. The LDAP servers must be properly configured to support LDAPS connections to perform LDAP authentication.

This chapter describes the following tasks:

- Displaying server authentication information
- Configuring server authentication

Displaying server authentication information

Enter the Show Setup Auth command to display RADIUS and LDAP server authentication information as shown in the following example. For a description of the RADIUS server authentication configuration parameters, see Table 38. For a description of the LDAP server authentication parameters, see Table 39.

```
IBM8Gb #> show setup auth
  Auth Information
  ----------------
  DeviceAuthOrder             Local
  UserAuthOrder               Local
  TotalRadiusServers          1
  TotalLdapServers            0

  Radius Information
  ------------------
  Radius Server: 1
  ServerIPAddress             10.1.1.1
  ServerUDPPort               1812
  DeviceAuthServer            False
  UserAuthServer              False
  AccountingServer            True
  Timeout                     2
  Retries                     0
  SignPackets                 False
  Secret                      12345
```

Configuring server authentication

Enter the Set Setup Auth command to configure RADIUS and LDAP server authentication on the switch. For a description of the RADIUS server authentication configuration parameters, see Table 38. For a description of the LDAP server authentication parameters, see Table 39.

```
IBM8Gb (admin) #> set setup auth

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the
attributes
  for the category being processed, press 'q' or 'Q' and the ENTER key to do
so.
  If you wish to terminate the configuration process completely, press 'qq' or
  'QQ' and the ENTER key to do so.

  PLEASE NOTE:
  -----------
  * SSL must be enabled in order to configure RADIUS and/or LDAP
  * user authentication.  SSL can be enabled in this mode or
  * via the 'set setup services' command.

  Current Values:
    DeviceAuthOrder     Local
    UserAuthOrder       Local
    TotalRadiusServers  1
    TotalLdapServers    0

  New Value (press ENTER to not specify value, 'q' to quit):

  * Specify authentication ordering using the strings 'Local', 'Radius' and/or
  * 'Ldap'.  For example, for Radius authentication first followed by Local
  * authentication, specify 'RadiusLocal'

    DeviceAuthOrder     ('Radius' 'Local')        :
    UserAuthOrder       ('Radius' 'Ldap' 'Local') :  ldap
    TotalRadiusServers  decimal value, 0-5        :  1
    TotalLdapServers    decimal value, 0-4        :  1

  Current Values:

  Radius Server 1
    ServerIPAddress   10.1.1.1
    ServerUDPPort     1812
    DeviceAuthServer  False
    UserAuthServer    False
    AccountingServer  True
    Timeout           2
    Retries           0
    SignPackets       False
    Secret            ********

  New Value (press ENTER to not specify value, 'q' to quit):

  Radius Server 1
    ServerIPAddress   (hostname, IPv4, or IPv6 Address) :
    ServerUDPPort     (decimal value)                   :
    DeviceAuthServer  (True / False)                    :
```

```
  UserAuthServer    (True / False)                    :
  AccountingServer  (True / False)                    :
  Timeout           (decimal value, 1-30 secs)        :
  Retries           (decimal value, 1-3, 0=None)      :
  SignPackets       (True / False)                    :
  Secret            (1-63 characters, recommend 22+)  :

Current Values:

Ldap Configuration
  RootDN         root DN ;""
  UIDSearchAttr  jlkj
  BindingMethod  Anonymous
  ClientDN       client ,."";,"
  Password       ********
  AdminAttr      sdasd
  AdminValue     sdsds

New Value (press ENTER to not specify value, 'q' to quit):

Ldap Configuration
  RootDN         (1-64)                       :
  UIDSearchAttr  (1-24)                       :
  BindingMethod  (1=Anonymous, 2=ClientAuth) :
  ClientDN       (1-64)                       :
  Password       (1-16)                       :
  AdminAttr      (1-24)                       :
  AdminValue     (1-24)                       :

Current Values:

Ldap Server 1
  ServerIPAddress  10.0.0.1
  Port             389

New Value (press ENTER to not specify value, 'q' to quit):

Ldap Server 1
  ServerIPAddress  (hostname, IPv4, or IPv6 Address) :
  Port             (decimal value)                   :

Do you want to save and activate this auth setup? (y/n): [n]
```

Chapter 11. Message logging

The switch maintains two message logs: the event log and the audit log. The event log is a record of all activity on the fabric. The audit log is a separate log containing messages associated with security-sensitive events on the switch.

- Managing the event log
- Managing the audit log

Managing the event log

This section describes the following tasks:

- Displaying the event log
- Configuring event logging
- Clearing the event log
- Logging to a remote host
- Creating and downloading an event log file

Event messages originate from the switch or from the management application in response to events that occur in the fabric. For a complete listing of event messages, see the *IBM Flex System FC3171 8 Gb SAN Switch and Pass-thru Event Message Guide*.

Events are classified by the following severity levels:

- Alarm. The alarm level describes events that are disruptive to the administration or operation of a fabric and require administrator intervention. Alarms are always logged and always displayed on the screen. Alarm thresholds can be defined for certain port errors to customize when to generate an alarm.
- Critical. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.
- Warning. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.
- Informative. The informative level describes routine events associated with a normal fabric.

Displaying the event log

Enter the Show Log command to display the event log. Each message has the following format:

```
[ordinal][time_stamp][severity][message_ID][source][message_text]
```

`[ordinal]`–A number assigned to each message in sequence since the last time the alarm history was cleared.

`[time_stamp]`–The time the alarm was issued in the format day month hh:mm:ss.ms UTC yyyy. This time stamp comes from the switch for events that originate with the switch, and from the workstation for events that originate with QuickTools.

`[severity]`–The event severity: A–Alarm, C–Critical, W–Warning, I–Informative.

`[message_ID]`–A number that identifies the message using the following format: category.message_number

`[source]`–The program module or application that generated the event. Sources include Zoning, Switch, PortApp, EPort, Management Server. Alarms do not include the source.

The following is an example of the Show Log command:

```
IBM8Gb #> show log
[1][Fri Jan 07 02:07:56.068 UTC 2000][I][8400.0023][Switch][Successful login
user (admin@OB-session8) with admin privilege from address 10.20.32.223-3852]
[2][Fri Jan 07 02:07:56.069 UTC 2000][W][8400.0058][Switch][User (USERID) is
using their initial/default password]
[3][Fri Jan 07 02:08:38.179 UTC 2000][I][8400.0023][Switch][Successful login
user (admin@OB-session9) with admin privilege from address 10.20.32.146]
[4][Fri Jan 07 02:08:38.180 UTC 2000][W][8400.0058][Switch][User (USERID) is
using their initial/default password]
[5][Fri Jan 07 02:09:39.793 UTC 2000][I][8400.0023][Switch][Successful login
user (admin@OB-session10) with admin privilege from address
10.20.32.223-3862]
[6][Fri Jan 07 02:09:39.795 UTC 2000][W][8400.0058][Switch][User (USERID) is
using their initial/default password]
[7][Fri Jan 07 02:17:10.205 UTC 2000][C][8400.002A][Switch][User (USERID)
attempted to log into switch with an incorrect password from 10.20.32.223]
```

You can also filter the event log display with the Show Log Display command and customize the messages that display automatically in the output stream. This section describes the following tasks:

- Filtering the event log display
- Controlling messages in the output stream

Filtering the event log display

You can customize what events are displayed according to the component or severity level. Enter the Show Log Display command to filter the events in the display. You can choose from the following severity levels and component events:

- Informative events
- Warning events
- Critical events
- E_Port events
- Management server events
- Name server events
- Port events
- Switch management events
- Simple Network Management Protocol (SNMP) events
- Zoning events
- Successful and unsuccessful user logins
- Changes to user access rights
- Password resets
- Changes to IP security configuration
- Changes to device security configuration
- Resets and restarts
- Firmware upgrades
- Changes to configuration attributes
- Changes to the switch, such as port state changes and port resets
- Audit log archiving

The following example filters the event log display for critical events.

```
IBM8Gb #> show log display critical
```

Controlling messages in the output stream

Enter the Set Log Display command to specify the severity level filter to use to determine what messages are automatically displayed on the screen when they occur. Alarms are always included in the output stream. The following example includes warning and critical level messages in the output stream:

```
IBM8Gb (admin) #> set log display warn
```

Configuring event logging

Configuring event logging consists of the following tasks:

- Configure the event log
- Display the event log configuration
- Restore the event log configuration

Configure the event log

You can customize what events are recorded in the switch event log according to component, severity level, and port. Enter the Set Log Component, Set Log Level, and Set Log Port commands to filter the events to be recorded. You can choose from the following component events:

- E_Port events
- Management server events
- Name server events
- Port events
- Switch management events
- Simple Network Management Protocol (SNMP) events
- Command Line Interface events
- Zoning events

The following example configures the event log to record switch management events with warning and critical severity levels associated with ports 0, 15, 16, and 17. Entering the Set Log Save command ensures that this configuration is preserved across switch resets.

```
IBM8Gb (admin) #> set log component switch
IBM8Gb (admin) #> set log level warn
IBM8Gb (admin) #> set log port 0 15-17
IBM8Gb (admin) #> set log save
```

Display the event log configuration

Enter the Show Log Settings command to display all event log configuration settings, as shown in the following example:

```
IBM8Gb #> show log settings
Current settings for log
------------------------
Started            True
FilterComponent    NameServer MgmtServer Zoning Switch Blade Port Eport Snmp
CLI
FilterLevel        Info
DisplayLevel       Critical
FilterPort         0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
```

Restore the event log configuration

Enter the Set Log Restore command to return the event log configuration to the factory default as shown in the following example:

```
IBM8Gb (admin) #> set log restore
```

Clearing the event log

Enter the Set Log Clear command to delete all entries in the event log, as shown in the following example:

```
IBM8Gb (admin) #> set log clear
```

Logging to a remote host

The switch comes from the factory with local logging enabled, which instructs the switch firmware to maintain an event log in switch memory. The switch can also be configured to log events to a remote host that supports the syslog protocol. This requires that you enable remote logging on the switch and specify an IP address for the remote host.

Notes:

To log event messages on a remote host, you must edit the syslog.conf file on the remote host and then restart the syslog daemon. The syslog.conf file must contain an entry that specifies the name of the log file. Add the following line to the syslog.conf file. A <tab> separates the selector field (local0.info) and action field which contains the log file path name (/var/adm/messages/messages.name).

```
local0.info <tab> /var/adm/messages/messages.name
```

Consult your host operating system documentation for information on how to configure remote logging.

The Set Setup System Logging command controls remote logging through the RemoteLogEnabled and RemoteLogHostAddress parameters, as shown in the following example:

```
IBM8Gb (admin) #> set setup system logging

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    RemoteLogEnabled        False
    RemoteLogHostAddress    10.0.0.254

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    RemoteLogEnabled        (True / False)                    :
    RemoteLogHostAddress    (hostname, IPv4, or IPv6 Address) :

  Do you want to save and activate this system setup? (y/n): [n]
```

Creating and downloading an event log file

Enter the Set Log Archive command to collect the event log messages in a file on the switch named *logfile*. This file can have a maximum of 1200 event messages.

Use sFTP to download the file from the switch to your workstation as follows:

1. Log into the switch through SSH and create an archive of the event log. The Set Log Archive command creates an event log file on the switch named *logfile*.

```
IBM8Gb  #> admin start
IBM8Gb (admin) #> set log archive
```

2. Open an sFTP session on the switch and log in with the account name *images* and password *images*. Transfer the event log file (*logfile*) in binary mode with the Get command.

```
sftp images@10.20.108.65
Connecting to 10.20.108.65...
Password:
sftp> get logfile
Fetching /logfile to logfile
/logfile                                    100%   38KB  38.2KB/s   00:00
sftp> quit
```

Managing the audit log

The audit log contains messages associated with security-sensitive events on the switch, such as the following:

- Successful and unsuccessful user logins
- Changes to user access rights
- Password resets
- Changes to IP security configuration
- Changes to device security configuration
- Resets and restarts
- Firmware upgrades
- Changes to configuration attributes
- Changes to the switch, such as port state changes and port resets
- Audit log archiving

When the switch initializes, it begins storing audit messages in the audit log, which resides in permanent memory. The audit log is divided into ten files (*audit.log*, *audit.log1*, . . . *audit.log9*) and can contain 2,000 messages or more. Audit messages fill *audit.log* first, then *audit.log1*, and so on to *audit.log9*.

You can perform the following audit log tasks:

- Displaying the audit log
- Creating and downloading an audit log file

Displaying the audit log

Enter the Show Audit command to display the contents of the audit log. You can display the entire audit log (Show Audit_Archive) or a specified number of the most recent messages (Show Audit *[number]*). If you enter Show Audit with no keywords, the system displays the most recent 250 messages. The following is an example of the Show Audit command:

```
IBM8Gb> show audit
[Fri Jan 30 16:03:23.824 UTC 2015][AU][0000.0000][sshd][[QL-00001]pam_unix(sshd:session):
session opened for user admin by (uid=0)]
[Fri Jan 30 16:03:23.957 UTC 2015][AU][0000.02E6][None][IP 10.20.200.230 User
admin@OB-session7 user session established.]
[Fri Jan 30 16:03:24.169 UTC 2015][AU][0000.0033][None][IP 10.20.200.230 User
admin@OB-session7 Admin Start]
[Fri Jan 30 16:03:25.164 UTC 2015][AU][0000.0043][None][IP 10.20.200.230 User
admin@OB-session7 Reset switch post]
[Fri Jan 30 16:03:25.165 UTC 2015][AU][0000.0042][None][IP 10.20.200.230 User
admin@OB-session7 Reset switch]
[Fri Jan 30 16:03:28.184 UTC 2015][AU][0000.02E7][None][IP 127.0.0.1-36119 user
cim@OB-session1 user session has been closed]
[Mon Feb 02 11:41:49.939 UTC 2015][AU][0000.0000][sshd][[QL-00001]pam_unix(sshd:session):
session opened for user admin by (uid=0)]
[Mon Feb 02 11:41:50.108 UTC 2015][AU][0000.02E6][None][IP 10.20.200.230 User
admin@OB-session10 user session established.]
[Mon Feb 02 11:41:50.293 UTC 2015][AU][0000.0033][None][IP 10.20.200.230 User
admin@OB-session10 Admin Start]
[Mon Feb 02 11:41:50.319 UTC 2015][AU][0000.02A1][None][IP 10.20.200.230 User
admin@OB-session10 Port 12 temporary admin state set to Online]
[Mon Feb 02 11:41:50.335 UTC 2015][AU][0000.0034][None][IP 10.20.200.230 User
admin@OB-session10 Admin End]
[Mon Feb 02 11:41:50.380 UTC 2015][AU][0000.0033][None][IP 10.20.200.230 User
admin@OB-session10 Admin Start]
[Mon Feb 02 11:41:50.406 UTC 2015][AU][0000.02A1][None][IP 10.20.200.230 User
admin@OB-session10 Port 13 temporary admin state set to Online]
[Mon Feb 02 11:41:50.423 UTC 2015][AU][0000.0034][None][IP 10.20.200.230 User
admin@OB-session10 Admin End]
[Mon Feb 02 11:41:50.475 UTC 2015][AU][0000.0033][None][IP 10.20.200.230 User
admin@OB-session10 Admin Start]
[Mon Feb 02 11:41:50.510 UTC 2015][AU][0000.02A1][None][IP 10.20.200.230 User
admin@OB-session10 Port 14 temporary admin state set to Online]
[Mon Feb 02 11:41:50.538 UTC 2015][AU][0000.0034][None][IP 10.20.200.230 User
admin@OB-session10 Admin End]
[Mon Feb 02 11:41:50.584 UTC 2015][AU][0000.0033][None][IP 10.20.200.230 User
admin@OB-session10 Admin Start]
```

Creating and downloading an audit log file

Enter the Set Audit Archive command to collect the individual audit log files in permanent memory (*audit.log*, *audit.log1*, . . . *audit.log9*) into one file named *audit.log*. Use sFTP to download the merged *audit.log* file from the switch to your workstation as follows:

1. Log into the switch through SSH and create an archive of the event log. The Set Audit Archive command creates an audit log file on the switch named *audit.log*.

```
IBM8Gb  #> admin start
IBM8Gb (admin) #> set audit archive
```

2. Open an sFTP session on the switch and log in with the account name *images* and password *images*. Transfer the event log file (*audit.log*) in binary mode with the Get command.

```
sftp images@10.20.108.65
Connecting to 10.20.108.65...
Password:
sftp> get audit.log
Fetching /audit.log to audit.log
/audit.log                                    100%   38KB  38.2KB/s   00:00
sftp> quit
```

Chapter 12. Call Home configuration

This chapter describes the following topics:

- Call Home concepts
- Configuring the Call Home service
- Managing the Call Home database
- Testing a Call Home profile
- Changing SMTP servers
- Clearing the Call Home message queue
- Resetting the Call Home database

Call Home concepts

The Call Home service improves fabric availability by notifying administrators by email of events that affect switch operation. The Call Home service is active by default and is controlled by the Set Setup Callhome command. To display the Call Home service status, enter the Show Setup Services command. To better understand the Call Home service, consider the following:

- Call Home requirements
- Call Home messages
- Technical support interface

Call Home requirements

In addition to enabling the Call Home service, you must also do the following to ensure that email messages can be sent:

- Configure the Call Home service. The Call Home service configuration consists of primary and secondary SMTP server specifications and contact information. You must enable and specify an address and service port for at least one SMTP server. See “Configuring the Call Home service” on page 130.
- Configure the Call Home database The Call Home database consists of up to 25 Call Home profiles. Each profile defines the following:
  - Event severity levels (Alarm, Critical, Warn) that will initiate an email message
  - Email message format and subject
  - Email recipients

  Multiple profiles make it possible to notify different audiences based on any combination of event severity, message format (short or full), or message length. You can configure profiles using the Profile command within a Callhome Edit session. See “Managing the Call Home database” on page 131.
- Ensure that each switch that is to support Call Home email notification has its own Ethernet connection.

Enter the Callhome Test command to test your Call Home service and database configurations. See “Testing a Call Home profile” on page 138.

Call Home messages

The Call Home service generates email messages for the specified event severity level and the following switch actions:

- Switch comes online
- Switch goes offline
- Reboot
- Power up
- Power down[1]
- SFP failure

When a qualifying switch action or event occurs, an email message is created and placed in the Call Home queue to be sent to the active SMTP server. You can monitor activity in the queue using the Callhome Queue Stats command. You can also clear the queue of email messages using the Callhome Queue Clear command.

There are three email message formats: full text, short text, and Tsc1. The full-text format contains the switch and event information, plus the contact information from the Call Home profile and SNMP configurations. The short-text and Tsc1 formats contains basic switch and event information; Tsc1 is formatted for automated parsing. The following is an example of a short-text email:

```
From: john.doe@lenovo.com [mailto:john.doe@lenovo.com]
Sent: Wednesday, July 25, 2007 5:03 PM
Subject: [CallHome: Test] Alarm generated on Switch_8


SwitchName:  Switch_8_83.215
SwitchIP:    10.20.30.40
SwitchWWN:   10:00:00:c0:dd:0c:66:f2
Level:       Alarm
Text:        CALLHOME TEST PROFILE MESSAGE
ID:          8B00.0002
Time:        Wed Jul 25 17:02:40.343 CDT 2007
```

[1] If the switch is forced to power-down before the message is sent to the SMTP server, no message will be transmitted.

The following is an example of a full-text email including profile and SNMP contact information:

```
From: john.doe@work.com [mailto:john.doe@work.com]
Sent: Wednesday, July 25, 2007 5:03 PM
Subject: [CallHome: Test] Alarm generated on Switch_8

------------ Event Details
SwitchName:  Switch_8_83.215
SwitchIP:    10.20.30.40
SwitchWWN:   10:00:00:c0:dd:0c:66:f2
Level:       Alarm
Text:        CALLHOME TEST PROFILE MESSAGE
ID:          8B00.0002
Time:        day mon date hh:mm:ss.xxx XXT yyy


------------ Switch Location
Room 123; Rack 9; Bay 3


------------ Contact Information
George Smith
12345 4th Street, City, State
952-999-9999
george.smith@work.com
```

Technical support interface

The Tech_Support_Center profile provides a way to collect and send switch status and trend data periodically by e-mail to specified technical support resources. To use this feature, you must create a profile named Tech_Support_Center. The Capture command enables you to add instructions to the Tech_Support_Center profile to specify the frequency with which to e-mail this data. For more information, see “Adding a data capture configuration” on page 136.

Configuring the Call Home service

Enter the Set Setup Callhome command in an Admin session to configure the Call Home service as shown in the following example. For a description of the Call Home service configuration settings, see Table 40.

```
IBM8Gb (admin) #> set setup callhome

A list of attributes with formatting and current values will follow. Enter a
new value or simply press the ENTER key to accept the current value. If you
wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.
If either the Primary or Secondary SMTP Servers are enabled, the
FromEmailAddress attribute must be configured or the switch will not attempt
to deliver messages.
Current Values:

  PrimarySMTPServerAddr      0.0.0.0
  PrimarySMTPServerPort      25
  PrimarySMTPServerEnable    False
  SecondarySMTPServerAddr    0.0.0.0
  SecondarySMTPServerPort    25
  SecondarySMTPServerEnable  False
  ContactEmailAddress        nobody@localhost.localdomain
  PhoneNumber                <undefined>
  StreetAddress              <undefined>
  FromEmailAddress           nobody@localhost.localdomain
  ReplyToEmailAddress        nobody@localhost.localdomain
  ThrottleDupsEnabled        True

New Value (press ENTER to accept current value, 'q' to quit):
  PrimarySMTPServerAddr      (IPv4, IPv6, or hostname)  :
  PrimarySMTPServerPort      (decimal value)            :
  PrimarySMTPServerEnable    (True / False)             :
  SecondarySMTPServerAddr    (IPv4, IPv6, or hostname)  :
  SecondarySMTPServerPort    (decimal value)            :
  SecondarySMTPServerEanble  (True / False)             :
  ContactEmailAddress        (ex: admin@company.com)    :
  PhoneNumber                (ex: +1-800-123-4567)      :
  StreetAddress              (include all address info) :
  FromEmailAddress           (ex: bldg3@company.com)    :
  ReplyToEmailAddress        (ex: admin3@company.com)   :
  ThrottleDupsEnabled        (True / False)             :

  Do you want to save and activate this Callhome setup? (y/n):
```

Enter the Show Setup Callhome command to display the Call Home service configuration, as shown in the following example.

```
IBM8Gb #> show setup callhome
  Callhome Information
  --------------------
  PrimarySMTPServerAddr       0.0.0.0
  PrimarySMTPServerPort       25
  PrimarySMTPServerEnabled    False
  SecondarySMTPServerAddr     0.0.0.0
  SecondarySMTPServerPort     25
  SecondarySMTPServerEnabled  False
  ContactEmailAddress         nobody@localhost.localdomain
  PhoneNumber                 <undefined>
  StreetAddress               <undefined>
  FromEmailAddress            nobody@localhost.localdomain
  ReplyToEmailAddress         nobody@localhost.localdomain
  ThrottleDupsEnabled         True

  + indicates active SMTP server
```

Managing the Call Home database

To modify the Call Home database, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time through SSH, Telnet, QuickTools, or another management application. You must also open a Callhome Edit session with the Callhome Edit command. The Callhome Edit session provides access to the Callhome, Capture, and Profile commands with which you make modifications to the Call Home database.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome)#> callhome . . .
IBM8Gb (admin-callhome)#> profile . . .
IBM8Gb (admin-callhome)#> capture . . .
```

When you are finished making changes, enter the Callhome Save command to save the changes and close the Callhome Edit session. Changes take effect immediately.

```
IBM8Gb (admin-callhome)#> callhome save
```

To close the Callhome Edit session without saving changes, enter the Callhome Cancel command.

```
IBM8Gb (admin-callhome)#> callhome cancel
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

To remove all Call Home profiles and restore the Call Home service configuration to its factory state, enter the Reset Callhome command.

```
IBM8Gb (admin) #> reset callhome
```

Managing the Call Home database consists of the following tasks:

- Displaying Call Home database information
- Creating a profile
- Deleting a profile
- Modifying a profile
- Renaming a profile
- Copying a profile
- Adding a data capture configuration
- Modifying a data capture configuration
- Deleting a data capture configuration

Displaying Call Home database information

Enter the Callhome History command to display the Call Home data base change history information, as shown in the following example:

```
IBM8Gb #> callhome history
   CallHome Database History
   -------------------------
   ConfigurationLastEditedBy        admin@OB-session2
   ConfigurationLastEditedOn        day mmm dd hh:mm:ss yyyy
   DatabaseChecksum                 000014a3
   ProfileName                      group4
   ProfileLevel                     Warn
   ProcessedCount                   286
   ProcessedLast                    day mmm dd hh:mm:ss yyyy
   ProfileName                      group5
   ProfileLevel                     Alarm
   ProcessedCount                   25
   ProcessedLast                    day mmm dd hh:mm:ss yyyy
```

Enter the Callhome List command to display a list of Call Home profiles, as shown in the following example:

```
IBM8Gb #> callhome list

 Configured Profiles:
 --------------------
 group4
 group5
```

Enter the Callhome List Profile command to display a list of Call Home profiles and their details, as shown in the following example:

```
IBM8Gb #> callhome list profile

ProfileName: group4
------------
Level             Warn
Format            FullText
MaxSize           any size up to max of 100000
EmailSubject      CallHome Warn
RecipientEmail    admin1@company.com
RecipientEmail    admin2@company.com
RecipientEmail    admin3@company.com
RecipientEmail    admin7@company.com
RecipientEmail    admin8@company.com
RecipientEmail    admin9@company.com
RecipientEmail    admin10@company.com

ProfileName:      group5
------------
Level             Alarm
Format            ShortText
MaxSize           any size up to max of 40000
EmailSubject      CallHome Alarm
RecipientEmail    me1@company.com
RecipientEmail    me10@company.com
```

Enter the Callhome Queue Stats command to display information about email messages in the Call Home queue, as shown in the following example:

```
IBM8Gb #> callhome queue stats
  Callhome Queue Information
  --------------------------
  FileSystemSpaceInUse        534 (bytes)
  EntriesInQueue                3
```

Creating a profile

Enter the Profile Create command to create a Call Home profile, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> profile create profile_1
A list of attributes with formatting and default values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

Default Values:
  Level           Alarm
  Format          FullText
  MaxSize         100000
  EmailSubject    <undefined>
  RecipientEmail  (up to 10 entries allowed)

New Value (press ENTER to accept default value, 'q' to quit):
  Level           (Alarm,Critical,Warn,None)        :
  Format          (1=FullText, 2=ShortText, 3=Tsc1) :
  MaxSize         (decimal value, 650-100000)       :
  EmailSubject    (string, max=64 chars, N=None)    : Technical problem
  RecipientEmail  (ex: admin@company.com, N=None)
  1. <undefined>                                    : admin0@company.com

The profile has been created.
This configuration must be saved with the callhome save command
before it can take effect, or to discard this configuration
use the callhome cancel command.

IBM8Gb (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Deleting a profile

Enter the Profile Delete command to delete a Call Home profile, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> profile delete profile_1

  The profile will be deleted. Please confirm (y/n): [n] y

IBM8Gb (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Modifying a profile

Enter the Profile Edit command to modify an existing Call Home profile, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> profile edit profile_1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    Level           Alarm
    Format          ShortText
    MaxSize         1000
    EmailSubject    Switch Problem
    RecipientEmail  (up to 10 entries allowed)
    1. john.smith@domain.com

  New Value (press ENTER to accept current value, 'q' to quit):
    Level           (Alarm,Critical,Warn,None)        :
    Format          (1=FullText, 2=ShortText, 3=Tsc1) : 1
    MaxSize         (decimal value, 650-100000)       :
    EmailSubject    (string, max=64 chars, N=None)    :
    RecipientEmail  (ex: admin@company.com, N=None)
    1. john.smith@domain.com                          :
    2. <undefined>                                    :

  The profile has been edited.
  This configuration must be saved with the 'callhome save' command
  before it can take effect, or to discard this configuration
  use the 'callhome cancel' command.

IBM8Gb (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Renaming a profile

Enter the Profile Rename command to rename profile_1, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> profile rename profile_1 profile_4

  The profile will be renamed. Please confirm (y/n): [n] y

IBM8Gb (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Copying a profile

Enter the Profile Copy command to copy profile_1, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> profile copy profile_1 profile_a
IBM8Gb (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Adding a data capture configuration

Enter the Capture Add command to add a data capture configuration to the Tech_Support_Center profile as shown in the following example. If the Tech_Support_Center profile does not exist, you must create it using the Profile Create command.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> capture add
  A list of attributes with formatting and default values will follow.
  Enter a value or simply press the ENTER key to accept the default value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Value (press ENTER to accept the default, 'q' to quit):
    TimeOfDay  (HH:MM)                       [02:00]
    DayOfWeek  (Sun,Mon,Tue,Wed,Thu,Fri,Sat)  [Sat  ]
    Interval   (decimal value, 1-26 weeks)    [1    ]

  A capture entry has been added to profile Tech_Support_Center.
  This configuration must be saved with the 'callhome save' command
  before it can take effect, or to discard this configuration
  use the 'callhome cancel' command.
```

Modifying a data capture configuration

Enter the Capture Edit command to modify a data capture configuration in the Tech_Support_Center profile, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> capture edit
Capture Entries for Profile:  Tech_Support_Center

  Index  TimeOfDay  DayOfWeek  Interval
  -----  ---------  ---------  --------
  1      02:00      Sat        1 (weeks)

Please select a capture entry from the list above ('q' to quit): 1

  A list of attributes with formatting and current values will follow.
  Enter a value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Value (press ENTER to accept the default, 'q' to quit):
    TimeOfDay  (HH:MM)                       [02:00]
    DayOfWeek  (Sun,Mon,Tue,Wed,Thu,Fri,Sat)  [Sat  ]
    Interval   (decimal value, 1-26 weeks)    [1    ]

  The selected capture entry has been edited for profile Tech_Support_Center.
  This configuration must be saved with the 'callhome save' command
  before it can take effect, or to discard this configuration
  use the 'callhome cancel' command.
```

Deleting a data capture configuration

Enter the Capture Remove command to delete a data capture configuration from the Tech_Support_Center profile, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> capture remove
Capture Entries for Profile:  Tech_Support_Center

  Index  TimeOfDay  DayOfWeek  Interval
  -----  ---------  ---------  --------
  1      02:00      Sat        1 (weeks)

  Please select a capture entry from the list above ('q' to quit): 1

  The selected capture entry has been removed from profile
Tech_Support_Center.
  This configuration must be saved with the 'callhome save' command
  before it can take effect, or to discard this configuration
  use the 'callhome cancel' command.
```

Testing a Call Home profile

Enter the Callhome Test Profile command to test a Call Home profile as shown in the following example. This command generates a test message and routes it to the email recipients specified in the profile.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome test profile group4
  A callhome profile test has been started.
  A notification with the test result will appear
  on the screen when the test has completed.
IBM8Gb (admin) #>
  Test for Callhome Profile group4 Passed.
```

Changing SMTP servers

The Call Home service configuration enables you to specify a primary and a secondary SMTP server to which the switch connects. The active server is the server that receives messages from the switch. By default, the primary SMTP server is the active server. Should the active server lose connection, control passes automatically to the other server. You can explicitly change the active server by entering the Callhome Changeover command, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb #> callhome edit
IBM8Gb #> (admin-callhome) #> callhome changeover

The currently active CallHome SMTP server will change.  Please confirm (y/n):
[n] y
```

Though the active server status changes, the primary SMTP server remains the primary, and the secondary SMTP server remains the secondary.

Clearing the Call Home message queue

Enter the Callhome Queue Clear command to clear email messages from the Call Home message queue, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome queue clear
  The callhome queue will be cleared. Please confirm (y/n): [n] y
```

For information about displaying the contents of the Call Home message queue, see the Callhome Queue Stats command.

Resetting the Call Home database

There are two ways to reset the Call Home database. Enter the Callhome Clear command to clear all Callhome profiles as shown in the following example. This command resets the Tech_Support_Center profile to the factory default, but does not affect the Call Home service configuration.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> callhome clear
IBM8Gb (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Enter the Reset Callhome command to clear all Call Home profiles and reset the Tech_Support_Center profile and Call Home service configuration to the factory defaults, as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> reset callhome
The callhome configuration will be reset and the default values activated.
Please confirm (y/n): [n] y

Reset and activation in progress ....
```

Chapter 13. Simple Network Management Protocol configuration

This chapter describes the following tasks:

- Displaying SNMP information
- Modifying the SNMP configuration
- Resetting the SNMP configuration
- Managing the SNMPv3 configuration

The Simple Network Management Protocol (SNMP) provides for the management of the switch through third-party applications that use SNMP. Security consists of a read community string and a write community string that serve as passwords that control read and write access to the switch. These strings are set at the factory to well-known defaults and should be changed if SNMP is to be enabled.

The switch CLI supports SNMPv3, which is enabled by default.

Displaying SNMP information

Enter the Show Setup SNMP command to display SNMP configuration information as shown in the following example. For a description of the SNMP parameters, see Table 42.

```
IBM8Gb #> show setup snmp
  SNMP Information
  ----------------
  Contact               <sysContact undefined>
  Location              N_107 System Test Lab
  Description           IBM Flex System FC3171 8Gb SAN Switch
  ObjectID              1.3.6.1.4.1.3873.1.33
  AuthFailureTrap       True
  ProxyEnabled          True
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Version          2
  Trap1Enabled          False
  Trap2Address          0.0.0.0
  Trap2Port             162
  Trap2Severity         warning
  Trap2Version          2
  Trap2Enabled          False
  Trap3Address          0.0.0.0
  Trap3Port             162
  Trap3Severity         warning
  Trap3Version          2
  Trap3Enabled          False
  Trap4Address          0.0.0.0
  Trap4Port             162
  Trap4Severity         warning
  Trap4Version          2
  Trap4Enabled          False
  Trap5Address          0.0.0.0
  Trap5Port             162
  Trap5Severity         warning
  Trap5Version          2
  Trap5Enabled          False
```

Modifying the SNMP configuration

Enter the Set Setup SNMP command in an Admin session to configure SNMP on the switch. There are two groups of configuration parameters. One group is common to all traps. The second group is trap specific. You can configure both groups of parameters for all SNMP traps, or you can configure the common and trap-specific parameters separately. For information about the SNMP parameters, see Table 42.

The following example configures the common SNMP trap configuration parameters:

```
IBM8Gb (admin) #> set setup snmp common

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    Contact          True
    Location         <sysContact undefined>
    ReadCommunity    <sysContact undefined>
    WriteCommunity   public
    AuthFailureTrap  private
    ProxyEnabled     True

  New Value (press ENTER to not specify value, 'q' to quit):
    Contact          (True / False)         :
    Location         (string, max=64 chars) :
    ReadCommunity    (string, max=64 chars) :
    WriteCommunity   (string, max=32 chars) :
    AuthFailureTrap  (string, max=32 chars) :
    ProxyEnabled     (True / False)         :

  Do you want to save and activate this snmp setup? (y/n): [n]
```

The following example configures SNMP trap 1:

```
IBM8Gb (admin) #> set setup snmp trap 1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    Trap1Enabled    True
    Trap1Address    10.20.33.181
    Trap1Port       5001
    Trap1Severity   info
    Trap1Version    2
    Trap1User       user1
    Trap1Community  northdakota

  New Value (press ENTER to not specify value, 'q' to quit):
    Trap1Enabled    (True / False)                    :
    Trap1Address    (hostname, IPv4, or IPv6 Address) :
    Trap1Port       (decimal value, 1-65535)          :
    Trap1Severity   (select a severity level)
                    1=unknown     6=warning
                    2=emergency   7=notify
                    3=alert       8=info
                    4=critical    9=debug
                    5=error       10=mark             :
    Trap1Version    (1 / 2 / 3)                       :
    Trap1User       (For V3 traps, max-32 chars)      :
    Trap1Community  (string, max=32 chars)            :

  Do you want to save and activate this snmp setup? (y/n): [n]
```

Resetting the SNMP configuration

Enter the Reset SNMP command to reset the SNMP configuration back to the factory defaults as shown in the following example. For a listing of the SNMP configuration factory defaults, see Table 22.

```
IBM8Gb (admin) #> reset snmp
```

Managing the SNMPv3 configuration

SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of packet authentication and encryption over the network. SNMPv3 provides the following security features:

- Message integrity. This feature ensures that packets have not been altered.
- Authentication. This feature ensures that the packet is coming from a valid source.
- Encryption. This feature ensures that packet contents cannot be read by an unauthorized source.

To configure SNMP version 3, you must create one or more SNMP version 3 user accounts. SNMPv3 is enabled by default. The default SNMPv3 user name is *snmpadmin1* and has the following attributes:

- Group type—ReadWrite
- Authentication type—SHA
- Authentication phrase—admin1pass
- Privacy type—DES
- Privacy phrase—PASSW0RD (the sixth character is the numeral zero [0])

Notes:

SNMPv3 users for which AuthType=MD5 or PrivType=DES are invalid when EncryptionMode=Strict. Before setting EncryptionMode=Strict, delete the noncompliant user accounts (Snmpv3user Delete command) and create new user accounts (Snmpv3user Add command) as needed. For more information about EncryptionMode, see Table 41.

Create an SNMPv3 user account

To create an SNMP version 3 user account, enter the Snmpv3user Add command, as shown in the following example. Shaded entries indicate options that are available only when EncryptionMode=Legacy. For more information about EncryptionMode, see Table 41.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> snmpv3user add

   A list of SNMPV3 user attributes with formatting and default values as
   applicable will follow.

   Enter a new value OR simply press the ENTER key where-ever allowed to
   accept the default value.

   If you wish to terminate this process before reaching the end of the
   list, press "q" or "Q" and the ENTER OR "Ctrl-C" key to do so.

  Username        (8-32 chars)                          : snmpuser1
  Group           (0=ReadOnly, 1=ReadWrite) [ReadOnly  ] : 1
  Authentication  (True/False)              [False     ] : t
  AuthType        (1=MD5, 2=SHA)            [SHA       ] : 1
  AuthPhrase      (8-32 chars)                          : ***********
  Confirm AuthPhrase                                    : ***********
  Privacy         (True/False)              [False     ] : t
  PrivType        (1=DES, 2-AES)            [AES       ] : 1
  PrivPhrase      (8-32 chars)                          : ********
  Confirm PrivPhrase                                    : ********

  Do you want to save and activate this snmpv3user setup ?   (y/n): [n] y

  SNMPV3 user added and activated.
```

Display SNMPv3 user accounts

To display SNMP version 3 user accounts, enter the Snmpv3user List command as shown in the following example:

```
IBM8Gb #> snmpv3user list

  Username                        Group           AuthType   PrivType
  --------                        -----           --------   --------
  snmpadmin1                      ReadWrite       SHA        AES
  snmpuser1                       ReadWrite       MD5        DES
```

Modify an SNMPv3 user account

To modify an SNMP version 3 user account, enter the Snmpv3user Edit command as shown in the following example:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> snmpv3user edit

  A list of SNMPV3 user attributes with formatting and current attribute
  values for the specified SNMPV3 user will follow.

  Enter a new value OR simply press the ENTER key where-ever allowed to
  accept the current value.

  If you wish to terminate this process before reaching the end of the
  list, press "q" or "Q" and the ENTER OR "Ctrl-C" key to do so.

  Username        (8-32 chars)                          : snmpuser1
  Group           (0=ReadOnly, 1=ReadWrite) [ReadWrite ] : 1
  Authentication  (True/False)              [True      ] : f

  Do you want to save and activate this setup ?   (y/n): [n] n

  SNMPV3 user account edited and activated.
```

Chapter 14. Command reference

This chapter describes the commands of the CLI and the format in which they are presented. The command format presents the following:

- Access authority
- Syntax and keywords
- Notes and examples

The commands are listed in "Command listing" on page 150.

Access authority

The Authority paragraph in each command description indicates what types of sessions are required to enter that command. Commands associated with monitoring tasks are available to all account names with no special session requirement. Commands associated with configuration tasks are available only within an Admin session. An account must have Admin authority to enter the Admin Start command, which opens an Admin session.

Some commands require that you open additional editing sessions within an Admin session such as the following:

- Commands that modify zoning require a Zoning Edit session, which is opened by the Zoning Edit command. These commands include the Alias, Zone, Zoneset, and Zoning commands.
- Commands that modify device security require a Security Edit session, which is opened by the Security Edit command. These command include the Group, Security, and Securityset commands.
- Commands that modify the switch configuration require a Config Edit session, which is opened by the Config Edit command. These command include all of the Set Config commands.
- Commands that modify the Call Home e-mail notification configuration require a Callhome Edit session, which is opened by the Callhome Edit command. These commands include the Callhome, Capture, and Profile commands.
- Commands that modify the Internet Protocol Security configuration require an Ipsec Edit session, which is opened by the Ipsec Edit command. These commands include the Ipsec, Ipsec Association, Ipsec Policy, Ike Peer, and Ike Policy commands.

Syntax and keywords

The **Syntax** paragraph defines the command syntax using the following convention:

command
key**word**
keyword *[value]*
keyword [value1] [value2]

The **Command** is followed by one or more keywords. Consider the following rules and conventions:

- Commands and keywords are case insensitive.
- Required keyword values appear in standard font: [value]. Optional values are shown in italics: *[value].*
- Underlined portions of the keyword in the command format indicate the abbreviated form that can be used. For example, the **delete** keyword can be abbreviated **del**.

The **Keywords** paragraph lists and describes each keyword and any applicable values.

Notes and examples

The **Notes** paragraph presents useful information about the command and its use, including special applications or effects on other commands. The **Examples** paragraph presents sample screen captures of the command and its output.

Command listing

The commands are listed in alphabetical order.

Admin

Opens and closes an Admin session. The Admin session provides access to commands that change the fabric and switch configurations. Only one Admin session can be open on the switch at any time. An inactive Admin session will time out after a period of time, which can be changed using the Set Setup System command.

Authority

User account with Admin authority

Syntax

admin
start (or begin)
end (or stop)
cancel

Keywords

start (or begin)
Opens the Admin session

end (or stop)
Closes the Admin session. The Hardreset, Hotreset, Quit, Show Voltage, and Reset Switch commands will also end an Admin session.

cancel
Terminates an Admin session opened by another user. Use this keyword with care because it terminates the Admin session without warning the other user and without saving pending changes.

Notes

Closing an SSH/Telnet window during an Admin session does not release the session. In this case, you must either wait for the Admin session to time out, or use the Admin Cancel command.

Examples

The following example shows how to open and close an Admin session:

```
IBM8Gb #> admin start
IBM8Gb (admin) #>
.
.
.
IBM8Gb (admin) #> admin end
```

Alias

Creates a named set of ports/devices. Aliases make it easier to assign a set of ports/devices to many zones. An alias cannot have a zone or another alias as a member.

Authority

Admin session and Zoning Edit session for all keywords except List and Members

Syntax

alias

add [alias] [member_list]
copy [alias_source] [alias_destination]
create [alias]
delete [alias]
list
members [alias]
remove [alias] [member_list]
rename [alias_old] [alias_new]

Keywords

add [alias] [member_list]

Specifies one or more ports/devices given by [member_list] to add to the alias named [alias]. Use a <space> to delimit ports/devices in [member_list]. An alias can have a maximum of 2000 members. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.

The application verifies that the [alias] format is correct, but does not validate that such a port/device exists.

copy [alias_source] [alias_destination]

Creates a new alias named [alias_destination] and copies the membership into it from the alias given by [alias_source].

create [alias]

Creates an alias with the name given by [alias]. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0–9, A–Z, a–z, _, $, ^, and -. The zoning database supports a maximum of 256 aliases.

delete [alias]

Deletes the specified alias given by [alias] from the zoning database. If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated.

list

Displays a list of all aliases. This keyword does not require an Admin session.

members [alias]

Displays all members of the alias given by [alias]. This keyword does not require an Admin session.

remove [alias] [member_list]

Removes the ports/devices given by [member_list] from the alias given by [alias]. Use a <space> to delimit ports/devices in [member_list]. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) for the device with the format xx:xx:xx:xx:xx:xx:xx:xx.

rename [alias_old] [alias_new]

Renames the alias given by [alias_old] to the alias given by [alias_new].

Examples

The following is an example of the Alias List command:

```
IBM8Gb #> alias list

  Current list of Zone Aliases
  ----------------------------
  alias1
  alias2
```

The following is an example of the Alias Members command:

```
IBM8Gb #> alias members alias1

  Current list of members for Zone Alias: alias1
  --------------------------------------
  50:06:04:82:bf:d2:18:c4
  50:06:04:82:bf:d2:18:c5
  50:06:04:82:bf:d2:18:c6
```

Callhome

Manages the Call Home database. The Callhome Edit command opens a session in which to create and manage Call Home profiles. For more information about Call Home profiles, see the "Profile" command on page 220.

Authority

Admin session except for the History and List keywords. The Clear keyword also requires a Callhome Edit session.

Syntax

callhome
cancel
changeover
clear
edit
history
list *profile [profile]*
queue [option]
save
test profile [profile]

Keywords

cancel

Closes the current Callhome Edit session. Any unsaved changes are lost.

changeover

Toggles activation between the primary SMTP server and the secondary SMTP server. Though the active server status changes, the primary SMTP server remains the primary, and the secondary SMTP server remains the secondary.

clear

Clears all Call Home profile information from the volatile edit copy of the Call Home database. This keyword requires a Callhome Edit session. This keyword does not affect the non-volatile Call Home database. However, if you enter the Callhome Clear command followed by the Callhome Save command, the non-volatile Call Home database will be cleared from the switch.

Notes:

The preferred method for clearing the Call Home database from the switch is the Reset Callhome command.

edit

Open a Callhome Edit session. Callhome Edit session commands include Callhome Clear and all Profile commands.

history

Displays a history of Call Home modifications. This keyword does not require an Admin session. History information includes the following:

- Time of the most recent Call Home database modification and the user who performed it.
- Checksum for the Call Home database
- Profile processing information

list *profile [profile]*

Lists the configuration for the profile given by [profile]. If you omit [profile], the command lists all profiles and their configurations. If you omit the profile keyword, the command lists the profile names.

queue [*option*]

Clears the Call Home e-mail queue or displays Call Home e-mail queue statistics depending on the value of [*option*]. [*option*] can be one of the following:

clear

Clears the Call Home e-mail queue.

stats

Displays Call Home e-mail queue statistics. Statistics include the number of e-mail messages in the queue and the amount of file system space in use.

save

Saves changes made during the current Callhome Edit session.

test profile [profile]

Tests the Call Home profile given by [profile].

Examples

The following is an example of the Callhome History command:

```
IBM8Gb #> callhome history
   CallHome Database History
   -------------------------
   ConfigurationLastEditedBy        admin@OB-session2
   ConfigurationLastEditedOn        day mmm dd hh:mm:ss yyyy
   DatabaseChecksum                 000014a3
   ProfileName                      group4
   ProfileLevel                     Warn
   ProcessedCount                   286
   ProcessedLast                    day mmm dd hh:mm:ss yyyy
   ProfileName                      group5
   ProfileLevel                     Alarm
   ProcessedCount                   25
   ProcessedLast                    day mmm dd hh:mm:ss yyyy
```

The following is an example of the Callhome List command:

```
IBM8Gb #> callhome list

 Configured Profiles:
 --------------------
 group4
 group5
```

The following is an example of the Callhome List Profile command:

```
IBM8Gb #> callhome list profile

ProfileName: group4
------------
Level             Warn
Format            FullText
MaxSize           any size up to max of 100000
EmailSubject      CallHome Warn
RecipientEmail    admin1@company.com
RecipientEmail    admin2@company.com
RecipientEmail    admin3@company.com
RecipientEmail    admin7@company.com
RecipientEmail    admin8@company.com
RecipientEmail    admin9@company.com
RecipientEmail    admin10@company.com

ProfileName:      group5
------------
Level             Alarm
Format            ShortText
MaxSize           any size up to max of 40000
EmailSubject      CallHome Alarm
RecipientEmail    me1@company.com
RecipientEmail    me10@company.com
```

The following is an example of the Callhome Test Profile command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome test profile group4
  A callhome profile test has been started.
  A notification with the test result will appear
  on the screen when the test has completed.
IBM8Gb (admin) #>
  Test for Callhome Profile group4 Passed.
```

The following is an example of the Callhome Queue Clear command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome queue clear
  The callhome queue will be cleared. Please confirm (y/n): [n] y
```

The following is an example of the Callhome Queue Stats command:

```
IBM8Gb #> callhome queue stats
  Callhome Queue Information
  --------------------------
  FileSystemSpaceInUse        534 (bytes)
  EntriesInQueue                3
```

Capture

Manages the data capture configuration for the Tech_Support_Center Call Home profile. The data capture configuration determines the time and frequency by which status and trend data is collected from the switch and sent to recipients specified in the Tech_Support_Center profile.

Authority

Admin session and a Callhome Edit session. For information about starting a Callhome Edit session, see the "Callhome" command on page 154.

Syntax

capture
add
edit
remove

Keywords

add

Adds data capture instructions to the Tech_Support_Center profile. Table 6 describes the data capture parameters.

Table 6. Data Capture configuration parameters

Parameters	Description
TimeOfDay	Time of day to send status and trend data to the Tech_Support_Center profile e-mail recipients. The format is hh:mm on a 24-hour clock. The default 02:00.
DayOfWeek	Day-of-the-week to send status and trend data to the Tech_Support_Center profile e-mail recipients. Values can be Sun, Mon, Tue, Wed, Thur, Fri, Sat. The default is Sat.
Interval	Number of weeks between capture data e-mails to the Tech_Support_Center profile e-mail recipients. Values can be 1–26. The default is 1.

edit

Opens an edit session in which to modify the data capture configuration of the Tech_Support_Center profile. For information about the data capture configuration parameters, see Table 6.

remove

Removes the data capture configuration from the Test_Support_Center profile.

Examples

The following is an example of the Capture Add command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> capture add
  A list of attributes with formatting and default values will follow.
  Enter a value or simply press the ENTER key to accept the default value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Value (press ENTER to accept the default, 'q' to quit):
    TimeOfDay  (HH:MM)                       [02:00]
    DayOfWeek  (Sun,Mon,Tue,Wed,Thu,Fri,Sat)  [Sat  ]
    Interval   (decimal value, 1-26 weeks)    [1    ]

  A capture entry has been added to profile Tech_Support_Center.
  This configuration must be saved with the 'callhome save' command
  before it can take effect, or to discard this configuration
  use the 'callhome cancel' command.
```

The following is an example of the Capture Edit command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> capture edit
Capture Entries for Profile:  Tech_Support_Center

  Index  TimeOfDay  DayOfWeek  Interval
  -----  ---------  ---------  --------
  1      02:00      Sat        1 (weeks)

Please select a capture entry from the list above ('q' to quit): 1

  A list of attributes with formatting and current values will follow.
  Enter a value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Value (press ENTER to accept the default, 'q' to quit):
    TimeOfDay  (HH:MM)                       [02:00]
    DayOfWeek  (Sun,Mon,Tue,Wed,Thu,Fri,Sat)  [Sat  ]
    Interval   (decimal value, 1-26 weeks)    [1    ]

  The selected capture entry has been edited for profile Tech_Support_Center.
  This configuration must be saved with the 'callhome save' command
  before it can take effect, or to discard this configuration
  use the 'callhome cancel' command.
```

The following is an example of the Capture Remove command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> capture remove
Capture Entries for Profile:  Tech_Support_Center

  Index  TimeOfDay  DayOfWeek  Interval
  -----  ---------  ---------  --------
  1      02:00      Sat        1 (weeks)

  Please select a capture entry from the list above ('q' to quit): 1

  The selected capture entry has been removed from profile
Tech_Support_Center.
  This configuration must be saved with the 'callhome save' command
  before it can take effect, or to discard this configuration
  use the 'callhome cancel' command.
```

Cert_Authority

Manages certificate authority certificates in the PKI database.

Authority

Admin. The List keyword does not require an Admin session.

Syntax

cert_authority
delete certificate [authority_name]
import certificate [authority_name] [file_name] *force*
list [authority_name]

Keywords

delete certificate [authority_name]

Deletes a certificate authority certificate associated with the certificate authority given by [authority_name].

import certificate [authority_name] [file_name] ***force***

Imports a certificate authority certificate file given by [file_name] and associates it with the certificate authority given by [authority_name]. The optional keyword Force overwrites an existing authority with the same name. For EncryptionMode=Legacy, certificate files must be built from keys of length 1,024 or greater. For EncryptionMode=Strict, certificate files must be built from keys of length 2,048 or greater. For more information about the Encryption Mode service, see Table 41.

list [authority_name]

Displays certificate authorities on the switch and associated certificate authority certificates.

Certificate

Creates certificate requests and manages signed certificates in the PKI database.

Authority

Admin

Syntax

certificate
delete local [certificate_name]
generate request
import local [certificate_name] [file_name] *force*
list l*ocal [certificate_name]*

Keywords

delete local [certificate_name]
Deletes a signed certificate from the PKI database.

generate request
Creates a certificate request and stores it as a file on the switch. This keyword prompts you for the following information:

KeyName

The name of a public/private key pair in the PKI database. For EncryptionMode=Legacy, keys must have a length of 1,024 or greater. For EncryptionMode=Strict, keys must have a length of 2,048 or greater. For more information about the Encryption Mode service, see Table 41.

SubjectDistinguishedName

The distinguished name for the switch.

SubjectAlternateName

One or more alternate distinguished names for the switch. These alternate names can be host names, IPv4 or IPv6 addresses, or e-mail addresses.

OutputFileName

The name of the certificate request file.

import local [certificate_name] [file_name] ***force***
Imports a signed certificate file given by [file_name] and places it in the PKI database with certificate name [certificate_name]. The optional keyword Force overwrites an existing certificate with the same name if one exists. For EncryptionMode=Legacy, certificate files must be built from keys of length 1,024 or greater. For EncryptionMode=Strict, certificate files must be built from keys of length 2,048 or greater. For more information about the Encryption Mode service, see Table 41.

list ***local [certificate_name]***
Displays information about the signed certificate given by [certificate_name]. If you omit Local [certificate_name], the List keyword lists all signed certificates in the PKI database.

Notes

Upload the certificate request file to your workstation and submit it to a certificate authority to obtain a signed certificate file.

For information about creating a public/private key pair, see the Key command.

Examples

The following is an example of a Certificate Generate Request command:

```
IBM8Gb (admin) #> admin start
IBM8Gb (admin) #> certificate generate request
  A list of attributes with formatting will follow.
  Enter a value or simply press the ENTER key to skip specifying a value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

   *KeyName                  (string, max=32 chars)           : key1024
   *SubjectDistinguishedName (string, max=128 chars)          : O=lenovo
    SubjectAlternateName     (may enter up to 16, 1 per line)
            1) enter a hostname, IPv4, IPv6 or Email Address : johndoe@xxx.com
             2) enter a hostname, IPv4, IPv6 or Email Address : 10.0.0.1
             3) enter a hostname, IPv4, IPv6 or Email Address :
    OutputFileName           (string, max=64 chars)           : dm5800

  Certificate Request has been created and placed in file:  dm5800
```

Clone Config Port

Duplicates a source port configuration on specified target ports.

Authority

Admin session and a Config Edit session

Syntax

clone config port
[source_port_number] [port_list]

Keywords

[source_port_number] [port_list]

Duplicates the configuration of a port given by [source_port_number] on a set of target ports given by [port_list]. [port_list] can be a list of port numbers or ranges delimited by spaces. You can clone only internal ports to internal ports or external ports to external ports.

Notes

For a description of the port configuration parameters, see Table 31.

Examples

The following example configures ports 15–19 based on port 0:

```
IBM8Gb #> admin start
IBM8Gb (admin) config edit
IBM8Gb (admin) #> clone config port 0 15-19
Port 0 configuration will be cloned to ports 15 16 17 18 19
  Please confirm (y/n): [n] y
IBM8Gb (admin-config)#> config save
IBM8Gb (admin)#> config activate
IBM8Gb (admin)#> admin end
```

Config

Manages the Fibre Channel configurations on a switch. For information about setting the port and switch configurations, see the "Set Config Switch" command on page 253.

Authority

Admin session for all keywords except Backup and List

Syntax

config
activate *[config_name]*
backup *[export]*
cancel
copy [config_source] [config_destination]
delete [config_name]
edit *[config_name]*
export [account_name] [ip_address] [file_name]
import [account_name] [ip_address] [file_name]
list
restore
save *[config_name]*

Keywords

activate ***[config_name]***

Activates the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used. Only one configuration can be active at a time.

backup ***[export]***

Creates a file named *configdata*, which contains the system configuration information. This keyword does not require an Admin session. Configuration backup files are deleted from the switch during a power cycle or switch reset.

The optional Export keyword creates the configuration backup file and exports it to a remote server prompting you for the server, an account name, the server IP address or DNS host name, destination file name, and a password if the server requires one.

cancel

Terminates the current configuration edit session without saving changes that were made.

copy [config_source] [config_destination]

Copies the configuration given by [config_source] to the configuration given by [config_destination]. The switch supports up to 10 configurations including the default configuration.

delete [config_name]

Deletes the configuration given by [config_name]. You cannot delete the default configuration (Default Config) nor the active configuration.

edit ***[config_name]***

Opens an edit session for the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used.

export [account_name] [ip_address] [file_name]

Exports an existing backup configuration file (*configdata*) from the switch to a remote server. The server IP address and corresponding user account are given by [ip_address] and [account_name] respectively. [ip_address] can be an IP address or a DNS host name. The file name on the remote server is given by [file_name]. The system will prompt for a password if the server requires one.

import [account_name] [ip_address] [file_name]

Imports a backup configuration file given by [file_name] from a remote server to the switch. The server IP address and corresponding user account are given by [ip_address] and [account_name] respectively. [ip_address] can be an IP address or a DNS host name. The file name on the remote server is given by [file_name]. The system will prompt for a password if the server requires one. You must enter the Config Restore command to apply the configuration to the switch.

list

Displays a list of all available configurations. This keyword does not require an Admin session.

restore *import*

Restores configuration settings to an out-of-band switch from a backup file named configdata, which must be first uploaded on the switch using sFTP. You create the backup file using the Config Backup command. Use sFTP to load the backup file on a switch, and then enter the Config Restore command. After the restore is complete, the switch automatically resets. See "Back up and restore a switch configuration" on page 53.

Notes:

- Configuration archive files created with the QuickTools Archive function are not compatible with the Config Restore command.
- The `configdata` backup file does not include the security group primary or secondary secrets, and therefore is not restored. You must edit the security database and reconfigure the secrets; otherwise, the switch will isolate from the fabric.

The optional Import keyword imports the backup file from a remote server prompting you for an account name, server IP address or DNS host name, configuration file name on the server, and a password if the server requires one. When the upload is complete, the switch restores the configuration.

save *[config_name]*

Saves changes made during a configuration edit session in the configuration given by [config_name]. If you omit [config_name], the value for [config_name] you chose for the most recent Config Edit command is used. [config_name] can be up to 31 characters excluding the number sign (#), semicolon (;), and comma (,). The switch supports up to 10 configurations including the default configuration.

Notes

Changes you make to an active or inactive configuration can be saved, but will not take effect until you activate that configuration.

Examples

The following is an example of how to open and close a Config Edit session:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
   The config named default is being edited.
.
.
IBM8Gb (admin-config) #> config cancel
  Configuration mode will be canceled. Please confirm (y/n): [n] y
IBM8Gb (admin) #> admin end
```

The following is an example of how to create a backup file (configdata) and download the file to the workstation.

```
IBM8Gb #> config backup
IBM8Gb #> exit

#>sftp images@symbolic_name or ip_address
Password: images
sftp>get configdata
    Fetching /configdata to configdata
    /configdata                100%  137KB 136.8KB/s   00:00
sftp> quit
```

The following is an example of how to upload a configuration backup file (configdata) from the workstation to the switch, and then restore the configuration.

```
#> sftp images@symbolic_name or ip_address
Password: images
sftp>put config_switch_169 configdata
    Uploading configdata-slot3 to /configdata
    configdata-slot3             100%  137KB 136.8KB/s   00:00
sftp>quit

IBM8Gb #> admin start
IBM8Gb (admin) #> config restore
The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
  Alarm Msg: [day month date time year][A1005.0021][SM][Configuration is
being      restored -  this could take several minutes]
  Alarm Msg: [day month date time year][A1000.000A][SM][The switch will be
reset in 3 seconds due to a config restore]
IBM8Gb (admin) #>
  Alarm Msg: [day month date time year][A1000.0005][SM][The switch is being
reset]
```

Create

Creates support files for troubleshooting switch problems, and certificates for secure communications for QuickTools and SMI-S.

Authority

Admin session for the Certificate keyword

Syntax

create
certificate
support

Keywords

certificate

Creates a security certificate on the switch. The security certificate is required to establish an SSL connection with a management application, such as QuickTools. The certificate is valid 24 hours before the certificate creation date and expires 365 days after the creation date. Should the current certificate become invalid, or if you change to EncryptionMode=Strict, use the Create Certificate command to create a new one. For information about EncryptionMode, see Table 41.

Notes:

To insure the creation of a valid certificate, be sure that the switch and the workstation time and date are the same. See the following:

- "Date" command on page 14-169 for information about setting the time and date
- "Set Timezone" command on page 14-288 for information about setting the time zone on the switch and workstation
- "Set Setup System" command on page 14-280 (System keyword) for information about enabling the Network Time Protocol for synchronizing the time and date on the switch and workstation from an NTP server.

support

Assembles all log files and switch memory data into a file (dump_support.tgz) on the switch. If your workstation has an sFTP server, you can proceed with the command prompts to send the file from the switch to a remote host. Otherwise, you can use sFTP to download the support file from the switch to your workstation. The support file is useful to technical support personnel for troubleshooting switch problems. Use this command when directed by your authorized maintenance provider. This keyword does not require an Admin session.

Examples

The following is an example of the Create Support command when an sFTP server is available on the workstation:

```
IBM8Gb #> create support

  This may take several seconds...

Log Msg: [Wed Nov 02 14:06:47.341 CDT 2011][C][8400.003B][Switch][Creating
the support file - this will take several seconds]
command result: Passed.

Transfer the dump support file to another machine? (y/n) : y
ftp or sftp [ftp]: sftp
Enter address of ftp server (IPv4 or IPv6) : 10.20.108.130
Login name: root
Enter a valid remote directory path.
:
Would you like to continue downloading support file? (y/n) : y
Enter host password for user 'root':
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  870k    0     0  100  870k      0   595k  0:00:01  0:00:01 --:--:--  595k
Transfer the dump support file to another machine? (y/n) : n
```

The following is an example of the Create Support command and how to download the support file to a Linux workstation. When prompted to send the support file to another machine, decline, and then close the SSH/Telnet session. Open an sFTP session on the switch and log in with the account name *images* and password *images*. Transfer the dump_support.tgz file in binary mode with the Get command.

```
IBM8Gb #> create support
  This may take several seconds...

Log Msg: [Wed Nov 02 14:06:47.341 CDT 2011][C][8400.003B][Switch][Creating
the support file - this will take several seconds]
command result: Passed.
Transfer the dump support file to another machine? (y/n) : n

IBM8Gb #> quit

>sftp@ip_address
Password: images
sftp>get dump_support.tgz
    Fetching /dump_support.tgz to dump_support.tgz
    /dump_support.tgz                100%  137KB 136.8KB/s   00:00
sftp> quit
```

The following is an example of the Create Certificate command:

```
IBM8Gb (admin) #> create certificate
  The current date and time is day mon date hh:mm:ss UTC yyyy.
  This is the time used to stamp onto the certificate.
  Is the date and time correct? (y/n): [n] y
  Certificate generation successful.
```

Date

Displays or sets the system date and time. To set the date and time, the information string must be provided in this format: MMDDhhmmCCYY. The new date and time takes effect immediately.

Authority

Admin session except to display the date.

Syntax

date
[MMDDhhmmCCYY]

Keywords

[MMDDhhmmCCYY]

Specifies the date – this requires an Admin session. If you omit [MMDDhhmmCCYY], the current date is displayed which does not require an Admin session.

Notes

Network Time Protocol (NTP) must be disabled to set the time with the Date command. Enter the Set Setup System command to disable the NTPClientEnabled parameter.

When setting the date and time on a switch that is enabled for SSL connections, the switch time must be within 24 hours of the workstation time. Otherwise, the connection will fail.

Examples

The following is an example of the Date command:

```
IBM8Gb #> date
  Mon Apr 07 07:51:24 20xx
```

Exit

Closes the current CLI session.

Authority None

Syntax **exit**

Notes You can also enter Control+D to close the session.

Fcping

Verifies a Fibre Channel connection with another switch or a device and reports status.

Authority

None

Syntax

fcping destination [address]
count [number]
timeout [seconds]

Keywords

[address]

The address of the port or device with which to verify the Fibre Channel connection. [address] can have one of the following formats:

- 6-character hexadecimal device Fibre Channel address (hex). Enter addresses with or without the "0x" prefix.
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx or xxxxxxxxxxxxxxxx.

count [number]

Number of times given by [number] to repeat the command. If you omit this keyword, the command is repeated once.

timeout [seconds]

Number of seconds given by [seconds] to wait for a response. If you omit this keyword, the switch waits 1 second for a response.

Examples

The following is an example of the Fcping command:

```
IBM8Gb #> fcping 970400 count 3
28 bytes from local switch to 0x970400 time = 10 usec
28 bytes from local switch to 0x970400 time = 11 usec
28 bytes from local switch to 0x970400 time = 119 usec
```

Fctrace

Displays the path from one port in the fabric to another in the same zone. Path information includes the following:

- Domain IDs
- Incoming port name and physical port number
- Outgoing port name and physical port number

Authority

None

Syntax

fctrace [port_source] [port_destination] ***[hop_count]***

Keywords

[port_source]

The Fibre Channel port from which to begin the trace. [port_source] can have the following formats:

- 6-character hexadecimal device Fibre Channel address (hex). Enter addresses with or without the "0x" prefix.
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx or xxxxxxxxxxxxxxxx.

[port_destination]

The Fibre Channel port at which to end the trace. [port_destination] can have the following formats:

- 6-character hexadecimal device Fibre Channel address (hex). Enter addresses with or without the "0x" prefix.
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx or xxxxxxxxxxxxxxxx.

[hop_count]

Maximum number of hops before stopping the trace. If you omit [hop_count], a value of 20 hops is used.

Examples

The following is an example of the Fctrace command:

```
IBM8Gb#> fctrace 970400 970e00 hops 5

  36 bytes from 0x970400 to 0x970e00, 5 hops max

  Domain  Ingress Port WWN         Port  Egress Port WWN          Port
  ------  ----------------         ----  ---------------          ----
  97      20:04:00:c0:dd:02:cc:2e  4     20:0e:00:c0:dd:02:cc:2e  14
  97      20:0e:00:c0:dd:02:cc:2e  14    20:04:00:c0:dd:02:cc:2e  4
```

Feature

Adds license key features to the switch and displays the license key feature log. There are currently no feature license keys for this product.

Authority

Admin session for Add keyword only

Syntax

feature
add [license_key]
log

Keywords

add [license_key]

Adds the feature that corresponds to the value given by [license_key]. [license_key] is case insensitive.

log

Displays a list of installed license key features.

Firmware Install

Downloads firmware from a remote host to the switch, installs the firmware, then resets the switch to activate the firmware. This operation is disruptive.

Notes:

The sFTP switch service is enabled by default, and the FTP and TFTP services are disabled. If you intend to use FTP or TFTP, you must first enable the service. For more information about switch services, see "Managing switch services" on page 50.

The command prompts you for the following:

- The file transfer protocol: FTP, TFTP, sFTP, or URL
- An account name and password on the remote host (FTP, sFTP)
- IP address of the remote host (FTP, TFTP, sFTP)
- Pathname for the firmware image file (FTP, TFTP, sFTP). For URL, enter a URL in the form http://, ftp://, or https://.

Authority

Admin session

Syntax

firmware install

Examples

The following is an example of the Firmware Install command using sFTP:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> firmware install
  The switch will be reset.  This process will cause a disruption
  to I/O traffic.
  Continuing with this action will terminate all management sessions,
  including any Telnet sessions. When the firmware activation is complete,
  you may log in to the switch again.

  Do you want to continue? [y/n]: y
      Press 'q' and the ENTER key to abort this command.

  FTP, TFTP, SFTP, or URL : sftp
  User Account            : johndoe
  Password:               : **********
  IP Address              : 10.0.0.254
  Source Filename         : 9.1.00.xx_ipc
  About to install image.  Do you want to continue? [y/n] y

Connected to 10.0.0.254 (10.0.0.254).
220 localhost.localdomain sFTP server (Version wu-2.6.1-18) ready.
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

Group

Creates groups, manages membership within the group, and manages the membership of groups in security sets.

Authority

Admin session and a Security Edit session. For information about starting a Security Edit session, see the "Security" command on page 236. The List, Members, Securitysets, and Type keywords are available without an Admin session.

Syntax

group

add [group]
copy [group_source] [group_destination]
create [group] *[type]*
delete [group]
edit [group] [member]
list
members [group]
remove [group] [member_list]
rename [group_old] [group_new]
securitysets [group]
type [group]

Keywords

add [group]

Initiates an editing session in which to specify a group member and its attributes for the existing group given by [group]. ISL, Port, and MS member attributes are described in Table 7, Table 8, and Table 9 respectively. The group name and group type attributes are read-only fields common to all three tables.

Table 7. ISL Group member attributes

Attribute	Description
Member	Worldwide name of the switch that would attach to the switch. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP). The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the ISL member. The hash functions are MD5 or SHA-1. If the ISL member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the ISL group member. The string has the following lengths depending on the Primary Hash function: • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the ISL group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the ISL group member. The Primary Hash and the Secondary Hash cannot be the same.

Table 7. ISL Group member attributes (Continued)

Attribute	Description
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Binding	Domain ID of the switch to which to bind the ISL group member worldwide name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. A value of 0 (zero) specifies no binding.

Table 8. Port group member attributes

Attribute	Description
Member	Port worldwide name for the N_Port device that would attach to the switch. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP). The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the Port group member. The hash functions are MD5 or SHA-1. If the Port group member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the Port group member. The string has the following lengths depending on the Primary Hash function: • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the Port group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the Port group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: • MD5 hash: 16-byte • SHA-1 hash: 20-byte

Table 9. MS group member attributes

Attribute	Description
Member	Port worldwide name for the N_Port device that would attach to the switch.
CTAuthentication	Common Transport (CT) authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Hash	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Secret	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: • MD5 hash: 16-byte • SHA-1 hash: 20-byte

copy [group_source] [group_destination]

Creates a new group named [group_destination] and copies the membership into it from the group given by [group_source].

create [group] ***[type]***

Creates a group with the name given by [group] with the type given by [type]. A group name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The security database supports a maximum of 16 groups. If you omit [type], ISL is used. The [type] parameter can be one of the following:

isl

Configures security for attachments to other switches.

Port

Configures security for attachments to N_Port devices.

ms

Configures security for attachments to N_Port devices that are issuing management server commands.

edit [group] [member]

Initiates an editing session in which to change the attributes of a worldwide name given by [member] in a group given by [group]. Member attributes that can be changed are described in Table 10.

Table 10. Group Member Attributes

Attribute	Description
Authentication (ISL and Port Groups)	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP).
CTAuthentication (MS Groups)	CT authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.

Table 10. Group Member Attributes (Continued)

Attribute	Description
Primary Hash (ISL and Port Groups)	The preferred hash function to use to decipher the encrypted Primary Secret sent by the member. The hash functions are MD5 or SHA-1. If the member does not support the Primary Hash, the switch will use the Secondary Hash.
Hash (MS Groups)	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Primary Secret (ISL and Port Groups)	Hexadecimal string that is encrypted by the Primary Hash for authentication with the member. The string has the following lengths depending on the Primary Hash function: • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Secondary Hash (ISL and Port Groups)	Hash function to use to decipher the encrypted Secondary Secret sent by the group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret (ISL and Port Groups)	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Secret (MS Groups)	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: • MD5 hash: 16-byte • SHA-1 hash: 20-byte
Binding (ISL Groups)	Domain ID of the switch to which to bind the ISL group member worldwide name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. 0 (zero) specifies no binding.

list

Displays a list of all groups and the security sets of which they are members. This keyword is available without an Admin session.

members [group]

Displays all members of the group given by [group]. This keyword is available without an Admin session.

remove [group] [member_list]

Remove the port/device worldwide name given by [member] from the group given by [group]. Use a <space> to delimit multiple member names in [member_list].

rename [group_old] [group_new]

Renames the group given by [group_old] to the group given by [group_new].

securitysets [group]

Displays the list of security sets of which the group given by [group] is a member. This keyword is available without an Admin session.

type [group]

Displays the group type for the group given by [group]. This keyword is available without an Admin session.

Notes

Primary and secondary secrets are not included in a switch configuration backup. Therefore, after restoring a switch configuration, you must re-enter the primary and secondary secrets. Otherwise, the switch will isolate because of an authentication failure.

For information about managing groups in security sets, see the "Securityset" command on page 239.

Examples

The following is an example of the Group Add command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> security edit
IBM8Gb (admin-security) #> group add Group_1
  A list of attributes with formatting and default values will follow
  Enter a new value or simply press the ENTER key to accept the current value
  with exception of the Group Member WWN field which is mandatory.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Group Name       Group_1
  Group Type       ISL
  Member          (WWN)                           [00:00:00:00:00:00:00:00]
  Authentication  (None / Chap)                   [None                    ]
  PrimaryHash     (MD5 / SHA-1)                   [MD5                     ]
  PrimarySecret   (32 hex or 16 ASCII char value) [                        ]
  SecondaryHash   (MD5 / SHA-1 / None)            [None                    ]
  SecondarySecret (40 hex or 20 ASCII char value) [                        ]
  Binding         (domain ID 1-239, 0=None)       [0                       ]

  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

The following is an example of the Group Edit command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> security edit
IBM8Gb (admin-security) #> group edit G1 10:00:00:c0:dd:00:90:a3
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Group Name        g1
  Group Type        ISL
  Group Member      10:00:00:c0:dd:00:90:a3
  Authentication    (None / Chap)                   [None]  chap
  PrimaryHash       (MD5 / SHA-1)                   [MD5 ]  sha-1
  PrimarySecret     (40 hex or 20 ASCII char value) [    ]
12345678901234567890
  SecondaryHash     (MD5 / SHA-1 / None)            [None]  md5
  SecondarySecret   (32 hex or 16 ASCII char value) [    ]  1234567890123456
  Binding           (domain ID 1-239, 0=None)       [3   ]

  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

The following is an example of the Group List command:

```
IBM8Gb #> group list
  Group       SecuritySet
  -----       -----------
  group1 (ISL)
              alpha
  group2 (Port)
              alpha
```

The following is an example of the Group Members command:

```
IBM8Gb #> group members group_1
  Current list of members for Group: group_1
  ---------------------------------
  10:00:00:c0:dd:00:71:ed
  10:00:00:c0:dd:00:72:45
  10:00:00:c0:dd:00:90:ef
  10:00:00:c0:dd:00:b8:b7
```

Hardreset

Resets the switch and performs a power-on self test. This reset disrupts I/O traffic, activates the pending firmware, and clears the alarm log. To save the alarm log before resetting, see the "Set Log" command on page 258.

Authority

Admin session

Syntax

hardreset

Notes

To reset the switch without a power-on self test, see the "Reset" command on page 226.

To reset the switch without disrupting traffic, see the "Hotreset" command on page 184.

Help

Displays a brief description of the specified command, its keywords, and usage.

Authority

None

Syntax

help ***[command] [keyword]***

Keywords

[command]

Displays a summary of the command given by [command] and its keywords. If you omit [command], the system displays all available commands.

[keyword]

Displays a summary of the keyword given by [keyword] belonging to the command given by [command]. If you omit [keyword], the system displays the available keywords for the specified command.

all

Displays a list of all available commands (including command variations).

Examples

The following is an example of the Help Config command:

```
IBM8Gb #> help config
config CONFIG_OPTIONS
The config command operates on configurations.

  Usage: config   { activate | backup   | cancel   | copy     | delete   |
                    edit     | list     | restore  | save }
```

The following is an example of the Help Config Edit command:

```
IBM8Gb #> help config edit
config edit [CONFIG_NAME]
This command initiates a configuration session and places the current session
into config edit mode.
If CONFIG_NAME is given and it exists, it gets edited; otherwise, it gets
created.  If it is not given, the currently active configuration is edited.

Admin mode is required for this command.

  Usage: config edit [CONFIG_NAME]
```

History

Displays a numbered list of the previously entered commands from which you can re-execute selected commands.

Authority

None

Syntax

history

Notes

Use the History command to provide context for the ! command:

- Enter ![command_string] to re-execute the most recent command that matches [command_string].
- Enter ![line number] to re-execute the corresponding command from the History display
- Enter ![partial command string] to re-execute a command that matches the command string.
- Enter !! to re-execute the most recent command.

Examples

The following is an example of the History command:

```
IBM8Gb #> history
   1 show switch
   2 date
   3 help set
   4 history

IBM8Gb #> !3
help set

set SET_OPTIONS
There are many attributes that can be set.
Type help with one of the following to get more information:

  Usage: set   { alarm     | beacon    | config    | log       | pagebreak |
                 port      | setup     | switch }
```

Hotreset

Resets the switch for the purpose of activating the pending firmware without disrupting traffic. This command terminates all management sessions, saves all configuration information, and clears the event log. After the pending firmware is activated, the configuration is recovered. This process may take a few minutes. To save the event log to a file before resetting, enter the Set Log Archive command.

Authority

Admin session

Syntax

hotreset

Notes

- You can load and activate version 9.1.*x* firmware on an operating switch without disrupting data traffic or having to re-initialize attached devices under the following conditions:
  - The current firmware version permits the installation and non-disruptive activation of 9.1 firmware. For information about compatibility with previous firmware versions, see the *Firmware Release Notes*.
  - No changes are being made to switches in the fabric including installing firmware, powering up, powering down, disconnecting or connecting ISLs, and switch configuration changes.
  - No port on the switch is in the diagnostic state.
  - No zoning changes are being made on the switch.
  - No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.
- Ports that are stable when the non-disruptive activation begins, then change states, will be reset. When the non-disruptive activation is complete, QuickTools sessions reconnect automatically. However, CLI and SSH sessions must be restarted manually.
- This command clears the event log and all counters.

Ike List

Displays IKE peer and policy information.

Authority

None

Syntax

ike list
active
configured
edited
peer *[option]*
policy *[option]*

Keywords

active
Displays the configurations for all active IKE peers and policies.

configured
Displays the configurations for all user-defined IKE peers and policies.

edited
Displays the configurations for all IKE peers and policies that have been modified in an Ipsec Edit session, but not saved.

peer *[option]*
Specifies the IKE peers given by [option] for which to display configuration information. [option] can have the following values:

[peer]
Displays the configuration for the peer given by [peer].

active
Displays the configuration for all active peers.

configured
Displays the configuration for all user-defined peers.

edited
Displays the configuration for all peers that have been modified, but not saved.

policy *[option]*
Specifies the IKE policies given by [option] for which to display configuration information. [option] can have the following values:

[policy]
Displays the configuration for the IKE policy given by [policy].

active
Displays the configuration for all active IKE policies.

configured
Displays the configuration for all user-defined IKE policies.

edited
Displays the configuration for all IKE policies that have been modified, but not saved.

Notes

If you omit the keywords, the Ike List command displays configuration information for all active IKE peers and policies.

Examples

The following is an example of the Ike List Configured command:

```
IBM8Gb #> ike list configured
  Configured (saved) IKE Information
  Peer                              Policy
  ------                            ----
  peer_1
                                    policy_1
                                    policy_2
  peer_2
                                    policy_3
  peer_3
                                    (no policies)
  (No peer)
                                    policy_4
Summary:
  Peer Count                        3
  Policy Count                      4
```

The following is an example of the Ike List Policy command:

```
IBM8Gb (admin-ipsec) #> ike list policy policy_2

  Edited (unsaved) IKE Information

  policy_2
    Description        65
    Mode               transport
    LocalAddress       10.0.0.3
    LocalPort          1234
    RemotePort         0 (All)
    Peer               peer_1
    Protocol           udp
    Action             ipsec
    ProtectionDesired  <undefined>
    LifetimeChild      3600 (seconds)
    RekeyChild         True
    Encryption         3des_cbc
    Integrity          md5_96 sha1_96 sha2_256
    DHGroup            1 5
    Restrict           True
```

Ike Peer

Creates and manages IKE peers.

Authority

Admin session and an Ipsec Edit session

Syntax

ike peer
copy [peer_source] [peer_destination]
create [peer]
delete [peer]
edit [peer]
list *[option]*
rename [peer_old] [peer_new]

Keywords

copy [peer_source] [peer_destination]

Creates a new peer named [peer_destination] and copies the configuration into it from the peer given by [peer_source]. You must enter the Ipsec Save command afterwards to save your changes.

create [peer]

Creates a peer with the name given by [peer]. A peer name must begin with a letter and be no longer than 32 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The IKE database supports a maximum of 16 user-defined peers. You must enter the Ipsec Save command afterwards to save your changes. See Table 11.

Table 11. IKE Peer Configuration Parameters

Parameter	Description
Description	Peer description of up to 127 characters or n (none).
Address	IP address (version 4 or 6) or DNS host name of the peer host, switch, or gateway.
Lifetime	Duration of the IKE security association connection in seconds. Lifetime is an integer from 900–86400.
Encryption	Algorithm that encrypts outbound data or decrypts inbound data. The encryption algorithm can be one or more of the following: • 3des_cbc • aes_cbc_128 • aes_cbc_192 • aes_cbc_256
Integrity	Integrity (authentication) algorithm. Integrity can be one or more of the following: • md5_96 (EncryptionMode=Legacy only) • sha1_96 • sha2_256 • aes_xcbc_96 (EncryptionMode=Legacy only) For information about EncryptionMode, see Table 41.

Table 11. IKE Peer Configuration Parameters (Continued)

Parameter	Description
DHGroup	Diffie-Hellman group number. You can specify one or more group numbers: 1, 2, 5, 14, or 24. 1, 2, and 5 are valid only when EncryptionMode=Legacy. For information about EncryptionMode, see Table 41.
Restrict	Algorithm and DH group restriction. The IKE responder accepts only algorithms and DH groups specified by the IKE initiator (True), or accepts all algorithms and DH groups (False).
Authentication	IKE authentication method. Authentication can have the following values: • Secret—Authenticate by pre-shared keys (PSK). See the Key parameter. • Pubkey—Authenticate by public key encryption (RSA) through digital certificates. See the CertificateName, SwitchIdentity, and PeerIdentity parameters.
Key (Authentication=Secret)	Pre-shared key that matches the key on the IKE peer. Key can be one of the following: • String in quotes up to 128 characters • Raw hex bytes up to 256 bytes. The number of bytes must be even.
CertificateName (Authentication=Pubkey)	Name of the local switch certificate to use to authenticate the peer device. CertificateName is a string of up to 32 characters. For more information about certificates, see the Certificate command.
SwitchIdentity (Authentication=Pubkey)	Identifier by which the switch is authenticated. SwitchIdentity can have the following values: • Unspecified—Identifier is set to the distinguished name (DN) of the local certificate's subject. • IPv4 or IPv6 address, DNS name, or e-mail address—This value must be included in a subjectAltName extension in the local certificate.
PeerIdentity (Authentication=Pubkey)	Identifier by which the peer is authenticated. PeerIdentity can have the following values: • Unspecified—Identifier is set to the IP address of the peer or remote tunnel end point. • IPv4 or IPv6 address, DNS name, or e-mail address—This value must be included in a subjectAltName extension in the peer certificate.

delete [peer]

Deletes the peer given by [peer] from the IKE database. You must enter the Ipsec Save command afterwards to save your changes.

edit [peer]

Opens an edit session in which to change the configuration of an existing peer given by [peer]. For descriptions of the peer parameters, refer to Table 11.

list ***[option]***

Displays the configuration for the peer or peers given by [option]. If you omit [option], the command displays the configuration of all active peers. [option] can be one of the following:

[peer]

Displays the configuration for the peer given by [peer].

active

Displays the configuration for all active peers.

configured

Displays the configuration for all user-defined peers.

edited

Displays the configuration for all peers that have been modified, but not saved.

rename [peer_old] [peer_new]

Renames the peer given by [peer_old] to the peer given by [peer_new]. You must enter the Ipsec Save command afterwards to save your changes.

Examples

The following is an example of the Ike Peer Create command. Shaded entries indicate options that are available only when EncryptionMode=Legacy. For more information about EncryptionMode, see Table 41. An asterisk (*) indicates a required entry.

```
IBM8Gb >># admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ike peer create peer_1

  A list of attributes with formatting will follow.
  Enter a value or simply press the ENTER key to skip specifying a value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

  Value (press ENTER to not specify value, 'q' to quit):
    Description      (string, max=127 chars, N=None)             :  Peer_1
   *Address          (hostname, IPv4, or IPv6 Address)           :  10.0.0.3
    Lifetime         (decimal value, 900-86400 seconds)          :  3600
   *Encryption       (select one or more encryption algorithms)
                          1=3des_cbc
                          2=aes_cbc_128
                          3=aes_cbc_192
                          4=aes_cbc_256                          :  1 4
   *Integrity        (select one or more integrity algorithms)
                          1=md5_96
                          2=sha1_96
                          3=sha2_256
                          4=aes_xcbc_96                          :  1 2 3
   *DHGroup          (select one or more Diffie-Hellman Groups)
                          1, 2, 5, 14, 24                        :  2 14
    Restrict         (True / False)                              :  True
   *Authentication   (1=secret, 2=public_key)                    :  1
   *Key              (quoted string or raw hex bytes)
                          maximum length for quoted string = 128
                          maximum length for raw hex bytes = 256
                         the raw hex length must be even        :  0x11223344

  The IKE peer has been created.
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.
IBM8Gb (admin-IPSEC) #> ipsec save
```

The following is an example of the Ike Peer Edit command. Shaded entries indicate options that are available only when EncryptionMode = Legacy. For more information about EncryptionMode, see Table 41. An asterisk (*) indicates a required entry.

```
IBM8Gb (admin-ipsec) #> ike peer edit peer_2

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

  Current Values:
    Description       Peer_2 description
    Address           10.0.0.4
    Lifetime          4800 (seconds)
    Encryption        aes_cbc_128 aes_cbc_192
    Integrity         aes_xcbc_96
    DHGroup           5 24
    Restrict          True
    Authentication    secret
    Key               ********

  New Value (press ENTER to not specify value, 'q' to quit, 'n' for none):
    Description      (string, max=127 chars, N=None)             :
   *Address          (hostname, IPv4, or IPv6 Address)           :
    Lifetime         (decimal value, 900-86400 seconds)          :  1200
   *Encryption       (select one or more encryption algorithms)
                          1=3des_cbc
                          2=aes_cbc_128
                          3=aes_cbc_192
                          4=aes_cbc_256                          :  1
   *Integrity        (select one or more integrity algorithms)
                          1=md5_96
                          2=sha1_96
                          3=sha2_256
                          4=aes_xcbc_96                          :  1
   *DHGroup          (select one or more Diffie-Hellman Groups)
                          1, 2, 5, 14, 24                        :  1
    Restrict         (True / False)                              :
   *Authentication   (1=secret, 2=public_key)                    :
   *Key              (quoted string or raw hex bytes)
                          maximum length for quoted string = 128
                          maximum length for raw hex bytes = 256
                          the raw hex length must be even        :

  The IKE peer has been edited.
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.
```

The following is an example of the Ike Peer List command:

```
IBM8Gb (admin-ipsec) #> ike peer list peer_1

  Edited (unsaved) IKE Information

  peer_1
    Description      Peer_1 description
    Address          10.0.0.3
    Lifetime         3600 (seconds)
    Encryption       3des_cbc aes_cbc_256
    Integrity        md5_96 sha1_96 sha2_256
    DHGroup          2 14
    Restrict         True
    Authentication   secret
    Key              ********
```

Ike Policy

Creates and manages IKE policies.

Authority

Admin session and an Ipsec Edit session

Syntax

ike policy
copy [policy_source] [policy_destination]
create [policy]
delete [policy]
edit [policy]
list *[option]*
rename [policy_old] [policy_new]

Keywords

copy [policy_source] [policy_destination]

Creates a new policy named [policy_destination] and copies the configuration into it from the policy given by [policy_source]. You must enter the Ipsec Save command afterwards to save your changes.

create [policy]

Creates a policy with the name given by [policy]. A policy name must begin with a letter and be no longer than 32 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The IKE database supports a maximum of 256 user-defined policies. You must enter the Ipsec Save command afterwards to save your changes. See Table 12.

Table 12. IKE policy configuration parameters

Parameter	Description
Description	Policy description of up to 127 characters.
Mode	IP security connection type. Mode can have one of the following values: • Transport—Encrypts the transport layer payload • Tunnel—Encrypts the IP header and the transport layer payload
LocalAddress	Local switch IP address (IPv4 or IPv6). The switch and the peer device must use the same IP address version. If you omit this value, all switch IP addresses are used. An IKE policy is created for each switch IP address.
LocalPort	Local port with which the policy traffic selector must match packets. LocalPort can be an integer from 1–65535. Zero (0) and the keyword All specifies all remote ports.
RemoteAddress (Mode=Tunnel)	IPv4 or IPv6 address of the traffic selector on the remote side of the IP security tunnel.
RemotePort (Mode=Tunnel)	Remote port with which the policy traffic selector must match packets. RemotePort can be an integer 1–65535. Zero (0) and the keyword All specifies all remote ports.
Peer	Name of an existing peer to be associated with this policy.

Table 12. IKE policy configuration parameters (Continued)

Parameter	Description
Protocol (LocalPort=1–65535 or RemotePort=1–65535)	Transport protocol with which the traffic selector matches packets. Protocol can have the following values: • icmp—Internet control message protocol for IP version 4 • icmp6—Internet control message protocol for IP version 6 • ip4—Internet protocol version 4 • tcp—Transmission control protocol • udp—User datagram protocol • any or 0—Any protocol • 1–255—Numeric equivalent for standard and custom protocols
Action	Action to apply for packets that match the policy. Action can be ipsec, which applies the policy's IP security protection to the packet.
ProtectionDesired (Mode=Transport)	IP security protection protocol to apply (encapsulating security payload).
LifetimeChild	Duration of the IP security association connection in seconds. LifetimeChild is an integer 900–86400. The default is 3600.
RekeyChild	IP security association renegotiation. Renegotiate an IP security association that is about to expire (True) or allow it to expire (False).
Encryption	One or more encryption algorithms. Encryption can be one of the following: • 3des_cbc • aes_cbc_128 • aes_cbc_192 • aes_cbc_256
Integrity	One or more authentication algorithms to apply to the policy: • md5_96 (EncryptionMode=Legacy only) • sha1_96 • sha2_256 • aes_xcbc_96 (EncryptionMode=Legacy only) For information about EncryptionMode, see Table 41.
DHGroup	Diffie-Hellman group number(s) to apply to the policy. DHGoup can be one or more of the following: 1, 2, 5, 14, 24. If you omit this value, no Diffie-Hellman exchanges will be done for IP security association setup and rekeying. 1, 2, and 5 are valid only when EncryptionMode = Legacy. For information about EncryptionMode, see Table 41.

Table 12. IKE policy configuration parameters (Continued)

Parameter	Description
Restrict	Algorithm and DH group restriction. The IKE responder accepts only the configured algorithms and DH groups for an IKE security association (True), or accepts any algorithm and DH group (False). If EncryptionMode=Strict, the system makes Restrict=True.

delete [policy]

Deletes the policy given by [policy] from the IKE database. You must enter the Ipsec Save command afterwards to save your changes.

edit [policy]

Opens an edit session in which to change the configuration of an existing IKE policy given by [policy]. For descriptions of the policy parameters, refer to Table 12.

list *[option]*

Displays the configuration for the policy or policies given by [option]. If you omit [option], the command displays the configuration of all active policies. [option] can be one of the following:

[policy]

Displays the configuration for the policy given by [policy].

active

Displays the configuration for all active policies.

configured

Displays the configuration for all user-defined policies.

edited

Displays the configuration for all policies that have been modified, but not saved.

rename [policy_old] [policy_new]

Renames the policy given by [policy_old] to the policy given by [policy_new]. You must enter the Ipsec Save command afterwards to save your changes.

Examples

The following is an example of the Ike Policy Create command. Shaded entries indicate options that are available only when EncryptionMode=Legacy. For more information about EncryptionMode, see Table 41. An asterisk (*) indicates a required entry.

```
IBM8Gb (admin-ipsec) #> ike policy create policy_2

  A list of attributes with formatting will follow.
  Enter a value or simply press the ENTER key to skip specifying a value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

  Value (press ENTER to not specify value, 'q' to quit):
    Description        (string, max=127 chars, N=None)           :  Policy 2
   *Mode               (1=transport, 2=tunnel)                   :  1
   *LocalAddress       (IPv4, IPv6 Address or keyword 'All'      :  10.0.0.3
    LocalPort          (decimal value, 0-65535 or keyword 'All'  :  1234
    RemotePort         (decimal value, 0-65535 or keyword 'All'  :  0
   *Peer               (string, max=32 chars)                    :  peer_1
   *Protocol           (decimal value, 0-255, or keyword)
                          0=NotSpecified
                          Allowed keywords
                            icmp, icmp6, ip4, tcp, udp or any    :  udp
    Action             (1=ipsec)                                 :  1
    ProtectionDesired  (select one, transport-mode only)
                          1=esp  Encapsulating Security Payload  :  1
    LifetimeChild      (decimal value, 900-86400 seconds)        :  3600
    RekeyChild         (True / False)                            :  True
   *Encryption         (select one or more encryption algorithms)
                          1=3des_cbc
                          2=aes_cbc_128
                          3=aes_cbc_192
                          4=aes_cbc_256                          :  1
    Integrity          (select one or more integrity algorithms)
                          1=md5_96
                          2=sha1_96
                          3=sha2_256
                          4=aes_xcbc_96
                          or the keyword 'None'                  :  1 2 3
    DHGroup            (select one or more Diffie-Hellman Groups)
                          1, 2, 5, 14, 24 or the keyword 'None'  :  1 5
    Restrict           (True / False)                            :  True

  The IKE policy has been created.
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.
IBM8Gb (admin-IPSEC) #> ipsec save
```

The following is an example of the Ike Policy Edit command. Shaded entries indicate options that are available only when EncryptionMode = Legacy. For more information about EncryptionMode, see Table 41. An asterisk (*) indicates a required entry.

```
IBM8Gb (admin-ipsec) #> ike policy edit policy_1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.
  Current Values:
    Description         Policy 1
    Mode                tunnel
    LocalAddress        10.0.0.6
    LocalPort           456
    RemotePort          0 (All)
    Action              ipsec
    LifetimeChild       3600 (seconds)
    RekeyChild          True
    Restrict            False

  New Value (press ENTER to not specify value, 'q' to quit, 'n' for none):
    Description        (string, max=127 chars, N=None)           :  Policy 1a
   *Mode               (1=transport, 2=tunnel)                   :  1
   *LocalAddress       (IPv4, IPv6 Address or keyword 'All'      :
    LocalPort          (decimal value, 0-65535 or keyword 'All'  :
    RemotePort         (decimal value, 0-65535 or keyword 'All'  :
   *Peer               (string, max=32 chars)                    :  peer_2
   *Protocol           (decimal value, 0-255, or keyword)
                          0=NotSpecified
                          Allowed keywords
                            icmp, icmp6, ip4, tcp, udp or any    :  udp
    Action             (1=ipsec)                                 :  1
    ProtectionDesired  (select one, transport-mode only)
                          1=esp  Encapsulating Security Payload  :  1
    LifetimeChild      (decimal value, 900-86400 seconds)        :  2000
    RekeyChild         (True / False)                            :  true
   *Encryption         (select one or more encryption algorithms)
                          1=3des_cbc
                          2=aes_cbc_128
                          3=aes_cbc_192
                          4=aes_cbc_256                          :  1 3
    Integrity          (select one or more integrity algorithms)
                          1=md5_96
                          2=sha1_96
                          3=sha2_256
                          4=aes_xcbc_96
                          or the keyword 'None'                  :  1 3
    DHGroup            (select one or more Diffie-Hellman Groups)
                          1, 2, 5, 14, 24 or the keyword 'None'  :  2 5
    Restrict           (True / False)                            :  true
The IKE policy has been edited.
This configuration must be saved with the 'ipsec save' command before it can
take effect, or to discard this configuration use the 'ipsec cancel' command.
IBM8Gb (admin-IPSEC) #> ipsec save
```

The following is an example of the Ike Policy List command:

```
IBM8Gb (admin-ipsec) #> ike policy list policy_2

  Edited (unsaved) IKE Information

  policy_2
    Description        Policy 2
    Mode               transport
    LocalAddress       10.0.0.3
    LocalPort          1234
    RemotePort         0 (All)
    Peer               peer_1
    Protocol           udp
    Action             ipsec
    ProtectionDesired  <undefined>
    LifetimeChild      3600 (seconds)
    RekeyChild         True
    Encryption         3des_cbc
    Integrity          md5_96 sha1_96 sha2_256
    DHGroup            1 5
    Restrict           True
```

Image

Manages and installs switch firmware.

Notes:

The sFTP switch service is enabled by default, and the FTP and TFTP services are disabled. If you intend to use FTP or TFTP, you must first enable the service. For more information about switch services, see "Managing switch services" on page 50.

Authority

Admin session

Syntax

image
cleanup
fetch [account_name] [ip_address] [file_source] [file_destination]
install
list
sftp [account_name] [ip_address] [file_source] [file_destination]
tftp [ip_address] [file_source] [file_destination]
unpack [file]
url [url] [file_destination]

Keywords

cleanup

Removes all firmware image files from the switch. All firmware image files are removed automatically each time the switch is reset.

fetch [account_name] [ip_address] [file_source] [file_destination]

Retrieves image file given by [file_source] using sFTP and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the host IP address given by [Ip_address]. [ip_address] can be an IP address or a DNS host name. If an account name needs a password to access the sFTP server, the system will prompt you for it.

install

Downloads firmware from a remote host to the switch, installs the firmware, then resets the switch to activate the firmware. This is disruptive. The command prompts you for the following:

- File transfer protocol: FTP, TFTP, sFTP, or URL
- IP address or DNS host name of the remote host (FTP, TFTP, sFTP)
- An account name and password on the remote host (FTP, sFTP)
- Pathname for the firmware image file. For URL, enter a URL in the form http://, ftp://, or https://.

list

Displays the list of image files that reside on the switch.

sftp [account_name] [ip_address] [file_source] [file_destination]

Retrieves image file given by [file_source] using sFTP and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the host IP address given by [Ip_address]. [ip_address] can be an IP address or a DNS host name. A host sFTP password is required.

tftp [ip_address] [file_source] [file_destination]

Retrieves image file given by [file_source] using TFTP and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the host IP address given by [Ip_address]. [ip_address] can be an IP address or a DNS host name.

unpack [file]

Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch must be reset for the new firmware to take effect.

url [url] [file_destination]

Retrieves image file given by [url] from the Internet and stores it on the switch with the file name given by [file_destination]. [url] can be any Internet URL.

Notes

To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

To install firmware when the management workstation has an FTP server, use the Image Install command or the Firmware Install command.

Examples

The following is an example of the Image Install command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> image install
  Warning: Installing new firmware requires a switch reset.

  Continuing with this action will terminate all management sessions,
  including any Telnet sessions. When the firmware activation is complete,
  you may log in to the switch again.

  Do you want to continue? [y/n]: y

      Press 'q' and the ENTER key to abort this command.

  FTP, TFTP, SFTP, or URL     : sftp
  User Account                : johndoe
  Password:                   : ***********
  IP Address                  : 10.0.0.254
  Source Filename             : 9.1.00.xx_ipc
  About to install image.  Do you want to continue? [y/n] y

Connected to 10.0.0.254 (10.0.0.254).
220 localhost.localdomain sFTP server (Version wu-2.6.1-18) ready.
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

The following is an example of the Image Fetch and Image Unpack commands:

```
IBM8Gb (admin) #> image fetch johndoe 10.0.0.254 9.1.00.11_ipc
>sftp images@10.0.0.254
Connecting to 10.0.0.254...
Password: images
sftp>put 9.1.00.11_ipc
    Uploading 9.1.00.11_ipc to /9.1.00.11_ipc
    9.1.00.11_ipc-slot3             100%  137KB 136.8KB/s   00:00
sftp>quit
IBM8Gb (admin) $>image list
IBM8Gb (admin) $>image unpack 9.1.00.11_ipc
Image unpack command result: Passed
```

Ipsec

Manages the IP security database. The IP security database consists of the Security Association database and the Security Policy database. The Ipsec Edit command opens a session in which to create and manage associations and policies.

Authority

Admin session except for the History keyword. The Clear keyword also requires an Ipsec Edit session.

Syntax

ipsec
cancel
clear
edit
history
limits
save

Keywords

cancel

Closes the current Ipsec Edit session. Any unsaved changes are lost.

clear

Deletes all IP security associations, IP security policies, IKE peers, and IKE policies from the volatile edit copies of the IP security and IKE databases. This keyword requires an Ipsec Edit session. This keyword does not affect the non-volatile IP security configuration. However, if you enter the Ipsec Clear command followed by the Ipsec Save command, the non-volatile IP security configuration will be deleted from the switch.

Notes:

The preferred method for deleting the IP security configuration from the switch is the Reset Ipsec command.

edit

Open an Ipsec Edit session in which to create and manage IP security associations and policies, and IKE peers and policies. Ipsec Edit session commands include the Ike Peer, Ike Policy, Ipsec Clear, Ipsec Association, and Ipsec Policy commands. This keyword requires an Admin session.

history

Displays a history of IP security modifications. This keyword does not require an Admin session. History information includes the following:

- Time of the most recent IP security database modification and the user who performed it
- Checksums for the active and inactive IP security databases, and the IKE database

limits

Displays the maximum and current numbers of configured IP security associations, IP security policies, IKE peers, and IKE policies. This keyword does not require an Admin session nor an Ipsec Edit session. However, in an Ipsec Edit session, this command displays the number of both configured associations, peers, and policies, plus those created in the edit session but not yet saved.

save

Saves changes made during the current Ipsec Edit session.

Examples

The following is an example of the Ipsec History command:

```
IBM8Gb #> ipsec history

  IPsec Database History
  ----------------------
  ConfigurationLastEditedBy      johndoe@OB-session5
  ConfigurationLastEditedOn      Sat Mar  8 07:14:36 2008
  Active Database Checksum       00000144
  Inactive Database Checksum     00000385
  IKE Database Checksum          00000023
```

The following is an example of the Ipsec Limits command:

```
IBM8Gb #> ipsec limits

  Configured (saved) IPsec Information

  IPsec Attribute            Maximum  Current
  ---------------            -------  -------
  MaxConfiguredSAs               512        0
  MaxConfiguredSPs               128        0
  MaxConfiguredIKEPeers           16        0
  MaxConfiguredIKEPolicies       256        0
```

Ipsec Association

Creates and manages associations in the Security Association database.

Authority

Admin session and an Ipsec Edit session

Syntax

ipsec association
copy [association_source] [association_destination]
create [association]
delete [association]
edit [association]
list [association]
rename [association_old] [association_new]

Keywords

copy [association_source] [association_destination]

Creates a new association named [association_destination] and copies the configuration into it from the association given by [association_source]. [association_destination] must not begin with *DynamicSA_*, which is reserved for dynamic associations. You must enter the Ipsec Save command afterwards to save your changes.

create [association]

Creates an association with the name given by [association]. An association name must begin with a letter and be no longer than 32 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The Security Association database supports a maximum of 512 user-defined associations. You must enter the Ipsec Save command afterwards to save your changes. The association configuration parameters are described in Table 13.

Table 13. Association configuration parameters

Parameter	Description
Description	Description of the association
SourceAddress	IP address or DNS host name of the host, switch, or gateway from which data originates.
DestinationAddress	IP address or DNS host name of the host, switch, or gateway receiving data. If you specified an IP address for the SourceAddress, the DestinationAddress must use the same IP version format.
Protocol	IP security protocol to be used to process data. The protocol can be one of the following: • Encapsulated Security Payload—RFC 2406 (esp) • Authentication Header—RFC 2402 (ah)
SPI	Security parameters index number
Authentication	Algorithm to use to authenticate the source or destination. The authentication algorithm can be one of the following: • hmac-md5 (EncryptionMode=Legacy only) • hmac-sha1 • hmac-sha256 • aes-xcbc-mac (EncryptionMode=Legacy only) For information about EncryptionMode, see Table 41.

Table 13. Association configuration parameters (Continued)

Parameter	Description
AuthenticationKey	Key string to use for authentication.
Encryption	Algorithm that encrypts outbound data or decrypts inbound data. The encryption algorithm can be one of the following: • 3des-cbc • null • blowfish-cbc (EncryptionMode=Legacy only) • aes-cbc • twofish-cbc (EncryptionMode=Legacy only) For information about EncryptionMode, see Table 41.
EncryptionKey	Key string to use in encrypting or decrypting data
Mode	IP security connection type. Mode can have one of the following values: • Transport—Encrypts the transport layer payload • Tunnel—Encrypts the IP header and the transport layer payload

delete [association]

Deletes the specified association given by [association] from the Security Association database. You must enter the Ipsec Save command afterwards to save your changes.

edit [association]

Opens an edit session in which to change the configuration of an existing association given by [association]. If the connection is not secure (SSH is disabled), the AuthenticationKey and EncryptionKey values are masked.

list *[option]*

Displays the configuration for the associations given by [option]. If you omit [option], the command displays the configuration of all active associations. [option] can be one of the following:

[association]

Displays the configuration for the association given by [association].

active

Displays the configuration for all active associations.

configured

Displays the configuration for all user-defined associations.

edited

Displays the configuration for all associations that have been modified, but not saved.

rename [association_old] [association_new]

Renames the association given by [association_old] to the association given by [association_new]. You must enter the Ipsec Save command afterwards to save your changes. Dynamic associations cannot be renamed. Dynamic associations cannot be renamed.

Examples

The following is an example of the Ipsec Association Create command. Shaded entries indicate options that are available only when EncryptionMode = Legacy. For more information about EncryptionMode, see Table 41. An asterisk (*) indicates a required entry.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec association create h2h-sh-sa

  A list of attributes with formatting will follow.
  Enter a value or simply press the ENTER key to skip specifying a value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

  Value (press ENTER to not specify value, 'q' to quit):
    Description        (string value, 0-127 bytes)           :  Host-to-host: switch->host
   *SourceAddress      (hostname, IPv4, or IPv6 Address)     :  fe80::2c0:ddff:fe03:d4c1
   *DestinationAddress (hostname, IPv4, or IPv6 Address)     :  fe80::250:daff:feb7:9d02
   *Protocol           (1=esp, 2=esp-old, 3=ah, 4=ah-old)    :  1
   *SPI                (decimal value, 256-4294967295)       :  333
    Authentication     (select an authentication algorithm)
                          1=hmac-md5       (16 byte key)
                          2=hmac-sha1      (20 byte key)
                          3=hmac-sha256    (32 byte key)
                          4=aes-xcbc-mac   (16 byte key)
                       authentication algorithm choice       :  2
   *AuthenticationKey  (quoted string or raw hex bytes)      :  "12345678901234567890"
   *Encryption         (select an encryption algorithm)
                          2=3des-cbc       (24 byte key)
                          3=null           (0 byte key)
                          4=blowfish-cbc   (5-56 byte key)
                          5=aes-cbc        (16/24/32 byte key)
                          6=twofish-cbc    (16-32 byte key)
                       encryption algorithm choice           :  1
   *EncryptionKey      (quoted string or raw hex bytes)      :  "123456789012345678901234"
    Mode               (1=transport, 2=tunnel)               :  1

  The security association has been created.
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.
```

Ipsec List

Displays information about IP security associations and policies.

Authority

None

Syntax

ipsec list
active
association *[option]*
configured
edited
policy *[option]*

Keywords

active

Displays a summary of active associations and policies. This is the default.

association *[option]*

Displays the configuration for the associations given by [option]. If you omit [option], the command displays the configuration of all active associations. [option] can be one of the following:

[association]

Displays the configuration for the association given by [association].

active

Displays the configuration for all active associations.

configured

Displays the configuration for all user-defined associations.

edited

Displays the configuration for all associations that have been modified, but not saved.

configured

Displays a summary of the user-defined associations and policies.

edited

Displays a summary of the associations and policies that have been modified, but not saved.

policy ***[option]***

Displays the configuration for the policies given by [option]. If you omit [option], the command displays the configuration of all active policies. [option] can be one of the following:

[policy]

Displays the configuration for the policy given by [policy].

active

Displays the configuration for all active policies.

configured

Displays the configuration for all user-defined policies.

edited

Displays the configuration for all policies that have been modified, but not saved.

Examples

The following is an example of the Ipsec List command:

```
IBM8Gb #> ipsec list

  Active IPsec Information

  Security Association Database
  -----------------------------
  h2h-sh-sa
  h2h-hs-sa

  Security Policy Database
  ------------------------
  h2h-hs-sp
  h2h-sh-sp

  Summary
  -------
    Security Association Count:   2
    Security Policy Count:        2
```

The following is an example of the Ipsec List Association command:

```
IBM8Gb #> ipsec list association

  Active IPsec Information

  h2h-sh-sa
    Description: Host-to-host: switch->host
    Source: fe80::2c0:ddff:fe03:d4c1
    Destination: fe80::250:daff:feb7:9d02
    Protocol: esp  SPI: 333 (0x14d)
    Authentication: hmac-sha1  ********
    Encryption: 3des-cbc  ********
    Mode: transport

  h2h-hs-sa
    Description: Host-to-host: host->switch
    Source: fe80::250:daff:feb7:9d02
    Destination: fe80::2c0:ddff:fe03:d4c1
    Protocol: esp  SPI: 444 (0x1bc)
    Authentication: hmac-sha1  ********
    Encryption: 3des-cbc  ********
    Mode: transport
```

The following is an example of the Ipsec List Policy command:

```
IBM8Gb #> ipsec list policy

  Active IPsec Information

  h2h-hs-sp
    Description: Host-to-host: host->switch
    Source: fe80::250:daff:feb7:9d02/128
    Destination: fe80::2c0:ddff:fe03:d4c1/128
    Protocol: any
    Direction: in  Priority: 0  Action: ipsec
    Mode: transport

    Rule  Protocol  Mode       Level
    ----  --------  ---------  -----
    1     esp       transport  require

  h2h-sh-sp
    Description: Host-to-host: switch->host
    Source: fe80::2c0:ddff:fe03:d4c1/128
    Destination: fe80::250:daff:feb7:9d02/128
    Protocol: any
    Direction: out  Priority: 0  Action: ipsec
    Mode: transport

    Rule  Protocol  Mode       Level
    ----  --------  ---------  -----
    1     esp       transport  require
```

Ipsec Policy

Manages policies in the Security Policy database.

Authority

Admin session and an Ipsec Edit session

Syntax

ipsec policy
copy [policy_source] [policy_destination]
create [policy]
delete [policy]
edit [policy]
list *[option]*
rename [policy_old] [policy_new]

Keywords

copy [policy_source] [policy_destination]

Creates a new policy named [policy_destination] and copies the configuration into it from the policy given by [policy_source]. You must enter the Ipsec Save command afterwards to save your changes. [policy_destination] must not begin with *DynamicSP_*, which is reserved for dynamic policies.

create [policy]

Creates a policy with the name given by [policy]. A policy name must begin with a letter and be no longer than 32 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The Security Policy database supports a maximum of 128 user-defined policies. You must enter the Ipsec Save command afterwards to save your changes. Table 14 describes the policy parameters.

Table 14. Policy configuration parameters

Parameter	Description
Description	Description of the policy
SourceAddress	IP address or DNS host name of the host, switch, or gateway from which data originates.
SourcePort	Source port number (1–65535)
DestinationAddress	IP address or DNS host name of the host, switch, or gateway receiving data. If you specified an IP address for the SourceAddress, the DestinationAddress must use the same IP version format.
DestinationPort	Destination port number (1–65535)
Protocol	Protocol or application to which to apply IP security. Enter a keyword for one of the following protocols or an integer (0–255): • Internet Control Message Protocol • Internet Protocol • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • Any protocol
ICMP6	ICMP number (0–255). You are prompted for this parameter only if you specify ICMP6 for the Protocol parameter.

Table 14. Policy configuration parameters (Continued)

Parameter	Description
Direction	Direction of the data traffic to which to apply the policy: • In–Data entering the destination • Out–Data leaving the source
Priority	A number from -2147483647 to +214783647 that determines priority for this policy in the security policy database. The higher the number, the higher the priority.
Action	Processing to apply to data traffic: • Discard—Unconditionally disallow all inbound or outbound data traffic. • None—Allow all inbound or outbound data traffic without encryption or decryption. • Ipsec—Apply IP security to inbound and outbound data traffic.
Mode (Action=Ipsec)	IP security connection type. Mode can have one of the following values: • Transport—Encrypts the transport layer payload. • Tunnel—Encrypts the IP header and the transport layer payload. See the TunnelSource and TunnelDestination parameters.
TunnelSource (Mode=Tunnel)	IP address (version 4 or 6) of the tunnel source.
TunnelDestination (Mode=Tunnel)	IP address (version 4 or 6) of the tunnel destination. TunnelSource and TunnelDestination must use the same IP version address format.
ProtectionDesired (Action=Ipsec)	Type of IP security protection to apply: • AH—Authentication header. Protects against modifications to the data. See the ahRuleLevel parameter. • ESP—Encapsulating security payload. Protects against viewing the data. See the espRuleLevel parameter. • Both—Apply both AH and ESP protection. See the ahRuleLevel and espRuleLevel parameters.
ahRuleLevel (ProtectionDesired= ahRuleLevel or Both)	Rule level to apply for AH protection. You are prompted for this parameter only if you specify AH or Both for the ProtectionDesired parameter. • Default—Use the system wide default for the protocol. • Use—Use a security association if one is available. • Require—A security association is required whenever a packet is sent that is matched with the policy.
espRuleLevel (ProtectionDesired= ESP or Both)	Rule level to apply for ESP protection: • Default—use the system wide default for the protocol • Use—use a security association if one is available • Require—a security association is required whenever a packet is sent that matches the policy

delete [policy]

Deletes the policy given by [policy] from the Security Policy database. You must enter the Ipsec Save command afterwards to save your changes.

edit [policy]

Opens an edit session in which to change the configuration of an existing policy given by [policy].

list *[option]*

Displays the configuration for the policies given by [option]. If you omit [option], the command displays the configuration of all active policies. [option] can be one of the following:

[policy]

Displays the configuration for the policy given by [policy].

active

Displays the configuration for all active policies.

configured

Displays the configuration for all user-defined policies.

edited

Displays the configuration for all policies that have been modified, but not saved.

rename [policy_old] [policy_new]

Renames the policy given by [policy_old] to the policy given by [policy_new]. You must enter the Ipsec Save command afterwards to save your changes. Dynamic policies cannot be renamed.

Examples

The following is an example of the Ipsec Policy Create command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> ipsec edit
IBM8Gb (admin-ipsec) #> ipsec policy create h2h-sh-sp

  A list of attributes with formatting will follow.
  Enter a value or simply press the ENTER key to skip specifying a value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Required attributes are preceded by an asterisk.

  Value (press ENTER to not specify value, 'q' to quit):
    Description        (string value, 0-127 bytes)               :  Host-to-host: switch->host
   *SourceAddress      (hostname, IPv4, or IPv6 Address/[PrefixLength]):
                                                                fe80::2c0:ddff:fe03:d4c1
    SourcePort         (decimal value, 1-65535)                      :
   *DestinationAddress (hostname, IPv4, or IPv6 Address/[PrefixLength]):
                                                                 fe80::250:daff:feb7:9d02
    DestinationPort    (decimal value, 1-65535)                      :
   *Protocol           (decimal value, or keyword)
                         Allowed keywords
                           icmp, icmp6, ip4, tcp, udp or any           :  any
   *Direction          (1=in, 2=out)                                 :  2
    Priority           (value, -2147483647 to +214783647)            :
   *Action             (1=discard, 2=none, 3=ipsec)                  :  3
    Mode               (1=transport, 2=tunnel)                       :  2
   *TunnelSource       (IPv4, or IPv6 Address)                       :
                                                                 fe91::3d1:eecc:bf14:e5d2
   *TunnelDestination  (IPv4, or IPv6 Address)                       :
                                                                 fe91::361:ebcc:bfc8:0e13
   *ProtectionDesired  (select one, transport-mode only)
                         1=ah   Authentication Header
                         2=esp  Encapsulating Security Payload
                         3=both                                      :  2
   *espRuleLevel       (1=default, 2=use, 3=require)                 :  3

  The security policy has been created.
  This configuration must be saved with the 'ipsec save' command
  before it can take effect, or to discard this configuration
  use the 'ipsec cancel' command.
```

Key

Creates and manages public/private key pairs in the PKI database.

Authority

Admin. The List keyword does not require an Admin session.

Syntax

key
delete [key_name]
generate [key_name] size [size] *force*
import [key_name] [file_name] *force*
list *[key_name]*

Keywords

delete [key_name]

Deletes a public/private key pair from the PKI database.

generate [key_name] size [size] ***force***

Creates a public/private key pair with the name given by [key_name] of the size in bits given by [size]. The optional keyword Force overwrites an existing key pair with the same name. [size] can be one of the following:

1024

Creates a public/private key of 1,024 bits. This value is valid only when EncryptionMode=Legacy. For more information about EncryptionMode, see Table 41.

2048

Creates a public/private key of 2,048 bits

import [key_name] [file_name] ***force***

Imports the public/private key pair file given by [file_name] into the PKI database with the name given by [key_name]. The optional keyword Force overwrites an existing key pair with the same name. For EncryptionMode=Strict, keys must have a length of 2,048 or greater. For more information about the EncryptionMode service, see Table 41.

list ***[key_name]***

Displays detailed information about the public/private key pair given by [key_name]. If you omit [key_name], the command lists all key pairs in the PKI database.

Notes

For information about creating a certificate request, see the Certificate Generate Request command.

Examples

The following is an example of the Key Generate command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> key generate key1024 size 1024
```

The following is an example of the Key List command for key1024:

```
IBM8Gb #> key list key1024
  Key key1024:
    private key with:
    pubkey:    RSA 1024 bits
    keyid:     49:80:4c:aa:d3:c3:bc:c7:f5:b1:41:34:ce:71:48:1d:b9:b3:d9:f9
    subjkey:   f4:b6:b9:27:25:7a:5a:69:a0:9e:cf:14:cd:3c:88:e9:d5:b1:aa:4a
```

The following is an example of the Key List command:

```
IBM8Gb #> key list
  Installed Keys:
    key2048
    key1024
  * indicates key has a matching local certificate
```

Lip

Reinitializes the specified loop port.

Authority Admin session

Syntax **lip [port_number]**

Keywords **[port_number]**
The number of the port to be reinitialized. Ports are numbered beginning with 0.

Examples The following is an example of the Lip command:

```
IBM8Gb (admin) #> lip 2
```

Logout

Closes the CLI session.

Authority

None

Syntax

logout

Notes

You can also enter Control-D to close the CLI session.

Passwd

Changes a user account's password.

Authority

Admin account name and an Admin session to change another account's password; You can change you own password without an Admin session.

Syntax

passwd [account_name]

Keywords

[account_name]

The user account name. To change the password for an account name other than your own, you must open an Admin session with the account name `USERID`. If you omit [account_name], you will be prompted to change the password for the current account name.

Examples

The following is an example of the Passwd command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> passwd user2

      Press 'q' and the ENTER key to abort this command.

  account OLD password               : ********
  account NEW password (8-20 chars)  : ********

  please confirm account NEW password: ********
  password has been changed.
```

Ping

Initiates an attempt to communicate with another switch over an Ethernet network and reports the result.

Authority

None

Syntax

ping [ip_address]
[host_name]
[host_address]

Keywords

[host_name]

DNS host name of the switch you want to query. [host_name] is a character string of 2–125 characters made up of one or more subdomains delimited by periods (.). The following naming rules apply:

- Valid characters are alphanumeric characters, period (.), and hyphen (-).
- Each subdomain must be a minimum of two alphanumeric characters.
- Each subdomain must start and end with an alphanumeric character.
- A host name can end with a period (.).

[host_address]

IP address or DNS host name of the switch you want to query. Broadcast IP addresses, such as 255.255.255.255, are not valid.

Examples

The following is an example of a successful Ping command:

```
IBM8Gb #> ping 10.20.11.57
  Ping command issued. Waiting for response...
IBM8Gb #>
  Response successfully received from 10.20.11.57.
```

This following is an example of an unsuccessful Ping command:

```
IBM8Gb #> ping 10.20.11.57
  Ping command issued. Waiting for response...
  No response from 10.20.11.57. Unreachable.
```

Profile

Creates and modifies profiles with which to customize Call Home e-mail notification. A profile defines the event severity level at which to generate e-mails, e-mail subject and text, and e-mail recipients.

Authority

Admin session and a Callhome Edit session. For information about starting a Callhome Edit session, see the "Callhome" command on page 154.

Syntax

profile

copy [profile_source] [profile_destination]
create [profile]
delete [profile]
edit [profile]
rename [profile_old] [profile_new]

Keywords

copy [profile_source] [profile_destination]

Creates a new profile named [profile_destination] and copies the configuration into it from the profile given by [profile_source]. You must enter the Callhome Save command afterwards to save your changes. Neither [profile_source] nor [profile_destination] can be Tech_Support_Center.

create [profile]

Creates a profile with the name given by [profile]. A profile name must begin with a letter and be no longer than 32 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The Tech_Support_Center profile name is reserved. You must enter the Callhome Save command afterwards to save your changes. The Call Home database supports a maximum of 25 profiles. Table 15 describes the profile configuration parameters.

Table 15. Profile configuration parameters

Parameter	Description
Level	Event severity level at which to generate a Call Home e-mail message: • None–Generates e-mail messages for all events. • Warn–Generates e-mail messages for Warning, Critical, and Alarm events. • Critical–Generates e-mail messages for Critical and Alarm events. • Alarm–Generates e-mail messages for Alarm events only.
Format	Level of detail to be included in the e-mail message: • ShortText–includes switch and event information. • FullText–includes switch information, event information, Call Home contact information, and SNMP contact information. • Tsc1–includes switch and event information in a format intended for automated e-mail readers.
MaxSize	Maximum number of characters allowed in the e-mail message. Decreasing this parameter makes for easier reading on small display devices such as cell phones. The minimum is 650. The maximum and default is 100,000.
EmailSubject	E-mail subject of up to 64 characters

Table 15. Profile configuration parameters (Continued)

Parameter	Description
RecipientMail	Recipient e-mail addresses; maximum of 10 addresses. The format is *account@domain*.
CaptureEnabled	Enables (True) or disables (False) the data capture configuration only when creating the Tech_Support_Center profile. For more information about the data capture configuration, see the "Capture" command on page 157.

delete [profile]

Deletes the specified profile given by [profile] from the Call Home database. You must enter the Callhome Save command afterwards to save your changes.

edit [profile]

Opens an edit session in which to change the configuration of an existing profile given by [profile]. The Tech_Support_Center profile can be edited. For information about the profile parameters, see Table 15. The CaptureEnabled parameter is displayed only when modifying the Tech_Support_Center profile.

rename [profile_old] [profile_new]

Renames the profile given by [profile_old] to the profile given by [profile_new]. You must enter the Callhome Save command afterwards to save your changes.

Examples

The following is an example of the Profile Create command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> profile create profile_1
A list of attributes with formatting and default values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press ’q’ or ’Q’ and the ENTER key to do so.

Default Values:
  Level           Alarm
  Format          FullText
  MaxSize         100000
  EmailSubject    <undefined>
  RecipientEmail  (up to 10 entries allowed)

New Value (press ENTER to accept default value, 'q' to quit):
  Level           (Alarm,Critical,Warn,None)        :
  Format          (1=FullText, 2=ShortText, 3=Tsc1) :
  MaxSize         (decimal value, 650-100000)       :
  EmailSubject    (string, max=64 chars, N=None)    : Technical problem
  RecipientEmail  (ex: admin@company.com, N=None)
  1. <undefined>                                    : admin0@company.com

The profile has been created.
This configuration must be saved with the callhome save command
before it can take effect, or to discard this configuration
use the callhome cancel command.

IBM8Gb (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

The following is an example of the Profile Edit command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> callhome edit
IBM8Gb (admin-callhome) #> profile edit profile_1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    Level           Alarm
    Format          ShortText
    MaxSize         1000
    EmailSubject    Switch Problem
    RecipientEmail  (up to 10 entries allowed)
    1. john.smith@domain.com

  New Value (press ENTER to accept current value, 'q' to quit):
    Level           (Alarm,Critical,Warn,None)        :
    Format          (1=FullText, 2=ShortText, 3=Tsc1) : 1
    MaxSize         (decimal value, 650-100000)       :
    EmailSubject    (string, max=64 chars, N=None)    :
    RecipientEmail  (ex: admin@company.com, N=None)
    1. john.smith@domain.com                          :
    2. <undefined>                                    :

  The profile has been edited.
  This configuration must be saved with the 'callhome save' command
  before it can take effect, or to discard this configuration
  use the 'callhome cancel' command.

IBM8Gb (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Ps

Displays current system process information.

Authority

None

Syntax

ps

Examples

The following is an example of the Ps command:

```
IBM8Gb #> ps
PID  PPID %CPU %MEM     TIME     ELAPSED COMMAND
286   260  0.0  9.0 00:00:00       55:52 cns
287   260  0.0  9.0 00:00:00       55:52 ens
288   260  0.0  9.0 00:00:00       55:52 dlog
289   260  0.4  9.3 00:00:14       55:52 ds
290   260  0.4 12.4 00:00:14       55:52 mgmtApp
291   260  0.0  9.0 00:00:00       55:52 sys2swlog
297   260  0.0  9.3 00:00:02       55:50 diagAgent
336   260  0.0  9.1 00:00:00       55:44 fc2
337   260  0.0  9.3 00:00:00       55:44 nserver
338   260  0.0  9.2 00:00:00       55:44 mserver
339   260  0.0  9.7 00:00:03       55:44 PortApp
340   260  0.0  9.3 00:00:00       55:44 qfsApp
341   260  0.0  9.3 00:00:00       55:44 eport
342   260  0.0  9.3 00:00:00       55:44 zoning
484   260  0.1  9.2 00:00:04       55:38 snmpservicepath
506   260  0.0  9.5 00:00:00       55:37 util
507   260  0.0  9.1 00:00:00       55:37 port_mon
508   260  0.0  9.1 00:00:00       55:37 diagExec
485   260  2.7  1.3 00:01:31       55:38 snmpd
486   260  0.8  1.2 00:00:28       55:38 snmpmain
```

Quit

Closes the CLI session.

Authority

None

Syntax

quit

Notes

You can also enter Control-D to close the CLI session.

Reset

Resets the switch configuration parameters. If you omit the keyword, the default is Reset Switch.

Authority

Admin session

Syntax

reset
- auth
- callhome
- config *[config_name]*
- factory
- ike
- ipsec
- port [port_list]
- security
- services
- snmp
- switch (default)
- system
- zoning

Keywords

auth

Resets the server authentication configuration to the default values as described in Table 16.

callhome

Resets the Call Home database configuration to its default values as described in Table 17.

config *[config_name]*

Resets the configuration given by [config_name] to the factory default values for switch, port, port threshold alarm, and zoning configuration as described in Table 18 through Table 30. If [config_name] does not exist on the switch, a configuration with that name will be created. If you omit [config_name], the active configuration is reset. You must activate the configuration for the changes to take effect.

factory

Resets switch configuration, port configuration, port threshold alarm configuration, zoning configuration, SNMP configuration, system configuration, security configuration, RADIUS configuration, switch services configuration, and zoning to the factory default values as described in Table 18 through Table 30. The switch configuration is activated automatically.

ike

Resets the IKE database configurations to their default values.

ipsec

Resets the IP security database and IKE database configurations to their default values.

port [port_list]

Reinitializes one or more ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15.

security

Clears the security database and deactivates the active security set. The security configuration value, autosave, and fabric binding remain unchanged.

services

Resets the switch services configuration to the default values as described in Table 23.

snmp

Resets the SNMP configuration settings to the factory default values. For information about SNMP configuration default values, see Table 22.

switch

Resets the switch without a power-on self test. This is the default. This reset disrupts traffic and does the following:

- Activates the pending firmware.
- Closes all management sessions.
- Clears the event log. To save the event log before resetting, see the "Set Log" command on page 258.

To reset the switch with a power-on self test, see the "Hardreset" command on page 181. To reset the switch without disrupting traffic, see the "Hotreset" command on page 184.

system

Resets the system configuration settings to the factory default values as described in Table 24.

Notes:

Because this keyword changes network parameters, the workstation could lose communication with the switch.

zoning

Clears the zoning database and deactivates the active zone set. The zoning configuration parameters (InteropAutoSave, DefaultZone, DiscardInactive) remain unchanged. For information about the zoning configuration parameters, see Table 21.

Notes

The following tables specify the various factory default settings:

Enter the Show Setup Auth command to display RADIUS configuration and LDAP configuration values. Table 16 shows the default authentication configuration values.

Table 16. Authentication configuration defaults

Parameter	Default
DeviceAuthOrder	Local
UserAuthOrder	Local
TotalRadiusServers	1
TotalLdapServers	0
ServerIPAddress	10.0.0.1
ServerUDPPort	1812
DeviceAuthServer	False
UserAuthServer	False
AccountingServer	False
Timeout	2 seconds
Retries	0
SignPackets	False
UIDSearchAttr	UID
BindingMethod	Anonymous
AdminAttr	AuthorizedService
AdminValue	Administrative
Port	389

Enter the Show Setup Callhome command to display the Call Home service configuration values. Table 17 shows the default Call Home service configuration values.

Table 17. Call Home service configuration defaults

Parameters	**Default**
PrimarySMTPServerAddr	0.0.0.0
PrimarySMTPServerPort	25
PrimarySMTPServerEnabled	False
SecondarySMTPServerAddr	0.0.0.0
SecondarySMTPServerPort	25
SecondarySMTPServerEnabled	False
ContactEmailAddress	nobody@localhost.localdomain
PhoneNumber	<undefined>
StreetAddress	<undefined>
FromEmailAddress	nobody@localhost.localdomain
ReplyToEmailAddress	nobody@localhost.localdomain
ThrottleDupsEnabled	True

Enter the Show Config Switch command to display switch configuration values. Table 18 shows the default switch configuration values.

Table 18. Switch configuration defaults

Parameter	**Default**
TransparentMode	False
Admin State	Online
Broadcast Enabled	True
InbandEnabled	True
FDMIEnabled	True
FDMIEntries	1000
DefaultDomain ID	1 (0x Hex)
Domain ID Lock	False
Symbolic Name	IBM8Gb
R_A_TOV	10000
E_D_TOV	2000
Principal Priority	254
Configuration Description	Default Config
InteropMode	Standard

Enter the Show Config Port command to display port configuration values. Table 19 shows the default port configuration values.

Table 19. Port configuration defaults

Parameter	External Port Defaults (Ports 0, 15, 16, 17, 18, 19)	Internal Port Defaults (Ports 1–14)
Admin State	Online	Online
Link Speed	Auto	8 Gbps
Port Type	GL (SAN switch) TF (pass-thru)	F (SAN switch) TH (pass-thru)
PrimaryTFPortMap (pass-thru only)	Not applicable	1, 2 map to port 0 3, 4 map to port 15 5–7 map to port 16 8, 9 map to port 17 10, 11 map to port 18 12–14 map to port 19
BackupTFPortMap (pass-thru only)	Not applicable	1, 2 map to port 15 3–14 map to port 0
Symbolic Name	Portn, where n is the port number	Portn, where n is the port number
ALFairness	False	False
DeviceScanEnabled	True	True
ForceOfflineRSCN	False	False
ARB_FF	False	False
InteropCredit	0	0
ExtCredit	0	0
FANEnable	True	True
AutoPerfTuning	True	True
LCFEnable	False	False
MFSEnable	False	False
MSEnable	True	False
NoClose	False	False
IOStreamGuard	Disabled	Disabled
VIEnable	False	False
PDISCPingEnable	True	True

Enter Show Config Threshold command to display threshold alarm configuration values. Table 20 shows the default port threshold configuration values.

Table 20. Port threshold alarm configuration defaults

Parameter	Default
ThresholdMonitoringEnabled	False
CRCErrorsMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 25 1 10
DecodeErrorsMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 25 0 10
ISLMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 2 0 10
LoginMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 5 1 10
LogoutMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 5 1 10
LOSMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 100 5 10

Enter the Show Config Zoning command to display zoning configuration values. Table 21 shows the default zoning configuration values.

Table 21. Zoning configuration defaults

Parameter	Default
MergeAutoSave	True
DefaultZone	Allow
DiscardInactive	False

Enter the Show Setup SNMP command to display SNMP configuration values. Table 22 shows the default SNMP configuration values.

Table 22. SNMP configuration defaults

Parameter	Default
Contact	<syscontact undefined>
Location	<sysLocation undefined>
Description	IBM Flex System FC3171 8Gb SAN Switch
ObjectID	1.3.6.1.4.1.3873.1.33
Trap [1-5] Address	Trap 1: 10.0.0.254; Traps 2–5: 0.0.0.0
Trap [1-5] Port	162
Trap [1-5] Severity	Warning
Trap [1-5] Version	2
Trap [1-5] Enabled	False
ObjectID	1.3.6.1.4.1.3873.1.8
AuthFailureTrap	False
ProxyEnabled	True

Enter the Show Setup Services command to display switch service configuration values. Table 23 shows the default switch services configuration values.

Table 23. Switch services configuration defaults

Parameter	Default
EncryptionMode	Legacy
TelnetEnabled	False
SSH/sFTPEnabled	True
GUIMgmtEnabled	False
SSLEnabled	True
EmbeddedGUIEnabled (HTTP)	False
EmbeddedGUIEnabled (HTTPs)	True
NTPEnabled	False
CIMEnabled	True
FTPEnabled	False.
MgmtServerEnabled	True
CallHomeEnabled	True

Enter the Show Setup System Dns command to display the DNS host configuration. Table 24 shows the default DNS host configuration values.

Table 24. DNS host configuration defaults

Parameter	Default
DNSClientEnabled False	False
DNSLocalHostname	Undefined
DNSServerDiscovery	Static
DNSServer1Address	Undefined
DNSServer2Addres	Undefined
DNSServer3Address	Undefined
DNSSearchListDiscovery	Static
DNSSearchList1	Undefined
DNSSearchList2	Undefined
DNSSearchList3	Undefined
DNSSearchList4	Undefined
DNSSearchList5	Undefined

Enter the Show Setup System Ipv4 command to display the IPv4 Ethernet configuration. Table 25 shows the default IPv4 Ethernet configuration values.

Table 25. IPv4 Ethernet configuration defaults

Parameter	Default
EthIpv4NetworkEnable	True
EthIpv4NetworkDiscovery	Static
EthIpv4NetworkAddress	10.0.0.1
EthIpv4NetworkMask	255.0.0.0
EthIpv4GatewayAddress	10.0.0.254

Enter the Show Setup System Ipv6 command to display the IPv6 Ethernet configuration. Table 26 shows the default IPv6 Ethernet configuration values.

Table 26. IPv6 Ethernet configuration defaults

Parameter	Default
EthIpv6NetworkEnable	True
EthIpv6NetworkDiscovery	Static
EthIpv6NetworkAddress	Undefined
EthIpv6GatewayAddress	Undefined

Enter the Show Setup System Logging command to display the event logging configuration. Table 27 shows the default event logging configuration values.

Table 27. Event logging configuration defaults

Parameter	Default
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254

Enter the Show Setup System Ntp command to display the NTP configuration. Table 28 shows the default NTP configuration values.

Table 28. NTP configuration defaults

Parameter	Default
NTPClientEnabled	False
NTPServerDiscovery	Static
NTPServerAddress	10.0.0.254
NTPAuthEnabled	False

Enter the Show Setup System Timer command to display the timer configuration. Table 29 shows the default timer configuration values.

Table 29. Timer configuration defaults

Parameter	Default
AdminTimeout	30
InactivityTimeout	0

Enter the Show Config Security command to display security configuration values. Table 30 shows the default Call Home service configuration values.

Table 30. Security configuration defaults

Parameter	Default
AutoSave	True
FabricBindingEnabled	False
PortBindingEnabled	False

Security

Opens a Security Edit session in which to manage the security database on a switch. See the "Group" command on page 175 and the "Securityset" command on page 239.

Authority

Admin session. The keywords Active, History, Limits, and List are available without an Admin session.

Syntax

security
- active
- cancel
- clear
- edit
- history
- limits
- list
- restore
- save

Keywords

active

Displays the active security set, its groups, and group members. This keyword does not require an Admin session.

cancel

Closes a Security Edit session without saving changes. Use the Edit keyword to open a Security Edit session.

clear

Clears all inactive security sets from the volatile edit copy of the security database. This keyword does not affect the non-volatile security database. However, if you enter the Security Clear command followed by the Security Save command, the non-volatile security database will be cleared from the switch.

Notes:

The preferred method for clearing the security database from the switch is the Reset Security command.

edit

Initiates a Security Edit session in which to make changes to the security database. A Security Edit session enables you to use the Group and Securityset commands to create, add, and delete security sets, groups, and group members. To close a Security Edit session and save changes, enter the Security Save command. To close a Security Edit session without saving changes, enter the Security Cancel command.

history

Displays history information about the security database and the active security set including the account name that made changes and when those changes were made. This keyword does not require an Admin session.

limits

Displays the current totals and the security database limits for the number of security sets, groups, members per group, and total members. This keyword does not require an Admin session.

list

Displays all security sets, groups, and group members in the security database. This keyword does not require an Admin session.

restore

Restores the volatile security database with the contents of the non-volatile security database. If the AutoSave parameter is False, you can use this keyword to revert changes to the volatile security database that were propagated from another switch in the fabric through security set activation or merging fabrics. For information about the AutoSave parameter, see Table 30.

save

Saves the changes that have been made to the security database during a Security Edit session. Changes you make to any security set will not take effect until you activate that security set. For information about activating a security set, see the "Securityset" command on page 239.

Examples

The following is an example of the Security Active command:

```
IBM8Gb #> security active
  Active Security Information

  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

The following is an example of the Security History command:

```
IBM8Gb #> security history
  Active Database Information
  ---------------------------
  SecuritySetLastActivated/DeactivatedBy  Remote
  SecuritySetLastActivated/DeactivatedOn  day month date time year
  Database Checksum                   00000000

  Inactive Database Information
  -----------------------------
  ConfigurationLastEditedBy           admin@IB-session11
  ConfigurationLastEditedOn           day month date time year
  Database Checksum                   00007558
```

The following is an example of the Security Limits command:

```
IBM8Gb #> security limits
  Security Attribute   Maximum   Current   [Name]
  ------------------   -------   -------   ------
  MaxSecuritySets      4         1
  MaxGroups            16        2
  MaxTotalMembers      1000      19
  MaxMembersPerGroup   1000
                                 4         group1
                                 15        group2
```

The following is an example of the Security List command:

```
IBM8Gb #> security list
  Active Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  No active securityset defined.

  Configured Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

Securityset

Manages security sets in the security database.

Authority

Admin session and a Security Edit session. For information about starting a Security Edit session, see the "Security" command on page 236. The Active, Groups, and List keywords are available without an Admin session. You must close the Security Edit session before using the Activate and Deactivate keywords.

Syntax

securityset
activate [security_set]
active
add [security_set] [group_list]
copy [security_set_source] [security_set_destination]
create [security_set]
deactivate
delete [security_set]
groups [security_set]
list
remove [security_set] [group]
rename [security_set_old] [security_set_new]

Keywords

activate [security_set]

Activates the security set given by [security_set]. This keyword deactivates the active security set. Close the Security Edit session using the Security Save or Security Cancel command before using this keyword.

active

Displays the name of the active security set. This keyword is available to without an Admin session.

add [security_set] [group_list]

Adds one or more groups given by [group_list] to the security set given by [security_set]. Use a <space> to delimit multiple group names in [group_list]. A security set can have a maximum of three groups with no more than one group of each group type.

copy [security_set_source] [security_set_destination]

Creates a new security set named [security_set_destination] and copies into it the membership from the security set given by [security_set_source].

create [security_set]

Creates the security set with the name given by [security_set]. A security set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The security database supports a maximum of 4 security sets.

deactivate

Deactivates the active security set. Close the Security Edit session before using this keyword.

delete [security_set]

Deletes the security set given by [security_set]. If the specified security set is active, the command is suspended until the security set is deactivated.

groups [security_set]

Displays all groups that are members of the security set given by [security_set]. This keyword is available without an Admin session.

list

Displays a list of all security sets. This keyword is available without an Admin session.

remove [security_set] [group]

Removes a group given by [group] from the security set given by [security_set]. If [security_set] is the active security set, the group will not be removed until the security set has been deactivated.

rename [security_set_old] [security_set_new]

Renames the security set given by [security_set_old] to the name given by [security_set_new].

Notes

For information about creating and managing groups, see the "Group" command on page 175.

Examples

The following is an example of the Securityset Active command

```
IBM8Gb #> securityset active
  Active SecuritySet Information
  ------------------------------
  ActiveSecuritySet alpha
  LastActivatedBy  Remote
  LastActivatedOn  day month date time year
```

The following is an example of the Securityset Groups command

```
IBM8Gb #> securityset groups alpha
  Current list of Groups for SecuritySet: alpha
  -------------------------------------
  group1 (ISL)
  group2 (Port)
```

The following is an example of the Securityset List command

```
IBM8Gb #> securityset list
Current list of SecuritySets
----------------------------
  alpha
  beta
```

Set Alarm

Controls the display of alarms in the session output stream or clears the alarm log.

Authority

Admin session for the Clear keyword. Otherwise, none.

Syntax

set alarm [option]

Keywords

[option]
[option] can be one of the following:

clear
Clears the alarm log history. This value requires an Admin session.

on
Enables the display of alarms in the session output stream.

off
Disables the display of alarms in the session output stream. Disabling the display of alarms in the output stream allows command scripts to run without interruption.

Examples

The following is an example of the Set Alarm command:

```
IBM8Gb #> set alarm on
```

Set Audit Archive

Collects all audit log entries and stores the result in a new file named *audit.log* that is maintained in switch memory. For information about downloading the *audit.log* file, see "Creating and downloading an audit log file" on page 126.

Authority

Admin session

Syntax

set audit archive

Set Beacon

Enables or disables the flashing of the Logged-In LEDs for the purpose of locating a switch.

Authority

None

Syntax

set beacon [state]

Keywords

[state]

[state] can be one of the following:

on

Enables the flashing beacon.

off

Disables the flashing beacon.

Examples

The following is an example of the Set Beacon command:

```
IBM8Gb #> set beacon on
```

Set Config Port

Sets the port configuration parameters for one or more ports. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command.

Authority

Admin session and a Config Edit session

Syntax

set config port ***[port_number]***
or
set config ports
internal
external

Keywords

port ***[port_number]***

Initiates an edit session in which to change configuration parameters for the port number given by [port_number]. If you omit [port_number], the system begins with port 0 and proceeds in order through the last port. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter "q" to end the configuration for one port, or "qq" to end the configuration for all ports. Table 31 describes the port configuration parameters.

Notes:

- For external ports (0, 15, 16, 17, 18, 19), all port parameters apply. For internal ports (1–14), only the port state setting is configurable.
- For information about port numbering and mapping, see Appendix A.

ports ***[port_set]***

Initiates an editing session in which to change configuration parameters (except symbolic port name) for the set of all external ports based on external port 0, or the set of all internal ports based on internal port 1, depending on the value given by [port_set]. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter "q" to end the configuration. Table 31 describes the port configuration parameters. [port_set] can have the following values:

external

The configurations for all external ports (0, 15, 16, 17, 18, 19) are made based on the configuration of external port 0.

internal

The configuration for all internal ports (1–14) are made based on the configuration of internal port 1.

Table 31. Port configuration parameters

Parameter	Description
AdminState	Port administrative state: • Online – Activates and prepares the port to send data. This is the default. • Offline – Prevents the port from receiving signal and accepting a device login. • Diagnostics – Prepares the port for testing and prevents the port from accepting a device login. • Down – Disables the port by removing power from the port lasers.
LinkSpeed	Transmission speed: 1-Gbps, 2-Gbps, 4-Gbps, 8-Gbps, or Auto. The default is Auto. 8-Gbps SFPs do not support the 1-Gbps setting. Setting a port to 1-Gbps that has an 8-Gbps SFP will down the port.
PortType (full fabric)	Full-fabric modules support the following port types: GL (default), G, F, FL, and Donor. The Donor port type disables the port and makes the buffer credits available to other ports. See the ExtCredit port configuration parameter.
PortType (pass-thru)	Pass-thru modules support the following port types: • TF—Transparent Fabric port connects to Fibre Channel switches that support NPIV. This is the default for external ports. • TH—Transparent Host port connects to an HBA. TH_Ports are mapped to TF_Ports. All internal ports are TH_Ports.
PrimaryTFPortMap (pass-thru only)	Primary mapping for TH_Ports. The mapping consists of a list of TF_Port numbers (delimited by spaces) that are assigned to pass traffic to and from the TH_Port. If you specify N, the TH_Port is unmapped, effectively disconnecting the TH_Port from the fabric. The default primary mapping is as follows: • Ports 1, 2 map to port 0 • Ports 3, 4 map to port 15 • Ports 5–7 map to port 16 • Ports 8, 9 map to port 17 • Ports 10, 11 map to port 18 • Ports 12–14 map to port 19 If all TF_Ports in the primary mapping fail, the backup port mapping is used (BackupTFPortMap). When a list is specified, the switch distributes the host NPIV logins across the TF ports in a round-robin fashion for better performance.

Table 31. Port configuration parameters (Continued)

Parameter	Description
BackupTFPortMap (pass-thru only)	Backup mapping for TH_Ports. The mapping consists of a list of TF_Port numbers (delimited by spaces) that are assigned to pass traffic to and from the TH_Port when all TF_Ports in the primary mapping (PrimaryTFPortMap) have failed. If you specify N, the TH_Port is unmapped, effectively disconnecting the TH_Port from the fabric. The default secondary mapping is as follows: • Ports 1, 2 map to port 15 • Ports 3–14 map to port 0 When a list is specified, the switch distributes the host NPIV logins across the TF ports in a round-robin fashion for better performance.
SymbolicPortName	Descriptive name for the port. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Port n where n is the port number. This parameter can be changed only with the Set Config Port command.
ALFairness	Arbitration loop fairness. Enables (True) or disables (False) the switch's priority to arbitrate on the loop. The default is False.
DeviceScanEnabled	Enables (True) or disables (False) the scanning of the connected device for FC-4 descriptor information during login. The default is True.
ForceOfflineRSCN	Enables (False) or disables (True) the immediate transmission of RSCN messages when communication between a port and a device is interrupted. If enabled, the RSCN message is delayed for 200 ms for locally attached devices and 400 ms for devices connected through other switches. The default is False. This parameter is ignored if IOStreamGuard is enabled.
ARB_FF	Send ARB_FF (True) instead of IDLEs (False) on the loop. The default is False.
InteropCredit	Interoperability credit. The number of buffer-to-buffer credits per port. 0 means the default is unchanged. Default buffer-to-buffer credits are 16 per port. Changing interoperability credits is necessary only for E_Ports that are connected to non-FC-SW-2-compliant switches. Contact your authorized maintenance provider for assistance in using this feature.
ExtCredit	Extended credits. The number of port buffer credits that this port can acquire from donor ports. The default is 0.
FANEnable	Fabric address notification. Enables (True) or disables (False) the communication of the FL_Port address, port name, and node name to the logged-in NL_Port. The default is True.

Table 31. Port configuration parameters (Continued)

Parameter	Description
AutoPerfTuning	Automatic performance tuning for FL_Ports only. The default is True. • If AutoPerfTuning is enabled (True) and the port is an FL_Port, MFSEnable is automatically enabled. LCFEnable and VIEnable are overridden to False. • If AutoPerfTuning is disabled (False), MFSEnable, LCFEnable, and VIEnable retain their original values.
LCFEnable	Link control frame preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) preferred routing of frames with R_CTL = 1100 (Class 2 responses). The default is False. Enabling LCFEnable will disable MFSEnable.
MFSEnable	Multi-Frame Sequence bundling. This parameter appears only if AutoPerfTuning is False. Prevents (True) or allows (False) the interleaving of frames in a sequence. The default is False. Enabling MFSEnable disables LCFEnable and VIEnable.
VIEnable	Virtual Interface (VI) preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) VI preference routing. The default is False. Enabling VIEnable will disable MFSEnable.
MSEnable	Management server enable. Enables (True) or disables (False) management server on this port. The default is True.
NoClose	Loop circuit closure prevention. Enables (True) or disables (False) the loop's ability to remain in the open state indefinitely. True reduces the amount of arbitration on a loop when there is only one device on the loop. The default is False.
IOStreamGuard	I/O Stream Guard. Enables or disables the suppression of RSCN messages. IOStreamGuard can have the following values: • Enable – Suppresses the reception of RSCN messages from other ports for which IOStreamGuard is enabled. • Disable – Allows free transmission and reception of RSCN messages. • Auto – Suppresses the reception of RSCN messages when the port is connected to an initiator device with a QLogic HBA. For older QLogic HBAs, such as the QLA2200, the DeviceScanEnabled parameter must also be enabled. The default is Auto.
PDISCPingEnable	Enables (True) or disables (False) the transmission of ping messages from the switch to all devices on a loop port. The default is True.

Examples

The following is an example of the Set Config Port command for external port 0 on a full-fabric switch:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config port 0
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  0
  ------------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down)   [Online]
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto)   [Auto  ]
  PortType         (GL / G / F / FL / Donor)                      [GL    ]
  SymPortName      (string, max=32 chars)                         [Port0 ]
  ALFairness       (True / False)                                 [False ]
  DeviceScanEnable (True / False)                                 [True  ]
  ForceOfflineRSCN (True / False)                                 [False ]
  ARB_FF           (True / False)                                 [False ]
  InteropCredit    (decimal value, 0-255)                         [0     ]
  ExtCredit        (dec value, increments of 15, non-loop only)   [0     ]
  FANEnable        (True / False)                                 [True  ]
  AutoPerfTuning   (True / False)                                 [False ]
  LCFEnable        (True / False)                                 [False ]
  MFSEnable        (True / False)                                 [False ]
  VIEnable         (True / False)                                 [False ]
  MSEnable         (True / False)                                 [True  ]
  NoClose          (True / False)                                 [False ]
  IOStreamGuard    (Enable / Disable / Auto)                      [Disable]
  PDISCPingEnable  (True / False)                                 [True  ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Port command for internal port 1 on a full-fabric switch:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config port 1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  1
  ------------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down)   [Online]
offline
  LinkSpeed        (2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto)            [2Gb/s ]
  PortType         (F / Donor)                                    [F     ]
  SymPortName      (string, max=32 chars)                         [Port1 ]
  ALFairness       (True / False)                                 [False ]
  DeviceScanEnable (True / False)                                 [True  ]
  ForceOfflineRSCN (True / False)                                 [False ]
  ARB_FF           (True / False)                                 [False ]
  InteropCredit    (decimal value, 0-255)                         [0     ]
  ExtCredit        (dec value, increments of 15, non-loop only)   [0     ]
  FANEnable        (True / False)                                 [True  ]
  AutoPerfTuning   (True / False)                                 [False ]
  LCFEnable        (True / False)                                 [False ]
  MFSEnable        (True / False)                                 [False ]
  VIEnable         (True / False)                                 [False ]
  MSEnable         (True / False)                                 [True  ]
  NoClose          (True / False)                                 [False ]
  IOStreamGuard    (Enable / Disable / Auto)                      [Auto  ]
  PDISCPingEnable  (True / False)                                 [True  ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
IBM8Gb (admin-config) #> config save
IBM8Gb (admin-config) #> config activate
```

The following is an example of the Set Config Port command for external port 0 on a pass-thru module:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config port 0
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  0
  -----------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down)   [Online]
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto)   [Auto  ]
  PortType         (TH / TF)                                      [TF    ]
  SymPortName      (string, max=32 chars)                         [Port0 ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Port command for internal port 1 on a pass-thru module:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config port 1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  1
  -----------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down)   [Online]
offline
  LinkSpeed        (2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto)            [2Gb/s ]
  PrimaryTFPortMap (decimal value for port, N=no mapping)         [0     ]
  BackupTFPortMap  (decimal value for port, N=no mapping)         [15    ]
  SymPortName      (string, max=32 chars)                         [Port1 ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
IBM8Gb (admin-config) #> config save
IBM8Gb (admin-config) #> config activate
```

Set Config Security

Configures the security database for the automatic saving of changes to the active security set and fabric binding. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command.

Authority

Admin session and a Config Edit session

Syntax

set config security

This command initiates an editing session in which to change the security database configuration. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” or "Q" to end the editing session. Table 32 describes the security configuration parameters.

Table 32. Security configuration parameters

Parameter	Description
AutoSave	Enables (True) or disables (False) the saving of changes to active security set in the switch’s permanent memory. The default is True.
FabricBindingEnabled	Enables (True) or disables (False) the configuration and enforcement of fabric binding on all switches in the fabric. Fabric binding associates switch worldwide names with a domain ID in the creation of ISL groups.

Examples

The following is an example of the Set Config Security command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config security
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  FabricBindingEnabled  (True / False)     [False]
  AutoSave              (True / False)     [True ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Set Config Security Portbinding

Configures port binding.

Authority

Admin session and a Config Edit session

Syntax

set config security portbinding [port_number]

Keywords

[port_number]
Initiates an editing session in which to change the port binding configuration for the port given by [port_number]. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” or "Q" to end the editing session. Table 33 describes the Set Config Security Port parameters.

Table 33. Port binding configuration parameters

Parameter	Description
PortBindingEnabled	Enables (True) or disables (False) port binding for the port given by [port_number].
WWN	Worldwide port name for the port/device that is allowed to connect to the port given by [port_number].

Examples

The following is an example of the Set Config Security Portbinding command:

```
IBM8Gb #> admin start
IBM8Gb (admin) config edit
IBM8Gb (admin-config) #> set config security portbinding 1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PortBindingEnabled (True / False)[False] true
  WWN                (N=None / WWN)[None ] 10:00:00:c0:dd:00:b9:f9
  WWN                (N=None / WWN)[None ] 10:00:00:c0:dd:00:b9:f8
  WWN                (N=None / WWN)[None ] n

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Set Config Switch

Sets the switch configuration parameters. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command.

Authority

Admin session and a Config Edit session

Syntax

set config switch

This command initiates an editing session in which to change switch configuration settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Table 34 describes the switch configuration parameters.

Table 34. switch configuration parameters

Parameter	Description
TransparentMode	Transparent mode control for the 20-Port full-fabric switch that is in transparent mode.
AdminState	Switch administrative state. • Online—Activates and prepares the ports to send data. This is the default. • Offline—Prevents the ports from receiving signal and accepting a device login. • Diagnostics—Prepares the ports for testing and prevents the ports from accepting a device login.
BroadcastEnabled	Broadcast. Enables (True) or disables (False) forwarding of broadcast frames. The default is True.
InbandEnabled	Inband management. Enables (True) or disables (False) the ability to manage the switch over an ISL. The default is True.
FDMIEnabled	Fabric Device Monitoring Interface. Enables (True) or disables (False) the monitoring of target and initiator device information. The default is True.
FDMIEntries	The number of device entries to maintain in the FDMI database. Enter a number from 0–1000. The default is 1000.
DefaultDomainID	Default domain ID. The default is 1.
DomainIDLock	Prevents (True) or allows (False) dynamic reassignment of the domain ID. The default is False.
SymbolicName	Descriptive name for the switch. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is IBM8Gb.
PrincipalPriority	The priority used in the FC-SW-2 principal switch selection algorithm. 1 is high, 255 is low. The default is 254.
ConfigDescription	Switch configuration description. The configuration description can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Default Config.

Examples

The following is an example of the Set Config Switch command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
IBM8Gb (admin-config) #> set config switch

  A list of attributes with formatting and default values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  TransparentMode     (True / False)                          [False         ]
  AdminState          (1=Online, 2=Offline, 3=Diagnostics)    [Online        ]
  BroadcastEnabled    (True / False)                          [True          ]
  InbandEnabled       (True / False)                          [True          ]
  FDMIEnabled         (True / False)                          [True          ]
  FDMIEntries         (decimal value, 0-1000)                 [1000          ]
  DefaultDomainID     (decimal value, 1-239)                  [2             ]
  DomainIDLock        (True / False)                          [False         ]
  SymbolicName        (string, max=32 chars)                  [IBM8Gb        ]
  PrincipalPriority   (decimal value, 1-255)                  [254           ]
  ConfigDescription   (string, max=64 chars)                  [Default Config]
```

Set Config Threshold

Sets the port alarm threshold parameters by which the switch monitors port performance and generates alarms. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command.

Authority

Admin session and a Config Edit session

Syntax

set config threshold
Initiates a configuration session by which to generate and log alarms for selected events. The system displays each event, its triggers, and sampling window one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Table 35 describes the port alarm threshold parameters.

Table 35. Port Alarm threshold parameters

Parameter	Description
Threshold Monitoring Enabled	Master enable/disable parameter for all events. Enables (True) or disables (False) the generation of all enabled event alarms. The default is False.
CRCErrorsMonitoringEnabled DecodeErrorsMonitoringEnabled ISLMonitoringEnabled LoginMonitoringEnabled LogoutMonitoringEnabled LOSMonitoringEnabled	The event type enable/disable parameter. Enables (True) or disables (False) the generation of alarms for each of the following events: • CRC errors • Decode errors • ISL connection count • Device login errors • Device logout errors • Loss-of-signal errors
Rising Trigger	The event count above which a rising trigger alarm is logged. The switch will not generate another rising trigger alarm for that event until the count descends below the falling trigger and again exceeds the rising trigger.
Falling Trigger	The event count below which a falling trigger alarm is logged. The switch will not generate another falling trigger alarm for that event until the count exceeds the rising trigger and descends again below the falling trigger.
Sample Window	The time in seconds in which to count events.

Notes

The switch will down a port if an alarm condition is not cleared within three consecutive sampling windows (by default 30 seconds). Reset the port to bring it back online. An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling trigger.

Examples

The following is an example of the Set Config Threshold command:

```
IBM8Gb #> admin start
IBM8Gb  (admin) #> config edit
IBM8Gb (admin-config) #> set config threshold
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

ThresholdMonitoringEnabled     (True / False)              [False     ]
CRCErrorsMonitoringEnabled     (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
DecodeErrorsMonitoringEnabled  (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
ISLMonitoringEnabled           (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [2         ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
LoginMonitoringEnabled         (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
LogoutMonitoringEnabled        (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
 LOSMonitoringEnabled           (True / False)             [True      ]
  RisingTrigger                (decimal value, 1-1000)     [100       ]
  FallingTrigger               (decimal value, 0-1000)     [5         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

Finished configuring attributes.
This configuration must be saved (see config save command) and activated (see
config activate command) before it can take effect.
To discard this configuration use the config cancel command.
```

Set Config Zoning

Configures the zoning database. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command.

Authority

Admin session and a Config Edit session

Syntax

set config zoning

Initiates an editing session in which to change the zoning database configuration. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Table 36 lists the zoning configuration parameters.

Table 36. Zoning configuration parameters

Parameter	Description
MergeAutoSave	Enables (True) or disables (False) the saving of changes to active zone set in the switch's non-volatile zoning database.The default is True. Disabling the MergeAutosave parameter can be useful to prevent the propagation of zoning information when experimenting with different zoning schemes. However, leaving the MergeAutosave parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the MergeAutosave parameter should be enabled in a production environment.
DefaultZone	Enables (Allow) or disables (Deny) communication among ports/devices that are not defined in the active zone set. The default is Allow.
DiscardInactive	Enables (True) or disables (False) the discarding of all inactive zone sets from that zoning database. Inactive zone sets are all zone sets except the active zone set. The default is False.

Examples

The following is an example of the Set Config Zoning command.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> config edit
   The config named default is being edited.
IBM8Gb (admin-config) #> set config zoning
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

  MergeAutoSave        (True / False)  [True ]
  DefaultZone          (Allow / Deny)  [Allow]
  DiscardInactive      (True / False)  [False]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Set Log

Specifies the events to record in the event log and display on the screen. You determine what events to record in the switch event log using the Component, Level, and Port keywords. You determine what events are automatically displayed on the screen using the Display keyword. Alarms are always displayed on the screen.

Authority

Admin session

Syntax

set log
archive
clear
component [filter_list]
display [filter]
level [filter]
port [port_list]
restore
save
start (default)
stop

Keywords

archive

Collects all log entries and stores the result in new file named *logfile* that is maintained in switch memory where it can be downloaded using FTP. To download *logfile*, open an FTP session, log in with account name/password of "images" for both, and type "get logfile".

clear

Clears all log entries.

component [filter_list]

Specifies one or more components given by [filter_list] to monitor for events. A component is a firmware module that is responsible for a particular portion of switch operation. Use a <space> to delimit values in the list. [filter_list] can be one or more of the following:

All

Monitors all components. To maintain optimal switch performance, do not use this setting with the Level keyword set to Info.

Eport

Monitors all E_Ports.

Mgmtserver

Monitors management server status.

Nameserver

Monitors name server status.

None

Monitor none of the component events.

Port

Monitors all port events.

SNMP

Monitors all SNMP events.

Switch

Monitors switch management events.

Zoning

Monitors zoning conflict events.

display [filter]

Specifies the log events to automatically display on the screen according to the event severity levels given by [filter]. [filter] can be one of the following values:

Critical

Critical severity level events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.

Warn

Warning severity level events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

Info

Informative severity level events. The informative level describes routine events associated with a normal fabric.

None

Specifies no severity levels for display on the screen.

level [filter]

Specifies the severity level given by [filter] to use in monitoring and logging events for the specified components or ports. [filter] can be one of the following values:

Critical

Monitors critical events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action. This is the default severity level.

Warn

Monitors warning and critical events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

Info

Monitors informative, warning, and critical events. The informative level describes routine events associated with a normal fabric.

Notes:

Logging events at the Info severity level can deplete switch resources because of the high volume of events.

None

Monitors none of the severity levels.

port [port_list]

Specifies one or more ports to monitor for events. Choose one of the following values:

[port_list]

Specifies the port or ports to monitor. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15.

All

Specifies all ports.

None

Disables monitoring on all ports.

restore

Restores and saves the port, component, and level settings to the default values.

save

Saves the log settings for the component, severity level, port, and display level. These settings remain in effect after a switch reset. The log settings can be viewed using the Show Log Settings command. To export log entries to a file, use the Set Log Archive command.

start

Starts the logging of events based on the Port, Component, and Level keywords assigned to the current configuration. The logging continues until you enter the Set Log Stop command.

stop

Stops logging of events.

Notes

In addition to critical, warn, and informative severity levels, the highest event severity level is alarm. The alarm level describes events that are disruptive to the administration or operation of a fabric and require administrator intervention. Alarms are always logged and always displayed on the screen.

Examples

The following is an example of the Set Log Archive command:

```
IBM8Gb: user1> admin start
IBM8Gb (admin): user1> set log archive
```

The following is an example of the Set Log Restore command:

```
IBM8Gb: user1> admin start
IBM8Gb (admin): user1> set log restore
```

Set Pagebreak

Specifies how much information is displayed on the screen at a time. This command is useful for disabling pagebreaks to allow command scripts to run without interruption.

Authority

None

Syntax

pagebreak [state]

Keywords

[state]

[state] can be one of the following:

on

Limits the display of information to 20 lines at a time. The page break function affects the following commands:

- Alias (List, Members)
- Show (Alarm, Log)
- Zone (List, Members)
- Zoneset (List, Zones)
- Zoning (Active, List)

off

Allows continuous display of information without a break. This is the default.

Examples

The following is an example of the Set Pagebreak command:

```
IBM8Gb #> set pagebreak on
IBM8Gb #> help
                                 General Help
                                 ------------

admin           ADMIN_OPTIONS
config          CONFIG_OPTIONS
create          CREATE_OPTIONS
date            [MMDDhhmmCCYY]
exit
feature         FEATURE_OPTIONS
firmware        install
hardreset
help            HELP_OPTIONS
history
hotreset
image           IMAGE_OPTIONS
logout
passwd          [USER_ACCT_NAME]
ping            IP_ADDR
ps
quit
reset           RESET_OPTIONS
set             SET_OPTIONS
show            SHOW_OPTIONS
shutdown
test            TEST_OPTIONS

        Press any key for more help or 'q' to end this list...
uptime
user            USER_OPTIONS
whoami
```

Set Port

Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. This command also clears port counters and moves port licenses from one port to another.

Notes:

For external ports (0, 15, 16, 17, 18, 19), all port parameters apply. For internal ports (1–14), only the port state setting is configurable.

Authority

Admin session

Syntax

set port clear
or
set port [port_number]
bypass [alpa]
clear
enable
speed [transmission_speed]
state [state]

Keywords

[port_number]

Specifies the port. Ports are numbered beginning with 0. For information about port numbering and mapping, see Appendix A.

bypass [alpa]

Sends a Loop Port Bypass (LPB) to a specific Arbitrated Loop Physical Address (ALPA) or to all ALPAs on the arbitrated loop. [alpa] can be a specific ALPA or the keyword ALL to choose all ALPAs.

clear

Clears the counters on all ports or the port given by [port_number].

enable

Sends a Loop Port Enable (LPE) to all ALPAs on the arbitrated loop.

speed [transmission_speed]

Specifies the transmission speed for the specified port. Choose one of the following port speed values:

1Gb/s

One gigabit per second.

2Gb/s

Two gigabits per second.

4Gb/s

Four gigabits per second.

8Gb/s

Eight gigabits per second.

Auto

The port speed is automatically detected.

state [state]

Specifies one of the following administrative states for the specified port:

Online

Activates and prepares the port to send data.

Offline

Prevents the port from receiving signal and accepting a device login.

Diagnostics

Prepares the port for testing and prevents the port from accepting a device login.

Down

Disables the port by removing power from the port lasers.

Examples

The following is an example of the Set Port State command:

```
IBM8Gb: user1> admin start
IBM8Gb (admin): user1> set port state down
```

Set Setup Auth

Configures RADIUS and LDAP server authentication parameters on the switch.

Authority

Admin session

Syntax

set setup auth
Prompts you in a line-by-line fashion to configure RADIUS and LDAP authentication parameters.

- Table 37 describes the initial configuration parameters that define the device authentication order, user authentication order, and the number of RADIUS and LDAP servers to configure.
- Table 38 describes the RADIUS server configuration parameters.
- Table 39 describes the LDAP server configuration parameters.

Table 37. Initial configuration parameters

Entry	Description
DeviceAuthOrder	Authenticator priority for devices: • Local: Authenticate devices using only the local security database. This is the default. • Radius: Authenticate devices using only the security database on the RADIUS server.
UserAuthOrder	Authenticator priority for user accounts: • Local: Authenticate users using only the local security database. This is the default. • Ldap: Authenticate users using only the security database on the LDAP server. • Radius: Authenticate users using only the security database on the RADIUS server.
TotalRadiusServers	Number of RADIUS servers to configure during this session. Setting TotalRadiusServers to 0 disables all RADIUS authentication. The default is 0.
TotalLdapServers	Number of LDAP servers to configure during this session. Setting TotalLdapServers to 0 disables all LDAP authentication. The default is 0.

Table 38. RADIUS server configuration parameters

Entry	Description
ServerIPAddress	IP address of the RADIUS server. The default is 10.0.0.1.
ServerUDPPort	User Datagram Protocol (UDP) port number on the RADIUS server. The default is 1812.
DeviceAuthServer	Enable (True) or disable (False) this server for device authentication. The default is False.
UserAuthServer	Enable (True) or disable (False) this server for user account authentication. A user authentication RADIUS server requires a secure management connection (SSL). The default is True.

Table 38. RADIUS server configuration parameters (Continued)

Entry	Description
AccountingServer	Enable (True) or disable (False) this server for auditing of activity during a user session. When enabled, user activity is audited whether UserAuthServer is enabled or not.The default is False. The accounting server UDP port number is the ServerUDPPort value plus 1 (default 1813).
Timeout	Number of seconds to wait to receive a response from the RADIUS server before timing out. The default is 2.
Retries	Number of retries after the first attempt to establish communication with the RADIUS server fails. The default is 0.
SignPackets	Enable (True) or disable (False) the use of sign packets to protect the RADIUS server packet integrity. The default is False.
Secret	32-byte hex string or 16-byte ASCII string used as a password for authentication purposes between the switch and the RADIUS server.

Table 39. LDAP server configuration parameters

Entry	Description
RootDN	The distinguished name of the superuser for the directory information tree. RootDN can be 1–64 characters.
UIDSearchAttr	User identifier search attribute that is expected in the directory information tree. UIDSearchAttr can be 1–24 characters.
BindingMethod	Specifies that the directory information tree bindings are anonymous (1=Anonymous) or require authentication (2=ClientAuth). The default is 1=Anonymous.
ClientDN	Distinguished name to use when BindingMethod is 2=ClientAuth. Access is granted to the directory information tree based on the ClientDN and Password. ClientDN can be 1–64 characters.
Password	Password associated with ClientDN when BindingMethod is 2=ClientAuth. Password can be 1–16 characters.
AdminAttr	Attribute in the directory information tree that grants administrative access to the device. AdminAttr can be 1–24 characters. The default is AuthorizedService.
AdminValue	Value to be matched when AdminAttr is consulted to determine if administrative privileges are to be granted. AdminValue can be 1–24 characters. The default is Administrative.
ServerIPAddress	IP address of the LDAP server. The default is 10.0.0.1.
Port	Number of the port through which to communicate with the LDAP server. The default is 389.

Note:
The Lenovo Flex System FC3171 8 Gb SAN Switch uses secure LDAP (LDAP over SSL–LDAPS) to connect to the configured LDAP servers, regardless of the LDAP server's port number. The LDAP servers must be properly configured to support LDAPS connections to perform LDAP authentication.

Examples

The following is an example of the Set Setup Auth command to configure one RADIUS server and one LDAP server.

```
IBM8Gb (admin) #> set setup auth

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the
attributes
  for the category being processed, press 'q' or 'Q' and the ENTER key to do
so.
  If you wish to terminate the configuration process completely, press 'qq' or
  'QQ' and the ENTER key to do so.

  PLEASE NOTE:
  -----------
  * SSL must be enabled in order to configure RADIUS and/or LDAP
  * user authentication.  SSL can be enabled in this mode or
  * via the 'set setup services' command.

  Current Values:
    DeviceAuthOrder     Local
    UserAuthOrder       Local
    TotalRadiusServers  1
    TotalLdapServers    0

  New Value (press ENTER to not specify value, 'q' to quit):

  * Specify authentication ordering using the strings 'Local', 'Radius' and/or
  * 'Ldap'.  For example, for Radius authentication first followed by Local
  * authentication, specify 'RadiusLocal'

    DeviceAuthOrder     ('Radius' 'Local')        :
    UserAuthOrder       ('Radius' 'Ldap' 'Local') :  ldap
    TotalRadiusServers  decimal value, 0-5        :  1
    TotalLdapServers    decimal value, 0-4        :  1

  Current Values:

  Radius Server 1
    ServerIPAddress   10.1.1.1
    ServerUDPPort     1812
    DeviceAuthServer  False
    UserAuthServer    False
    AccountingServer  True
    Timeout           2
    Retries           0
    SignPackets       False
    Secret            ********

  New Value (press ENTER to not specify value, 'q' to quit):

  Radius Server 1
    ServerIPAddress   (hostname, IPv4, or IPv6 Address) :
    ServerUDPPort     (decimal value)                   :
    DeviceAuthServer  (True / False)                    :
    UserAuthServer    (True / False)                    :
    AccountingServer  (True / False)                    :
    Timeout           (decimal value, 1-30 secs)        :
    Retries           (decimal value, 1-3, 0=None)      :
```

```
  SignPackets       (True / False)                    :
  Secret            (1-63 characters, recommend 22+)  :

Current Values:

Ldap Configuration
  RootDN         root DN ;""
  UIDSearchAttr  jlkj
  BindingMethod  Anonymous
  ClientDN       client ,."";,"
  Password       ********
  AdminAttr      sdasd
  AdminValue     sdsds

New Value (press ENTER to not specify value, 'q' to quit):

Ldap Configuration
  RootDN         (1-64)                       :
  UIDSearchAttr  (1-24)                       :
  BindingMethod  (1=Anonymous, 2=ClientAuth) :
  ClientDN       (1-64)                       :
  Password       (1-16)                       :
  AdminAttr      (1-24)                       :
  AdminValue     (1-24)                       :

Current Values:

Ldap Server 1
  ServerIPAddress  10.0.0.1
  Port             389

New Value (press ENTER to not specify value, 'q' to quit):

Ldap Server 1
  ServerIPAddress  (hostname, IPv4, or IPv6 Address) :
  Port             (decimal value)                   :

Do you want to save and activate this auth setup? (y/n): [n]
```

Set Setup Callhome

Configures the Call Home database for managing e-mail notifications of fabric problems.

Authority

Admin session

Syntax

set setup callhome
Prompts you in a line-by-line fashion to configure the Call Home database. Table 40 describes the Call Home configuration fields.

Table 40. Call Home service configuration settings

Entry	Description
PrimarySMTPServerAddr	IP address or DNS host name of the primary SMTP server. The default is 0.0.0.0.
PrimarySMTPServerPort	Service port number that the primary SMTP server is monitoring for SMTP agents. The default is 25.
PrimarySMTPServerEnabled	Enables (True) or disables (False) the primary SMTP server. The default is False.
SecondarySMTPServerAddr	IP address or DNS host name of the secondary SMTP server. The default is 0.0.0.0.
SecondarySMTPServerPort	Service port number that the secondary SMTP server is monitoring for SMTP agents. The default is 25.
SecondarySMTPServerEnabled	Enable (True) or disable (False) the secondary SMTP server. The default is False.
ContactEmailAddress	E-mail address of the person to be notified to respond to the e-mail message. The format is *account@domain*. This information is included in the e-mail message when the profile format is FullText.
PhoneNumber	Contact phone number to be included in the e-mail message text. This information is included in the e-mail message when the profile format is FullText.
StreetAddress	Contact street address to be included in the e-mail message text. This information is included in the e-mail message when the profile format is FullText.
FromEmailAddress	E-mail address that is defined as the sending address in the *From:* field of the e-mail message. The format is *account@domain*. This field is required. Undeliverable messages are returned to this address unless overridden by the ReplayToEmailAddress parameter.
ReplyToEmailAddress	E-mail address that is to receive replies to the out-bound e-mail message. The format is *account@domain*. This parameter overrides the FromEmailAddress parameter.

Table 40. Call Home service configuration settings (Continued)

Entry	Description
ThrottleDupsEnabled	Enables (True) or disables (False) the throttling of duplicate e-mail messages in the message queue. When enabled, duplicate e-mail messages that enter the queue within 15 seconds of the original are suppressed. The original message is sent with a report of the number of suppressed duplicates.

Notes

- The Call Home service must be active to support Call Home e-mail notification. See the "Set Setup Services" command on page 273.
- The primary, secondary, or both SMTP servers must be properly addressed and enabled on the switch to activate Call Home e-mail notification. If both SMTP servers are enabled, the primary server is active.
- The switch will reroute Call Home e-mail messages to the secondary SMTP server if the primary should become unavailable. Primary and secondary identities do not change upon transfer of control.
- Call Home profiles determine the events, conditions, and e-mail recipients of Call Home e-mail messages. For information about creating Call Home profiles, see the "Profile" command on page 220.

Examples

The following is an example of the Set Setup Callhome command:

```
IBM8Gb (admin) #> set setup callhome

A list of attributes with formatting and current values will follow. Enter a
new value or simply press the ENTER key to accept the current value. If you
wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.
If either the Primary or Secondary SMTP Servers are enabled, the
FromEmailAddress attribute must be configured or the switch will not attempt
to deliver messages.
Current Values:

  PrimarySMTPServerAddr      0.0.0.0
  PrimarySMTPServerPort      25
  PrimarySMTPServerEnable    False
  SecondarySMTPServerAddr    0.0.0.0
  SecondarySMTPServerPort    25
  SecondarySMTPServerEnable  False
  ContactEmailAddress        nobody@localhost.localdomain
  PhoneNumber                <undefined>
  StreetAddress              <undefined>
  FromEmailAddress           nobody@localhost.localdomain
  ReplyToEmailAddress        nobody@localhost.localdomain
  ThrottleDupsEnabled        True

New Value (press ENTER to accept current value, 'q' to quit):
  PrimarySMTPServerAddr      (IPv4, IPv6, or hostname)  :
  PrimarySMTPServerPort      (decimal value)            :
  PrimarySMTPServerEnable    (True / False)             :
  SecondarySMTPServerAddr    (IPv4, IPv6, or hostname)  :
  SecondarySMTPServerPort    (decimal value)            :
  SecondarySMTPServerEanble  (True / False)             :
  ContactEmailAddress        (ex: admin@company.com)    :
  PhoneNumber                (ex: +1-800-123-4567)      :
  StreetAddress              (include all address info) :
  FromEmailAddress           (ex: bldg3@company.com)    :
  ReplyToEmailAddress        (ex: admin3@company.com)   :
  ThrottleDupsEnabled        (True / False)             :

  Do you want to save and activate this Callhome setup? (y/n):
```

Set Setup Services

Configures services on the switch.

Authority

Admin session

Syntax

set setup services

Prompts you in a line-by-line fashion to enable or disable switch services. Table 41 describes the switch service parameters. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Notes:

Use caution when disabling SSH/sFTPEnabled and GUIMgmtEnabled; it is possible to disable all Ethernet access to the switch.

Table 41. Switch services settings

Entry	Description
EncryptionMode	Applies Legacy (default) or Strict security affecting encryption algorithms, key lengths, and Diffie-Hellman groups. Legacy mode uses encryption algorithms with a strength of 80 bits or greater, and keys with a length of 1,024 or greater, thus excluding the following: • IP security association encryption: des-cbc • 512-bit public/private keys Strict mode uses encryption algorithms with a strength of 112 bits or greater, and keys with a length of 2,048 or greater, thus excluding the following: • IP security association authentication: hmac-md5, aes-xcbc-mac encryption • IP security association encryption: des-cbc, blowfish-cbc, twofish-cbc encryption • IKE peer/policy integrity: md5_96, aes_xcbc_96 encryption • Diffie-Hellman groups: 1, 2, 5 • 1,024-bit public/private keys For more information, see the command Notes.
TelnetEnabled	Enables (True) or disables (False) the ability to manage the switch over an unsecured Telnet connection. Disabling this service is not recommended. The default is False.
SSH/sFTPEnabled	Enables (True) or disables (False) Secure Shell (SSH) and secure FTP (sFTP) connections to the switch. SSH secures the remote connection to the switch. To establish a secure remote connection, your workstation must use an SSH client. The default is True.
GUIMgmtEnabled	Enables (True) or disables (False) out-of-band management of the switch with QuickTools, the Application Programming Interface, SNMP, and SMI-S. The default is False.

Table 41. Switch services settings (Continued)

Entry	Description
SSLEnabled	Enables (True) or disables (False) secure SSL connections for management applications including QuickTools, Application Programming Interface, and SMI-S. The default is True. • To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation. • This service must be enabled to authenticate users through a RADIUS server or an LDAP server. • Enabling SSL automatically creates a security certificate on the switch. • To disable SSL when using a user authentication RADIUS or LDAP server, the RADIUS or LDAP server authentication order must be local.
EmbeddedGUIEnabled (HTTP)	Enables (True) or disables (False) the QuickTools embedded management application over a nonsecure connection. QuickTools enables you to point at a switch with an Internet browser and manage the switch. The default is False.
EmbeddedGUIEnabled (HTTPs)	Enables (True) or disables (False) the QuickTools embedded management application over a secure connection. QuickTools enables you to point at a switch with an internet browser and manage the switch. The default is True.
NTPEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) which allows the synchronizing of switch and workstation dates and times with an NTP server. This helps to prevent invalid SSL certificates and timestamp confusion in the event log. The default is False. This parameter is the master control for the Set Setup System command parameter, NTPClientEnabled. The default is False.
CIMEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use SMI-S.
FTPEnabled	Enables (True) or disables (False) the File Transfer Protocol (FTP) for transferring files rapidly between the workstation and the switch. The default is False.
MgmtServerEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use GS-3 Management Server (MS). This parameter is the master control for the Set Config Port command parameter, MSEnable. The default is True.
CallHomeEnabled	Enables (True) or disables (False) the Call Home service which controls e-mail notification. The default is True.

Notes

- At startup, the switch assesses IP security associations, IKE peers, IKE policies, certificates, and keys against the Encryption Mode service. Under Strict mode, if these elements use excluded encryption algorithms, key lengths, or Diffie-Hellman groups, the switch applies the configurations unchanged, but generates an alarm indicating the conflict. To resolve the alarm, you must reconfigure the association, peer, policy, certificate, or key to comply with Strict mode limits.
- After changing to EncryptionMode=Strict, external clients may not be able to connect to the switch if they do not support the same encryption algorithms. Upgrade the following applications as needed:
  - openssl
  - SSH clients
  - SNMPv3 clients
  - SMI-S/CIM clients
  - LDAP/RADIUS servers
  - Web browsers/HTTPs clients
  - sFTP, HTTPs servers
- Before you can use QuickTools in Strict mode, you must enable Transport Layer Security (TLS) 1.2 in the Internet browser and in Java® 2 Runtime Environment 8. For more information, see *Lenovo Flex System FC3171 8 Gb SAN Switch QuickTools User's Guide*.

Examples

The following is an example of the Set Setup Services command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> set setup services

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PLEASE NOTE:
  -----------
  * Further configuration may be required after enabling a service.

  * If services are disabled, the connection to the switch may be lost.

  * When enabling SSL, please verify that the date/time settings
    on this switch and the workstation from where the SSL connection
    will be started match, and then a new certificate may need to be
    created to ensure a secure connection to this switch.

  EncryptionMode           (1=Legacy, 2=Strict) [Legacy ]
  TelnetEnabled                 (True / False)  [False]
  SSH/sFTPEnabled               (True / False)  [True]
  GUIMgmtEnabled                (True / False)  [False]
  SSLEnabled                    (True / False)  [True]
  EmbeddedGUIEnabled (HTTP)     (True / False)  [False]
  EmbeddedGUIEnabled (HTTPs)    (True / False)  [True]
  NTPEnabled                    (True / False)  [True]
  CIMEnabled                    (True / False)  [True]
  FTPEnabled                    (True / False)  [False]
  MgmtServerEnabled             (True / False)  [True]
  CallHomeEnabled               (True / False)  [True]
  SLPEnabled                    (True / False)  [True]

  Do you want to save and activate this services setup? (y/n): [n]
```

Set Setup SNMP

Configures SNMP on the switch.

Authority

Admin session

Syntax

set setup snmp
common
trap [trap_number]

Keywords

common
Prompts you in a line-by-line fashion to change SNMP configuration parameters that are common for all traps. For each parameter, enter a new value or press ENTER to accept the current value. To configure common parameters and trap parameters, omit the keyword. Table 42 describes the common SNMP configuration parameters.

Table 42. SNMP common configuration settings

Entry	Description
Contact	Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters excluding #, semicolon (;), and comma (,). The default is undefined. This value is also passed to the Call Home service configuration
Location	Specifies the name of the switch location. The name can be up to 64 characters excluding #, semicolon (;), and comma (,). The default is undefined. This value is also passed to the Call Home service configuration
ReadCommunity	Read community password that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The read community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is "public".
WriteCommunity	Write community password that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The write community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is "private".
AuthFailureTrap	Enables (True) or disables (False) the generation of traps in response to trap authentication failures. The default is False.
ProxyEnabled	Enables (True) or disables (False) SNMP communication with other switches in the fabric. The default is True.

trap [trap_number]

Prompts you in a line-by-line fashion to change SNMP trap parameters for the trap number given by [trap_number]. [trap_number] can be 1–5. For each parameter, enter a new value or press ENTER to accept the current value. To configure common parameters and trap parameters, omit the keyword. Table 43 describes the SNMP trap parameters.

Table 43. SNMP trap configuration settings

Parameter	Description
Trap*n*Enabled	Enables (True) or disables (False) the SNMP trap.
Trap*n*Address	Workstation IP address or DNS host name to which SNMP traps are sent. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0. Addresses, other than 0.0.0.0, for all traps must be unique.
Trap*n*Port	Workstation port to which SNMP traps are sent. Valid workstation port numbers are 1–65535. The default is 162.
Trap*n*Severity	Severity level to use when monitoring trap events. The values are: • 1=unknown • 2=emergency • 3=alert • 4=critical • 5=error • 6=warning • 7=notify • 8=info • 9=debut • 10=mark The default is Warning.
Trap*n*Version	SNMP version (1, 2, or 3) to use in formatting the trap. The default is 2.
TrapnUser	SNMP version 3 trap user name. The user name can be up to 32 characters excluding #, semicolon (;), and comma (,).
Trap*n*Community	Trap community password that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The trap community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “public”.

Examples

The following is an example of the Set Setup SNMP Common command:

```
IBM8Gb (admin) #> set setup snmp common

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    Contact          True
    Location         <sysContact undefined>
    ReadCommunity    <sysContact undefined>
    WriteCommunity   public
    AuthFailureTrap  private
    ProxyEnabled     True

  New Value (press ENTER to not specify value, 'q' to quit):
    Contact          (True / False)         :
    Location         (string, max=64 chars) :
    ReadCommunity    (string, max=64 chars) :
    WriteCommunity   (string, max=32 chars) :
    AuthFailureTrap  (string, max=32 chars) :
    ProxyEnabled     (True / False)         :

  Do you want to save and activate this snmp setup? (y/n): [n]
```

The following is an example of the Set Setup SNMP Trap command:

```
IBM8Gb (admin) #> set setup snmp trap 1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    Trap1Enabled    True
    Trap1Address    10.20.33.181
    Trap1Port       5001
    Trap1Severity   info
    Trap1Version    2
    Trap1User       user1
    Trap1Community  northdakota

  New Value (press ENTER to not specify value, 'q' to quit):
    Trap1Enabled    (True / False)                    :
    Trap1Address    (hostname, IPv4, or IPv6 Address) :
    Trap1Port       (decimal value, 1-65535)          :
    Trap1Severity   (select a severity level)
                    1=unknown     6=warning
                    2=emergency   7=notify
                    3=alert       8=info
                    4=critical    9=debug
                    5=error       10=mark             :
    Trap1Version    (1 / 2 / 3)                       :
    Trap1User       (For V3 traps, max-32 chars)      :
    Trap1Community  (string, max=32 chars)            :

  Do you want to save and activate this snmp setup? (y/n): [n]
```

Set Setup System

Configures the network, logging, NTP server, and timer configurations on the switch.

Authority

Admin session

Syntax

set setup system
dns
ipv4
ipv6
logging
ntp
timers

Keywords

dns
Prompts you in a line-by-line fashion to DNS host name configuration settings described in Table 44. To configure all system parameters, omit the keyword. For each parameter, enter a new value or press the Enter key to accept the current value.

Table 44. DNS host name configuration parameters

Parameter	Description
DNSClientEnabled	Enables (True) or disables (False) the DNS client.
DNSLocalHostname	Name of local DNS server
DNSServerDiscovery	DNS server boot method: 1 – Static, 2 – DHCP, 3 – DHCP version 6. The default is 1 – Static.
DNSServer1Address DNSServer2Address DNSServer3Address	IP addresses of up to three DNS servers.
DNSSearchListDiscovery	DNS search list discovery method: • Static
DNSSearchList1 DNSSearchList2 DNSSearchList3 DNSSearchList4 DNSSearchList5	A suffix that is appended to unqualified host names to extend the DNS search. You can specify up to five search-lists (or suffixes).

ipv4
Prompts you in a line-by-line fashion to change the switch IPv4 Ethernet configuration parameters described in Table 45. To configure all system parameters, omit the keyword. For each parameter, enter a new value or press ENTER to accept the current value.

Notes:
Changing the IP address will terminate all Ethernet management sessions.

Table 45. IP version 4 Ethernet configuration parameters

Entry	Description
EthIPv4NetworkEnable	Enables (True) or disables (False) the IP version 4 interface. The default is True.
EthIPv4NetworkDiscovery	Ethernet boot method: 1 - Static, 2 - Bootp, 3 - DHCP, 4 - RARP. The default is 1 - Static.
EthIPv4NetworkAddress	Ethernet IP address. The default is 10.0.0.1.
EthIPv4NetworkMask	Ethernet IP subnet mask address. The default is 255.0.0.0.
EthIPv4GatewayAddress	Ethernet address gateway. The default is 10.0.0.254

ipv6
Prompts you in a line-by-line fashion to change the switch IP version 6 Ethernet configuration parameters described in Table 46. To configure all system parameters, omit the keyword. For each parameter, enter a new value or press the Enter key to accept the current value.

Notes:
Changing the IP address will terminate all Ethernet management sessions.

Table 46. IP version 6 Ethernet configuration parameters

Entry	Description
EthIPv6NetworkEnable	Enables (True) or disables (False) the IP version 6 interface. The default is True.
EthIPv6Discovery	Ethernet boot method: 1 – Static, 2 – DHCPv6, 3 – Ndp. The default is 1 - Static.
EthIPv6NetworkAddress	Ethernet IP address
EthIPv6NetworkMask	Ethernet IP subnet mask address.
EthIPv6GatewayAddress	Ethernet IP address gateway.

logging

Prompts you in a line-by-line fashion to change the event logging configuration parameters described in Table 47. To configure all system parameters, omit the keyword. For each parameter, enter a new value or press the Enter key to accept the current value.

Table 47. Event logging configuration parameters

Parameter	Description
RemoteLogEnabled	Enables (True) or disables (False) the recording of the switch event log on a remote host that supports the syslog protocol. The default is False.
RemoteLogHostAddress	The IP address or DNS host name of the host that will receive the switch event log information if remote logging is enabled. The default is 10.0.0.254.

ntp

Prompts you in a line-by-line fashion to change the NTP server configuration parameters described in Table 48. To configure all system parameters, omit the keyword. For each parameter, enter a new value or press ENTER to accept the current value.

Table 48. NTP server configuration parameters

Parameter	Description
NTPClientEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) client on the switch. This client enables the switch to synchronize its time with an NTP server. This feature supports NTP version 4 and is compatible with version 3. An Ethernet connection to the server is required and you must first set an initial time and date on the switch. The synchronized time becomes effective immediately. The default is False.
NTPServerDiscovery	Ethernet boot method: 1—Static, 2—DHCP, 3—DHCPv6. The default is 1—Static.
NTPServerAddress	The IP address or DNS host name of the NTP server from which the NTP client acquires the time and date. The default is 10.0.0.254.
NTPAuthEnabled	Enables (True) or disables (False) a secure connection with an NTP server. The default is False.
NTPAuthKey	The NTP shared secret to be used to encrypt communication with the NTP server when NTPAuthEnabled is True. The shared secret can be an alphanumeric string of up to 32 characters.
NTPAuthKeyIndex	The NTP shared secret index number. The index number is an integer from 1–65535.

timers

Prompts you in a line-by-line fashion to change the timer configuration parameters described in Table 49. To configure all system parameters, omit the keyword. For each parameter, enter a new value or press the Enter key to accept the current value.

Table 49. Timer configuration parameters

Parameter	Description
AdminTimeout	Amount of time in minutes the switch waits before terminating an idle Admin session. Zero (0) disables the time out threshold. The default is 30, the maximum is 1440.
InactivityTimeout	Amount of time in minutes the switch waits before terminating an idle command line interface session. Zero (0) disables the time out threshold. The default is 10, the maximum is 1440.

Examples

The following is an example of the Set Setup System Dns command:

```
IBM8Gb (admin) #> set setup system dns
A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    DNSClientEnabled        False
    DNSLocalHostname        <undefined>
    DNSServerDiscovery      Static
    DNSServer1Address       <undefined>
    DNSServer2Address       <undefined>
    DNSServer3Address       <undefined>
    DNSSearchListDiscovery  Static
    DNSSearchList1          <undefined>
    DNSSearchList2          <undefined>
    DNSSearchList3          <undefined>
    DNSSearchList4          <undefined>
    DNSSearchList5          <undefined>

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    DNSClientEnabled        (True / False)              :
    DNSLocalHostname        (hostname)                  :
    DNSServerDiscovery      (1=Static, 2=Dhcp, 3=Dhcpv6) :
    DNSServer1Address       (IPv4, or IPv6 Address)     :
    DNSServer2Address       (IPv4, or IPv6 Address)     :
    DNSServer3Address       (IPv4, or IPv6 Address)     :
    DNSSearchListDiscovery  (1=Static, 2=Dhcp, 3=Dhcpv6) :
    DNSSearchList1          (domain name)               :
    DNSSearchList2          (domain name)               :
    DNSSearchList3          (domain name)               :
    DNSSearchList4          (domain name)               :
    DNSSearchList5          (domain name)               :

  Do you want to save and activate this system setup? (y/n): [n]
```

The following is an example of the Set Setup System Ipv4 command:

```
IBM8Gb (admin) #> set setup system ipv4

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    EthIPv4NetworkEnable    True
    EthIPv4NetworkDiscovery Static
    EthIPv4NetworkAddress   10.20.116.133
    EthIPv4NetworkMask      255.255.255.0
    EthIPv4GatewayAddress   10.20.116.1

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    EthIPv4NetworkEnable    (True / False)                      :
    EthIPv4NetworkDiscovery (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp) :
    EthIPv4NetworkAddress   (dot-notated IP Address)            : 10:20:30:40
    EthIPv4NetworkMask      (dot-notated IP Address)            : 255.0.0.0
    EthIPv4GatewayAddress   (dot-notated IPv4 Address)          : 10.20.30.254

  Do you want to save and activate this system setup? (y/n): [n] y
```

The following is an example of the Set Setup System Ipv6 command:

```
IBM8Gb (admin) #> set setup system ipv6

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    EthIPv6NetworkEnable    False
    EthIPv6Discovery        Static
    EthIPv6NetworkAddress   <undefined>
    EthIPv6GatewayAddress   <undefined>

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    EthIPv6NetworkEnable    (True / False)                    :
    EthIPv6Discovery        (1=Static, 2=Dhcpv6, 3=Ndp)       :
    EthIPv6NetworkAddress   (IPv6 Address/Mask Length format) :
    EthIPv6GatewayAddress   (IPv6 Address)                    :

  Do you want to save and activate this system setup? (y/n): [n]
```

The following is an example of the Set Setup System Logging command:

```
IBM8Gb (admin) #> set setup system logging

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    RemoteLogEnabled        False
    RemoteLogHostAddress    10.0.0.254

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    RemoteLogEnabled        (True / False)                    :
    RemoteLogHostAddress    (hostname, IPv4, or IPv6 Address) :

  Do you want to save and activate this system setup? (y/n): [n]
```

The following is an example of the Set Setup System Ntp command:

```
IBM8Gb (admin):#> set setup system ntp

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    NTPClientEnabled        False
    NTPServerDiscovery      Static
    NTPServerAddress        10.20.10.10
    NTPAuthEnabled          False
    NTPAuthKey
    NTPAuthKeyIndex

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    NTPClientEnabled        (True / False)                    : True
    NTPServerDiscovery      (1=Static, 2=Dhcp, 3=Dhcpv6)      :
    NTPServerAddress        (hostname, IPv4, or IPv6 Address) : 10.20.3.4
    NTPAuthEnabled          (True / False)                    : True
    NTPAuthKey              (string, max=31 chars)            : **********
    NTPAuthKeyIndex         (dec value 1-65535)               : 1

  Do you want to save and activate this system setup? (y/n): [y]
```

The following is an example of the Set Setup System Timers command:

```
IBM8Gb (admin) #> set setup system timers

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Current Values:
    AdminTimeout            30
    InactivityTimeout       0

  New Value (press ENTER to accept current value, 'q' to quit):
    AdminTimeout            (dec value 0-1440 minutes, 0=never) :
    InactivityTimeout       (dec value 0-1440 minutes, 0=never) :

  Do you want to save and activate this system setup? (y/n): [n]
```

Set Switch State

Changes the administrative state for all ports on the switch. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a switch configuration.

Authority

Admin session

Syntax

set switch state [state]

Keywords

[state]

[state] can be one of the following:

online

Activates and prepares the ports to send data. This is the default.

offline

Prevents the ports from receiving signal and accepting a device login.

diagnostics

Prepares the ports for testing and prevents each port from accepting a device login. When you leave the diagnostics state, the switch automatically resets.

Examples

The following is an example of the Set Switch command:

```
IBM8Gb #>admin start
IBM8Gb (admin) #>set switch state offline
```

Set Timezone

Specifies the time zone for the switch and the workstation. The default is Universal Time (UTC) also known as Greenwich Mean Time (GMT). This keyword prompts you to choose a region, then a subregion to specify the time zone.

Authority

Admin session

Syntax

set timezone

Examples

The following is an example of the Set Timezone command:

```
IBM8Gb (admin) #> set timezone
 Africa                                America
 Antarctica                            Asia
 Atlantic                              Australia
 CET                                   EET
 Etc                                   Europe
 Extended                              Indian
 MET                                   Pacific
 UTC                                   WET

        Press ENTER for more options or 'q' to make a selection.

 America/Adak                          America/Anchorage
 America/Anguilla                      America/Antigua
 America/Araguaina                     America/Argentina
 America/Aruba                         America/Asuncion
 America/Bahia                         America/Barbados
 America/Belem                         America/Belize
 America/Boa_Vista                     America/Bogota
 America/Boise                         America/Cambridge_Bay
 America/Campo_Grande                  America/Cancun
 America/Caracas                       America/Cayenne
 America/Cayman                        America/Chicago
 America/Chihuahua                     America/Coral_Harbour
 America/Costa_Rica                    America/Cuiaba
 America/Curacao                       America/Danmarkshavn
 America/Dawson                        America/Dawson_Creek
 America/Denver                        America/Detroit
 America/Dominica                      America/Edmonton
 America/Eirunepe                      America/El_Salvador
 America/Fortaleza                     America/Glace_Bay
 America/Godthab                       America/Goose_Bay

        Press ENTER for more options or 'q' to make a selection.
q
  Enter selection (or 'q' to quit): america/north_dakota
  America/North_Dakota/Center
  Enter selection (or 'q' to quit): america/north_dakota/center
```

Show About

Displays an introductory set of information about operational attributes of the switch. This command is equivalent to the Show Version command.

Authority

None

Syntax

show about

Notes

Table 50 describes the entries in the Show About command display.

Table 50. Show About display entries

Entry	Description
SystemDescription	Switch system description
HostName	DNS host name
EthIPv4NetworkAddress	External Ethernet port IP address, version 4
Eth1IPv4NetworkAddress	Internal Ethernet port IP address, version 4
EthIPv6NetworkAddress	External Ethernet port IP address, version 6
Eth1IPv6NetworkAddress	Internal Ethernet port IP address, version 6
MacAddress	MAC address for Eth0
Mac1Address	MAC address for Eth1
SwitchUUID	Switch universal unique identifier
WorldWideName	Switch worldwide name
SerialNumber	Switch serial number
SymbolicName	Switch symbolic name
ActiveSWVersion	Firmware version
ActiveTimestamp	Date and time that the firmware was activated
POSTStatus	Results of the Power-on Self Test
LicensedExernalPorts	Number of licensed external ports
LicensedInternalPorts	Number of licensed internal ports
SwitchMode	Full fabric indicates that the switch operates with the standard Fibre Channel port types: G, GL, F, FL, E. Transparent indicates the switch operates as a pass-thru module with port types TF and TH.

Examples

The following is an example of the Show About command:

```
IBM8Gb #> show about

       ************************************************
       *                                              *
       *       Command Line Interface SHell  (CLISH)  *
       *                                              *
       ************************************************

       SystemDescription   IBM Flex System FC3171 8Gb SAN Switch
       HostName            hsb5802-2
       EthIPv4NetworkAddr  10.20.125.47
       Eth1IPv4NetworkAddr 10.20.3.12
       EthIPv6NetworkAddr  fe80::2c0:ddff:fe01:6f27
       Eth1IPv6NetworkAddr fe80::2c0:ddff:fe01:6f28
       MACAddress          00:c0:dd:01:6f:27
       MAC1Address         00:c0:dd:01:6f:28
       SwitchUUID          20202020202020202020202020202020
       WorldWideName       10:00:00:c0:dd:01:6f:27
       SerialNumber        1029E00021
       SymbolicName        IBM8Gb
       ActiveSWVersion     V9.1.0.9.32
       ActiveTimestamp     Wed Aug  3 14:02:30 2011
       POSTStatus          Passed
       LicensedExternalPorts 6
       LicensedInternalPorts 14
       SwitchMode          Full Fabric
```

Show Alarm

Displays the alarm log and session output stream display setting.

Authority

None

Syntax

show alarm
settings

Keywords

settings
Displays the status of the parameter that controls the display of alarms in the session output stream. This parameter is set using the Set Alarm command.

Notes

The alarm log is cleared when the switch is reset or power cycled.

Examples

The following is an example of the Show Alarm Settings command:

```
IBM8Gb #> show alarm settings

  Current settings for alarm
  --------------------------
  display  ON
```

Show Audit

Displays the contents of the audit logs.

Authority

None

Syntax

show audit
archive
[number]

Keywords

archive

Displays all messages in the audit log in chronological order. If you omit this keyword, the command displays the most recent 250 audit log entries.

[number]

Displays the most recent number of audit log messages given by [number].

Examples

The following is an example of the Show Audit command:

```
IBM8Gb> show audit
[Fri Jan 30 16:03:23.824 UTC
2015][AU][0000.0000][sshd][[QL-00001]pam_unix(sshd:session): session opened
for user admin by (uid=0)]
[Fri Jan 30 16:03:23.957 UTC 2015][AU][0000.02E6][None][IP 10.20.200.230 User
admin@OB-session7 user session established.]
[Fri Jan 30 16:03:24.169 UTC 2015][AU][0000.0033][None][IP 10.20.200.230 User
admin@OB-session7 Admin Start]
[Fri Jan 30 16:03:25.164 UTC 2015][AU][0000.0043][None][IP 10.20.200.230 User
admin@OB-session7 Reset switch post]
[Fri Jan 30 16:03:25.165 UTC 2015][AU][0000.0042][None][IP 10.20.200.230 User
admin@OB-session7 Reset switch]
[Fri Jan 30 16:03:28.184 UTC 2015][AU][0000.02E7][None][IP 127.0.0.1-36119
user cim@OB-session1 user session has been closed]
[Mon Feb 02 11:41:49.939 UTC
2015][AU][0000.0000][sshd][[QL-00001]pam_unix(sshd:session): session opened
for user admin by (uid=0)]
[Mon Feb 02 11:41:50.108 UTC 2015][AU][0000.02E6][None][IP 10.20.200.230 User
admin@OB-session10 user session established.]
[Mon Feb 02 11:41:50.293 UTC 2015][AU][0000.0033][None][IP 10.20.200.230 User
admin@OB-session10 Admin Start]
[Mon Feb 02 11:41:50.319 UTC 2015][AU][0000.02A1][None][IP 10.20.200.230 User
admin@OB-session10 Port 12 temporary admin state set to Online]
[Mon Feb 02 11:41:50.335 UTC 2015][AU][0000.0034][None][IP 10.20.200.230 User
admin@OB-session10 Admin End]
[Mon Feb 02 11:41:50.380 UTC 2015][AU][0000.0033][None][IP 10.20.200.230 User
admin@OB-session10 Admin Start]
[Mon Feb 02 11:41:50.406 UTC 2015][AU][0000.02A1][None][IP 10.20.200.230 User
admin@OB-session10 Port 13 temporary admin state set to Online]
[Mon Feb 02 11:41:50.423 UTC 2015][AU][0000.0034][None][IP 10.20.200.230 User
admin@OB-session10 Admin End]
[Mon Feb 02 11:41:50.475 UTC 2015][AU][0000.0033][None][IP 10.20.200.230 User
admin@OB-session10 Admin Start]
[Mon Feb 02 11:41:50.510 UTC 2015][AU][0000.02A1][None][IP 10.20.200.230 User
admin@OB-session10 Port 14 temporary admin state set to Online]
[Mon Feb 02 11:41:50.538 UTC 2015][AU][0000.0034][None][IP 10.20.200.230 User
admin@OB-session10 Admin End]
[Mon Feb 02 11:41:50.584 UTC 2015][AU][0000.0033][None][IP 10.20.200.230 User
admin@OB-session10 Admin Start]
```

The following is an example of the Show Audit Archive command showing a portion of the full audit log:

```
IBM8Gb: root> show audit archive
========================
/itasca/conf/audit.log.1
========================
[Wed Nov 27 12:44:35.288 UTC 2013][AU][0000.00FF][None][Zoning Default
Zone changed in Config default to True]
[Wed Nov 27 12:44:38.001 UTC 2013][AU][0000.0033][None][IP Unknown User
root@OB-session1 Admin Start]
[Wed Nov 27 12:44:38.009 UTC 2013][AU][0000.003A][None][IP Unknown User
root@OB-session1 Config Edit (Config = default)]
7 of 9
Audit Logging Design Rev: 2014-01-17.14:44:14
DRAFT - QLOGIC CONFIDENTIAL
[Wed Nov 27 12:44:38.248 UTC 2013][AU][0000.0058][None][IP Unknown User
root@OB-session1 All port Admin States being set to (null) in Config Online]
[Wed Nov 27 12:44:38.251 UTC 2013][AU][0000.003B][None][IP Unknown User
root@OB-session1 Config Save default.pending]
[Wed Nov 27 12:44:38.343 UTC 2013][AU][0000.003D][None][IP Unknown User
root@OB-session1 Config Activate default]
[Wed Nov 27 12:44:39.546 UTC 2013][AU][0000.0034][None][IP Unknown User
root@OB-session1 Admin End]
[Wed Nov 27 12:44:40.106 UTC 2013][AU][0000.0033][None][IP Unknown User
root@OB-session2 Admin Start]
[Wed Nov 27 12:44:40.108 UTC 2013][AU][0000.00CE][None][IP Unknown User
root@OB-session2 Start System Setup]
[Wed Nov 27 12:44:40.109 UTC 2013][AU][0000.0156][None][IP Unknown User
root@OB-session2 Ethernet 0 Enable has been set to True]
[Wed Nov 27 12:44:40.111 UTC 2013][AU][0000.00D0][None][IP Unknown User
root@OB-session2 Save System Setup]
[Wed Nov 27 12:44:40.113 UTC 2013][AU][0000.003D][None][IP Unknown User
root@OB-session2 Config Activate default]
========================
/itasca/conf/audit.log
========================
[Wed Nov 27 12:51:32.284 UTC 2013][AU][0000.00FF][None][Zoning Default
Zone changed in Config default to True]
[Wed Nov 27 12:51:35.614 UTC 2013][AU][0000.0033][None][IP Unknown User
root@OB-session1 Admin Start]
[Wed Nov 27 12:51:35.618 UTC 2013][AU][0000.003A][None][IP Unknown User
root@OB-session1 Config Edit (Config = default)]
[Wed Nov 27 12:51:35.886 UTC 2013][AU][0000.0058][None][IP Unknown User
root@OB-session1 All port Admin States being set to (null) in Config Online]
[Wed Nov 27 12:51:35.889 UTC 2013][AU][0000.003B][None][IP Unknown User
root@OB-session1 Config Save default.pending]
[Wed Nov 27 12:51:35.985 UTC 2013][AU][0000.003D][None][IP Unknown User
root@OB-session1 Config Activate default]
[Wed Nov 27 12:51:37.335 UTC 2013][AU][0000.0034][None][IP Unknown User
root@OB-session1 Admin End]
[Wed Nov 27 12:51:37.762 UTC 2013][AU][0000.0033][None][IP Unknown User
root@OB-session2 Admin Start]
[Wed Nov 27 12:51:37.764 UTC 2013][AU][0000.00CE][None][IP Unknown User
root@OB-session2 Start System Setup]
[Wed Nov 27 12:51:37.765 UTC 2013][AU][0000.0156][None][IP Unknown User
root@OB-session2 Ethernet 0 Enable has been set to True]
[Wed Nov 27 12:51:37.767 UTC 2013][AU][0000.00D0][None][IP Unknown User
root@OB-session2 Save System Setup]
[Wed Nov 27 12:51:37.769 UTC 2013][AU][0000.003D][None][IP Unknown User
```

```
root@OB-session2 Config Activate default]
[Thu Nov 28 12:42:55.362 UTC 2013][AU][0000.0033][None][IP 10.0.0.251 User
root@OB-session9 Admin Start]
[Thu Nov 28 12:43:01.027 UTC 2013][AU][0000.003D][None][IP 10.0.0.251 User
root@OB-session9 Config Activate default]
[Thu Nov 28 12:43:04.593 UTC 2013][AU][0000.0034][None][IP 10.0.0.251 User
root@OB-session9 Admin End]
```

Show Backtrace

Displays the backtrace file. This file is useful for debugging.

Authority

None

Syntax

show backtrace

Examples

The following is an example of the Show Backtrace command:

```
IBM8Gb #> show backtrace
  Filename         : backtrace-snmpd
  Modification time: day mon date hh:mm:ss yyyy
  ----------------------------------------
  *** Segmentation fault
  Register dump:
  fp0-3:   0000000000000000 0000000000000000 0000000000000000
0000000000000000
  fp4-7:   0000000000000000 0000000000000000 0000000000000000
0000000000000000
  fp8-11:  0000000000000000 0000000000000000 0000000000000000
0000000000000000
  fp12-15: 0000000000000000 0000000000000000 0000000000000000
0000000000000000
  fp16-19: 0000000000000000 0000000000000000 0000000000000000
0000000000000000
  fp20-23: 0000000000000000 0000000000000000 0000000000000000
0000000000000000
  fp24-27: 0000000000000000 0000000000000000 0000000000000000
0000000000000000
  fp28-31: 0000000000000000 0000000000000000 0000000000000000
0000000000000000
  r0 =0fed8540 sp =7fffe130 r2 =00000000 r3 =00000000  trap=00000300
  r4 =10049d48 r5 =00000001 r6 =10049ee0 r7 =00000148   sr0=0fed854c
sr1=0002d000
  r8 =00000198 r9 =00000000 r10=0fc1a1cc r11=00000000   dar=00000000
dsi=00000000
  r12=300169b0 r13=1001d13c r14=100d9610 r15=00000000   r3*=0fdea678
  r16=ffffffff r17=7fffe1a0 r18=00000000 r19=ffffffff
  r20=00000000 r21=00000000 r22=00000000 r23=7ffffef4    lr=0fed8540
xer=20000000
  r24=00000001 r25=00000006 r26=00000000 r27=00000002    mq=00000000
ctr=00000000
  r28=00000000 r29=00000003 r30=0feff078 r31=0fef85a8  fscr=00000000
ccr=24000422
    Backtrace:
  /usr/local/lib/libsnmp-0.4.2.3.so(init_usm_post_config+0x64)[0xfed854c]
  /usr/local/lib/libsnmp-0.4.2.3.so(snmp_call_callbacks+0xac)[0xfedaf88]
  /usr/local/lib/libsnmp-0.4.2.3.so(read_premib_configs+0xdc)[0xfecd928]
  /usr/local/lib/libsnmp-0.4.2.3.so(init_snmp+0x128)[0xfeb6a48]
  /usr/local/sbin/snmpd[0x10002c48]
  /lib/libc.so.6(__libc_start_main+0x170)[0xfafd594]

  Process Status:
  Name:      snmpd
  State:     R (running)
  SleepAVG:  82%
  Tgid:      306
  Pid:       306
  PPid:      222
  TracerPid: 0
  Uid:       0 0 0 0
  Gid:       0 0 0 0
  FDSize:    32
  Groups:
  VmSize:     5616 kB
  VmLck:      0 kB
```

```
VmRSS:      2016 kB
VmData:     468 kB
VmStk:      28 kB
VmExe:      88 kB
VmLib:      3968 kB
VmPTE:      28 kB
Threads:    1
SigPnd:     0000000000000000
ShdPnd:     0000000000000000
SigBlk:     0000000000000400
SigIgn:     8000000000000006
SigCgt:     00000000000004e0
CapInh:     0000000000000000
CapPrm:     00000000ffffffff
CapEff:     00000000ffffffff
```

Show Broadcast

Displays the broadcast tree information and all ports that are currently transmitting and receiving broadcast frames.

Authority

None

Syntax

show broadcast

Examples

The following is an example of the Show Broadcast command:

```
IBM8Gb #> show broadcast

  Group Member Ports ISL Ports
  ----- ------------ ---------
  0     3            16
        15
        16
```

Show Chassis

Displays chassis component status, and temperature.

Authority

None

Syntax

show chassis

Examples

The following is an example of the Show Chassis command.

```
IBM8Gb #> show chassis

  Chassis Information
  -------------------
  BoardTemp (1) - Degrees Celsius   22
  BoardTemp (2) - Degrees Celsius   23
  BoardTemp (3) - Degrees Celsius   25
  PowerSupplyStatus (1)             Good
  HeartBeatCode                     1
  HeartBeatStatus                   Normal
```

Show Config Port

Displays configuration parameters for one or more ports.

Authority

None

Syntax

show config port ***[port_number]***

Keywords

[port_number]

The number of the port. Ports are numbered beginning with 0. If you omit [port_number], all ports are specified.

Examples

The following is an example of the Show Config Port command for external port 0 on a full-fabric switch:

```
IBM8Gb #> show config port 0

  Configuration Name: default
  ---------------------------

  Port Number: 0
  ------------
  AdminState         Online
  LinkSpeed          Auto
  PortType           GL
  SymbolicName       Port0
  ALFairness         False
  DeviceScanEnabled  True
  ForceOfflineRSCN   False
  ARB_FF             False
  InteropCredit      0
  ExtCredit          0
  FANEnabled         True
  AutoPerfTuning     False
  LCFEnabled         False
  MSEnabled          True
  NoClose            False
  IOStreamGuard      Auto
  VIEnabled          False
  MFSEnabled         True
  PDISCPingEnable    True
```

The following is an example of the Show Config Port command for port 0 on a pass-thru module:

```
IBM8Gb #> show config port 0

  Configuration Name: default
  ---------------------------

  Port Number: 0
  ------------
  AdminState         Online
  LinkSpeed          Auto
  PortType           TF
  SymbolicName       Port0
```

Show Config Security

Displays the security database configuration parameters.

Authority

None

Syntax

show config security

Examples

The following is an example of the Show Config Security command:

```
IBM8Gb #> show config security
  Configuration Name: default
  -------------------
  Switch Security Configuration Information
  -----------------------------------------
  FabricBindingEnabled  False
  AutoSave              True

  Port     Binding Status  WWN
  ----     --------------  ---
  0        False           No port binding entries found.
  15       False           No port binding entries found.
  16       False           No port binding entries found.
  17       False           No port binding entries found.
  18       False           No port binding entries found.
  19       False           No port binding entries found.
  1        False           No port binding entries found.
  2        False           No port binding entries found.
  3        False           No port binding entries found.
  4        False           No port binding entries found.
  5        False           No port binding entries found.
  6        False           No port binding entries found.
  7        False           No port binding entries found.
  8        False           No port binding entries found.
  9        False           No port binding entries found.
  10       False           No port binding entries found.
  11       False           No port binding entries found.
  12       False           No port binding entries found.
  13       False           No port binding entries found.
  14       False           No port binding entries found.
```

Show Config Security Portbinding

Displays the port binding configuration for one or more ports.

Authority

None

Syntax

show config security portbinding *[port_number]*

Keywords

[port_number]

The number of the port. If you omit [port_number], the port binding configuration for all ports is displayed.

Examples

The following is an example of the Show Config Security Port command:

```
IBM8Gb: admin> show config security portbinding

  Configuration Name: default
  -------------------

  Port     Binding Status  WWN
  ----     --------------  ---
  Ext1:0   False           No port binding entries found.
  Ext2:15  False           No port binding entries found.
  Ext3:16  False           No port binding entries found.
  Ext4:17  False           No port binding entries found.
  Ext5:18  False           No port binding entries found.
  Ext6:19  False           No port binding entries found.
  Bay1     False           No port binding entries found.
  Bay2     False           No port binding entries found.
  Bay3     False           No port binding entries found.
  Bay4     False           No port binding entries found.
  Bay5     False           No port binding entries found.
  Bay6     False           No port binding entries found.
  Bay7     False           No port binding entries found.
  Bay8     False           No port binding entries found.
  Bay9     False           No port binding entries found.
  Bay10    False           No port binding entries found.
  Bay11    False           No port binding entries found.
  Bay12    False           No port binding entries found.
  Bay13    False           No port binding entries found.
  Bay14    False           No port binding entries found.
```

Show Config Switch

Displays the switch configuration parameters.

Authority

None

Syntax

show config switch

Examples

The following is an example of the Show Config Switch command:

```
IBM8Gb #> show config switch
 Configuration Name: default
 -------------------
  Switch Configuration Information
  --------------------------------
  TransparentMode       False
  AdminState            Online
  BroadcastEnabled      True
  InbandEnabled         True
  FDMIEnabled           True
  FDMIEntries           1000
  DefaultDomainID       19 (0x13)
  DomainIDLock          True
  SymbolicName          IBM8Gb
  PrincipalPriority     254
  ConfigDescription     Default Config
  ConfigLastSavedBy     admin@OB-session5
  ConfigLastSavedOn     day month date time year
  InteropMode           Standard
```

Show Config Threshold

Displays alarm threshold parameters for the switch.

Authority

None

Syntax

show config threshold

Examples

The following is an example of the Show Config Threshold command:

```
IBM8Gb #> show config threshold
  Configuration Name: default
  ------------
  Threshold Configuration Information
  ----------------------------------
  ThresholdMonitoringEnabled      False
  CRCErrorsMonitoringEnabled      True
    RisingTrigger                 25
    FallingTrigger                1
    SampleWindow                  10
  DecodeErrorsMonitoringEnabled   True
    RisingTrigger                 25
    FallingTrigger                0
    SampleWindow                  10
  ISLMonitoringEnabled            True
    RisingTrigger                 2
    FallingTrigger                0
    SampleWindow                  10
  LoginMonitoringEnabled          True
    RisingTrigger                 5
    FallingTrigger                1
    SampleWindow                  10
  LogoutMonitoringEnabled         True
    RisingTrigger                 5
    FallingTrigger                1
    SampleWindow                  10
  LOSMonitoringEnabled            True
    RisingTrigger                 100
    FallingTrigger                5
    SampleWindow                  10
```

Show Config Zoning

Displays zoning configuration parameters for the switch.

Authority

None

Syntax

show config zoning

Examples

The following is an example of the Show Config Zoning command:

```
IBM8Gb #> show config zoning

 Configuration Name: default
  -------------------

  Zoning Configuration Information
  --------------------------------
  InteropAutoSave       True
  DefaultZone           Allow
  DiscardInactive       False
```

Show Domains

Displays list of each domain and its worldwide name in the fabric.

Authority

None

Syntax

show domains

Examples

The following is an example of the Show Domains command:

```
IBM8Gb #> show domains
  Principal switch is (remote): 10:00:00:60:69:50:0b:6c
  Upstream Principal ISL is   : 1
  Domain ID List:
        Domain 97  (0x61)  WWN = 10:00:00:c0:dd:00:71:ed
        Domain 98  (0x62)  WWN = 10:00:00:60:df:22:2e:0c
        Domain 99  (0x63)  WWN = 10:00:00:c0:dd:00:72:45
        Domain 100 (0x64)  WWN = 10:00:00:c0:dd:00:ba:68
        Domain 101 (0x65)  WWN = 10:00:00:60:df:22:2e:06
        Domain 102 (0x66)  WWN = 10:00:00:c0:dd:00:90:ef
        Domain 103 (0x67)  WWN = 10:00:00:60:69:50:0b:6c
        Domain 104 (0x68)  WWN = 10:00:00:c0:dd:00:b8:b7
```

Show Donor

Displays list of current donor and extended credit configuration for all ports.

Authority

None

Syntax

show donor

Examples

The following is an example of the Show Donor command:

```
IBM8Gb #> show donor

          Config Ext Credit Max Credit Donated Donor Valid Groups to
  Port    Type   Requested  Available  to Port Group Extend Credit
  ----    ------ ---------- ---------- ------- ----- ---------------
  Ext1:0  G      15         30         None    0           0
  Ext2:15 Donor  0          0          None    0           0
  Ext3:16 GL     0          16         None    0           0
  Ext4:17 GL     0          16         None    0           0
  Ext5:18 GL     0          16         None    0           0
  Ext6:19 GL     0          16         None    0           0

  Bay1    F      0          16         None    0           0
  Bay2    F      0          16         None    0           0
  Bay3    F      0          16         None    0           0
  Bay4    F      0          16         None    0           0
  Bay5    F      0          16         None    0           0
  Bay6    F      0          16         None    0           0
  Bay7    F      0          16         None    0           0
  Bay8    F      0          16         None    0           0
  Bay9    F      0          16         None    0           0
  Bay10   F      0          16         None    0           0
  Bay11   F      0          16         None    0           0
  Bay12   F      0          16         None    0           0
  Bay13   F      0          16         None    0           0
  Bay14   F      0          16         None    0           0

  Donor Group  Credit Pool
  -----------  -----------
  0            0
```

Show Env

Displays temperature and voltage information.

Authority

None

Syntax

show env

Examples

The following is an example of the Show Env command:

```
IBM8Gb #> show env
  Temperature(C) Sensors:

  Sensor  Description          Status  Current  High Warn  High Alarm
  ------  -------------------  ------  -------  ---------  ----------
       0  BOARD                Normal       22         65          70
       1  DS1780               Normal       22        n/a         n/a
       2  MAX1617              Normal       26         65          70
       3  ASIC                 Normal       33        102         105
       4  LM75 0 (exhaust)     Normal       21         65          70
       5  LM75 1 (inlet)       Normal       24         65          70

  Voltage Sensors:

  Sensor  Description  Status  Current  Low Alarm  High Alarm
  ------  -----------  ------  -------  ---------  ----------
       0  1.5V         Good       1.50       1.31        1.68
       1  1.25V        Good       1.24       1.00        1.50
       2  2.5V         Good       2.49       2.20        2.82
       3  3.3V         Good       3.31       2.99        3.62
       4  12V          Good      11.44      10.81       13.31
       5  1.2V         Good       1.23       1.04        1.38
       6  1.8V         Good       1.78       1.61        1.99
       7  1.8V_ANALOG  Good       1.78       1.58        2.02
       8  2.5V_ANALOG  Good       2.39       2.10        2.82
```

Show Fabric

Displays list of each domain, symbolic name, worldwide name, node IP address, and port IP address.

Authority

None

Syntax

show fabric *brief*

Keywords

brief

Displays a table of switches in the fabric including domain ID, WWN, and symbolic name. If you omit the Brief keyword, the command displays information only for the local switch.

Examples

The following is an example of the Show Fabric command:

```
IBM8Gb #> show fabric
  Domain           *133(0x85)
  WWN              10:00:00:c0:dd:0d:53:91
  SymbolicName     IBM8Gb
  HostName         <undefined>
  EthIPv4Address   10.20.116.133
  EthIPv6Address   <undefined>

  * indicates principal switch
```

The following is an example of the Show Fabric Brief command:

```
IBM8Gb #> show fabric brief
 Domain     WWN                     SymbolicName
 ------     ---                     ------------
*16 (0x10)  10:00:00:c0:dd:00:77:81 swsb1.11
 17 (0x11)  10:00:00:c0:dd:00:6a:2d sw12
 18 (0x12)  10:00:00:c0:dd:00:c3:04 sw.160
 19 (0x13)  10:00:00:c0:dd:00:bc:56 Sb2.108

  * indicates principal switch
```

Show FDMI

Displays detailed information about the device host bus adapter.

Authority

None

Syntax

show fdmi *[port_wwn]*

Keywords

[port_wwn]

The device world wide port name for which to display information. If you omit [port_wwn], the command displays a summary of host bus adapter information for all attached devices in the fabric. Illegal characters in the display appear as question marks (?).

Examples

The following is an example of the Show FDMI command:

```
IBM8Gb #> show fdmi
HBA ID                  PortID  Manufacturer           Model    Ports
--------                ------  ---------------       -------   -----
21:01:00:e0:8b:27:aa:bc 610000  QLogic Corporation    QLA2342   2
21:00:00:00:ca:25:9b:96 180100  QLogic Corporation    QL2330    2
```

The following is an example of the Show FDMI WWN command:

```
IBM8Gb #> show fdmi 21:00:00:e0:8b:85:41:71

  FDMI Information
  ----------------
  Manufacturer            QLogic Corporation
  SerialNumber            D56673
  Model                   QMC2462S
  ModelDescription        IBM eServer BC 4Gb FC Expansion Card SFF
  PortID                  6f0200
  NodeWWN                 20:00:00:e0:8b:85:41:71
  HardwareVersion
  DriverVersion           8.02.14
  OptionRomVersion        2.02
  FirmwareVersion         4.04.00 [IP] [84XX]
  OperatingSystem         Linux 2.6.9-67.EL ?1 day mon date hh:mm:ss EST yyyy
  MaximumCTPayload
  NumberOfPorts           1

  Port  21:00:00:e0:8b:85:41:71

  SupportedFC4Types       FCP
  SupportedSpeed          1Gb/s,2Gb/s,4Gb/s
  CurrentSpeed            4Gb/s
  MaximumFrameSize        2048
  OSDeviceName            /proc/scsi/qla2xxx/1
  HostName                sb-3.ibm.org
```

Show Interface

Displays the status of the active network interfaces.

Authority

None

Syntax

show interface

Examples

The following is an example of the Show Interface command:

```
IBM8Gb #> show interface
eth0      Link encap:Ethernet  HWaddr 00:C0:DD:1F:26:8F
          inet addr:10.20.90.68  Bcast:10.20.90.255  Mask:255.255.255.0
          inet6 addr: fd70:c154:c2df:90:2c0:ddff:fe1f:268f/64 Scope:Global
          inet6 addr: fc20:2224::2c0:ddff:fe1f:268f/64 Scope:Global
          inet6 addr: fc00:2::2c0:ddff:fe1f:268f/64 Scope:Global
          inet6 addr: 2040::2c0:ddff:fe1f:268f/64 Scope:Global
          inet6 addr: fe80::2c0:ddff:fe1f:268f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2456811 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:687025905 (655.1 Mb)  TX bytes:569589 (556.2 Kb)

eth1      Link encap:Ethernet  HWaddr 00:C0:DD:1F:26:90
          inet addr:10.20.108.66  Bcast:10.20.108.255  Mask:255.255.255.0
          inet6 addr: fd70:c154:c2df:108:2c0:ddff:fe1f:2690/64 Scope:Global
          inet6 addr: fc20:2222::2c0:ddff:fe1f:2690/64 Scope:Global
          inet6 addr: fc00:1::2c0:ddff:fe1f:2690/64 Scope:Global
          inet6 addr: 2030::2c0:ddff:fe1f:2690/64 Scope:Global
          inet6 addr: fe80::2c0:ddff:fe1f:2690/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:224901 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1362432 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29440966 (28.0 Mb)  TX bytes:693392907 (661.2 Mb)
          Interrupt:25

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1653515 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1653515 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:220868174 (210.6 Mb)  TX bytes:220868174 (210.6 Mb)
```

Show Log

Displays the contents of the log or the parameters used to create and display entries in the log. The log contains a maximum of 1200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority

None

Syntax

show log
[number_of_events]
component
display [filter]
level
options
port
settings

Keywords

[number_of_events]

Specifies the number of the most recent events to display from the event log. [number_of_events] must be a positive integer.

component

Displays the components currently being monitored for events. Table 51 describes the log monitoring components.

Table 51. Log monitoring components

Component	Description
Chassis	Chassis hardware components such as fans and power supplies
CLI	Command line interface events
Eport	E_Port events
Mgmtserver	Management server events
Nameserver	Name server events
Other	Miscellaneous events
Port	Port events
SNMP	SNMP events
Switch	Switch management events
Zoning	Zoning conflict events

display [filter]

Displays log events on the screen according to the component or severity level filter given by [filter]. [filter] can be one of the following:

Info

Displays all informative events.

Warning

Displays all warning events.

Critical

Displays all critical events.

Eport

Displays all events related to E_Ports.

Mgmtserver

Displays all events related to the management server.

Nameserver

Displays all events related to the name server.

Port [port_number]

Displays all events related to the port given by [port_number].

SNMP

Displays all events related to SNMP.

Switch

Displays all events related to switch management.

Zoning

Displays all events related to zoning.

level

Displays the event severity level logging setting and the display level setting.

options

Displays the options that are available for configuring event logging and automatic display to the screen. For information about how to configure event logging and display level, see the "Set Log" command on page 258.

port

Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but not on a defined port, no entry is made in the log.

settings

Displays the current filter settings for component, severity level, port, and display level. This command is equivalent to executing the following commands separately: Show Log Component, Show Log Level, and Show Log Port.

Examples

The following is an example of the Show Log Component command:

```
IBM8Gb #> show log component
Current settings for log
   ------------------------
   FilterComponent   NameServer MgmtServer Zoning Switch Blade Port Eport Snmp
```

The following is an example of the Show Log Level command:

```
IBM8Gb #> show log level
   Current settings for log
   ------------------------
   FilterLevel       Info
   DisplayLevel      Critical
```

The following is an example of the Show Log Options command:

```
IBM8Gb #> show log options
  Allowed options for log
  -----------------------
  FilterComponent   All,None,NameServer,MgmtServer,Zoning,Switch,Port,
                    Eport,Snmp,CLI,Qfs,QT
  FilterLevel       Critical,Warn,Info,None
  DisplayLevel      Critical,Warn,Info,None
```

The following is an example of the Show Log command:

```
IBM8Gb #> show log
[1][Fri Jan 07 02:07:56.068 UTC 2011][I][8400.0023][Switch][Successful login
user (admin@OB-session8) with admin privilege from address 10.20.32.223-3852]
[2][Fri Jan 07 02:07:56.069 UTC 2011][W][8400.0058][Switch][User (USERID) is
using their initial/default password]
[3][Fri Jan 07 02:08:38.179 UTC 2011][I][8400.0023][Switch][Successful login
user (admin@OB-session9) with admin privilege from address 10.20.32.146]
[4][Fri Jan 07 02:08:38.180 UTC 2011][W][8400.0058][Switch][User (USERID) is
using their initial/default password]
[5][Fri Jan 07 02:09:39.793 UTC 2000][I][8400.0023][Switch][Successful login
user (admin@OB-session10) with admin privilege from address
10.20.32.223-3862]
[6][Fri Jan 07 02:09:39.795 UTC 2011][W][8400.0058][Switch][User (USERID) is
using their initial/default password]
[7][Fri Jan 07 02:17:10.205 UTC 2011][C][8400.002A][Switch][User (USERID)
attempted to log into switch with an incorrect password from 10.20.32.223]
```

Show LSDB

Displays Link State database information.

Authority

None

Syntax

show lsdb

Examples

The following is an example of the Show LSDB command:

```
IBM8Gb #> show lsdb

  Link State Database Information
  -------------------------------
  LsID 34:  Age=1176, Incarnation=0x800000e5
    NeighborDomain=36, LocalPort=6, RemotePort=7, Cost=500
    NeighborDomain=35, LocalPort=16, RemotePort=16, Cost=100
    NeighborDomain=35, LocalPort=18, RemotePort=19, Cost=100
    NeighborDomain=35, LocalPort=7, RemotePort=7, Cost=500
    NeighborDomain=35, LocalPort=5, RemotePort=4, Cost=500

    Local Domain

  LsID 35:  Age=1166, Incarnation=0x800000cc
    NeighborDomain=34, LocalPort=16, RemotePort=16, Cost=100
    NeighborDomain=34, LocalPort=19, RemotePort=18, Cost=100
    NeighborDomain=36, LocalPort=5, RemotePort=4, Cost=250
    NeighborDomain=34, LocalPort=7, RemotePort=7, Cost=500
    NeighborDomain=34, LocalPort=4, RemotePort=5, Cost=500

    Route: OutPort=18, Hops=1, Cost=100

  LsID 36:  Age=1162, Incarnation=0x80000046
    NeighborDomain=34, LocalPort=7, RemotePort=6, Cost=500
    NeighborDomain=35, LocalPort=4, RemotePort=5, Cost=250

    Route: OutPort=16, Hops=2, Cost=350
```

Show Media

Displays transceiver operational and diagnostic information for one or more external ports.

Authority

None

Syntax

show media
[port_list]
all
installed

Keywords

[port_list]

The external port or ports for which to display transceiver information. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 15-19] specifies ports 0, 15, 16, 17, 18, and 19.

all

Displays transceiver information for all ports.

installed

Displays transceiver information for all ports that have transceivers installed.

Notes

Table 52 describes the transceiver information in the Show Media display.

Table 52. Transceiver information

Information type	Description
MediaType	Media physical variant. The variant indicates speed, media, transmitter, and distance. The media designator may be M5 (multimode 50 micron), M6 (multimode 62.5 micron), or MX. MX indicates that the media supports both multimode 50 and 62.5 micron. MediaType may also be on of the following: • NotInstalled–transceiver is not installed. • Unknown–transceiver does not have a serial ID. • NotApplicable–transceiver is not needed.
MediaVendor	Vendor name
MediaPartNumber	Vendor media part number
MediaRevision	Vender media revision level
MediaSerialNumber	Vendor media serial number
MediaSpeeds	Transmission speed capabilities
Temp	Temperature in degrees Celsius.
Voltage	Supply voltage in Volts. The range is 0–6.55.
Tx Bias	Transmitter laster bias current in milliamps. The range is 0–655.
Tx Power	Transmitter coupled output power in milliWatts. The range is 0–6.55.
Rx Power	Received optical power in milliWatts. The range is 0–6.55.

Table 52. Transceiver information (Continued)

Information type	Description
Value	Measured value.
Status	State associated with the measured value: • Normal: Value is in the normal operating range. • HighAlarm: Value exceeds the high alarm threshold. • HighWarning: Value exceeds the high warning threshold. • LowWarning: Value is less than the low warning threshold. • LowAlarm: Value is less than the low alarm threshold.
HighAlarm	Vendor specified threshold above which an alarm is issued.
HighWarning	Vendor specified threshold above which a warning is issued.
LowWarning	Vendor specified threshold below which a warning is issued.
LowAlarm	Vendor specified threshold below which an alarm is issued.

Examples

The following is an example of the Show Media command for port 19:

```
IBM8Gb #> show media 19
  Port Number: 19
  ------------
  MediaType             800-MX-SN-I
  MediaVendor           AVAGO
  MediaPartNumber       AFBR-57D5APZ
  MediaRevision         Q12
  MediaSerialNumber     AD0724E0569
  MediaSpeeds           2Gb/s, 4Gb/s 8Gb/s

                           Temp     Voltage     Tx Bias      Tx Pwr      Rx Pwr
                            (C)         (V)        (mA)        (mW)        (mW)
                     ----------- ----------- ----------- ----------- -----------
        Value              26.14        3.33        5.38       0.581       0.612
        Status            Normal      Normal      Normal      Normal      Normal
        HighAlarm          90.00        3.80        8.50       0.800       6.550
        HighWarning        85.00        3.63        8.50       0.700       1.100
        LowWarning        -10.00        2.97        2.00       0.100       0.049
        LowAlarm          -15.00        2.80        2.00       0.050       0.000
```

The following is an example of the Show Media command for all ports:

```
IBM8Gb#> show media
Note:  -- LowAlarm; - LowWarning; + HighWarning; ++ HighAlarm

                              Temp    Voltage   Tx Bias   Tx Pwr   Rx Pwr
  Port    Vendor Name          (C)       (V)      (mA)     (mW)     (mW)
  ----    -----------      -------   -------   -------   ------   ------

  Ext1:0  Intel Corp.        35.25      3.34      6.45    0.314    0.366
  Ext2:15 Intel Corp.        34.28      3.34      6.60    0.342    0.377
  Ext3:16 NotInstalled         N/A       N/A       N/A      N/A      N/A
  Ext4:17 NotInstalled         N/A       N/A       N/A      N/A      N/A
  Ext5:18 NotInstalled         N/A       N/A       N/A      N/A      N/A
  Ext6:19 Intel Corp.        34.78      3.33      7.08    0.348    0.211
  Bay1    NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay2    NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay3    NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay4    NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay5    NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay6    NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay7    NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay8    NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay9    NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay10   NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay11   NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay12   NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay13   NotApplicable        N/A       N/A       N/A      N/A      N/A
  Bay14   NotApplicable        N/A       N/A       N/A      N/A      N/A
```

Show Mem

Displays information about memory activity.

Authority

None

Syntax

show mem *[count]*

Keywords

[count]

The number of seconds for which to display memory information. If you omit [count], the value 1 is used. Displayed memory values are in 1K block units.

Notes:

This keyword will display memory activity updates until [count] is reached–it cannot be interrupted. Therefore, avoid using large values for [count].

Examples

The following is an example of the Show Mem command:

```
procs -----------memory---------- ---swap-- -----io---- --system-- ----cpu----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in    cs us sy id wa
 0  0      0 136292   1040  68092    0    0     2     0  434   152  1  2 97  0

Filesystem space in use: 36808/41297 KB (89%)
```

Show NS

Displays the WWNs for devices in the fabric.

Authority

None

Syntax

show ns ***[option]***

Keywords

[option]

The domain IDs or port IDs for which to display name server information. If you omit [option], name server information for the local domain ID is displayed. [option] can have the following values:

all

Displays WWNs for all switches and ports.

[domain_id]

Displays WWNs for all devices connected to the switch given by [domain_id]. [domain_id] is a switch domain ID.

[port_id]

Displays the WWNs for the devices connected to the port given by [port_id]. [port_id] is a port Fibre Channel address.

Examples

The following is an example of the Show NS (local domain) command:

```
IBM8Gb #> show ns
  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   19 (0x13) 1301e1 NL   3   21:00:00:20:37:73:13:69
20:00:00:20:37:73:13:69
  2   19 (0x13) 1301e2 NL   3   21:00:00:20:37:73:12:9b
20:00:00:20:37:73:12:9b
  3   19 (0x13) 1301e4 NL   3   21:00:00:20:37:73:05:26
20:00:00:20:37:73:05:26
  4   19 (0x13) 130d00 N    3   21:01:00:e0:8b:27:a7:bc
20:01:00:e0:8b:27:a7:bc
```

The following is an example of the Show NS [domain_ID] command:

```
IBM8Gb #> show ns 18
    Seq Domain    Port   Port
    No  ID        ID     Type COS PortWWN                 NodeWWN
    --- ------    ------ ---- --- -------                 -------
    1   18 (0x12) 120700 N    3   21:00:00:e0:8b:07:a7:bc 20:00:00:e0:8b:07:a7:bc
```

The following is an example of the Show NS [port_ID] command:

```
IBM8Gb #> show ns 1301e1
  Port ID: 1301e1
  --------
  PortType          NL
  PortWWN           21:00:00:20:37:73:13:69
  SymbolicPortName
  NodeWWN           20:00:00:20:37:73:13:69
  SymbolicNodeName
  NodeIPAddress     diskarray7.anycompany.com
  ClassOfService    3
  PortIPAddress     0.0.0.0
  FabricPortName    20:01:00:c0:dd:00:bc:56
  FC4Type           FCP
  FC4Desc           (NULL)
```

Show Pagebreak

Displays the current pagebreak setting.

Authority

None

Syntax

show pagebreak

Notes

The pagebreak setting limits the display of information to 20 lines or allows the continuous display of information without a break.

Examples

The following is an example of the Show Pagebreak command:

```
IBM8Gb #> show pagebreak

  current setting: ON
```

Show Perf

Displays port performance in frames/second and bytes/second. If you omit the keyword, the command displays data transmitted (out), data received (in), and total data transmitted and received in frames/second and bytes per second. Transmission rates are expressed in thousands (K) and millions (M).

Authority

None

Syntax

show perf *[port_list]*
or
show perf
byte *[port_list]*
inbyte *[port_list]*
outbyte *[port_list]*
frame *[port_list]*
inframe *[port_list]*
outframe *[port_list]*
errors *[port_list]*

Keywords

[port_list]

Displays the instantaneous performance data for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. If you omit [port_list], the command displays performance data for all ports.

byte ***[port_list]***

Displays continuous performance data in total bytes/second transmitted and received for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. If you omit [port_list], the command displays performance data for all ports. Press any key to stop the display.

inbyte ***[port_list]***

Displays continuous performance data in bytes/second received for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. If you omit [port_list], the command displays performance data for all ports. Press any key to stop the display.

outbyte ***[port_list]***

Displays continuous performance data in bytes/second transmitted for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. If you omit [port_list], the command displays performance data for all ports. Press any key to stop the display.

frame ***[port_list]***

Displays continuous performance data in total frames/second transmitted and received for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. If you omit [port_list], the command displays performance data for all ports. Press any key to stop the display.

inframe ***[port_list]***

Displays continuous performance data in frames/second received for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. If you omit [port_list], the command displays performance data for all ports. Press any key to stop the display.

outframe ***[port_list]***

Displays continuous performance data in frames/second transmitted for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. If you omit [port_list], the command displays performance data for all ports. Press any key to stop the display.

errors ***[port_list]***

Displays continuous error counts for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. If you omit [port_list], the command displays performance data for all ports. Press any key to stop the display.

Examples

The following is an example of the Show Perf command:

```
IBM8Gb #> show perf
         Bytes/s    Bytes/s    Bytes/s    Frames/s   Frames/s   Frames/s
Port      (in)       (out)    (total)      (in)       (out)    (total)
----     -------    -------    -------    --------   --------   --------
Ext1:0   0          0          0          0          0          0
Ext2:15  49M        3M         52M        32K        2K         34K
Ext3:16  0          0          0          0          0          0
Ext4:17  0          0          0          0          0          0
Ext5:18  0          0          0          0          0          0
Ext6:19  0          0          0          0          0          0

Bay1    2M         23M        26M        1K         15K        17K
Bay2    0          0          0          0          0          0
Bay3    1M         25M        26M        972        16K        17K
Bay4    0          0          0          0          0          0
Bay5    0          0          0          0          0          0
Bay6    0          0          0          0          0          0
Bay7    0          0          0          0          0          0
Bay8    0          0          0          0          0          0
Bay9    0          0          0          0          0          0
Bay10   0          0          0          0          0          0
Bay11   0          0          0          0          0          0
Bay12   0          0          0          0          0          0
Bay13   0          0          0          0          0          0
Bay14   0          0          0          0          0          0
```

The following is an example of the Show Perf Byte command:

```
IBM8Gb#> show perf byte
 Displaying bytes/sec (total)...  (Press any key to stop display)

0   15   16  17  18  19  1    2   3    4   5   6   7   8   9   10  11  12  13  14
-------------------------------------------------------------------------------
0   63M  0   0   0   0   31M  0   31M  0   0   0   0   0   0   0   0   0   0   0
0   65M  0   0   0   0   31M  0   34M  0   0   0   0   0   0   0   0   0   0   0
0   60M  0   0   0   0   29M  0   30M  0   0   0   0   0   0   0   0   0   0   0
0   62M  0   0   0   0   28M  0   33M  0   0   0   0   0   0   0   0   0   0   0
0   58M  0   0   0   0   26M  0   31M  0   0   0   0   0   0   0   0   0   0   0
0   52M  0   0   0   0   26M  0   26M  0   0   0   0   0   0   0   0   0   0   0
0   61M  0   0   0   0   34M  0   26M  0   0   0   0   0   0   0   0   0   0   0
0   58M  0   0   0   0   29M  0   28M  0   0   0   0   0   0   0   0   0   0   0
0   54M  0   0   0   0   28M  0   26M  0   0   0   0   0   0   0   0   0   0   0
0   66M  0   0   0   0   32M  0   34M  0   0   0   0   0   0   0   0   0   0   0
0   64M  0   0   0   0   35M  0   29M  0   0   0   0   0   0   0   0   0   0   0
0   59M  0   0   0   0   30M  0   29M  0   0   0   0   0   0   0   0   0   0   0
0   56M  0   0   0   0   26M  0   29M  0   0   0   0   0   0   0   0   0   0   0
0   54M  0   0   0   0   26M  0   27M  0   0   0   0   0   0   0   0   0   0   0
0   50M  0   0   0   0   24M  0   25M  0   0   0   0   0   0   0   0   0   0   0
0   61M  0   0   0   0   31M  0   30M  0   0   0   0   0   0   0   0   0   0   0
q
```

Show Port

Displays operational information for one or more ports.

Authority

None

Syntax

show port
[port_list]

Keywords

[port_list]
The number of the port for which to display information. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 15-19] specifies ports 0,15, 16, 17, 18, and 19.

Notes

Table 53 describes the port parameters.

Table 53. Show Port parameters

Entry	Description
ActiveTHPortList (pass-thru only)	The list of TH_Ports to which the TF_Port is mapped.
ActiveTFPortMap (pass-thru only)	The list of TF_Ports that are mapped to the TH_Port.
AdminState	Administrative state
AIinit	Incremented each time the port begins AL initialization.
AIinitError	Number of times the port entered initialization and the initialization failed.
AsicNumber	ASIC number
AsicPort	ASIC port number
Bad Frames	Number of frames that have framing errors.
BBCR_FrameFailures	Number of times more frames were lost during a credit recovery period than the recovery process could resolve. This causes a Link Reset to recover the credits.
BBCR_RRDYFailures	Number of times more R_RDYs were lost during a credit recovery period than the recovery process could resolve. This causes a Link Reset to recover the credits.
ClassXFramesIn	Number of class *x* frames received by this port.
ClassXFramesOut	Number of class *x* frames sent by this port.
ClassXWordsIn	Number of class *x* words received by this port.
ClassXWordsOut	Number of class *x* words sent by this port.
ClassXToss	Number of times an SOFi3 or SOFn3 frame is tossed from TBUF.
ConfigType	Configured port type
DecodeError	Number of decode errors detected
DiagFaultCode	Fault code from the most recent Power-on self test

Table 53. Show Port parameters (Continued)

Entry	Description
DiagStatus	Status from the most recent Power-on self test
EpConnects	Number of times an E_Port connected through ISL negotiation.
EpConnState	E_Port connection status
EpIsoReason	E_Port isolation reason
FBusy	Number of times the switch sent a F_BSY because Class 2 frame could not be delivered within ED_TOV time. Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_Port that is preventing delivery of this frame.
Flowerrors	Number of frames received there were no available credits.
FReject	Number of frames from devices that were rejected.
InvalidCRC	Invalid CRC detected.
InvalidDestAddr	Invalid destination address detected.
IOStreamGuard	I/O StreamGuard status
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or a loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
LinkSpeed	Port transmission speed
LinkState	Port activity status
LIP_AL_PD_ALPS	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.
LIP_F7_AL_PS	This LIP is used to reinitialize the loop. An L_Port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.
LIP_F8_AL_PS	This LIP denotes a loop failure detected by the L_Port identified by AL_PS.
LIP_F7_F7	A loop initialization primitive frame used to acquire a valid AL_PA.
LIP_F8_F7	A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.
Login	Number of device logins
LoginStatus	Login status
Logout	Number of device logouts
LongFramesIn	Number of incidents when one or more frames are received that are greater than the maximum size.
LoopTimeouts	A two (2) second timeout as specified by FC-AL-2.

Table 53. Show Port parameters (Continued)

Entry	Description
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
LostFrames	Number of incidents of lost frames.
Lost RRDYs	Number of incidents of lost R_RDYs.
MaxCredit	Maximum number of port buffer credits
MediaSpeeds	Possible transmission speeds
MediaPartNumber	Transceiver vendor part number
MediaRevision	Transceiver revision
MediaType	Media physical variant. The variant indicates speed, media, transmitter, and distance. The media designator may be M5 (multimode 50 micron), M6 (multimode 62.5 micron), or MX. MX indicates that the media supports both multimode 50 and 62.5 micron.
MediaVendor	Transceiver manufacturer
MediaVendorID	Transceiver manufacturer identifier
OperationalState	Operational state
PerfTuningMode	AutoPerfTuning status
PortID	Fibre Channel port address
PortWWN	World wide port name
PrimSeqErrors	Primitive sequence errors detected.
RunningType	Operational port type
RxLinkResets	Number of link reset primitives received from an attached device.
RxOfflineSeq	Number of offline sequences received. An OLS is issued for link initialization, a Receive & Recognize Not_Operational (NOS) state, or to enter the offline state.
ShortFramesIn	Number of incidents when one or more frames are received that are less than the minimum size.
SymbolicName	Port symbolic name
SyncStatus	Synchronization status
TestFaultCode	Fault code from the most recent port test
TestStatus	Status from the most recent port test
TotalErrors	Total number of errors detected.
TotalLinkResets	Total number of link resets.
TotalLIPsRecvd	Number of loop initialization primitive frames received by this port.

Table 53. Show Port parameters (Continued)

Entry	Description
TotalLIPsXmitd	Number of loop initialization primitive frames transmitted by this port.
TotalOfflineSeq	Total number of Offline Sequences issued and received by this port.
TotalRxFrames	Total number of frames received by this port.
TotalRxWords	Total number of words received by this port.
TotalTxFrames	Total number of frames issued by this port.
TotalTxWords	Total number of words issued by this port.
TxLinkResets	Number of Link Resets issued by this port.
TxOfflineSeq	Number of Offline Sequences issued by this port.
XmitterEnabled	Transmitter status

Examples

The following is an example of the Show Port command for external port 0 on a full-fabric switch:

```
IBM8Gb #> show port 0
 Port Number: 0
  ------------
  AdminState         Online
  AsicNumber         0
  AsicPort           0
  ConfigType         GL
  DownstreamISL      True
  EpConnState        Connected
  EpIsoReason        NotApplicable
  IOStreamGuard      Disabled
  Licensed           True
  LinkSpeed          8Gb/s
  LinkState          Active
  LoginStatus        LoggedIn
  MaxCredit          16
  MediaPartNumber    FTLF8528P2BCV
  MediaRevision      A
  MediaSpeeds        2, 4, 8Gb/s
  MediaType          800-MX-SN-S
  MediaVendor        FINISAR CORP.
  MediaVendorID      00009065
  OperationalState   Online
  PerfTuningMode     Normal
  PortID             6f0000
  PortWWN            20:00:00:c0:dd:0d:8d:ab
  POSTFaultCode      00000000
  POSTStatus         Passed
  RunningType        E
  SupportedSpeeds    1, 2, 4, 8Gb/s
  SymbolicName       Port0
  SyncStatus         SyncAcquired
  TestFaultCode      00000000
  TestStatus         NeverRun
  UpstreamISL        False
  XmitterEnabled     True

                      Port Statistics

  ALInit             37                 LIP_F8_F7          0
  ALInitError        0                  LinkFailures       0
  BadFrames          0                  Login              3
  BBCR_FrameFailures 0                  Logout             2
  BBCR_RRDYFailures  0                  LongFramesIn       0
  Class2FramesIn     0                  LoopTimeouts       0
  Class2FramesOut    0                  LossOfSync         1
  Class2WordsIn      0                  LostFrames         0
  Class2WordsOut     0                  LostRRDYs          0
  Class3FramesIn     0                  PrimSeqErrors      0
  Class3FramesOut    0                  RxLinkResets       3
  Class3Toss         0                  RxOfflineSeq       2
  Class3WordsIn      0                  ShortFramesIn      0
  Class3WordsOut     0                  TotalErrors        0
  DecodeErrors       0                  TotalLinkResets    41
  EpConnects         3                  TotalLIPsRecvd     8
  FBusy              0                  TotalLIPsXmitd     39
  FlowErrors         0                  TotalOfflineSeq    40
```

```
FReject            0                  TotalRxFrames      0
InvalidCRC         0                  TotalRxWords       0
InvalidDestAddr    0                  TotalTxFrames      0
LIP_AL_PD_AL_PS    0                  TotalTxWords       0
LIP_F7_AL_PS       0                  TxLinkResets       38
LIP_F7_F7          8                  TxOfflineSeq       38
LIP_F8_AL_PS       0
```

Show Post Log

Displays the Power On Self Test (POST) log which contains results from the most recently failed POST.

Authority

None

Syntax

show post log

Examples

The following is an example of the Show Post Log command:

```
IBM8Gb #> show postlog

    Queue:              POST
    Sequence Count:     467
    Success Count:      452
    Failed Count:       42
    Records:            53

    Record:             1 of 53
    Time:               day mmm dd hh:mm:ss yyyy
    Sequence Number:    5
    Consecutive Passes: 5

    Record:             2 of 53
    Time:               day mmm dd hh:mm:ss yyyy
    Sequence Number:    6
    Test:               TEST_SUITE_POST (0x13)
    Subtest:            TEST_STATIC_PORTADDR (0x72)
    Fault Code:         DIAGS_ERR_CPORT_VERIFY (0x34)
    Loops:              0
    Blade/Asic:         0/0
    Register Address:   0x00000005
    Received Data:      0x0082202b
    Expected Data:      0x00a2202b
    .
    .
    .
```

Show Power

Displays the status of power sensors.

Authority

None

Syntax

show power

Examples

The following is an example of the show power command:

```
IBM8Gb: admin> show power

  Power Sensors:

  Sensor  Description       Value
  ------  ----------------  -------
       0  Current             46.84
       1  1-Second Avg        46.32
       2  30-Second Avg       46.25
```

Show Setup Auth

Displays RADIUS and LDAP authentication information.

Authority

None

Syntax

show setup auth

Examples

The following is an example of the Show Setup Auth command:

```
IBM8Gb #> show setup auth
  Auth Information
  ----------------
  DeviceAuthOrder             Local
  UserAuthOrder               Local
  TotalRadiusServers          1
  TotalLdapServers            0

  Radius Information
  ------------------
  Radius Server: 1
  ServerIPAddress             10.1.1.1
  ServerUDPPort               1812
  DeviceAuthServer            False
  UserAuthServer              False
  AccountingServer            True
  Timeout                     2
  Retries                     0
  SignPackets                 False
  Secret                      12345
```

Show Setup Callhome

Displays the Call Home database configuration.

Authority

None

Syntax

show setup callhome

Examples

The following is an example of the Show Setup Callhome command:

```
IBM8Gb #> show setup callhome
  Callhome Information
  --------------------
  PrimarySMTPServerAddr       0.0.0.0
  PrimarySMTPServerPort       25
  PrimarySMTPServerEnabled    False
  SecondarySMTPServerAddr     0.0.0.0
  SecondarySMTPServerPort     25
  SecondarySMTPServerEnabled  False
  ContactEmailAddress         nobody@localhost.localdomain
  PhoneNumber                 <undefined>
  StreetAddress               <undefined>
  FromEmailAddress            nobody@localhost.localdomain
  ReplyToEmailAddress         nobody@localhost.localdomain
  ThrottleDupsEnabled         True

  + indicates active SMTP server
```

Show Setup Mfg

Displays manufacturing information about the switch.

Authority

None

Syntax

show setup mfg

Examples

The following is an example of the Show Setup Mfg command:

```
IBM8Gb #> show setup mfg
 Manufacturing Information
  -------------------------
  BrandName                IBM
  BuildDate                day, month day, yyyy hh:mm
  PartNumber               1234567890
  SerialNumber             5678901234
  LicensedExternalPorts    6
  LicensedInternalPorts    14
  MACAddress               00:c0:dd:0d:2b:40
  MAC1Address              00:c0:dd:0d:2b:41
  SwitchUUID               20202020202020202020202020202020
  PlanarPartNumber         Unknown
  SwitchSymbolicName       IBM8Gb
  SwitchWWN                10:00:00:c0:dd:0d:2b:40
  SystemDescription        IBM Flex System FC3171 8Gb SAN Switch
  SystemObjectID           1.3.6.1.4.1.3873.1.33
  CPLD Revision            0x410000,0x8
  MicroChip Version        107
```

Show Setup Services

Displays switch service status information.

Authority

None

Syntax

show setup services

Examples

The following is an example of the Show Setup Services command:

```
IBM8Gb #> show setup services
  System Services Information
  -----------------------------------
  EncryptionMode                 Legacy
  TelnetEnabled                  False
  SSH/sFTPEnabled                True
  GUIMgmtEnabled                 False
  SSLEnabled                     True
  EmbeddedGUIEnabled (HTTP)      False
  EmbeddedGUIEnabled (HTTPs)     True
  NTPEnabled                     True
  CIMEnabled                     True
  FTPEnabled                     False
  MgmtServerEnabled              True
  CallHomeEnabled                True
  SLPEnabled                     True
```

Show Setup SNMP

Displays the current SNMP settings.

Authority

None

Syntax

show setup snmp
common
trap

Keywords

common

Displays SNMP configuration parameters that are common to all traps. To display common and trap-specific parameters, omit the keyword. For information about the common configuration parameters, see Table 42.

trap

Displays trap-specific SNMP configuration parameters. To display common and trap-specific parameters, omit the keyword. For information about trap-specific configuration parameters, see Table 43.

Examples

The following is an example of the Show Setup Snmp Common command:

```
IBM8Gb #> show setup snmp common
  SNMP Information
  ----------------
  Contact               <sysContact undefined>
  Location              N_107 System
  Description           Lenovo Flex System FC3171 8 Gb SAN Switch
  ObjectID              1.3.6.1.4.1.3873.1.33
  AuthFailureTrap       True
  ProxyEnabled          True
```

The following is an example of the Show Setup Snmp Trap command:

```
IBM8Gb #> show setup snmp trap 1
  SNMP Information
  ----------------
  Trap1Enabled          False
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Version          2
  Trap1User             user1
```

Show Setup System

Displays network, logging, NTP server, and timer parameters on the switch.

Authority

None

Syntax

show setup system
dns
ipv4
ipv6
logging
ntp
timers

Keywords

dns

Displays DNS host name configuration parameters. To display all system configuration parameters, omit the keyword. For a information about the DNS host name configuration parameters, see Table 44.

ipv4

Displays IPv4 configuration parameters. To display all system configuration parameters, omit the keyword. For information about the IPv4 Ethernet configuration parameters, see Table 45.

ipv6

Displays IPv6 Ethernet configuration parameters. To display all system configuration parameters, omit the keyword. For information about the IPv6 Ethernet configuration parameters, see Table 46.

logging

Displays event logging configuration parameters. To display all system configuration parameters, omit the keyword. For information about the event logging configuration parameters, see Table 47.

ntp

Displays NTP server configuration parameters. To display all system configuration parameters, omit the keyword. For information about the NTP server configuration parameters, see Table 48.

timers

Displays timer configuration parameters. To display all system configuration parameters, omit the keyword. For information about timer configuration parameters, see Table 49.

Examples

The following is an example of the Show Setup System Dns command:

```
IBM8Gb #> show setup system dns

System Information
  ------------------
  DNSClientEnabled        False
  DNSLocalHostname        <undefined>
  DNSServerDiscovery      Static
  DNSServer1Address       <undefined>
  DNSServer2Address       <undefined>
  DNSServer3Address       <undefined>
  DNSSearchListDiscovery  Static
  DNSSearchList1          <undefined>
  DNSSearchList2          <undefined>
  DNSSearchList3          <undefined>
  DNSSearchList4          <undefined>
  DNSSearchList5          <undefined>
```

The following example of the Show Setup System Logging command:

```
IBM8Gb #> show setup system logging

  System Information
  ------------------
  RemoteLogEnabled         False
  RemoteLogHostAddress     10.0.0.254
```

The following is an example of the Show Setup System Ntp command:

```
IBM8Gb #> show setup system ntp

  System Information
  ------------------
  NTPClientEnabled    True
  NTPServerDiscovery  Static
  NTPServerAddress    10.35.4.203
  NTPAuthEnabled      True
  NTPAuthKey          ********
  NTPAuthKeyIndex     1
```

The following example of the Show Setup System Timers command:

```
IBM8Gb #> show setup system timers

  System Information
  ------------------
  AdminTimeout             30
  InactivityTimeout        0
```

Show Steering

Displays the routes that data takes in the fabric.

Authority

None

Syntax

show steering ***[domain_id]***

Keywords

[domain_id]
The domain ID for which to display route information. If you omit [domain_id], the system displays routes for all switches in the fabric.

Examples

The following is an example of the Show Steering command:

```
IBM8Gb #> show steering 35

  DomainID    DefaultOutPort    InPort OutPort
  --------    --------------    ------ -------
  35          18                3      16/18/16/18
                                5      18/16/18/16
                                6      16/18/16/18
                                7      16/18/16/18
                                15     18/16/18/16
```

Show Switch

Displays switch operational information.

Authority

None

Syntax

show switch

Notes

Table 54 describes the switch operational parameters.

Table 54. Switch operational parameters

Parameter	Description
SymbolicName	Descriptive name for the switch
SwitchWWN	Switch world wide name
BootVersion	PROM boot version
CreditPool	Number of port buffer credits available to recipient ports
DomainID	Switch domain ID
FirstPortAddress	FC address of switch port 0
FlashSize - MBytes	Size of the flash memory in megabytes
LogFilterLevel	Event severity level used to record events in the event log
MaxPorts	Number of ports available on the switch
NumberOfResets	Number of times the switch has been reset over its service life
ReasonForLastReset	Action that caused the last reset
ActiveImageVersion - build date	Active firmware image version and build date.
PendingImageVersion - build date	Firmware image version and build date that is pending. This image will become active at the next reset or power cycle.
ActiveConfiguration	Name of the switch configuration that is in use.
AdminState	Switch administrative state
AdminModeActive	Admin session status
BeaconOnStatus	Beacon status as set by the Set Beacon command.
OperationalState	Switch operational state
PrincipalSwitchRole	Principal switch status. True indicates that this switch is the principal switch.
POSTFaultCode	Fault code from the most recent Power-on self test
POSTStatus	Status from the most recent Power-on self test
TestFaultCode	Fault code from the most recent port test
TestStatus	Status from the most recent port test

Table 54. Switch operational parameters (Continued)

Parameter	Description
BoardTemp (1, 2, 3) - Degrees Celsius	Internal switch temperature at circuit board sensors 1, 2, and 3.
SwitchTemperatureStatus	Switch temperature status: normal, warning, failure.

Examples

The following is an example of the Show Switch command:

```
IBM8Gb #> show switch
Switch Information
------------------
SymbolicName                      IBM8Gb
SwitchWWN                         10:00:00:c0:dd:12:c8:b0
BootVersion                       V1.12.5.97.0 (day mon date hh:mm:ss yyyy)
CreditPool                        0
DomainID                          110 (0x6e)
FirstPortAddress                  6e0000
FlashSize - MBytes                256
LogFilterLevel                    Info
MaxPorts                          20
NumberOfResets                    7
ReasonForLastReset                HotReset
ActiveImageVersion - build date   V9.1.0.x.x (day mon date hh:mm:ss yyyy)
PendingImageVersion - build date  V9.1.0.x.x (day mon date hh:mm:ss yyyy)
ActiveConfiguration               default
AdminState                        Online
AdminModeActive                   False
BeaconOnStatus                    False
OperationalState                  Online
PrincipalSwitchRole               False
POSTFaultCode                     00000000
POSTStatus                        Passed
TestFaultCode                     00000000
TestStatus                        NeverRun
BoardTemp (1) - Degrees Celsius   22
BoardTemp (2) - Degrees Celsius   23
BoardTemp (3) - Degrees Celsius   24
SwitchTemperatureStatus           Normal
```

Show System

Displays the operational status of the Ethernet and DNS host name configuration parameters.

Authority

None

Syntax

show system

Examples

The following is an example of the Show System command:

```
IBM8Gb #> show system

  Assigned System Network Information
  ----------------------------------
  Hostname               hsb5802-2
  EthIPv4NetworkAddress  10.20.125.47
  EthIPv6NetworkAddress  fe80::2c0:ddff:fe01:6f27
  Eth1IPv4NetworkAddress 10.20.3.12
  DNSServer1             10.20.33.109
  DNSServer2             10.33.2.50
  DNSSearchList1         <undefined>
  DNSSearchList2         <undefined>
  IPv4GatewayList1       10.20.125.1
  IPv6GatewayList1       <undefined>
  NTPServer              10.35.4.203
```

Show Temp

Displays the current temperature, high warning threshold, and high alarm threshold for the switch temperature sensors.

Authority

None

Syntax

show temp

Examples

The following is an example of the Show Temp command.

```
IBM8Gb #> show temp
Temperature(C) Sensors:

  Sensor  Description          Status  Current  High Warn  High Alarm
  ------  -------------------  ------  -------  ---------  ----------
       0  BOARD                Normal       22         75          81
       1  DS1780               Normal       23        n/a         n/a
       2  MAX1617              Normal       24         75          80
       3  ASIC                 Normal       35        102         105
       4  LM75 0 (exhaust)     Normal       20         75          80
       5  LM75 1 (inlet)       Normal       24         75          80
```

Show Testlog

Displays the contents of the diagnostic field test log file.

Authority

None

Syntax

show testlog
or
show test log

Examples

The following is an example of the Show Testlog command:

```
IBM8Gb #> show testlog
    Queue:              UID
    Sequence Count:     676
    Success Count:      420
    Failed Count:       2023
    Records:            127

    Record:             1 of 127
    Time:               day mon dd hh:mm:ss yyyy
    Sequence Number:    211
    Test:               TEST_SUITE_BLADE_OFFLINE (0x12)
    Subtest:            TEST_FLOW_TC (0x97)
    Fault Code:         DIAGS_ERR_DATA_VERIFY (0x1e)
    Loops:              1
    Blade/Asic/Port:    0/0/0

    Record:             2 of 127
    Time:               day mon dd hh:mm:ss yyyy
    Sequence Number:    211
    Test:               TEST_SUITE_BLADE_OFFLINE (0x12)
    Subtest:            TEST_FLOW_TC (0x97)
    Fault Code:         DIAGS_ERR_DATA_VERIFY (0x1e)
    Loops:              1
    Blade/Asic/Port:    0/0/0
    .
    .
    .
```

Show Timezone

Displays the current time zone setting.

Authority

None

Syntax

show timezone

Examples

The following is an example of the Show Timezone command:

```
IBM8Gb #> show timezone

  America/Chicago
```

Show Topology

Displays information about devices connected to the switch.

Authority

None

Syntax

show topology *[port_number]*

Keywords

[port_number]
Displays the devices connected to the port given by [port_number].

Examples

The following is an example of the Show Topology command:

```
IBM8Gb #> show topology
  Unique ID Key
  -------------
  A = ALPA,  D = Domain ID,  P = Port ID

          Loc   Local                   Rem  Remote                  Unique
  Port    Type  PortWWN                 Type NodeWWN                 ID
  ----    ----  -------                 ---- -------                 ------
  Ext1:0  E     20:00:00:c0:dd:12:c8:b0 E    10:00:00:c0:dd:0c:a6:c0 102(0x66) D
  Ext6:19 E     20:13:00:c0:dd:12:c8:b0 E    10:00:00:c0:dd:0c:a6:84 103(0x67) D
  Bay2    F     20:02:00:c0:dd:12:c8:b0 N    20:01:00:e0:8b:a5:41:71 6e0200   P
  Bay3    F     20:03:00:c0:dd:12:c8:b0 N    20:01:00:e0:8b:a5:86:71 6e0300   P
  Bay4    F     20:04:00:c0:dd:12:c8:b0 N    20:01:00:e0:8b:a5:a7:71 6e0400   P
  Bay11   F     20:0b:00:c0:dd:12:c8:b0 N    20:00:00:0d:60:d3:b3:eb 6e0b00   P
```

The following is an example of the Show Topology command for port 0.

```
IBM8Gb  #> show topology 0
    Local Link Information
  ----------------------

  Port       Ext1:0
  PortID     6e0000
  PortWWN    20:00:00:c0:dd:12:c8:b0
  PortType   E

  Remote Link Information
  -----------------------

  Remote Switch

    PortNumber  48
    DomainID    66
    NodeWWN     10:00:00:c0:dd:0c:a6:c0
    PortType    E
    Description Switch
    IPAddress   10.20.108.185
```

Show Users

Displays a list of logged-in users. This is equivalent to the User List command.

Authority

None

Syntax

show users ***brief***

Keywords

brief

Displays just the account name and client.

Examples

The following is an example of the Show Users command:

```
IBM8Gb #> show users
  User             cim@OB-session1
  Client           cim
  Logged in Since  day mon  date hh:mm:ss yyyy

  User             snmp@IB-session2
  Client           Unknown
  Logged in Since  day mon  date hh:mm:ss yyyy

  User             snmp@OB-session3
  Client           Unknown
  Logged in Since  day mon  date hh:mm:ss yyyy

  User             admin@OB-session5
  Client           10.33.21.27
  Logged in Since  day mon  date hh:mm:ss yyyy
```

The following is an example of the Show Users Brief command:

```
IBM8Gb #> show users brief
  User                          Client
  ----                          ------
  cim@OB-session1               cim
  snmp@IB-session2              Unknown
  snmp@OB-session3              Unknown
  admin@OB-session5             10.33.21.27
```

Show Version

Displays an introductory set of information about operational attributes of the switch. This command is equivalent to the Show About command.

Authority

None

Syntax

show version

Notes

Table 55 describes the Show Version command display entries.

Table 55. Show Version display entries

Entry	Description
SystemDescription	Switch system description
HostName	DNS host name
EthIPv4NetworkAddress	External Ethernet port IP address, version 4
Eth1IPv4NetworkAddress	Internal Ethernet port IP address, version 4
EthIPv6NetworkAddress	External Ethernet port IP address, version 6
Eth1IPv6NetworkAddress	Internal Ethernet port IP address, version 6
MacAddress	MAC address for Eth0
Mac1Address	MAC address for Eth1
SwitchUUID	Switch universal unique identifier
WorldWideName	Switch worldwide name
SerialNumber	Switch serial number
SymbolicName	Switch symbolic name
ActiveSWVersion	Firmware version
ActiveTimestamp	Date and time that the firmware was activated
POSTStatus	Results of the Power-on Self Test
LicensedExernalPorts	Number of licensed external ports
LicensedInternalPorts	Number of licensed internal ports
SwitchMode	Full Fabric indicates that the switch operates with the standard Fibre Channel port types: G, GL, F, FL, E. Transparent indicates the switch operates as a pass-thru module with transparent port types TF and TH.

Examples

The following is an example of the Show Version command.

```
IBM8Gb #> show version
      ************************************************
      *                                              *
      *       Command Line Interface SHell  (CLISH)  *
      *                                              *
      ************************************************

       SystemDescription   Lenovo Flex System FC3171 8 Gb SAN Switch
       HostName            hsb5802-2
       EthIPv4NetworkAddr  10.20.125.47
       Eth1IPv4NetworkAddr 10.20.3.12
       EthIPv6NetworkAddr  fe80::2c0:ddff:fe01:6f27
       Eth1IPv6NetworkAddr fe80::2c0:ddff:fe01:6f28
       MACAddress          00:c0:dd:01:6f:27
       MAC1Address         00:c0:dd:01:6f:28
       SwitchUUID          20202020202020202020202020202020
       WorldWideName       10:00:00:c0:dd:01:6f:27
       SerialNumber        1029E00021
       SymbolicName        IBM8Gb
       ActiveSWVersion     V9.1.x.x.xxx
       ActiveTimestamp     day mon date hh:mm:ss yyyy
       POSTStatus          Passed
       LicensedExternalPorts 6
       LicensedInternalPorts 14
       SwitchMode          Full Fabric
```

Show Voltage

Displays current voltage, low alarm threshold voltage, and high alarm voltage threshold for the switch voltage sensors.

Authority

Admin session

Syntax

show voltage

Examples

The following is an example of the Show Voltage command:

```
IBM8Gb #> show voltage

  Voltage Sensors:

  Sensor  Description  Status  Current  Low Alarm  High Alarm
  ------  -----------  ------  -------  ---------  ----------
       0  1.5V         Good       1.50       1.31        1.68
       1  1.25V        Good       1.24       1.00        1.50
       2  2.5V         Good       2.49       2.20        2.82
       3  3.3V         Good       3.31       2.99        3.62
       4  12V          Good      11.44      10.81       13.31
       5  1.2V         Good       1.23       1.04        1.38
       6  1.8V         Good       1.78       1.61        1.99
       7  1.8V_ANALOG  Good       1.78       1.58        2.02
       8  2.5V_ANALOG  Good       2.39       2.10        2.82
```

Snmpv3user

Manages SNMP version 3 user accounts on the switch.

Authority

Admin session except for the List keyword

Syntax

snmpv3user
add
delete [account]
edit
list

Keywords

add

Creates an SNMP version 3 user account, prompting you for the parameters that are described in Table 56.

Table 56. SNMP Version 3 user account parameters

Parameter	Description
Username	Account user name
Group	Group type: Read-Only or Read-Write. The default is Read-Only.
Authentication	Enables (True) or disables (False) authentication. The default is False.
AuthType	Authentication type can be MD5 or SHA. The default is SHA. For EncryptionMode=Strict, only SHA is allowed. For information about EncryptionMode, see Table 41.
AuthPhrase	Authentication phrase
Confirm AuthPhrase	Authentication phrase confirmation. Re-enter the phrase.
Privacy	Enables (True) or disables (False) privacy. The default is False.
PrivType	Privacy type can be DES or AES. The default is DES. For EncryptionMode=Strict, only AES is allowed. For information about EncryptionMode, see Table 41.
PrivPhrase	Privacy phrase
Confirm PrivPhrase	Privacy phrase confirmation. Re-enter the phrase.

delete [account]

Deletes the SNMP version 3 user account given by [account].

edit

Modifies an SNMP version 3 user account, prompting you first for the account name to edit. For information about the SNMP version 3 user account parameters, see Table 56.

list

Displays SNMP version 3 user accounts, group, authentication type, and privacy type. This keyword does not require an Admin session.

Examples

The following is an example of the Snmpv3user Add command. Shaded entries indicate options that are available only when EncryptionMode=Legacy. For more information about EncryptionMode, see Table 41.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> snmpv3user add

      A list of SNMPV3 user attributes with formatting and default values as
      applicable will follow.

      Enter a new value OR simply press the ENTER key where-ever allowed to
      accept the default value.

      If you wish to terminate this process before reaching the end of the
list,
      press "q" or "Q" and the ENTER OR "Ctrl-C" key to do so.

  Username        (8-32 chars)                          : snmpuser1
  Group           (0=ReadOnly, 1=ReadWrite) [ReadOnly  ] : 1
  Authentication  (True/False)              [False     ] : t
  AuthType        (1=MD5, 2=SHA)            [SHA       ] : 1
  AuthPhrase      (8-32 chars)                          : ***********
  Confirm AuthPhrase                                    : ***********
  Privacy         (True/False)              [False     ] : t
  PrivType        (1=DES, 2=AES)            [DES       ] : 1
  PrivPhrase      (8-32 chars)                          : ********
  Confirm PrivPhrase                                    : ********

  Do you want to save and activate this snmpv3user setup ?   (y/n): [n] y

  SNMPV3 user added and activated.
```

The following is an example of the Snmpv3user Delete command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> snmpv3user delete snmpuser1

  The user account will be deleted. Please confirm (y/n): [n] y
  SNMPV3 user deleted.
```

The following is an example of the Snmpv3user List command:

```
IBM8Gb #> snmpv3user list

  Username                        Group           AuthType   PrivType
  --------                        -----           --------   --------
  snmpadmin1                      ReadWrite       SHA        DES
  snmpuser1                       ReadWrite       MD5        DES
```

Test Cancel

Cancels a port test that is in progress.

Authority

Admin session

Syntax

test cancel
port [port_number]

Keywords

port [port_number]
Cancel the test for the port given by [port_number]. [port_number] can be 0–19.

Examples

The following example cancels the test running on port 15:

```
IBM8Gb (admin) #> test cancel port 15
```

Test Port

Tests individual port performance.

Authority

Admin session

Syntax

test port [port_number]
offline [loopback_type]
online

Keywords

[port_number]

The port to be tested. [port_number] can be 0–19.

offline [loopback_type]

Performs an offline test of the type given by [loopback_type] on the port given by [port_number]. Use the Set Port command to place the port in the diagnostics state before running the test. [loopback_type] can have the following values:

internal

Exercises the internal port connections.

external

Exercises the port and its transceiver. A transceiver with a loopback plug is required for the port.

online

Exercises the port, transceiver, and device connections while the port is online. This test does not disrupt communication on the port.

Notes

Table 57 describes the port test parameters.

Table 57. Port Test parameters

Parameter	Description
LoopCount	Number of frames sent
FrameSize	Number of bytes in each test frame
DataPattern	Pattern in the payload
StopOnError	Stops the test when an error occurs (True). Otherwise, the test continues to completion.
LoopForever	Restarts the test after completion and continues until you cancel it (True). Otherwise, the test ends normally after completion.

To cancel a port test that is in progress, enter the Test Cancel Port command.

To display the status of the most recent port test or port test in progress, enter the Test Status Port command.

Examples

The following is an example of an internal test on port 1.

```
IBM8Gb #> admin start
IBM8Gb (admin) #> set port 1 state diagnostics
IBM8Gb (admin) #> test port 1 offline internal

  A list of attributes with formatting and current values will follow. Enter
a new
  value or simply press the ENTER key to accept the default value. If you wish
to
  terminate this process before reaching the end of the list press 'q' or 'Q'
and
  the ENTER key to do so.

  LoopCount     (decimal value, 1-4294967295)   [100      ]
  FrameSize     (decimal value, 40-2148)        [256      ]
  DataPattern   (32-bit hex value or 'Default') [Default  ]
  StopOnError   (True / False)                  [True     ]
  LoopForever   (True / False)                  [False    ]

  Do you want to start the test? (y/n) [n] y

  The test has been started.
  A notification with the test result(s) will appear
  on the screen when the test has completed.

IBM8Gb (admin) #>
  Test for port 1 Passed.
When the test is complete, remember to place the port back online.
IBM8Gb (admin) #> set port 1 state online
```

The following example performs an online test on port 0:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> test port 1 online

A list of attributes with formatting and current values will follow. Enter a
new value or simply press the ENTER key to accept the default value. If you
wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

LoopCount     (decimal value, 1-4294967295)   [100      ]
FrameSize     (decimal value, 40-2148)        [256      ]
DataPattern   (32-bit hex value or 'Default') [Default  ]
StopOnError   (True / False)                  [True     ]
LoopForever   (True / False)                  [False    ]

Do you want to start the test? (y/n) [n] y

The test has been started.
A notification with the test result(s) will appear
on the screen when the test has completed.

IBM8Gb (admin) #>
  Test for port 1 Passed.
```

Test Status

Displays the status of a test in progress, or if there is no test in progress, the status of the test that was executed last.

Authority

None

Syntax

test status

Examples

The following is an example of the Test Status command:

```
IBM8Gb (admin) #> test status port 1
Port               Test                Test                Loop      Test
Num      Port      Type                Status             Count  Failures
----     --------  ----                ------             -----  --------
1        1         Offline Internal    Passed                12         0
```

Test Switch

Tests all ports on the switch using a connectivity test, an offline test, or an online test.

Authority

Admin session

Syntax

test switch
connectivity [loopback_type]
offline [loopback_type]
online

Keywords

connectivity [loopback_type]
Performs a connectivity test of the type given by [loopback_type] on all switch ports. You must place the switch in the diagnostics state using the Set Switch State command before starting the test. [loopback_type] can be one of the following:

internal

Exercises all internal port and inter-port connections.

external

Exercises all internal port, transceiver, and inter-port connections. A transceiver with a loopback plug is required for all ports.

offline [loopback_type]

Performs an offline test of the type given by [loopback_type] on all switch ports. You must place the switch in the diagnostics state using the Set Switch State command before starting the test. [loopback_type] can have the following values:

internal

Exercises all internal port connections.

external

Exercises all port and transceiver connections. A transceiver with a loopback plug is required for all ports.

online

Exercises port-to-device connections for all ports that are online. This test does not disrupt communication on the ports.

Notes

Table 58 describes the switch test parameters.

Table 58. Switch test parameters

Parameter	Description
LoopCount	Number of frames sent: 1–4294967295. The default is 100.
FrameSize	Number of bytes in each test frame: 40–2148. The default is 256.
DataPattern	32-bit hexadecimal test value, or default, which defines random data
StopOnError	Stops the test when an error occurs (True). Otherwise, the test continues to completion.
LoopForever	Restarts the test after completion and continues until you cancel it (True). Otherwise, the test ends normally after completion.

To cancel a switch test in progress, enter the Test Cancel Switch command.

To display the status of a recent switch test or switch test in progress, enter the Test Status Switch command.

Examples

The following example performs an offline internal test on a switch:

```
IBM8Gb #> admin start
IBM8Gb (admin) #>set switch state diagnostics
IBM8Gb (admin) #> test switch offline internal

A list of attributes with formatting and current values will follow. Enter a
new value or simply press the ENTER key to accept the default value. If you
wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

LoopCount     (decimal value, 1-4294967295)   [100    ]
FrameSize     (decimal value, 40-2148)        [256    ]
DataPattern   (32-bit hex value or 'Default') [Default]
StopOnError   (True / False)                  [True   ]
LoopForever   (True / False)                  [False  ]

Do you want to start the test? (y/n) [n] y
```

Uptime

Displays the elapsed up time since the switch was last reset and reset method. A hot reset or non-disruptive firmware activation does not reset the elapsed up time reported by this command.

Authority

None

Syntax

uptime

Examples

The following is an example of the Uptime command:

```
IBM8Gb #> uptime

  Elapsed up time  : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
  Reason last reset: NormalReset
```

User

Administers and displays user accounts.

Authority

`USERID` account name and an Admin session. The Accounts and List keywords are available to all account names without an Admin session.

Syntax

user
accounts
add
delete [account_name]
edit
list *brief*

Keywords

accounts

Displays all user accounts that exist on the switch. This keyword is available to all account names without an Admin session.

add

Add a user account to the switch. You will be prompted for an account name, a password, authority, and an expiration date.

- a switch can have a maximum of 15 user accounts.
- Account names are limited to 15 characters; passwords must be 8–20 characters.
- Admin authority grants permission to use the Admin command to open an Admin session, from which all commands can be entered. Without Admin authority, you are limited to view-only commands.
- The expiration date is expressed in the number of days until the account expires (2000 maximum). The switch will issue an expiration alarm every day for seven days prior to expiration. 0 (zero) specifies that the account has no expiration date.

delete [account_name]

Deletes the account name given by [account_name] from the switch.

edit

Initiates an edit session that prompts you for the account name for which to change the expiration date and authority.

list *brief*

Displays the list of users currently logged in, the login date, and the login time. The User List command is equivalent to the Show Users command. This keyword is available to all account names without an Admin session. To display just the account name and client, enter the User List Brief command.

Notes

Authority level or password changes that you make to an account that is currently logged in do not take effect until that account logs in again.

Examples

The following is an example of the User Accounts command:

```
IBM8Gb (admin) #> user accounts

  Current list of user accounts
  -----------------------------
  images       (admin authority = False, never expires)
  admin        (admin authority = True , never expires)
  USERID       (admin authority = True , never expires)
  user1        (admin authority = True , never expires)
  user2        (admin authority = False, expires in < 50 days)
  user3        (admin authority = True , expires in < 100 days)
```

The following is an example of the User Add command:

```
IBM8Gb (admin) #> user add
    Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (8-20 chars)  : *******

please confirm account password: *******

set account expiration in days (0-2000, 0=never): [0] 100

should this account have admin authority? (y/n): [n] y

OK to add user account 'user1' with admin authority
and to expire in 100 days?

Please confirm (y/n): [n] y
```

The following is an example of the User Edit command:

```
IBM8Gb (admin) #> user edit

      Press 'q' and the ENTER key to abort this command.

  account name (1-15 chars)      : user1
  set account expiration in days (0-2000, 0=never): [0]
  should this account have admin authority? (y/n): [n]

  OK to modify user account 'user1' with no admin authority
  and to expire in 0 days?

  Please confirm (y/n): [n]
```

The following is an example of the User Delete command:

```
IBM8Gb (admin) #> user del user3

  The user account will be deleted.  Please confirm (y/n): [n] y
```

The following is an example of the User List command:

```
IBM8Gb (admin) #> user list

  User             cim@OB-session1
  Client           cim
  Logged in Since  day month date time year

  User             snmp@IB-session2
  Client           Unknown
  Logged in Since  day month date time year

  User             snmp@OB-session3
  Client           Unknown
  Logged in Since  day month date time year

  User             admin@OB-session8
  Client           10.33.21.27
  Logged in Since  day month date time year
```

Whoami

Displays the account name, session number, and switch domain ID for the session.

Authority

None

Syntax

whoami

Examples

The following is an example of the Whoami command:

```
IBM8Gb #> whoami

User name       : USERID@session2
Switch name     : IBM8Gb
Switch domain ID: 1 (0x1)
```

Zone

Manages zones and zone membership on a switch.

Authority

Admin session and a Zoning Edit session. For information about starting a Zoning Edit session, see the "Zoning Edit" command on page 377. The List, Members, and Zonesets keywords are available without an Admin session.

Syntax

zone
add [zone] [member_list]
copy [zone_source] [zone_destination]
create [zone]
delete [zone]
list
ophans
members [zone]
remove [zone] [member_list]
rename [zone_old [zone_new]
zonesets [zone]

Keywords

add [zone] [member_list]

Specifies one or more ports/devices given by [members] to add to the zone named [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. A zone can have a maximum of 2000 members. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format *xx:xx:xx:xx:xx:xx:xx:xx*.
- Alias name

The application verifies that the [members] format is correct, but does not validate that such a member exists.

copy [zone_source] [zone_destination]

Creates a new zone named [zone_destination] and copies the membership into it from the zone given by [zone_source].

create [zone]

Creates a zone with the name given by [zone]. An zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 2000 zones.

delete [zone]

Deletes the specified zone given by [zone] from the zoning database. If the zone is a component of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated.

list

Displays a list of all zones and the zone sets of which they are components. This keyword does not require an Admin session.

orphans

Displays a list of zones that are not members of any zone set.

members [zone]

Displays all members of the zone given by [zone]. This keyword does not require an Admin session.

remove [zone] [member_list]

Removes the ports/devices given by [member_list] from the zone given by [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format *xx:xx:xx:xx:xx:xx:xx:xx*.
- Alias name

rename [zone_old] [zone_new]

Renames the zone given by [zone_old] to the zone given by [zone_new].

zonesets [zone]

Displays all zone sets of which the zone given by [zone] is a component. This keyword does not require an Admin session.

Examples

The following is an example of the Zone List command:

```
IBM8Gb #> zone list

  Zone        ZoneSet
  -------------------
  wwn_b0241f
              zone_set_1

  wwn_23bd31
              zone_set_1

  wwn_221416
              zone_set_1

  wwn_2215c3
              zone_set_1

  wwn_0160ed
              zone_set_1

  wwn_c001b0
              zone_set_1

  wwn_401248
              zone_set_1

  wwn_02402f
              zone_set_1

  wwn_22412f
              zone_set_1
```

The following is an example of the Zone Members command:

```
IBM8Gb #> zone members wwn_b0241f

  Current List of Members for Zone: wwn_b0241f
  --------------------------------
  50:06:04:82:bf:d2:18:c2
  50:06:04:82:bf:d2:18:d2
  21:00:00:e0:8b:02:41:2f
```

The following is an example of the Zone Zonesets command:

```
IBM8Gb #> zone zonesets zone1

  Current List of ZoneSets for Zone: zone1
  --------------------------------
  zone_set_1
```

Zoneset

Manages zone sets and component zones across the fabric.

Authority

Admin session and a Zoning Edit session. For information about starting a Zoning Edit session, see the Chapter , "Zoning Edit" on page 377. The Active, List, and Zones keywords are available without an Admin session. You must close the Zoning Edit session before using the Activate and Deactivate keywords.

Syntax

zoneset
activate [zone_set]
active
add [zone_set] [zone_list]
copy [zone_set_source] [zone_set_destination]
create [zone_set]
deactivate
delete [zone_set]
list
remove [zone_set] [zone_list]
rename [zone_set_old] [zone_set_new]
zones [zone_set]

Keywords

activate [zone_set]

Activates the zone set given by [zone_set]. This keyword deactivates the active zone set. Close the Zoning Edit session before using this keyword.

active

Displays the name of the active zone set. This keyword does not require Admin session.

add [zone_set] [zone_list]

Adds a list of zones and aliases given by [zone_list] to the zone set given by [zone_set]. Use a <space> to delimit zone and alias names in [zone_list].

copy [zone_set_source] [zone_set_destination]

Creates a new zone set named [zone_set_destination] and copies into it the zones from the zone set given by [zone_set_source].

create [zone_set]

Creates the zone set with the name given by [zone_set]. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 zone sets.

deactivate

Deactivates the active zone set. Close the Zoning Edit session before using this keyword.

delete [zone_set]

Deletes the zone set given by [zone_set]. If the specified zone set is active, the command is suspended until the zone set is deactivated.

list

Displays a list of all zone sets. This keyword does not require an Admin session.

remove [zone_set] [zone_list]

Removes a list of zones given by [zone_list] from the zone set given by [zone_set]. Use a <space> to delimit zone names in [zone_list]. If [zone_set] is the active zone set, the zone will not be removed until the zone set has been deactivated.

rename [zone_set_old] [zone_set_new]

Renames the zone set given by [zone_set_old] to the name given by [zone_set_new]. You can rename the active zone set.

zones [zone_set]

Displays all zones that are components of the zone set given by [zone_set]. This keyword does not require an Admin session.

Notes

- A zone set must be active for its definitions to be applied to the fabric.
- Only one zone set can be active at one time.
- A zone can be a component of more than one zone set.

Examples

The following is an example of the Zoneset Active command:

```
IBM8Gb #> zoneset active

Active ZoneSet Information
--------------------------
  ActiveZoneSet    Beta
  LastActivatedBy  admin@OB-session6
  LastActivatedOn  day month date time year
```

The following is an example of the Zoneset List command:

```
IBM8Gb #> zoneset list

  Current List of ZoneSets
  ------------------------
  alpha
  beta
```

The following is an example of the Zoneset Zones command:

```
IBM8Gb #> zoneset zones ssss

  Current List of Zones for ZoneSet: ssss
  ---------------------------------
  zone1
  zone2
  zone3
```

Zoning Active

Displays information for the active zone set or saves the active zone set to the non-volatile zoning database.

Authority

Admin session for the Capture keyword.

Syntax

zoning active
capture

Keywords

capture
Saves the active zone set to the non-volatile zoning data base.

Examples

The following is an example of the Zoning Active command:

```
IBM8Gb #> zoning active
Active (enforced) ZoneSet Information
  ZoneSet     Zone      ZoneMember
  -------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3
```

The following is an example of the Zoning Active Capture command:

```
IBM8Gb (admin) #> zoning active capture
  This command will overwrite the configured zoning database in NVRAM.
  Please confirm (y/n): [n] y

  The active zoning database has been saved.
```

Zoning Cancel

Closes the current Zoning Edit session. Any unsaved changes are lost.

Authority

Admin session and a Zoning Edit session.

Syntax

zoning cancel

Examples

The following is an example of the Zoning Cancel command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
.
.
.
IBM8Gb (admin-zoning) #> zoning cancel
  Zoning edit mode will be canceled.  Please confirm (y/n): [n] y
```

Zoning Clear

Clears all inactive zone sets from the volatile edit copy of the zoning database. This keyword requires a zoning edit session. This keyword does not affect the non-volatile zoning database. However, if you enter the Zoning Clear command followed by the Zoning Save command, the non-volatile zoning database will be cleared from the switch.

Authority

Admin session and a Zoning Edit session.

Syntax

zoning clear

Notes

The preferred method for clearing the zoning database from the switch is the Reset Zoning command

Examples

The following is an example of the Zoning Clear command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #> zoning clear
IBM8Gb (admin-zoning) #> zoning save
```

Zoning Configured

Displays the contents of the non-volatile zoning database.

Authority

None

Syntax

zoning configured

Examples

The following is an example of the Zoning Configured command:

```
IBM8Gb #> zoning configured

  Configured (saved in NVRAM) Zoning Information
  ZoneSet     Zone      ZoneMember
  -------     ----      ----------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:16
```

Zoning Delete Orphans

Deletes all objects that are not part of the active zone set, including zone sets, zones, and aliases.

Authority

Admin session

Syntax

zoning delete orphans

Examples

The following is an example of the Zoning Delete Orphans command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning delete orphans
   This command will remove all zonesets, zones, and aliases
   that are not currently active.
Please confirm (y/n): [n] y
IBM8Gb (admin) #> zoning save
```

Zoning Edit

Opens a Zoning Edit session for the non-volatile zoning database or the merged zone set in which to create and manage zone sets and zones. See the "Zone" command on page 367 and the "Zoneset" command on page 370.

Authority

Admin session

Syntax

zoning edit ***[database]***

Keywords

[database]

Opens an edit session for the zoning database given by [database]. If you omit [database], an edit session for the non-volatile zoning database is opened. [database] can have the following values:

configured
Opens a zoning edit session for the non-volatile zoning database.

merged
Opens a zoning edit session for the temporary merged zone set received from another switch.

Examples

The following is an example of the Zoning Edit command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #>
.
.
IBM8Gb (admin-zoning) #> zoning save
  The changes have been saved; however, they must be activated
   before they can take effect -- see zoneset activate command.
```

Zoning Edited

Displays the contents of the edited zoning database.

Authority

Admin session and a Zoning Edit session

Syntax

zoning edited

Examples

The following is an example of the Zoning Edited command:

```
IBM8Gb (admin-zoning) #> zoning edited
Edited (unsaved) Zoning Information
ZoneSet         Zone             ZoneMember
-------         ----             ----------
ZS1
                Z1
                                 10:00:00:c0:dd:00:b9:f9
                                 10:00:00:c0:dd:00:b9:fa
```

Zoning History

Displays a history of zoning modifications. This keyword does not require an Admin session. History information includes the following:

- Time of the most recent zone set activation or deactivation and the user who performed it
- Time of the most recent modifications to the zoning database and the user who made them.
- Checksum for the zoning database

Authority

None

Syntax

zoning history

Examples

The following is an example of the Zoning History command:

```
IBM8Gb #> zoning history
  Active Database Information
  ---------------------------
  ZoneSetLastActivated/DeactivatedBy  Remote
  ZoneSetLastActivated/DeactivatedOn  day mon date hh:mm:ss yyyy
  Database Checksum                   00000000

  Inactive Database Information
  -----------------------------
  ConfigurationLastEditedBy           admin@OB-session17
  ConfigurationLastEditedOn           day mon date hh:mm:ss yyyy
  Database Checksum                   00000000
```

Zoning Limits

Displays the limits and numbers of zone sets, zones, aliases, members per zone, members per alias, and total members in the zoning database.

Authority

None

Syntax

zoning limits
brief

Keywords

brief
Displays zoning limits for each category, the current number of objects, and the applicable zoning database (non-volatile or active). If you omit this keyword, the display includes a membership breakdown for each zone.

Notes

The specific zoning database limits are described in Table 59.

Table 59. Zoning database limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256)
MaxZones	Maximum number of zones (2000)
MaxAliases	Maximum number of aliases (2500)
MaxTotalMembers	Maximum number of zone and alias members (10000) that can be stored in the switch's zoning database. Each instance of a zone member or alias member counts toward this maximum.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (2000), excluding those in the orphan zone set, that can be stored in the switch's zoning database. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2000)
MaxMembersPerAlias	Maximum number of members in an alias (2000)

Zoning List

Lists all zoning definitions, including the applicable zoning database.

Authority

None

Syntax

zoning list

Examples

The following is an example of the Zoning List command:

```
IBM8Gb #> zoning list

  Active (enforced) ZoneSet Information
  ZoneSet     Zone      ZoneMember
  -------------------------------
  wwn
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3

  Configured (saved in NVRAM) Zoning Information
  ZoneSet     Zone      ZoneMember
  -------------------------------
  wwn
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:16
```

Zoning Merged

Displays the contents of the merged zone set, or saves the merged zone set to the non-volatile zoning database.

Authority

Admin session for the Capture keyword.

Syntax

zoning merged
capture

Keywords

capture

Saves the merged zone set to the non-volatile zoning database. You must enter the Zoning Save command afterwards to save your changes. If you omit this keyword, this command displays the contents of the merged zone set.

Examples

The following is an example of the Zoning Merged command:

```
IBM8Gb #> zoning merged
*****************************************************************
To permanently save the merged database locally, execute the
'zoning merged capture' command. To edit the merged database
use the ’zoning edit merged’ command. To remove the merged database
use the ’zoning restore’ command.
*****************************************************************
Merged (unsaved) Zoning Information
ZoneSet         Zone             ZoneMember
-------         ----             ----------
ZS1
                Z1
                                 10:00:00:c0:dd:00:b9:f9
                                 10:00:00:c0:dd:00:b9:fa
                Z2
                                 10:00:00:c0:dd:00:b9:fb
                                 10:00:00:c0:dd:00:b9:fc
```

The following is an example of the Zoning Merged Capture command:

```
IBM8Gb (admin) #> zoning merged capture
  This command will overwrite the configured zoning database in NVRAM.
  Please confirm (y/n): [n] y

  The merged zoning database has been saved.
```

Zoning Restore

Restores the volatile zoning database with the contents of the non-volatile zoning database. If the MergeAutoSave parameter is False (see Table 21), you can use this command to revert changes to the merged zone set that were propagated from another switch in the fabric through zone set activation or merging fabrics.

Authority

Admin session

Syntax

zoning restore

Zoning Save

Saves changes made during the current Zoning Edit session. The system informs you that the zone set must be activated to implement any changes.

Authority

Admin session and a Zoning Edit session.

Syntax

zoning save

Examples

The following is an example of the Zoning Save command:

```
IBM8Gb #> admin start
IBM8Gb (admin) #> zoning edit
IBM8Gb (admin-zoning) #>
.
.
IBM8Gb (admin-zoning) #> zoning save
  The changes have been saved; however, they must be activated
   before they can take effect -- see zoneset activate command.
```

Appendix A. Mapping port locations and software numbering

The switch has six external Fibre Channel ports (0, 15, 16, 17, 18, and 19) and 14 internal Fibre Channel ports that connect to each of the 14 blade server bays (ports 1 to 14). QuickTools and the CLI require port numbering from 0 to 19. The SNMP monitoring agent for the switch module numbers the ports from 1 to 20.

Table 60 shows the mapping of switch port numbering for Lenovo Flex System configurations and whether these ports can be configured.

Table 60. Port mapping for server units

Physical Port Connection	QuickTools, CLI, Logical Port Number	SNMP Port Numbering	Configurable
External port 1	0 Ext(1:0[1])	1	Yes
Server bay 1	1	2	No
Server bay 2	2	3	No
Server bay 3	3	4	No
Server bay 4	4	5	No
Server bay 5	5	6	No
Server bay 6	6	7	No
Server bay 7	7	8	No
Server bay 8	8	9	No
Server bay 9	9	10	No
Server bay 10	10	11	No
Server bay 11	11	12	No
Server bay 12	12	13	No
Server bay 13	13	14	No
Server bay 14	14	15	No
External port 2	15 Ext(2:15[1])	16	Yes
External port 3	16 Ext(3:16[1])	17	Yes
External port 4	17 Ext(4:17[1])	18	Yes
External port 5	18 Ext(5:18[1])	19	Yes
External port 6	19 Ext(6:19[1])	20	Yes

[1] Indicates a symbolic port name if it is different from the logical port number.

Appendix B. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Use this information to obtain additional information about Lenovo and Lenovo products, and determine what to do if you experience a problem with your Lenovo system or optional device.

Note: This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for the BladeCenter, System x, Flex System, and NeXtScale System products.

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 warranty service for your Lenovo product, the 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 software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your 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 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 the service technician. This data will help the service technician 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 (Lenovo 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 the service technicians. The 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 Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs 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 Lenovo system and preinstalled software, if any, or optional device is available in the product documentation. 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. Lenovo 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 Lenovo products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about Lenovo systems, optional devices, services, and support is available at http://www.ibm.com/supportportal. The most current version of the Flex System product documentation is available at http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with your Lenovo 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

IBM is Lenovo's preferred service provider for the BladeCenter, System x, Flex System and NeXtScale System products.

You can receive hardware service through your Lenovo reseller or from IBM. To locate a reseller authorized by Lenovo to provide warranty service, go to http://www.ibm.com/partnerworld and click Business Partner Locator. 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.

Taiwan product service

IBM is Lenovo's preferred service provider for the BladeCenter, System x, Flex System and NeXtScale System products. 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

Appendix C. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo 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:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO 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 jurisdictions 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. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

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

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

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo, the Lenovo logo, BladeCenter, Flex System, NeXtScale System, and System x are trademarks of Lenovo in the United States, other countries, or both.

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

Important notes

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

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 1 024 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 Lenovo.

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. Lenovo 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.

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

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

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Part Number: 00WA190

Printed in USA

(1P) P/N: 00WA190