HP 8/20q Fibre Channel Switch Command Line Interface Guide

This guide provides information about using the HP 8/20q Fibre Channel Switch Command Line Interface (CLI), including fabric, switch, and port management tasks. This guide also provides an alphabetical listing of the CLI commands, including the command syntax, operands, and notes, and examples of their use. This guide is for users who are responsible for installing and servicing Fibre Channel equipment using the command line interface.

Part number: 5697-1319
Published January 2012
Edition: 3

Legal and notice information

© Copyright 2008-2012 Hewlett-Packard Development Company, L.P.

© Copyright 2008-2012 This software includes technology under a license from QLogic Corporation. All rights reserved.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, Windows, Windows XP, and Windows NT and Internet Explorer are U.S. registered trademarks of Microsoft Corporation.

HP 8/20q Fibre Channel Switch Command Line Interface Guide

Contents

Tables

1 Command Line Interface Usage

This section describes how to use the command line interface.

NOTE: Throughout this document, references in the text to commands and keywords use initial capitalization for clarity. Actual command and operand entries are not case-sensitive.

Logging in to the switch through Telnet

To log in to a switch through Telnet:

1. Open a command line window on the workstation and then enter the `telnet` command followed by the switch Internet Protocol (IP) address:

   ```
   # telnet ip_address
   ```

   The IP address can be one of the following:

   - 4-byte IP version 4 (IPv4) address
   - 16-byte IP version 6 (IPv6) address
   - Domain Name System (DNS) host name (requires a DNS server)

   The Telnet window opens prompting you for a login.
2. Enter an account name and password. The default account name is `admin`, and the password is `password`.

   ```
   switch login:admin
   password: xxxxxxxx
   ```

   The following warning appears each time you log in until you change the default password.

   ```
   Warning:  Your user account password has not been changed. It is strongly
   recommended that you do so before proceeding.
   ```

To log off, enter the `exit` command:

```
8/20q FC Switch #> exit
```

To log in to a switch through the serial port:

1. Configure the workstation port with the following settings:
   - 9,600 baud
   - 8-bit character
   - 1 stop bit
   - No parity
2. Enter an account name and password when prompted. The default account name is `admin`, and the password is `password`.

NOTE: A switch supports a combined maximum of 19 logins or sessions, which are reserved as follows:

- 4 logins or sessions for internal applications, such as management server and Simple Network Management Protocol (SNMP)
- 9 high priority Telnet sessions
- 6 logins or sessions for SAN Connection Manager (SCM) inband and out-of-band logins, QuickTools logins, Enterprise Fabric Management Suite logins, and 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #>
.
.
.
8/20q FC Switch (admin) #> admin end
```

Entering commands

The command-line completion feature makes entering and repeating commands easier. 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 you are inquiring about. The following is an example of the help that is available for the `config edit` command.

```
8/20q FC Switch #> 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 by too quickly to read it. You can limit the display to 20 lines at a time by turning on page breaks. By default, page breaks are turned off. The following example shows how to turn page breaks on and how it affects the display.

```
8/20q FC Switch #> set pagebreak on
8/20q FC Switch #> zone list

  Zone         ZoneSet
  ----         -------
  Zone1
               alpha
               beta

  Zone2
               delta
               echo

  Zone3
               sierra
               tango

  Zone4
               gamma
               delta

Press any key to continue, 'q' to quit ...
```

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, which 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 File Transfer Protocol (FTP) server, you can proceed with the command prompts to send the file from the switch to a remote host. Otherwise, you can use FTP to download the support file from the switch to your workstation.

NOTE: Support files are deleted from the switch during a power-cycle or switch reset.

The following example creates a support file and sends it to a remote host using a workstation with an FTP server.

```
8/20q FC Switch #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): y
Enter address of ftp server (hostname, IPv4, or IPv6): 10.20.33.130
Login name: johndoe
Enter remote directory name: bin/support
Would you like to continue downloading support file? (y/n) [n]: y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password:  xxxxxxx

230 User johndoe logged in.
cd bin/support
250 CWD command successful.
lcd /itasca/conf/images
Local directory now /itasca/conf/images
bin
200 Type set to I.
put dump_support.tgz
local: dump_support.tgz remote: dump_support.tgz
227 Entering Passive Mode (10,20,33,130,232,133)
150 Opening BINARY mode data connection for dump_support.tgz.
226 Transfer complete.
43430 bytes sent in 0.292 secs (1.5e+02 Kbytes/sec)
Remote system type is UNIX.
Using binary mode to transfer files.
221-You have transferred 43430 bytes in 1 files.
221-Total traffic for this session was 43888 bytes in 1 transfers.
221 Thank you for using the FTP service on localhost.localdomain.
```

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

```
8/20q FC Switch #> 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:

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

   ```
   >ftp 10.0.0.1
   ```
3. When prompted for a user and password, enter the FTP account name and password (`images`, `images`).

   ```
   user: images
   password: images
   ```
4. Set binary mode and use the `get` command to download the file (`dump_support.tgz`).

   ```
   ftp>bin
   ftp>get dump_support.tgz
       xxxxx bytes sent in xx secs.
   ftp>quit
   ```

Downloading and uploading files

Several files that reside on the switch can be downloaded to the workstation for examination or for safekeeping. These files include the following:

- Backup configuration file (`configdata`)
- Log files (`logfile`)
- 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. The switch uses FTP to exchange files between the switch and the workstation.

To download a file from the switch to the workstation:

1. Enter the `ftp` command and the switch IP address or symbolic name.

```
>ftp 10.0.0.1
```

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

```
user: images
password: images
```

3. Set binary mode and use the `get` command to download the file (`configdata`).

```
ftp>bin
ftp>get configdata
    xxxxx bytes sent in xx secs.
ftp>quit
```

To upload a file from the workstation to the switch:

1. Enter the `ftp` command and the switch IP address or symbolic name.

```
>ftp 10.0.0.1
```

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

```
user:images
password: images
```

3. Set binary mode and use the `put` command to upload the file (`config_switch_169`).

```
ftp>put config_switch_169 configdata
    xxxxx bytes sent in xx secs.
ftp>quit
```

For more information about reinstallation, backup and restore, and creating support and log files:

- See "Installing firmware" (page 58).
- See "Backing up and restoring a switch configuration" (page 54).
- See "Creating and downloading a log file" (page 111).
- See "Creating a support file" (page 13).

2 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 purpose. These accounts cannot be deleted from the switch.

Table 2 Factory user accounts

User Account Name	Password	Purpose
admin	password	Provides access to the Telnet server for managing the switch. Admin is the only account name that has permission to create and modify other user accounts. To secure your admin user account, be sure to change the password for this account.
images	images	Provides access to the FTP server for exchanging files between the switch and the workstation.
prom	prom	When in Maintenance mode, provides access to the Maintenance menu to perform switch recovery tasks. For information about using Maintenance mode, see the *HP 8/20q Fibre Channel Switch Installation and Reference Guide*.

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` commands).

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

```
8/20q FC Switch (admin) #> user accounts

  Current list of user accounts
-----------------------------
images       (admin authority = False, never expires)
admin        (admin authority = True , never expires)
chuckca      (admin authority = False, expires in < 50 days)
gregj        (admin authority = True , expires in < 100 days)
fred         (admin authority = True , never expires)
```

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

```
8/20q FC Switch (admin) #> user list

User                          Ethernet Addr-Port    Logged in Since
----                          ------------------    ---------------
admin@OB-session1             10.20.68.108-1031     day month date time year
admin@OB-session2             10.20.68.108-1034     day month date time year
snmp@OB-session3              Unknown               day month date time year
snmp@IB-session4              Unknown               day month date time year
admin@OB-session5             Unknown               day month date time year
```

Creating user accounts

A user account consists of an account name, an authority level, and an expiration date, which have the following requirements:

- The account name can be up to 15 characters: the first character must be alphanumeric; the remaining characters must be American Standard Code for Information Interchange (ASCII) characters except semicolon (;), comma (,), #, and period (.).
- The authority level grants admin authority (true) or denies it (false).
- The expiration date sets the date when the user account expires.

Only the Admin user account can create user accounts. Add user accounts with the `user add` command.

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

```
8/20q FC Switch (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 `admin` user 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 edits 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`.

```
8/20q FC Switch (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`.

```
8/20q FC Switch (admin) #> user delete user3

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

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

```
8/20q FC Switch #> admin start
8/20q FC Switch (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.
```

3 Network Configuration

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

Displaying the network configuration

The `show fabric` command displays IP addresses (`Enet IP Addr`) for all switches in the fabric, as shown in the following example.

```
8/20q FC Switch #> show fabric
  Domain           *133(0x85)
  WWN              10:00:00:c0:dd:0d:53:91
  SymbolicName     8/20q FC Switch
  HostName         <undefined>
  EthIPv4Address   10.20.116.133
  EthIPv6Address   <undefined>

  * indicates principal switch
```

The `show setup system` command displays the entire switch network configuration, which includes the following:

- IP configurations (versions 4 and 6)
- DNS server configuration

To display specific information, add the corresponding keyword. For example, to display IPv6 configuration information, enter the `show setup system ipv6` command:

```
8/20q FC Switch #> show setup system ipv6

  System Information
  ------------------
  EthIPv6NetworkEnable          False
  EthIPv6NetworkDiscovery       Static
  EthIPv6NetworkAddress         2001::1/64
  EthIPv6GatewayAddress         fe80::1
```

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, page 22
- IPv6 configuration, page 23
- DNS server configuration, page 24

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 supports network discovery from the following server types:

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

To configure the IPv4 parameters, enter the `set setup system ipv4` command:

```
8/20q FC Switch (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 or from a DHCP server; or it can be learned from a router through the Neighbor Discovery Protocol (NDP). To configure the IPv6 parameters, enter the `set setup system ipv6` command:

```
8/20q FC Switch (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. This enables you to specify servers and switches by a meaningful name rather than IP address. To configure a DNS server, enter the `set setup system dns` command in an Admin session, as shown in the following example:

```
8/20q FC Switch (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 use the `ping` command to verify that a switch is communicating in the network. The following example successfully tests the network for a switch with IP address 10.20.11.57.

```
8/20q FC Switch #> ping 10.20.11.57
  Ping command issued. Waiting for response...
8/20q FC Switch #>
  Response successfully received from 10.20.11.57.
```

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

```
8/20q FC Switch #> ping 10.20.11.57
  Ping command issued. Waiting for response...
  No response from 10.20.11.57. Unreachable.
```

Managing IP security

To modify IP security, you must open an Admin session with the `admin start` command, then open an Ipsec Edit session with the `ipsec edit` command. The Admin session prevents other accounts from making changes at the same time through Telnet, SAN Connection Manager, or any other management application. 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 configuration, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec)#> ipsec . . .
8/20q FC Switch (admin-ipsec)#> ipsec policy . . .
8/20q FC Switch (admin-ipsec)#> ipsec association. . .
8/20q FC Switch (admin-ipsec)#> ike peer . . .
8/20q FC Switch (admin-ipsec)#> ike policy . . .
```

The `ipsec save` command saves the changes you made during the Ipsec Edit session. Changes take effect immediately.

```
8/20q FC Switch (admin-ipsec)#> ipsec save
```

To close the Ipsec Edit session without saving changes, enter the `ipsec cancel` command.

```
8/20q FC Switch (admin-ipsec)#> ipsec cancel
```

The `admin end` command releases the Admin session for other administrators when you are finished making changes to the switch.

To remove all IP security policies, security associations, IKE peers, and IKE polices, enter the `reset ipsec` command.

```
8/20q FC Switch (admin) #> reset ipsec
```

The following subsections describe IP security concepts and IP security management tasks:

IP security concepts

IP security provides encryption-based security for IPv4 and IPv6 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.

IMPORTANT: IP security configurations can be complex: it is possible to unintentionally configure policies and associations that isolate a switch from all communication. If this happens, you can disable IP security by placing the switch in maintenance mode, and correct the problem through the serial port interface. For information about using maintenance mode and connecting through the serial port, see the *HP 8/20q Fibre Channel Switch Installation and Reference Guide*.

Security policies and associations

Security policies are located in the security policy database and define 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 the Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), or the User Datagram Protocol (UDP). Furthermore, instead of applying IP security, you can choose to discard all inbound or outbound traffic, or to 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 configuration of matching IP security associations on the switch and on the connected device (or peer). The IKE peer defines the IKE security association connection through which the IKE policy 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 configuration information:

- IP security policy and association information, page 26
- IKE peer and policy information, page 27
- Public key infrastructure information, page 27
- IP security configuration history, page 28
- IP security configuration limits, page 28

IP security 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:

```
8/20q FC Switch #> 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. Within 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:

```
8/20q FC Switch #> 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 key512:

```
8/20q FC Switch #> key list key512
  Key key512:
    private key with:
    pubkey:    RSA 512 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:
8/20q FC Switch #> key list
  Installed Keys:
    key512
    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:

```
8/20q FC Switch #> 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
```

History includes the following information:

- 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
- Checksum for the IKE database

IP security configuration limits

To display a summary of the objects in the IP security configuration and their maximum limits, enter the `ipsec limits` command, as shown in the following example:

```
8/20q FC Switch #> ipsec limits

  Configured (saved) IPsec Information

  IPsec Attribute            Maximum  Current
  ---------------            -------  -------
  MaxConfiguredSAs               512        0
  MaxConfiguredSPs               128        0
  MaxConfiguredIKEPeers           16        0
  MaxConfiguredIKEPolicies       256        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.

Creating a policy

To create a policy, enter the `ipsec policy create` command as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (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      (IPv4, IPv6 or hostname/[PrefixLength])   :
                                                   fe80::2c0:ddff:fe03:d4c1
    SourcePort         (decimal value, 1-65535)                  :
   *DestinationAddress (IPv4, IPv6 or hostname/[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.
```

Deleting a policy

To delete a user-defined policy, enter the `ipsec policy delete` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ipsec policy delete policy_1
  The security policy will be deleted. Please confirm (y/n): [n] y

8/20q FC Switch (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.

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (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)                        :
    Mode                (1=transport, 2=tunnel)                :
   *TunnelSource        (IPv4, or IPv6 Address)                :
   *TunnelDestination   (IPv4, or IPv6 Address)                :
   *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.

8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ipsec policy rename policy_1 policy_4

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

8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ipsec policy copy policy_1 policy_a
8/20q FC Switch (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.

Creating an association

To create an association, enter the `ipsec association create` command as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (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)
                          1=des-cbc        (8 byte key)
                          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)      :
                                                 "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.
```

Deleting an association

To delete a user-defined association, enter the `ipsec association delete` command as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ipsec association delete association_1
  The security association will be deleted. Please confirm (y/n): [n] y

8/20q FC Switch (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.

```
8/20q FC Switch (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       (hostname, IPv4, or IPv6 Address)   :
    *DestinationAddress  (hostname, IPv4, or IPv6 Address)   :
    *Protocol            (1=esp, 2=esp-old, 3=ah, 4=ah-old)  : 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)
                            1=des-cbc (8 byte key)
                            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)              :  1

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.

8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ipsec association rename association_1 association_4

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

8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ipsec association copy association_1 association_a
8/20q FC Switch (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 and peer device establish 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:

```
8/20q FC Switch ># admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (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.
8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ike peer delete peer_1

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

8/20q FC Switch (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.

```
8/20q FC Switch ># admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (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_192                          :
 *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.
8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ike peer rename peer_1 peer_4

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

8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ike peer copy peer_1 peer_a
8/20q FC Switch (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 the IP security association on 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 peer, enter the `ike policy create` command as shown in the following example:

```
8/20q FC Switch (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
                          5=null                                   :  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.
8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ike policy delete policy_1

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

8/20q FC Switch (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.

```
8/20q FC Switch (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
                           5=null                                 :  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.
8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ike policy rename policy_1 policy_4
  The IKE policy will be renamed. Please confirm (y/n): [n] y

8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ike policy copy policy_1 policy_a
8/20q FC Switch (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. You can use either the `ipsec clear` command or the `reset ipsec` command to do this. In an Ipsec Edit session, enter the `ipsec clear` command, then save the changes as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (admin-ipsec) #> ipsec clear
8/20q FC Switch (admin-ipsec) #> ipsec save
  The IPsec configuration will be saved and activated.
  Please confirm (y/n): [n] y
```

The `reset ipsec` command deletes all security polices, security associations, IKE peers, and IKE policies from the switch, but does not require an Ipsec Edit session.

```
8/20q FC Switch #> admin start
8/20q FC Switch (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 ....
```

4 Switch Configuration

Switch configuration consists of the following tasks:

Displaying switch information

You can display the following types of the switch information:

Name server information

The `show ns all` command displays the list of worldwide names (WWNs) in the fabric, as shown in the following example. The `show ns` command displays the WWNs that are local to the switch.

```
8/20q FC Switch #> show ns all
  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  No entries found for domain ID 1.

  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  No entries found for domain ID 4.

  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   8 (0x8)   0824ba NL   3   22:00:00:20:37:2b:08:00 20:00:00:20:37:2b:08:00
  2   8 (0x8)   0824c3 NL   3   22:00:00:20:37:2b:08:78 20:00:00:20:37:2b:08:78
  3   8 (0x8)   0824c5 NL   3   22:00:00:20:37:1b:cf:fd 20:00:00:20:37:1b:cf:fd
  4   8 (0x8)   0824c6 NL   3   22:00:00:20:37:2b:07:b4 20:00:00:20:37:2b:07:b4
  5   8 (0x8)   0824c9 NL   3   22:00:00:20:37:2b:08:57 20:00:00:20:37:2b:08:57
  6   8 (0x8)   0824cb NL   3   22:00:00:20:37:1b:cf:f6 20:00:00:20:37:1b:cf:f6
  7   8 (0x8)   0824cc NL   3   22:00:00:20:37:2b:0b:ec 20:00:00:20:37:2b:0b:ec
  8   8 (0x8)   0824d6 NL   3   22:00:00:20:37:2b:07:e1 20:00:00:20:37:2b:07:e1
  9   8 (0x8)   0824da NL   3   22:00:00:20:37:2b:0b:1a 20:00:00:20:37:2b:0b:1a
  10  8 (0x8)   0824e0 NL   3   22:00:00:20:37:1b:f0:7d 20:00:00:20:37:1b:f0:7d
  11  8 (0x8)   0824e1 NL   3   22:00:00:20:37:2b:02:f6 20:00:00:20:37:2b:02:f6
  12  8 (0x8)   0824e2 NL   3   22:00:00:20:37:1b:ea:b7 20:00:00:20:37:1b:ea:b7
  13  8 (0x8)   0824e8 NL   3   22:00:00:20:37:1b:cb:e5 20:00:00:20:37:1b:cb:e5

  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  No entries found for domain ID 10.

  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  No entries found for domain ID 34.
```

Switch operational information

The `show switch` command displays a variety of switch operational information. These include the switch WWN, domain ID, firmware version, administrative state, and operational state, as shown in the following example:

```
8/20q FC Switch #> show switch
  Switch Information
  ------------------
  SymbolicName                       8/20q FC Switch
  SwitchWWN                          10:00:00:c0:dd:00:bc:56
  BootVersion                        Vx.x.x.x-0 (day month date time year)
  CreditPool                         0
  DomainID                           19 (0x13)
  FirstPortAddress                   130000
  FlashSize - MBytes                 128
  LogFilterLevel                     Critical
  MaxPorts                           20
  NumberOfResets                     15
  ReasonForLastReset                 PowerUp
  ActiveImageVersion - build date    Vx.x.x.0 (day month date time year)
  PendingImageVersion - build date   Vx.x.x.0 (day month date time year)
  ActiveConfiguration                default
  AdminState                         Online
  AdminModeActive                    False
  BeaconOnStatus                     Off
  OperationalState                   Online
  PrincipalSwitchRole                False
  POSTFaultCode                      00000000
  POSTStatus                         Passed
  TestFaultCode                      00000000
  TestStatus                         NeverRun
  BoardTemp (1) - Degrees Celsius    32
  SwitchTemperatureStatus            Normal
```

System process information

The `ps` command displays system process information to help you determine what processes are running and central processing unit (CPU) usage.

The column titles in the following example are:

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

The following example displays current system processes.

```
8/20q FC Switch #> ps
  PID  PPID %CPU %MEM     TIME     ELAPSED COMMAND
  244   224  0.0  0.3 00:00:04  2-03:02:31 cns
  245   224  0.0  0.3 00:00:06  2-03:02:31 ens
  246   224  0.0  0.3 00:00:09  2-03:02:31 dlog
  247   224  0.0  0.6 00:00:33  2-03:02:31 ds
  248   224  0.3  2.8 00:09:59  2-03:02:31 mgmtApp
  249   224  0.0  0.3 00:00:16  2-03:02:31 sys2swlog
  251   224  0.0  0.4 00:00:06  2-03:02:30 fc2
  252   224  0.0  0.6 00:00:16  2-03:02:30 nserver
  253   224  0.0  0.8 00:00:08  2-03:02:30 PortApp
  254   224  0.0  0.5 00:00:03  2-03:02:30 qfsApp
  255   224  0.0  0.5 00:00:09  2-03:02:30 mserver
  256   224  0.0  0.7 00:00:06  2-03:02:30 eport
  257   224  0.0  0.6 00:00:13  2-03:02:30 zoning
  282   254  0.0  0.5 00:00:00  2-03:02:26 qfsApp
  284   224  0.0  0.6 00:00:08  2-03:02:26 snmpservicepath
  285   282  0.0  0.5 00:00:00  2-03:02:26 qfsApp
  308   224  0.0  0.8 00:00:29  2-03:02:25 cim_server
```

Elapsed time between resets

The `uptime` command displays the elapsed time since the switch was last reset and the reset method. Note that 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.

```
8/20q FC Switch #> 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, page 47
- Zoning configuration parameters, page 47
- Security configuration parameters, page 48

See also "Displaying port information" (page 65).

Switch configuration parameters

To display the switch configuration parameters, enter the `show config switch` command. These parameters determine the operational characteristics of the switch. See Table 38 for descriptions these parameters.

```
8/20q FC Switch #> show config switch
 Configuration Name: default
 -------------------
  Switch Configuration Information
  --------------------------------
  AdminState            Online
  BroadcastEnabled      False
  InbandEnabled         True
  FDMIEnabled           False
  FDMIEntries           10
  DefaultDomainID       19 (0x13)
  DomainIDLock          True
  SymbolicName          sw108
  R_A_TOV               10000
  E_D_TOV               2000
  PrincipalPriority     254
  ConfigDescription     Default Config
  ConfigLastSavedBy     admin@OB-session5
  ConfigLastSavedOn     day month date time year
  InteropMode           Standard
```

Zoning configuration parameters

To display the zoning configuration parameters, enter the `show config zoning` command. These determine how zoning is applied to the switch. See Table 40 for descriptions of these parameters.

```
8/20q FC Switch #> show config zoning

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

  Zoning Configuration Information
  --------------------------------
  MergeAutoSave         True
  DefaultZone           Allow
  DiscardInactive       False
```

Security configuration parameters

To display security configuration and port binding parameters, enter the `show config security` command. These parameters determine how security is applied to the switch. See Table 36 for descriptions of the switch security configuration parameters. See Table 37 for descriptions of the port binding parameters.

```
8/20q FC Switch #> show config security

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

  Switch Security Configuration Information
  -----------------------------------------
  FabricBindingEnabled  False
  AutoSave              True

  Port  Binding Status  WWN
  ----  --------------  ---
  0       True             10:20:30:40:50:60:70:80
  1       True             10:20:30:40:50:60:70:80
  2       False            No port binding entries found.
  3       True             10:20:30:40:50:60:70:80
  4       True             10:20:30:40:50:60:70:80
  5       False            No port binding entries found.
  6       True             10:20:30:40:50:60:70:81
  7       False            No port binding entries found.
  8       True             10:20:30:40:50:60:70:80
  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.
  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.
```

Hardware information

To display the status of the switch hardware, including fans, power supplies, internal temperature, and Heartbeat LED status, enter the `show chassis` command.

The following is an example of the `show chassis` command:

```
8/20q FC Switch #> show chassis
   Chassis Information
  -------------------
  BoardTemp (1) - Degrees Celsius   26
  BoardTemp (2) - Degrees Celsius   31
  BoardTemp (3) - Degrees Celsius   31
  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 information about Heartbeat LED blink patterns, see the *HP 8/20q Fibre Channel Switch Installation and Reference 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

Firmware information

To display a summary of switch identity information, including the firmware version, enter the `show version` command. The following is an example of the `show version` command:

```
8/20q FC Switch #> show version
       ************************************************
       *                                              *
       *       Command Line Interface SHell  (CLISH)  *
       *                                              *
       ************************************************

       SystemDescription         HP 8/20q Fibre Channel Switch
       HostName                  <undefined>
       EthIPv4NetworkAddress     10.20.11.192
       EthIPv6NetworkAddress     ::
       MACAddress                00:c0:dd:00:71:ee
       WorldWideName             10:00:00:c0:dd:00:71:ed
       SerialNumber              FAM033100024
       SymbolicName              8/20q FC Switch
       ActiveSWVersion           V8.0.4.xx.xx
       ActiveTimestamp           day month date time year
       POSTStatus                Passed
       LicensedPorts             20
       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 using the `set setup services` commands. To display the status of the switch services, use the `show setup services` command. See Table 51 for descriptions of the switch services settings.

IMPORTANT: SAN Connection Manager version 1.0 does not support the SSL service. If SSL is enabled, you will be unable to manage the switch using this version of SAN Connection Manager.

To display the current switch services settings, enter the `show setup services` command, as shown in the following example:

```
8/20q FC Switch #> show setup services
System Services
----------------------------
Telnet Enabled             True
SSHEnabled                False
GUIMgmtEnabled            True
SSLEnabled                False
EmbeddedGUIEnabled        True
SNMPEnabled               True
NTPEnabled                True
CIMEnabled                True
FTPEnabled                True
MgmtServerEnabled         True
CallHomeEnabled           True
```

To configure the switch services, enter the `set setup services` command in an Admin session, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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.

  TelnetEnabled       (True / False)   [True ]
  SSHEnabled          (True / False)   [False]
  GUIMgmtEnabled      (True / False)   [True ]
  SSLEnabled          (True / False)   [False]
  EmbeddedGUIEnabled  (True / False)   [True ]
  SNMPEnabled         (True / False)   [True ]
  NTPEnabled          (True / False)   [False]
  CIMEnabled          (True / False)   [False]
  FTPEnabled          (True / False)   [True ]
  MgmtServerEnabled   (True / False)   [True ]
  CallHomeEnabled     (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 can store up to 10 configurations, including the default configuration (`Default Config`). The current switch operating characteristics are determined by the active configuration. Only one configuration can be active at a time.

Each switch configuration contains switch, port, port threshold alarm, and zoning configuration components.

Displaying a list of switch configurations

To display the configurations stored on the switch, enter the `config list` command, as shown in the following example. Notice that the `config list` command does not require an Admin session.

```
8/20q FC Switch #> config list

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

Activating a switch configuration

To activate a switch configuration (`config_1`), enter the `config activate` command in an Admin session, as shown in the following example:

```
8/20q FC Switch (admin) config activate config_1
```

Copying a switch configuration

To create a copy of an existing configuration, enter the `config copy` command in an Admin session, as shown in the following example:

```
8/20q FC Switch (admin) config copy config_1 config_2
```

Deleting a switch configuration

To delete a configuration from the switch, enter the `config delete` command in an Admin session, as shown in the following example. You cannot delete either the active configuration or the default configuration (`Default Config`).

```
8/20q FC Switch (admin) config delete config_2
```

Modifying a switch configuration

To modify a switch configuration, open an Admin session with the `admin start` command. The Admin session prevents other accounts from making changes at the same time through Telnet, SAN Connection Manager, or any other management application. To open a Config Edit session, enter 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 in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
   The config named default is being edited.
8/20q FC Switch (admin-config)#> set config port . . .
8/20q FC Switch (admin-config)#> set config switch . . .
8/20q FC Switch (admin-config)#> set config security . . .
8/20q FC Switch (admin-config)#> set config threshold . . .
8/20q FC Switch (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:

```
8/20q FC Switch (admin-config)#> config save config_10132003
8/20q FC Switch (admin)#> config activate config_10132003
8/20q FC Switch (admin)#> admin end
```

The `admin end` command releases the Admin session for other administrators when you are finished making changes to the switch. To make temporary changes to the switch administrative state, enter the `set switch state` command.

The following is an example of the `set config switch` command. See Table 38 for descriptions of the switch configuration parameters.

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
8/20q FC Switch (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.

  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)                 [8/20q FC Switch]
  R_A_TOV             (decimal value, 100-100000 msec)       [10000         ]
  E_D_TOV             (decimal value, 10-20000 msec)         [2000          ]
  PrincipalPriority   (decimal value, 1-255)                 [254           ]
  ConfigDescription   (string, max=64 chars)                 [Default Config]
```

Backing up and restoring a switch configuration

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

- Creating the backup file, page 54
- Downloading the configuration file, page 54
- Restoring the configuration file, page 54

Creating the backup file

The `config backup` command creates the `configdata` file on the switch. This file can be used to restore a switch configuration only from the CLI; it cannot be used with QuickTools or Enterprise Fabric Management Suite to restore a switch.

```
8/20q FC Switch #> config backup
```

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

- All named switch configurations including port, switch, port threshold alarm and zoning configurations.
- All SNMP and network information defined with the `set setup` command.
- The zoning database includes all zonesets, zones, and aliases.
- The security database, except the group primary and secondary secrets.
- The Call Home database and Call Home service configuration.

NOTE: Configuration backup files are deleted from the switch during a power-cycle or a switch reset.

Downloading the configuration file

Use FTP to download the `configdata` file to your workstation for safekeeping and to upload the file back to the switch for the restore function. To download the `configdata` file, open an FTP session on the switch and login with the account name `images` and password `images`. Transfer the file in binary mode with the `get` command, as shown in the following example:

```
>ftp ip_address
user:images
password: images
ftp>bin
ftp>get configdata
    xxxxx bytes sent in xx secs.
ftp>quit
```

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

Restoring the configuration file

The restore operation begins by using FTP to upload the configuration file from the workstation to the switch, then finishes with a Telnet session and the `config restore` command. To upload the configuration file, `config_switch_169_10112003` in this case, open an FTP session with account name `images` and password `images`. Transfer the file in binary mode with the `put` command, as shown in the following example:

```
ftp ip_address
user: images
password: images
ftp> bin
ftp> put config_switch_169_10112003 configdata
  Local file config_switch_169_10112003
  Remote file configdata
ftp>quit
```

The restore process replaces all configuration information on the switch and afterwards the switch is automatically reset. If the restore process changes the IP address, all management sessions are terminated. Use the `set setup system` command to return the IP configuration to the values you want. To restore the switch, open a Telnet session (a new IP address may be required), then enter the `config restore` command from in an Admin session, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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]
8/20q FC Switch (admin) #>
  Alarm Msg: [day month date time year][A1000.0005][SM][The switch is being reset]
```

Paging a switch

To help you locate a particular switch in a rack of switches, 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:

```
8/20q FC Switch #> set beacon on
8/20q FC Switch $> set beacon off
```

Managing 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, which is required for SSL connections.

NOTE: To set the date with the `date` command, the switch NTP client must be disabled. For information about disabling the `NTPClientEnabled` parameter, see "set setup system" (page 247).

If you use the `date` command, you can set the time zone using the `set timezone` command. The default time zone is Universal Time (UTC), also known as Greenwich Mean Time (GMT). Changing the time zone converts the current time to the time in the new time zone. For this reason, if you are not using an NTP server, set the time zone first, then set the date and time.

Displaying the date and time

To display the date and time, enter the `date` command, as shown in the following example:

```
8/20q FC Switch #> date
  Mon Apr 07 07:51:24 2008
```

Setting the date and time explicitly

To set the switch date and time explicitly, use the `set timezone` and `date` commands.

1. To change the time zone (to America/North Dakota, for example), enter the `set timezone` command in an Admin session, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> set timezone
  Africa                                America
  Antarctica                            Asia
  Atlantic                              Australia
  Europe                                Indian
  Pacific                               UTC
        Press ENTER for more options or 'q' to make a selection.

  America/Grenada                       America/Guadeloupe
  America/Guatemala                     America/Guayaquil
  America/Guyana                        America/Halifax
  America/Havana                        America/Hermosillo
  America/Indiana                       America/Indianapolis
  .
  .
  .
  America/Monterrey                     America/Montevideo
  America/Montreal                      America/Montserrat
  America/Nassau                        America/New_York
  America/Nipigon                       America/Nome
  America/Noronha                       America/North_Dakota
  America/Panama                        America/Pangnirtung

        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): q
```

2. To set the date and time (January 31, 10:15 AM, 2008), enter the `date` command, as shown in the following example:

```
8/20q FC Switch (admin) #> date 013110152008
8/20q FC Switch (admin) #> date
  Thu Jan 31 10:15:03 america/north_dakota/center 2008
```

Setting the time through an NTP server

An NTP server can automatically set the switch date and time. 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 specify the NTP server IP address, as shown in the following example:

```
8/20q FC Switch  #> admin start
8/20q FC Switch (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

  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

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

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` command
Activates pending firmware	X	X	X
Disrupts I/O traffic		X	X
Reconnects SAN Connection Manager, QuickTools, and Enterprise Fabric Management Suite sessions afterwards	X	X	X
Clears the event log	X	X	X
Deletes supports files, firmware image files that have not been unpacked, and configuration backup files		X	X
Closes all management sessions	X	X	X
Performs power-on self test (POST)			X

Installing firmware

New firmware becomes available periodically, either on CD-ROM or from the HP website. To install firmware on a switch, follow these 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. See "Non-disruptive activation" (page 58).

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" (page 59). To perform a non-disruptive activation, see "Custom firmware installation" (page 60).

Non-disruptive activation

You can load and activate firmware upgrades on an operating switch without disrupting data traffic or having to re-initialize attached devices. If the non-disruptive activation fails, you will usually be prompted to try again later. Otherwise, the switch performs a disruptive activation. A disruptive activation interrupts Fibre Channel data traffic on the switch, while a non-disruptive activation does not. For information about non-disruptive firmware versions, see the *Firmware Release Notes*.

To ensure a successful non-disruptive activation, you should first satisfy the following conditions:

- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting inter-switch links (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 Host Bus Adapter (HBA) configuration changes.

If you are installing firmware on more than one switch in the fabric, wait until the activation is complete on the first switch before installing firmware on a second switch. If you attempt to activate firmware on a second switch before activation is complete on the first, you will receive a message advising you to wait and perform a hot reset later on the second switch to complete the installation.

Ports that change states during the non-disruptive activations are reset. When the non-disruptive activation is complete, SAN Connection Manager sessions, QuickTools sessions, and Enterprise Fabric Management Suite sessions automatically reconnect. However, Telnet sessions must be restarted manually.

TIP: After upgrading firmware that includes changes to QuickTools, a QuickTools session that was open during the upgrade may indicate that the new firmware is not supported. To correct this, close the QuickTools session and the browser window, then open a new QuickTools session.

One-step firmware installation

The `firmware install` and `image install` commands download the firmware image file from an FTP or Trivial File Transfer Protocol (TFTP) server to the switch, unpack the image file, and perform a disruptive activation all in one step.

To install the firmware:

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

```
8/20q FC Switch #> admin start
8/20q FC Switch #> 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 requires an user account and a password; TFTP does not.

```
  FTP or TFTP     : ftp
```

3. Enter your account name on the remote host (FTP only) 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
  IP Address      : 10.20.20.200
  Source Filename : 8.0.4.xx.xx_epc
  About to install image.  Do you want to continue? [y/n] y
```

4. When prompted to install the new firmware, enter `y` to continue or `n` to cancel. Entering `y` 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).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
```

5. Enter the password for your account name (FTP only).

```
331 Password required for johndoe.
Password:******
230 User johndoe logged in.
```

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 switch reset and whether the activation will be disruptive (`reset switch` command) or non-disruptive (`Hotreset` command). The following example illustrates a custom firmware installation with a non-disruptive activation.

1. Download the firmware image file from the workstation to the switch.
   - If your workstation has an FTP server, enter the `image fetch` command:

     ```
     8/20q FC Switch #> admin start
     8/20q FC Switch (admin) #> image fetch account_name ip_address
     filename
     ```

   - If your workstation has a TFTP server, enter the `image tftp` command to download the firmware image file.

     ```
     8/20q FC Switch (admin) #> image tftp ip_address filename
     ```

   - If your workstation has neither an FTP nor a TFTP server, open an FTP session and download the firmware image file by entering the following FTP commands:

     ```
     >ftp ip_address or switchname
     user:images
     password: images
     ftp>bin
     ftp>put filename
     ftp>quit
     ```

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

   ```
   8/20q FC Switch #> admin start
   8/20q FC Switch (admin) $> image list
   ```

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

   ```
   8/20q FC Switch (admin) $> image unpack filename
   ```

4. Wait for the unpack to be completed.

   ```
   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. If the non-disruptive activation fails, you will usually be prompted to try again later. Otherwise, the switch will perform a disruptive activation.

   ```
   8/20q FC Switch (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. See "Testing a port" (page 75).

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 online switch test excludes TR_Ports. The following is an example of an online test:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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. The test requires that you place the switch in the diagnostics state using the `set switch state` command before starting. 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #>set switch state diagnostics
8/20q FC Switch (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
```

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

```
8/20q FC Switch (admin) #> set switch state online
```

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. Therefore, before starting the test, you must place the switch in the diagnostics state using the `set switch state` command. There are two types of connectivity tests: internal loopback and external loopback.

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

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

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> set switch state diagnostics
8/20q FC Switch (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 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
```

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

```
8/20q FC Switch (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:

```
8/20q FC Switch #> test status switch

  Test    Test                  Test                Loop      Test
  Level   Type                  Status             Count  Failures
  -----   ----                  ------             -----  --------
  Switch  Offline internal      Passed                 4         0

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

Canceling a switch test

To cancel a switch test that is in progress, enter the `test cancel switch` command.

Verifying and tracing Fibre Channel connections

You can verify Fibre Channel connections between the switch and the fabric and 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.

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> 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.

```
8/20q FC Switch#> 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 switch feature upgrades

A feature license key is a password that you can purchase from your switch distributor or authorized reseller to upgrade your switch. License keys vary according to the features you purchase. The following license key features are available:

- The HP 8/20q Port Activation Upgrade LTU enables additional SFP ports in increments of four for totals of 16 or 20 ports.

Installing a feature license key is not disruptive, nor does it require a switch reset. To order a license key, contact your switch distributor or your authorized reseller.

TIP: To obtain the switch serial number and license key, follow the step-by-step instructions on the *firmware feature entitlement request certificate* for the license key.

Displaying feature licenses

To display the license keys that are installed, enter the `feature log` command on your switch, as shown in the following example:

```
8/20q FC Switch #> feature log
  Mfg Feature Log:
  ----------------
  Switch Licensed for 8 ports
  Customer Feature Log:
  ---------------------
  1) day month date 19:39:24 year - Switch Licensed for 20 ports
  1-LCVXOWUNOJBE6
```

Installing a feature license key

To install a license key on your switch, enter the `feature add` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> feature add 1-LCVXOWUNOJBE6
License upgrade to 20 ports

Do you want to continue with license upgrade procedure? (y/n): [n] y
Alarm Msg:[day mon date time year][A1005.0030][SM][Upgrading Licensed Ports to
20]
```

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 duration. Idle login sessions that exceed the timeout limit are logged off (`InactivityTimeout`). An idle Admin session that exceeds the timeout limit is ended, but the login session may be maintained (`AdminTimeout`). By default, no timeout limit is enforced on idle login sessions; idle Admin sessions are ended after 30 minutes.

To display the idle login and Admin session configuration, enter the `show setup system timers` command, as shown in the following example:

```
8/20q FC Switch #> show setup system timers

  System Information
  ------------------
  AdminTimeout             30
  InactivityTimeout        0
```

To configure idle login and Admin session limits, enter the `set setup system timers` command as shown in the following example:

```
8/20q FC Switch (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]
```

5 Port Configuration

This section describes the port configuration task.

Displaying port information

You can display the following port information:

- Port configuration parameters, page 65
- Port operational information, page 66
- Port threshold alarm configuration parameters, page 67
- Port performance, page 68
- Transceiver information, page 68

Port configuration parameters

To display the port configuration parameters, enter the `show config port` command. These parameters determine the operational characteristics of the port. See Table 35 for descriptions of these parameters.

```
8/20q FC Switch #> show config port 3

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

  Port Number: 3
  ------------
  AdminState           Online
  LinkSpeed            Auto
  PortType             GL
  SymbolicName         Port3
  ALFairness           False
  DeviceScanEnabled    True
  ForceOfflineRSCN     False
  ARB_FF               False
  InteropCredit        0
  ExtCredit            0
  FANEnabled           True
  AutoPerfTuning       True
  MSEnabled            True
  NoClose              False
  IOStreamGuard        Auto
  PDISCPingEnabled     True
```

Port operational information

To display port operational information, enter the `show port` command.

```
8/20q FC Switch #> show port 1
  Port Number: 1
  ------------
  AdminState          Online
  AsicNumber          0
  AsicPort            2
  ConfigType          GL
  DownstreamISL       False
  EpConnState         Connected
  EpIsoReason         NotApplicable
  IOStreamGuard       Disabled
  Licensed            True
  LinkSpeed           8Gb/s
  LinkState           Active
  LoginStatus         LoggedIn
  MaxCredit           16
  MediaPartNumber     PLRXPLVCSH422N
  MediaRevision       1
  MediaSpeeds         2, 4, 8Gb/s
  MediaType           800-MX-SN-I
  MediaVendor         JDSU
  MediaVendorID       0000019c
  OperationalState    Online
  PerfTuningMode      Normal
  PortID              2d0100
  PortWWN             20:01:00:c0:dd:0d:70:c9
  POSTFaultCode       00000000
  POSTStatus          Passed
  RunningType         E
  SupportedSpeeds     1, 2, 4, 8Gb/s
  SymbolicName        Port1
  SyncStatus          SyncAcquired
  TestFaultCode       00000000
  TestStatus          NeverRun
  UpstreamISL         False
  XmitterEnabled      True

                      Port Statistics

  ALInit              2                   LIP_F8_F7           0
  ALInitError         0                   LinkFailures        0
  BadFrames           0                   Login               1
  BBCR_FrameFailures  0                   Logout              0
  BBCR_RRDYFailures   0                   LongFramesIn        0
  Class2FramesIn      0                   LoopTimeouts        0
  Class2FramesOut     0                   LossOfSync          0
  Class2WordsIn       0                   LostFrames          0
  Class2WordsOut      0                   LostRRDYs           0
  Class3FramesIn      4432                PrimSeqErrors       0
  Class3FramesOut     28640               RxLinkResets        2
  Class3Toss          0                   RxOfflineSeq        0
  Class3WordsIn       300995              ShortFramesIn       0
  Class3WordsOut      483225              TotalErrors         0
  DecodeErrors        0                   TotalLinkResets     2
  EpConnects          1                   TotalLIPsRecvd      2
  FBusy               0                   TotalLIPsXmitd      3
```

```
FlowErrors          0                   TotalOfflineSeq     1
FReject             0                   TotalRxFrames       4432
InvalidCRC          0                   TotalRxWords        300995
InvalidDestAddr     0                   TotalTxFrames       28640
LIP_AL_PD_AL_PS     0                   TotalTxWords        483225
LIP_F7_AL_PS        0                   TxLinkResets        0
LIP_F7_F7           2                   TxOfflineSeq        1
LIP_F8_AL_PS        0
```

Port threshold alarm configuration parameters

To display the port threshold alarm parameters, enter the `show config threshold` command. These parameters determine the error thresholds at which the switch issues alarms. See Table 39 for descriptions of these parameters.

```
8/20q FC Switch #> 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

To display port performance in terms of the volume of data transmitted, data received, or errors, enter the `show perf` command. 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.

```
8/20q FC Switch #> show perf
  Port    Bytes/s     Bytes/s     Bytes/s     Frames/s    Frames/s    Frames/s
  Number    (in)        (out)     (total)       (in)        (out)     (total)
  ------ -------     -------     -------     --------    --------    --------
  0       7K          136M        136M        245         68K         68K
  1       58K         0           58K         1K          0           1K
  2       0           0           0           0           0           0
  3       0           0           0           0           0           0
  4       0           0           0           0           0           0
  5       0           0           0           0           0           0
  6       0           7K          7K          0           245         245
  7       136M        58K         136M        68K         1K          70K
  8       7K          136M        136M        245         68K         68K
  9       58K         0           58K         1K          0           1K
  10      0           0           0           0           0           0
  11      0           0           0           0           0           0
  12      0           0           0           0           0           0
  13      0           0           0           0           0           0
  14      0           7K          7K          0           245         245
  15      136M        58K         136M        68K         1K          70K
  16      47M         23K         47M         23K         726         24K
  17      0           0           0           0           0           0
  18      23K         47M         47M         726         23K         24K
  19      0           0           0           0           0           0
```

Transceiver information

Enter the `show media` command to display operational information about a transceiver, as shown in the following example. For a description of the transceiver information in the `show media` display, see Table 64.

```
8/20q FC Switch #> show media 4
Port Number: 4
-------------
MediaType           800-MX-SN-S
MediaVendor         FINISAR CORP.
MediaPartNumber     FTLF8528P2BNV
MediaRevision       A
MediaSerialNumber   P6G22RL
MediaSpeeds         2Gb/s, 4Gb/s, 8Gb/s

                      Temp      Voltage      Tx Bias      Tx Pwr      Rx Pwr
                       (C)          (V)         (mA)        (mW)        (mW)
                ----------- ----------- ------------ ----------- -----------
      Value           37.32        3.73         7.30       0.373       0.000
      Status         Normal HighWarning       Normal      Normal    LowAlarm
      HighAlarm       95.00        3.90        17.00       0.637       1.264
      HighWarning     90.00        3.70        14.00       0.637       0.791
      LowWarning     -20.00        2.90         2.00       0.082       0.028
      LowAlarm       -25.00        2.70         1.00       0.073       0.019
```

Modifying port operating characteristics

You can make permanent or temporary changes to port operating characteristics. The `set config port` command makes permanent port configuration changes. 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.

IMPORTANT: 8 Gb/s SFPs do not support the 1 Gb/s setting. Setting a Fibre Channel port that has an 8-Gb/s SFP transceiver to 1-Gb/s will down the port.

The following example permanently changes port administrative state of port 1:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
8/20q FC Switch (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        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto) [Auto   ]
  PortType         (GL, G, F, FL, TR)                            [GL     ]
  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      ]
  FANEnable        (True / False)                                [True   ]
  AutoPerfTuning   (True / False)                                [True   ]
  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.
8/20q FC Switch (admin-config) #> config save
8/20q FC Switch (admin-config) #> config activate
```

You can configure all ports based on a specified source port using the `set config ports` command. The `set config ports` command prompts you to configure the parameters of the source port, and then applies those values to all of the ports. The following example configures all ports based on port 3:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) config edit
8/20q FC Switch (admin) #> set config ports 3
.
.
.
8/20q FC Switch (admin-config)#> config save
8/20q FC Switch (admin)#> config activate
8/20q FC Switch (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 8–19 based on port 0:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) config edit
8/20q FC Switch (admin) #> clone config port 0 8-19
8/20q FC Switch (admin-config)#> config save
8/20q FC Switch (admin)#> config activate
8/20q FC Switch (admin)#> admin end
```

The following example temporarily changes the administrative state of port 1 to `down`:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> set port 1 state down
```

Configuring transparent routing

IMPORTANT: The SAN Connection Manager (SCM) application version 2.10 can manage 8/20q Fibre Channel Switches with active TR_Ports; however, SCM cannot manage or discover remote switches or devices in the remote fabric. Use QuickTools or Enterprise Fabric Management Suite and the storage management interface to present Logical Unit Numbers (LUNs) to remote devices. SCM version 2.0 and earlier versions do not support the management of fabrics that include 8/20q Fibre Channel Switches with active TR_Ports and may disrupt communication between the 8/20q Fibre Channel Switch and the remote fabric.

The transparent routing feature provides inter-fabric routing to allow controlled and limited access between devices on a 8/20q Fibre Channel Switch (local) fabric and devices on a remote fabric consisting of switches made by other vendors. For a list of switches that are supported in a remote fabric, see the *HP 8/20q Fibre Channel Switch release notes*, and the *HP SAN Design Reference Guide* located at the HP website: http://www.hp.com/go/sandesignguide. This type of inter-fabric connection uses the Fibre Channel industry N-Port ID Virtualization (NPIV), and makes local and remote devices accessible to each other while maintaining the local and remote fabrics as separate fabrics.

You can connect multiple 8/20q Fibre Channel Switches to one or more remote fabrics using multiple TR_Ports. Local and remote devices are identified by their respective port worldwide names. Consider the following mapping rules:

- A TR_Port can support a maximum of 32 local device/remote device mappings.
- A specific local device can be mapped to devices on only one remote fabric. Local devices on the same 8/20q Fibre Channel Switch can each be mapped to different remote fabrics.
- For mappings between a specific 8/20q Fibre Channel Switch and a remote fabric, each local device or remote device can be mapped over only one TR_Port. Additional mappings to either device must use that same TR_Port.
- Mulitple local devices connected to different local switches can be mapped to the same remote device over one TR_Port on each local switch.
- A local device cannot be mapped over an E_Port to another local switch, then over a TR_Port to the remote device. The local switch to which the local device is connected must connect directly to the remote fabric over a TR_Port.

NOTE: When a local device is mapped over a TR_Port to a remote device, the local device and its TR_Port appear as an NPIV connected device in the remote fabric. It is possible, though not recommended, to map such a local device over a second TR_Port to a local device in a second local fabric. In this case, if you merge the two local fabrics, the transparent route becomes inactive for the devices that now have a path over an ISL, and an alarm is generated.

NOTE: Although transparent routing can be configured with the CLI, the QuickTools web applet and Enterprise Fabric Management Suite are designed to simplify the configuration process. See the *HP 8/20q Fibre Channel Switch QuickTools Switch Management User Guide* and the *HP 8/20q and SN6000 Fibre Channel Switch Enterprise Fabric Management Suite User Guide*.

To configure transparent routing:

1. Determine what devices on the local fabric require access to devices on the remote fabric. Local devices must be attached directly to the 8/20q Fibre Channel Switch. In this example, the device WWNs are as follows:
   - Local device: 21:00:00:e0:8b:0e:d3:59
   - Remote device: 22:00:00:04:cf:a8:7f:2d
2. Configure one or more TR_Ports on the local 8/20q Fibre Channel Switch:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
8/20q FC Switch (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]
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto) [Auto  ]
  PortType         (GL, G, F, FL, TR)                           [GL    ] TR
  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.
  8/20q FC Switch (admin-config) #> config save
  8/20q FC Switch (admin-config) #> config activate
```

3. Connect the TR_Port to the remote fabric. For remote HP B-Series or C-Series fabrics, the switch to which the TR_Port is connected must support NPIV, and for B-Series fabrics, the interoperability mode must be configured to InteropMode=0. Other B-Series switches in the remote fabric need not support NPIV.
4. Map local devices to remote devices by creating an inter-fabric zone. The inter-fabric zone contains the port WWNs of the local device, the remote device, and the TR_Port. The name of the inter-fabric zone begins with IFZ followed by the lowest device port WWN followed by the remaining port WWN, all uppercase, separated by underscores (_).
   a. Create the inter-fabric zone:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #>zone create
IFZ_210000E08B0ED359_22000004CFA87F2D
```

   b. Add the device and TR_Port WWNs to the inter-fabric zone:

```
8/20q FC Switch (admin-zoning) #>zone add IFZ_210000E08B0ED359_22000004CFA87F2D
21:00:00:e0:8b:0e:d3:59 22:00:00:04:cf:a8:7f:2d 20:01:00:c0:dd:0d:53:a5
```

c. Add the new zone to the active zoneset, save the zoneset, and activate it.

```
8/20q FC Switch (admin-zoning) #>zoneset add zoneset_alpha
IFZ_210000E08B0ED359_22000004CFA87F2D
8/20q FC Switch (admin-zoning) #> zoning save
  The changes have been saved; however, they must be activated
   before they can take effect -- see Zoneset Activate command.
8/20q FC Switch (admin) #> zoneset activate zoneset_alpha
```

5. Apply the same inter-fabric zone that was created on the local fabric to the active zoning on the remote HP B-series or C-Series fabric. When modifications to the active zoning on both fabrics are complete, the transparent routing connection becomes active, and local devices will discover remote devices.

To remove a transparent route, in addition to removing the local inter-fabric zone, you must also remove the corresponding remote inter-fabric zone.

Port binding

Port binding establishes up to 32 switches or devices that are permitted to log in to a particular switch port. Switches or devices that are not among the established 32 are refused access to the port. To display the port binding configuration for all ports, enter the `show config security portbinding` command, as shown in the following example:

```
8/20q FC Switch #> show config security portbinding

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

  Port    Binding Status   WWN
  ----    --------------   -----------------------
  0       True             10:20:30:40:50:60:70:80
  1       True             10:20:30:40:50:60:70:80
  2       False            No port binding entries found.
  3       True             10:20:30:40:50:60:70:80
  4       True             10:20:30:40:50:60:70:80
  5       False            No port binding entries found.
  6       True             10:20:30:40:50:60:70:81
  7       False            No port binding entries found.
  8       True             10:20:30:40:50:60:70:80
  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.
  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.
```

To enable port binding for the selected port and to specify the WWNs of the authorized ports/devices, enter the `set config security portbinding` command. The following example enables port binding on port 1 and specifies two device world wide names:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
8/20q FC Switch (admin-config) #> set config security 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.

  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

To reinitialize one or more ports and to discard any temporary changes that have been made to the administrative state or link speed, enter the `reset port` command. The following example reinitializes port 1:

```
8/20q FC Switch #> reset port 1
```

Configuring port threshold alarms

The switch can monitor a set of port errors and generate 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 "Modifying a switch configuration" (page 53). See Table 39 for a description of the port alarm threshold parameters.

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.

To enable and configure port threshold monitoring on the switch, enter the `set config threshold` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
8/20q FC Switch (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.
8/20q FC Switch (admin-config) #> config save
8/20q FC Switch (admin-config) #> config activate
```

Testing a port

You can test a port using the `test port` command using online or offline tests. The following describe the test types, displaying test results, and cancelling a 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. Online testing of TR_Ports is not allowed. The following is an example of an online test:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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)   [429496729]
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.

8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> set port 1 state diagnostics
8/20q FC Switch (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)    [429496729]
  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.

8/20q FC Switch (admin) #>
  Test for port 1 Passed.
```

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

```
8/20q FC Switch (admin) #> set port 1 state online
```

Displaying 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:

```
8/20q FC Switch #> test status port 1
Port              Test                Test               Loop      Test
Num      Port     Type                Status            Count  Failures
----     -------- ----                ------            -----  --------
1        1        Offline Internal    Passed               12         0
```

Canceling a port test

To cancel a port test that is in progress, enter the `test cancel port` command.

6 Zoning Configuration

Access to devices within the fabric is controlled by zoning. Some zoning strategies are:

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

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.

Zoning divides the fabric for purposes of controlling discovery and inbound traffic. Zoning is hardware-enforced only when a port/device is a member of no more than eight zones whose combined membership does not exceed 64. If this condition is not satisfied, that port behaves as a soft zone member. You can assign ports/devices to a zone individually or as a group by creating an alias.

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

Displaying zoning database information

A switch maintains three zoning databases:

- Non-volatile—This zoning database is permanent and contains all zonesets, zones, and aliases that you create and save on a switch. The zonesets in the non-volatile zoning database are known as configured zonesets.
- Volatile—This zoning database is temporary. This means it is not retained across switch resets. The volatile zoning database can be the working copy of a zoneset being edited or an active zoneset received from another switch. In the latter case, this is also known as the merged zoneset.
- Active—This zoning database is the active zoneset.

You can display the following information about the zoning database:

- Configured zoneset information, page 77
- Active zoneset information, page 79
- Merged zoneset information, page 80
- Edited zoneset information, page 80
- Zoneset membership information, page 80
- Orphan zone information, page 81
- Alias and alias membership information, page 82
- Zoning modification history, page 82
- Zoning database limits, page 83

Configured zoneset information

The `zoneset list` and the `zoning list` commands display information about all zonesets in the non-volatile zoning database. To display a list of the zonesets, enter the `zoneset list` command, as shown in the following example:

```
8/20q FC Switch #> zoneset list

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

To display all zonesets, zones, and zone members in the active zoneset and configured zonesets, enter the `zoning list` command, as shown in the following example. Merged and edited zonesets are displayed if they exist.

```
8/20q FC Switch #> 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 zoneset information

The `zoning list` and `zoneset active` commands display information about the active zoneset. To display component zones and zone members, enter the `zoning active` command, as shown in the following example:

```
8/20q FC Switch #> 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
```

To display the name of the active zoneset and its activation history, enter the `zoneset active` command, as shown in the following example:

```
8/20q FC Switch #> zoneset active

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

Merged zoneset information

A merged zoneset is a zoneset that is received from another switch as a result of a change to the active zoneset. You can display the merged zoneset on your switch if the `MergeAutoSave` parameter is set to False. For more information about the `MergeAutoSave` parameter, see "Configuring the zoning database" (page 83). To display merged zoneset information, enter the `zoning merged` command, as shown in the following example:

```
8/20q FC Switch #> 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
```

Edited zoneset information

The edited zoneset is a zoneset that you were modifying when a change occurred to the active zoneset or a fabric merge occurred. To display the unsaved edited zoneset information, enter the `zoning edited` command in an Admin session and a Zoning Edit session, as shown in the following example:

```
8/20q FC Switch (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
```

Zoneset membership information

The `zoneset zones`, `zone list`, and `zone zonesets` commands display zoneset membership information.

To display the member zones for a specified zoneset, enter the `zoneset zones` command, as shown in the following example:

```
8/20q FC Switch #> zoneset zones ssss

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

To display the zones and the zonesets to which they belong, enter the `zone list` command, as shown in the following example:

```
8/20q FC Switch #> zone list

  Zone         ZoneSet
  ----         -------
  wwn_b0241f
               zone_set_1

  wwn_23bd31
               zone_set_1

  wwn_221416
               zone_set_2

  wwn_2215c3
               zone_set_2

  wwn_0160ed
               zone_set_3
```

To display the zonesets for which a specified zone is a member, enter the `zone zonesets` command, as shown in the following example:

```
8/20q FC Switch #> zone zonesets zone1

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

Zone membership information

To display the members for a specified zone, enter the `zone members` command, as shown in the following example:

```
8/20q FC Switch #> 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
```

Orphan zone information

To display a list of zones that are not members of any zoneset, enter the `zone orphans` command, as shown in the following example:

```
8/20q FC Switch #> zone orphans
Current list of orphan zones
----------------------------
zone3
zone4
```

Alias and alias membership information

The `alias list` and `alias members` commands display information about aliases.

To display a list of all aliases, enter the `alias list` command, as shown in the following example:

```
8/20q FC Switch #> alias list

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

To display the membership for a specified alias, enter the `alias members` command, as shown in the following example:

```
8/20q FC Switch #> 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

To display a record of zoning modifications, enter the `zoning history` command, as shown in the following example:

```
8/20q FC Switch #> 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 data:

- Time of the most recent zoneset 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

To display a summary of the objects in the zoning database and their maximum limits, enter the `zoning limits` command, as shown in the following example:

```
8/20q FC Switch #> zoning limits

Configured (saved in NVRAM) Zoning Information

  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
  ActiveZones                    19
  ActiveZoneMembers              160
```

To display abbreviated limits information, enter the `zoning limits brief` command.

Configuring the zoning database

You can configure how the zoning database is applied to the switch and exchanged with the fabric by using 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 40.

- `MergeAutoSave`—Enables or disables the automatic saving of a new active zoneset to the switch non-volatile zoning database.
- `DefaultZone`—Allows or denies communication among ports/devices that are not defined in the active zoneset.
- `DiscardInactive`—Enables or disables the discarding of all zonesets except the active zoneset.

If `MergeAutoSave` is False on a switch, and a new zoneset is activated elsewhere in the fabric or a fabric merge occurs, you can choose how to dispose of the merged zoneset:

- To display the merged zoneset, enter the `zoning merged` command.
- To edit the merged zoneset, enter the `zoning edit merged` command.
- To save the merged zoneset to the non-volatile zoning database, enter the `zoning merged capture` command.
- To discard the merged zoneset, enter the `zoning restore` command.

If you are editing the configured zoneset that corresponds to the active zoneset and a zoneset merge occurs, you have the same editing options. In addition, you can enter the `zoning edited` command to display the edited zoning database.

To restore the zoning configuration to its factory values, enter the `reset config` or `reset factory` commands. Notice, however, these commands restore other aspects of the switch configuration as well.

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 Telnet, QuickTools, Enterprise Fabric Management Suite, 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
   The config named default is being edited.
8/20q FC Switch (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.

8/20q FC Switch (admin-config)#> config save
8/20q FC Switch (admin)#> config activate
8/20q FC Switch (admin)#> admin end
```

Modifying the zoning database

To modify the non-volatile zoning database:

1. Enter the `admin start` command.

   ```
   8/20q FC Switch #> admin start
   ```

   An Admin session prevents other accounts from making changes at the same time through Telnet, QuickTools, Enterprise Fabric Management Suite, or any other management application.
2. Take one of the following actions:
   - To open a Zoning Edit session, enter the `zoning edit configured` command. The Zoning Edit session provides access to the `zoneset`, `zone`, `alias`, and `zoning` commands with which you make modifications to the zoning database

     ```
     8/20q FC Switch (admin) #> zoning edit
     8/20q FC Switch (admin-zoning)#> zoneset . . .
     8/20q FC Switch (admin-zoning)#> zone . . .
     8/20q FC Switch (admin-zoning)#> alias . . .
     8/20q FC Switch (admin-zoning)#> zoning . . .
     ```
   - To modify the temporary merged zoneset (if one exists), enter the `zoning edit merged` command.

     ```
     8/20q FC Switch (admin) #> zoning edit merged
     ```
3. When you are finished making changes:
   - To save the changes and close the Zoning Edit session, enter the `zoning save` command.

     ```
     8/20q FC Switch (admin-zoning)#> zoning save
     ```
   - To close the Zoning Edit session without saving changes, enter the `zoning cancel` command.

     ```
     8/20q FC Switch (admin-zoning)#> zoning cancel
     ```
4. To activate the changes to the active zoneset, enter the `zoneset activate` command.

   ```
   8/20q FC Switch (admin)#> zoneset activate zoneset_1
   ```

   The active zoneset is propagated throughout the fabric.
5. When you are finished making changes to the switch, enter the `admin end` command to release the Admin session for other administrators.

   ```
   8/20q FC Switch (admin)#> admin end
   ```

To remove all zoning database objects (aliases, zones, and zonesets) and restore the zoning database to its factory state, enter the `reset zoning` command, as shown in the following example:

```
8/20q FC Switch (admin) #> reset zoning
```

Saving the active and merged zonesets

You can save the active zoneset and merged zoneset to the non-volatile zoning database. To save the active zoneset, enter the `zoning active capture` command, as shown in the following example:

```
8/20q FC Switch (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.
```

To the save the merged zoneset, enter the `zoning merged capture` command, as shown in the following example:

```
8/20q FC Switch (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.
```

Resetting the zoning database

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

- Enter the `reset zoning` command, as shown in the following example. This is the preferred method.

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> reset zoning
```

  The zoning configuration parameters, `MergeAutoSave`, `DefaultZone`, and `DiscardInactive` remain unchanged.

- Enter the `zoning clear` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zoning clear
8/20q FC Switch (admin-zoning) #> zoning save
```

Deleting inactive zonesets, zones, and aliases

To delete all objects from the zoning database except those in the active zoneset, enter the `zoning delete orphans` command.

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning delete orphans
   This command will remove all zonesets, zones, and aliases
   that are not currently active.
Please confirm (y/n): [n] y
8/20q FC Switch (admin) #> zoning save
```

Managing zonesets

This sub-section describes the zoneset management tasks. All of these tasks except "Activating a zoneset" (page 87) and "Deactivating a zoneset" (page 87) require an Admin session and a Zoning Edit session.

Creating a zoneset

To create a new zoneset, enter the `zoneset create` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zoneset create zoneset_1
8/20q FC Switch (admin-zoning) #>zoning save
```

Deleting a zoneset

To delete a zoneset, enter the `zoneset delete` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zoneset delete zoneset_1
8/20q FC Switch (admin-zoning) #>zoning save
```

Renaming a zoneset

To rename a zoneset, enter the `zoneset rename` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zoneset rename zoneset_old zoneset_new
8/20q FC Switch (admin-zoning) #>zoning save
```

Copying a zoneset

To copy a zoneset and its contents to a new zoneset, enter the `zoneset copy` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zoneset copy zoneset_1 zoneset_2
8/20q FC Switch (admin-zoning) #>zoning save
```

Adding zones to a zoneset

To add a zone to a zoneset, enter the `zoneset add` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zoneset add zoneset_1 zone_1 zone_2
8/20q FC Switch (admin-zoning) #>zoning save
```

Removing zones from a zoneset

To remove zones from a zoneset, enter the `zoneset remove` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zoneset remove zoneset_1 zone_1 zone_2
8/20q FC Switch (admin-zoning) #>zoning save
```

Activating a zoneset

To apply zoning to the fabric, enter the `zoneset activate` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoneset activate zoneset_1
```

Deactivating a zoneset

To deactivate the active zoneset and disable zoning in the fabric, enter the `zoneset deactivate` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoneset deactivate
```

Managing zones

This sub-section describes the zone management tasks. All of these tasks require an Admin session and a Zoning Edit session.

Creating a zone

To create a new zone, enter the `zone create` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zone create zone_1
8/20q FC Switch (admin-zoning) #> zoning save
```

Deleting a zone

To delete zone_1 from the zoning database, enter the `zone delete` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zone delete zone_1
8/20q FC Switch (admin-zoning) #> zoning save
```

Renaming a zone

To rename zone_1 to zone_a, enter the `zone rename` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zone rename zone_1 zone_a
8/20q FC Switch (admin-zoning) #> zoning save
```

Copying a zone

To copy the contents of an existing zone (zone_1) to a new zone (zone_2), enter the `zone copy` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zone copy zone_1 zone_2
8/20q FC Switch (admin-zoning) #> zoning save
```

Adding members to a zone

To add ports/devices to zone_1, enter the `zone add` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zone add zone_1 alias_1 1,4 1,5
8/20q FC Switch (admin-zoning) #> zoning save
```

Removing members from a zone

To remove ports/devices from zone_1, enter the `zone remove` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zone remove zone_1 alias_1 1,4 1,5
8/20q FC Switch (admin-zoning) #> zoning save
```

Managing aliases

This sub-section describes the alias management tasks. All of these tasks require an Admin session and a Zoning Edit session.

Creating an alias

To create a new alias, enter the `alias create` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> alias create alias_1
8/20q FC Switch (admin-zoning) #> zoning save
```

Deleting an alias

To delete alias_1 from the zoning database, enter the `alias delete` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> alias delete alias_1
8/20q FC Switch (admin-zoning) #> zoning save
```

Renaming an alias

To rename alias_1 to alias_a, enter the `alias rename` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> alias rename alias_1 alias_a
8/20q FC Switch (admin-zoning) #> zoning save
```

Copying an alias

To copy alias_1 and its contents to alias_2, enter the `alias copy` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> alias copy alias_1 alias_2
8/20q FC Switch (admin-zoning) #> zoning save
```

Adding members to an alias

To add ports/devices to alias_1, enter the `alias add` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> alias add alias_1  1,4 1,5
8/20q FC Switch (admin-zoning) #> zoning save
```

Removing members from an alias

To remove ports/devices from alias_1, enter the `alias remove` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> alias remove alias_1 1,4 1,5
8/20q FC Switch (admin-zoning) #> zoning save
```

7 Connection Security Configuration

The 8/20q Fibre Channel Switch supports secure connections with Telnet and switch management applications. The Secure Shell protocol (SSH) secures Telnet connections to the switch. The Secure Sockets Layer (SSL) protocol secures switch connections to the following management applications:

- SAN Connection Manager
- QuickTools
- Enterprise Fabric Management Suite
- Storage Management Initiative-Specification (SMI-S)

Managing SSL and SSH services

Consider the following when enabling SSH and SSL services:

- SAN Connection Manager version 1.0 does not support the SSL service. If SSL is enabled, you will be unable to manage the switch using this version of SAN Connection Manager.
- To establish a secure Telnet 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 "Managing the date and time" (page 55).
- The SSL service must be enabled to authenticate users through a Remote Authentication Dial-In Service (RADIUS) server. See "Configuring a RADIUS server on the switch" (page 94).
- 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 manage both SSH and SSL services, enter the `set setup services` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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.

  TelnetEnabled       (True / False)   [True ]
  SSHEnabled          (True / False)   [False] True
  GUIMgmtEnabled      (True / False)   [True ]
  SSLEnabled          (True / False)   [False] True
  EmbeddedGUIEnabled  (True / False)   [True ]
  SNMPEnabled         (True / False)   [True ]
  NTPEnabled          (True / False)   [False]
  CIMEnabled          (True / False)   [False]
  FTPEnabled          (True / False)   [True ]
  MgmtServerEnabled   (True / False)   [True ]

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

Displaying SSL and SSH services

To display the status of the SSH and SSL services, enter the `show setup services` command, as shown in the following example:

```
8/20q FC Switch #> show setup services
System Services
-----------------------------
TelnetEnabled             True
SSHEnabled                False
GUIMgmtEnabled            True
SSLEnabled                False
EmbeddedGUIEnabled        True
SNMPEnabled               True
NTPEnabled                True
CIMEnabled                True
FTPEnabled                True
MgmtServerEnabled         True
CallHomeEnabled           True
```

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 SAN Connection Manager, QuickTools, or Enterprise Fabric Management Suite. The certificate is valid 24 hours before the certificate creation date and expires 365 days after the creation date. Should the original certificate become invalid, enter the `create certificate` command to create a new one, as shown in the following example:

```
8/20q FC Switch (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 that the security certificate will be valid, be sure that the switch and the workstation date and time are the same. See "Managing the date and time" (page 55).

8 RADIUS Server 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. With a RADIUS server, the security database for the entire fabric resides on the server. In this way, the security database can be managed centrally, rather than on each switch. However, when using a RADIUS server, every switch in the fabric must have a network connection. You can configure up to five RADIUS servers to provide failover.

You can configure a RADIUS server to authenticate only the switch or both the switch and the initiator device, if the device supports authentication. A RADIUS server can also be configured to authenticate user accounts. See "User Account Configuration" (page 17). A secure connection is required to authenticate user logins with a RADIUS server. See "Connection Security Configuration" (page 91).

Displaying RADIUS server information

To display RADIUS server information, enter the `show setup radius` command, as shown in the following example. For information about RADIUS server configuration parameters, see Table 49.

```
8/20q FC Switch #> show setup radius
    Radius Information
  ------------------
  DeviceAuthOrder   Local
  UserAuthOrder     Local
  TotalServers      2

  Server: 1

  ServerIPAddress   10.0.0.13
  ServerUDPPort     1812
  DeviceAuthServer  False
  UserAuthServer    False
  AccountingServer  False
  Timeout           2
  Retries           0
  SignPackets       False
  Secret            ********

  Server: 2

  ServerIPAddress   bacd:1234:bacd:1234:bacd:1234:bacd:1234
  ServerUDPPort     1812
  DeviceAuthServer  True
  UserAuthServer    True
  AccountingServer  True
  Timeout           2
  Retries           0
  SignPackets       False
  Secret            ********
```

Configuring a RADIUS server on the switch

To configure a RADIUS server on the switch, enter the `set setup radius` command. There are two groups of RADIUS configuration parameters. One group of parameters is common to all RADIUS server configurations. The second group is server-specific. You can configure both groups of parameters for all RADIUS servers, or you can configure the common and server-specific parameters separately. See Table 49 and Table 50 for descriptions of the common and server-specific RADIUS configuration parameters.

The following example configures the common RADIUS server configuration parameters:

```
8/20q FC Switch (admin) #> set setup radius 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 attributes
  for the server 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.

  PLEASE NOTE:
  -----------
  * SSL must be enabled in order to configure RADIUS User Authentication
    SSL can be enabled using the 'set setup services' command.

  Current Values:
    DeviceAuthOrder  Local
    UserAuthOrder    Local
    TotalServers     1

  New Value (press ENTER to not specify value, 'q' to quit):
    DeviceAuthOrder  1=Local, 2=Radius, 3=RadiusLocal :
    UserAuthOrder    1=Local, 2=Radius, 3=RadiusLocal :
    TotalServers     decimal value, 0-5               :

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

The following example configures RADIUS server 1:

```
8/20q FC Switch (admin) #> set setup radius server 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 attributes
  for the server 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.

  PLEASE NOTE:
  -----------
  * SSL must be enabled in order to configure RADIUS User Authentication
    SSL can be enabled using the 'set setup services' command.


Server 1 Current Values:
  ServerIPAddress    10.20.11.8
  ServerUDPPort      1812
  DeviceAuthServer   True
  UserAuthServer     True
  AccountingServer   False
  Timeout            10
  Retries            0
  SignPackets        False
  Secret             **********

New Server 1 Value (press ENTER to accept current value, 'q' to skip):
  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+)      :

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

9 Device Security Configuration

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 WWNs 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 that issue 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 providing 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 a RADIUS server such as Microsoft RADIUS.

Displaying security database information

You can display the following information about the security database:

Configured security set information

The `securityset list` and the `security list` commands display information about all security sets in the security database.

To display a list of the security sets, enter the `securityset list` command, as shown in the following example:

```
8/20q FC Switch #> securityset list
Current list of SecuritySets
----------------------------
  alpha
  beta
```

To display all security sets, groups, and group members in the security database, enter the `security list` command, as shown in the following example:

```
8/20q FC Switch #> 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.

To display component groups and group members, enter the `security active` command, as shown in the following example:

```
8/20q FC Switch #> 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
```

To display the name of the active security set and its activation history, enter the `securityset active` command, as shown in the following example:

```
8/20q FC Switch #> 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.

To display the member groups for a specified security set, enter the `securityset groups` command, as shown in the following example:

```
8/20q FC Switch #> securityset groups alpha
  Current list of Groups for SecuritySet: alpha
  --------------------------------------
  group1 (ISL)
  group2 (Port)
```

To display the security sets for which a specified group is a member, enter the `group securitysets` command, as shown in the following example:

```
8/20q FC Switch #> group securitysets group_1

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

Group membership information

To display the members for a specified group, enter the `group members` command, as shown in the following example:

```
8/20q FC Switch #> 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

To display a record of security database modifications, enter the `security history` command, as shown in the following example:

```
8/20q FC Switch #> 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
```

Security database history includes the following information:

- 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

To display a summary of the objects in the security database and their maximum limit, enter the `security limits` command, as shown in the following example:

```
8/20q FC Switch #> 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 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 reverse device security changes that have been received from another switch through the activation of a security set or the merging of fabrics. To replace the volatile security database with the contents of the non-volatile security database, enter the `security restore` command.

To restore the security configuration to its factory values, you can enter the `reset config` or `reset factory` command. Notice however, that these commands restore other aspects of the switch configuration as well.

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 Telnet, QuickTools, SAN Connection Manager, or Enterprise Fabric Management Suite. In addition, you must 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
8/20q FC Switch (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.

8/20q FC Switch (admin-config)#> config save
8/20q FC Switch (admin)#> config activate
8/20q FC Switch (admin)#> admin end
```

Modifying the security database

To modify the security database:

1. Open an Admin session with the `admin start` command.

   ```
   8/20q FC Switch #> admin start
   ```

   An Admin session prevents other accounts from making changes at the same time either through Telnet, QuickTools, Enterprise Fabric Management Suite, or SAN Connection Manager.
2. To open a Security Edit session, enter the `security edit` command. The Security Edit session provides access to the `securityset`, `group`, and `security` commands used to make modifications to the security database.

   ```
   8/20q FC Switch (admin) #> security edit
   8/20q FC Switch (admin-security)#> securityset . . .
   8/20q FC Switch (admin-security)#> group . . .
   8/20q FC Switch (admin-security)#> security . . .
   ```
3. When you finish making changes, take one of the following actions:
   - To save the changes and close the Security Edit session, enter the `security save` command.

     ```
     8/20q FC Switch (admin-security)#> security save
     ```
   - To close the Security Edit session without saving changes, enter the `security cancel` command.

     ```
     8/20q FC Switch (admin-security)#> security cancel
     ```
4. To activate the changes to the active security set, enter the `security activate` command.

   ```
   8/20q FC Switch (admin)#> security activate
   ```
5. To release the Admin session for other administrators, enter the `admin end` command.

   ```
   8/20q FC Switch (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:

  ```
  8/20q FC Switch (admin-security) #> security clear
    All security information will be cleared.  Please confirm (y/n): [n] y
  8/20q FC Switch (admin-security) #> security save
  ```
- Enter the `reset security` command, as shown in the following example.

  ```
  8/20q FC Switch (admin) #> reset security
  ```

  The security configuration values, `Autosave` and `FabricBindingEnabled`, remain unchanged.

Managing security sets

This sub-section describes the security set management tasks. All of these tasks except Activating a security set, page 103 and Deactivating a security set, page 103 require a Security Edit session.

Creating a security set

To create a new security set, enter the `securityset create` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> securityset create securityset_1
```

Deleting a security set

To delete a security set, enter the `securityset delete` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> securityset delete securityset_1
```

Renaming a security set

To rename a security set. enter the `securityset rename` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> securityset rename securityset_old
securityset_new
```

Copying a security set

To copy a security set and its contents to a new security set, enter the `securityset copy` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> securityset copy securityset_1 securityset_2
```

Adding groups to a security set

To add a group to a security set, enter the `securityset add` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> securityset add securityset_1 group_isl
group_port
```

Removing groups from a security set

To remove groups from a security set, enter the `securityset remove` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> sescurityset remove securityset_1 group_isl
group_port
```

Activating a security set

To apply security to the fabric, enter the `securityset activate` command, as shown in the following example:

```
8/20q FC Switch (admin) #> securityset activate securityset_1
```

Deactivating a security set

To deactivate the active security set and disable security in the fabric, enter the `securityset deactivate` command, as shown in the following example:

```
8/20q FC Switch (admin) #> securityset deactivate
```

Managing groups

This sub-section describes the group managment tasks. All of these tasks require an Admin session and a Security Edit session.

Creating 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

To create a new port group, enter the `group create` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> group create group_port port
```

Deleting a group

To delete group_port from the security database, enter the `group delete` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> group delete group_port
```

Renaming a group

To rename group_port to port_1, enter the `group rename` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> group rename group_port port_1
```

Copying a group

To copy the contents of an existing group (group_port) to a new group (port_1), enter the `group copy` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> group copy group_port port_1
```

Adding 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 8.
- For Port member attributes, see Table 9.
- For MS member attributes, see Table 10.

To add a member to a group, enter the `group add` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> security edit
8/20q FC Switch (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.
```

Modifying 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 8.
- For Port member attributes, see Table 9.
- For MS member attributes, see Table 10.

To change the attributes of a group member, enter the `group edit` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> security edit
8/20q FC Switch (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.
```

Removing members from a group

To remove a member from a group, enter the `group remove` command, as shown in the following example:

```
8/20q FC Switch (admin-security) #> group remove group_1 10:00:00:c0:dd:00:90:a3
```

10 Event Log Configuration

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 switch event messages, see the *HP 8/20q and SN6000 Fibre Channel Switch Event Messages Reference 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.
- **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.

Starting and stopping event logging

To stop recording event messages in the switch log, enter the `set log stop` command in an Admin session, as shown in the following example:

```
8/20q FC Switch (admin) #> set log stop
```

To start recording event messages in the switch log, enter the `set log start` command in an Admin session, as shown in the following example:

```
8/20q FC Switch (admin) #> set log start
```

Displaying the event log

To display the event log, enter the `show log` command. Each log message has the following format:

```
[ordinal] [time_stamp] [severity] [message_ID] [source] [message_text]
```

Table 5 describes the message format components.

Table 5 Event log message format

Component	Description
`[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 date hh:mm:ss.ms zone yyyy>. For events that originate with the switch, the time stamp comes from the switch; for events that originate with SAN Connection Manager, QuickTools, or Enterprise Fabric Management Suite the time stamp comes from the workstation.
`[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.
`[message_text]`	The text of the message

The following is an example of the `show log` command:

```
8/20q FC Switch #> show log
   [327][day month date time year][I][Eport Port:0/8][Eport State=
   E_A0_GET_DOMAIN_ID]
   [328][day month date time year][I][Eport Port: 0/8][FSPF PortUp state=0]
   [329][day month date time year][I][Eport Port: 0/8][Sending init hello]
   [330][day month date time year][I][Eport Port: 0/8][Processing EFP, oxid= 0x8]
   [331][day month date time year][I][Eport Port: 0/8][Eport State = E_A2_IDLE]
   [332][day month date time year][I][Eport Port: 0/8][EFP,WWN=
0x100000c0dd00b845,
   len= 0x30]
   [333][day month date time year][I][Eport Port: 0/8][Sending LSU
oxid=0xc:type=1]
   [334][day month date time year][I][Eport Port: 0/8][Send Zone Merge Request]
   [335][day month date time year][I][Eport Port: 0/8][LSDB Xchg timer set]
```

You can also filter the event log display with the `show log display` command and customize which messages are displayed automatically in the output stream.

Filtering the event log display

You can customize which events are displayed according to either the component or the severity level. To filter the events in the display, enter the `show log display` command with an operand that corresponds to one of 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
- SNMP events
- Zoning events

The following example filters the event log display for critical events.

```
8/20q FC Switch #> show log display critical
```

Controlling messages in the output stream

Alarms are always included in the output stream. To specify the additional severity level messages to be automatically displayed on the screen when they occur, enter the `set log display` command in an Admin session naming the lowest level message to be displayed. For example, the following command includes warning and critical level messages in the output stream:

```
8/20q FC Switch (admin) #> set log display warn
```

Managing the event log configuration

This sub-section describes the event log configuration management tasks.

Configuring the event log

You can customize which events are recorded in the switch event log according to component, severity level, and port. To filter the events to record, enter the `set log component`, `set log level`, and `set log port` commands in an Admin session. 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
- Zoning events
- Call Home events

The following example configures the event log to record switch management events with warning and critical severity levels associated with ports 0–3. Entering the `set log save` command ensures that this configuration is preserved across switch resets.

```
8/20q FC Switch (admin) #> set log component switch
8/20q FC Switch (admin) #> set log level warn
8/20q FC Switch (admin) #> set log port 0 1 2 3
8/20q FC Switch (admin) #> set log save
```

Displaying the event log configuration

To display all event log configuration settings, enter the `show log settings` command, as shown in the following example:

```
8/20q FC Switch #> show log settings
Current settings for log
------------------------
Started             True
FilterComponent     NameServer MgmtServer Zoning Switch Blade Port Eport Snmp CLI
QFS
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 20
```

Restoring the event log configuration

To return the event log configuration to the factory default, enter the `set log restore` command in an Admin session, as shown in the following example:

```
8/20q FC Switch (admin) #> set log restore
```

Clearing the event log

To delete all entries in the event log, enter the `set log clear` command in an Admin session, as shown in the following example:

```
8/20q FC Switch (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, however, requires that you enable remote logging on the switch and specify an IP address for the remote host.

NOTE: To log event messages on a remote host, 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. In this command, a `<tab>` separates the selector field (local0.info) from the 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.

To control local logging (`LocalLogEnabled` parameter) and remote logging (`RemoteLogEnabled` and `RemoteLogHostAddress` parameters), enter the `set setup system` command in an Admin session, as shown in the following example:

```
8/20q FC Switch (admin) #> set setup system
  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.

EthNetworkDiscovery     (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp)  [Static       ]
EthNetworkAddress       (dot-notated IP Address)             [10.0.0.1     ]
EthNetworkMask          (dot-notated IP Address)             [255.255.255.0]
EthGatewayAddress       (dot-notated IP Address)             [10.0.0.254   ]
AdminTimeout            (dec value 0-1440 minutes, 0=never)  [30           ]
InactivityTimeout       (dec value 0-1440 minutes, 0=never)  [0            ]
LocalLogEnabled         (True / False)                       [True         ]
RemoteLogEnabled        (True / False)                       [False        ]
RemoteLogHostAddress    (dot-notated IP Address)             [10.0.0.254   ]
NTPClientEnabled        (True / False)                       [False        ]
NTPServerAddress        (dot-notated IP Address)             [10.0.0.254   ]
EmbeddedGUIEnabled      (True / False)                       [True         ]
```

Creating and downloading a log file

To collect the event log messages in a file (`logfile`) on the switch, enter the `set log archive` command. `logfile` can have a maximum of 1,200 event messages. Use FTP to download the file from the switch to your workstation as follows:

1. Log into the switch through Telnet and create an archive of the event log. To create a file on the switch named `logfile`, enter the `set log archive` command.

   ```
   8/20q FC Switch #> admin start
   8/20q FC Switch (admin) #> set log archive
   ```

2. Open an FTP session on the switch and log in with the account name `images` and password `images`. Transfer the file `logfile` in binary mode with the `get` command.

   ```
   >ftp ip_address
   user:images
   password: images
   ftp>bin
   ftp>get logfile
       xxxxx bytes sent in xx secs.
   ftp>quit
   ```

11 Call Home Configuration

NOTE: The 8/20q Fibre Channel Switch Call Home service provides an email notification capability for the switch. This service has no relationship with the HP Call Home feature, which notifies HP services.

This section describes Call Home configuration tasks.

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 services` command. To display the Call Home service status, enter the `show setup services` command.

For a better understanding of the Call Home service, consider the following:

- Call Home requirements, page 113
- Call Home messages, page 114
- Technical support interface, page 115

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 Simple Mail Transfer Protocol (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" (page 116).
- Configure the Call Home database. The Call Home database allows up to 25 Call Home profiles. Each profile defines the following:
  - Event severity levels (Alarm, Critical, Warn) that will initiate an email message
  - E-mail message format and subject
  - E-mail recipients

  Having multiple profiles makes it possible to notify different audiences based on any combination of event severity, message format (short or full), or message length. You configure profiles using the `profile` command in a Callhome Edit session. See "Managing the Call Home database" (page 117).
- Ensure that each switch that is to support Call Home e-mail notification has its own Ethernet connection.

To test your Call Home service and database configurations, enter the `callhome test` command. See "Testing a Call Home profile" (page 123).

Call Home messages

The Call Home service generates e-mail messages for the specified event severity level and the following switch actions:

- Switch comes online
- Switch goes offline
- Reboot
- Power up
- Power down
- SFP failure

NOTE: For a power-down event, if the switch is forced to power down before the message is sent to the SMTP server, no message will be transmitted.

When a qualifying switch action or event occurs, an e-mail 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 e-mail messages using the `callhome queue clear` command.

There are three e-mail 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 contain basic switch and event information; Tsc1 is formatted for automated parsing.

The following is an example of a short-text e-mail:

```
From: john.doe@mycompany.com [mailto:john.doe@mycompany.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
```

The following is an example of a full-text e-mail, 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:        Wed Jul 25 17:02:40.343 CDT 2007

------------ 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 the collected data. For more information, see "Adding a data capture configuration" (page 122).

Configuring the Call Home service

To configure the Call Home service, enter the `set setup callhome` command in an Admin session, as shown in the following example. See Table 48 for a description of the Call Home service configuration entries.

```
8/20q FC Switch (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      (hostname, IPv4, or IPv6 Address):
  PrimarySMTPServerPort      (decimal value)                  :
  PrimarySMTPServerEnable    (True / False)                   :
  SecondarySMTPServerAddr    (hostname, IPv4, or IPv6 Address):
  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):
```

To display the Call Home service configuration, enter the `show setup callhome` command, as shown in the following example.

```
8/20q FC Switch (admin) #> 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:

1. Open an Admin session with the `admin start` command. An Admin session prevents other accounts from making changes at the same time through Telnet, QuickTools, SAN Connection Manager, Enterprise Fabric Management Suite, or any other management application.

   ```
   8/20q FC Switch #> admin start
   ```

2. Open a Callhome Edit session with the `callhome edit` command. The Callhome Edit session provides access to the `profile`, `callhome`, and `capture` commands that are used to make modifications to the Call Home database.

   ```
   8/20q FC Switch (admin) #> callhome edit
   8/20q FC Switch (admin-callhome)#> callhome . . .
   8/20q FC Switch (admin-callhome)#> profile . . .
   8/20q FC Switch (admin-callhome)#> capture . . .
   ```

3. When you finish making changes, take one of the following actions:
   - To save the changes and close the Callhome Edit session, enter the `callhome save` command. Changes take effect immediately.

     ```
     8/20q FC Switch (admin-callhome)#> callhome save
     ```

   - To close the Callhome Edit session without saving changes, enter the `callhome cancel` command.

     ```
     8/20q FC Switch (admin-callhome)#> callhome cancel
     ```

4. To release the Admin session for other administrators, enter the `admin end` command.

To remove all Call Home profiles and restore the Call Home service configuration to its factory state, enter the `reset callhome` command.

```
8/20q FC Switch (admin) #> reset callhome
```

Displaying Call Home database information

You can display the following Call Home database information:

- Change history
- List of profiles
- List of profiles and their details
- E-mail messages in the Call Home queue

To display the Call Home data base change history information, enter the `callhome history` command, as shown in the following example:

```
8/20q FC Switch #> 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
```

To display a list of Call Home profiles, enter the `callhome list` command, as shown in the following example:

```
8/20q FC Switch #> callhome list

 Configured Profiles:
 --------------------
 group4
 group5
```

To display a list of Call Home profiles and their details, enter the `callhome list profile` command, as shown in the following example:

```
8/20q FC Switch #> 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
```

To display information about e-mail messages in the Call Home queue, enter the `callhome queue stats` command, as shown in the following example:

```
8/20q FC Switch #> callhome queue stats
  Callhome Queue Information
  --------------------------
  FileSystemSpaceInUse        534 (bytes)
  EntriesInQueue                3
```

Creating a profile

To create a Call Home profile, enter the `profile create` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (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         2000000
  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, 650-2000000)      :
  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.

8/20q FC Switch (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Deleting a profile

To delete a Call Home profile, enter the `profile delete` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (admin-callhome) #> profile delete profile_1

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

8/20q FC Switch (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Modifying a profile

To modify an existing Call Home profile, enter the `profile edit` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (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) :
    MaxSize         (decimal value, 650-2000000)      :
    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.

8/20q FC Switch (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Renaming a profile

To rename profile_1, enter the `profile rename` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (admin-callhome) #> profile rename profile_1 profile_4

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

8/20q FC Switch (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Copying a profile

To copy profile_1, enter the `profile copy` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (admin-callhome) #> profile copy profile_1 profile_a
8/20q FC Switch (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

Adding a data capture configuration

To add a data capture configuration to the Tech_Support_Center profile, enter the `capture add` command, as shown in the following example. If the Tech_Support_Center profile does not exist, you must create it using the `profile create` command.

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (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

to modify a data capture configuration in the Tech_Support_Center profile, enter the `capture edit` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (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

To delete a data capture configuration from the Tech_Support_Center profile, enter the `capture remove` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (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

To test a Call Home profile, enter the `callhome test profile` command, as shown in the following example. This command generates a test message and routes it to the e-mail recipients specified in the profile.

```
8/20q FC Switch #> admin start
8/20q FC Switch (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.
8/20q FC Switch (admin) #>
  Test for Callhome Profile group4 Passed.
```

Changing Simple Mail Transfer Protocol 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch #> callhome edit
8/20q FC Switch #> (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

To clear e-mail messages from the Call Home message queue, enter the `callhome queue clear` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome queue clear
  The callhome queue will be cleared. Please confirm (y/n): [n] y
```

To display the contents of the Call Home message queue, see "Displaying Call Home database information" (page 118).

Resetting the Call Home database

There are two ways to reset the Call Home database. To clear all Callhome profiles, enter the `callhome clear` command, as shown in the following example. This command does not affect the Call Home service configuration.

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (admin-callhome) #> callhome clear
8/20q FC Switch (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

To clear all Call Home profiles and reset the Call Home service configuration to the factory defaults, enter the `reset callhome` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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 ....
```

12 Simple Network Management Protocol 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 `ReadCommunity` string and a `WriteCommunity` 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 supports SNMP version 3 in the CLI, which is disabled by default.

Managing the SNMP service

You control the SNMP service `SNMPEnabled` parameters through the `set setup snmp` or `set setup services` commands. See "Modifying the SNMP configuration" (page 127).

To enable SNMP, enter the `set setup services` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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.

  TelnetEnabled       (True / False)   [True ]
  SSHEnabled          (True / False)   [False]
  GUIMgmtEnabled      (True / False)   [True ]
  SSLEnabled          (True / False)   [False]
  EmbeddedGUIEnabled  (True / False)   [True ]
  SNMPEnabled         (True / False)   [True ]
  NTPEnabled          (True / False)   [False]
  CIMEnabled          (True / False)   [False]
  FTPEnabled          (True / False)   [True ]
  MgmtServerEnabled   (True / False)   [True ]
  CallHomeEnabled     (True / False)   [True ]

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

You can display the `SNMPEnabled` parameters using the `show setup snmp` or `show setup services` commands.

Displaying SNMP information

To display common and trap-specific SNMP configuration information, enter the `show setup snmp` command, as shown in the following example. See Table 52 for a description of the SNMP parameters.

```
8/20q FC Switch #> show setup snmp
  SNMP Information
  ----------------
  SNMPEnabled           True
  Contact               <sysContact undefined>
  Location              N_107 System Test Lab
  Description           HP 8/20q FC Switch
  ObjectID              1.3.6.1.4.1.3873.1.11
  AuthFailureTrap       True
  ProxyEnabled          True
  SNMPv3Enabled         False
  Trap1Enabled          False
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Version          2
  Trap2Enabled          False
  Trap2Address          0.0.0.0
  Trap2Port             162
  Trap2Severity         warning
  Trap2Version          2
  Trap3Enabled          False
  Trap3Address          0.0.0.0
  Trap3Port             162
  Trap3Severity         warning
  Trap3Version          2
  Trap4Enabled          False
  Trap4Address          0.0.0.0
  Trap4Port             162
  Trap4Severity         warning
  Trap4Version          2
  Trap5Enabled          False
  Trap5Address          0.0.0.0
  Trap5Port             162
  Trap5Severity         warning
  Trap5Version          2
```

Modifying the SNMP configuration

To modify the SNMP configuration, enter the `set setup snmp` command in an Admin session. 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. See Table 52 for descriptions of the common SNMP parameters.

The following example sets the common trap parameters for all SNMP traps:

```
8/20q FC Switch (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:
    SnmpEnabled      True
    Contact          <sysContact undefined>
    Location         <sysLocation undefined>
    ReadCommunity    public
    WriteCommunity   private
    AuthFailureTrap  False
    ProxyEnabled     True
    SNMPv3Enabled    False

  New Value (press ENTER to not specify value, 'q' to quit):
    SnmpEnabled      (True / False)         :
    Contact          (string, max=64 chars) :
    Location         (string, max=64 chars) :
    ReadCommunity    (string, max=32 chars) :
    WriteCommunity   (string, max=32 chars) :
    AuthFailureTrap  (True / False)         :
    ProxyEnabled     (True / False)         :
    SNMPv3Enabled    (True / False)         :

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

The following example configures SNMP trap 1:

```
8/20q FC Switch (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
    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)                           :
    Trap1Community  (string, max=32 chars)            :

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

Resetting the SNMP configuration

To reset the SNMP configuration back to the factory defaults, enter the `reset snmp` command in an Admin session, as shown in the following example. See Table 23 for a listing of the SNMP configuration factory defaults.

```
8/20q FC Switch (admin) #> reset snmp
```

Managing the SNMP version 3 configuration

SNMP version 3 is an interoperable, standards-based protocol for network management. SNMP version 3 provides secure access to devices using a combination of packet authentication and encryption over the network. SNMP version 3 provides the following security features:

- Message integrity—ensures that packets have not been altered
- Authentication—ensures that the packet is coming from a valid source
- Encryption—ensures that packet contents cannot be read by an unauthorized source

To configure SNMP version 3, you must enable SNMP version 3 on the switch and create one or more SNMP version 3 user accounts.

To enable SNMP version 3, enter the `set setup snmp common` command and set the `SNMPv3Enabled` parameter to `True`:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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:
    SnmpEnabled      True
    Contact          <sysContact undefined>
    Location         <sysLocation undefined>
    ReadCommunity    public
    WriteCommunity   private
    AuthFailureTrap  False
    ProxyEnabled     True
    SNMPv3Enabled    False

  New Value (press ENTER to not specify value, 'q' to quit):
    SnmpEnabled      (True / False)         :
    Contact          (string, max=64 chars) :
    Location         (string, max=64 chars) :
    ReadCommunity    (string, max=32 chars) :
    WriteCommunity   (string, max=32 chars) :
    AuthFailureTrap  (True / False)         :
    ProxyEnabled     (True / False)         :
    SNMPv3Enabled    (True / False)         : t

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

The following sub-sections describe how to create, display, and modify SNMP version 3 user accounts.

Creating an SNMP version 3 user account

To create an SNMP version 3 user account, enter the `snmpv3user add` command as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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)            [MD5       ] : 1
  AuthPhrase      (8-32 chars)                          : ***********
  Confirm AuthPhrase                                    : ***********
  Privacy         (True/False)              [False     ] : t
  PrivType        (1=DES)                   [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.
```

Displaying SNMP version 3 user accounts

To display SNMP version 3 user accounts, enter the `snmpv3user list` command as shown in the following example:

```
8/20q FC Switch #> snmpv3user list

  Username                        Group           AuthType   PrivType
  --------                        -----           --------   --------
  snmpuser1                       ReadWrite       MD5        DES
```

Modifying an SNMP version 3 user account

To modify an SNMP version 3 user account, enter the `snmpv3user edit` command as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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] y

  SNMPV3 user account edited and activated.
```

13 Command Reference

This chapter provides an alphabetical listing of the CLI commands and provides information for each command.

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 without any special session requirement. Commands associated with configuration tasks are available only in 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 in 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 `ike peer`, `ike policy`, `ipsec`, `ipsec association` and `ipsec policy` commands.

Syntax and operands

The **Syntax** paragraph defines the grammatical scheme for using operands in the command:

```
command
    operand
    operand [value]
    operand [value1] [value2]
```

The `command` is followed by one or more `operands`. Consider the following rules and conventions for using commands and operands:

- Commands and operands are case-insensitive.
- Required operand values appear in brackets: `[value]`. Optional operands and values are shown in italics: *`operand [value]`*.
- Underlined portions of the operand in the command format indicate the abbreviated form that can be used. For example, the **`delete`** operand can be abbreviated **`del`**.

The **Operands** paragraph lists and describes each operand that can be used with the command and any applicable values.

Notes and examples

The **Notes** paragraph presents information about the command and its use, including special applications or its effects on other commands. The **Examples** paragraph presents sample screen captures of the command and its output.

admin

Description 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 specified period of time, which is changed using the `set setup system` command.

Authority User account with Admin authority

Syntax

```
admin
    start or begin
    end or stop
    cancel
```

Operands

`start` or `begin`)
Opens the Admin session

`end` or `stop`
Closes the Admin session. The `hardreset`, `hotreset`, `quit`, `shutdown`, and `reset switch` commands will also end an Admin session.

`cancel`
Terminates an Admin session opened by another user. Use this operand with care because it terminates the Admin session without warning the other user and without saving pending changes.

Notes Closing a 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #>
.
.
.
8/20q FC Switch (admin) #> admin end
```

See also set setup system, page 247

alias

Description Creates a named set of ports/devices. Aliases make it easier to assign a set of ports/devices to many zones. An alias can not have a zone or another alias as a member.

Authority Admin session and Zoning Edit session for all operands 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]
```

Operands

`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 2,000 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 operand does not require an Admin session.

`members [alias]`
Displays all members of the alias given by [alias]. This operand 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 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:

```
8/20q FC Switch #> alias list

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

The following is an example of the `alias members` command:

```
8/20q FC Switch #> 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
```

See also zoning edit, page 335

callhome

Description Opens a Callhome Edit session in which to create and manage Call Home profiles.

NOTE: The 8/20q Fibre Channel Switch Call Home service provides an e-mail notification capability for the switch. This service has no relationship with the HP Call Home feature, which notifies HP services.

Authority Admin session, except for the `history` and `list` operands. The `clear` operand also requires an Callhome Edit session.

Syntax

```
callhome
    cancel
    changeover
    clear
    edit
    history
    list profile [profile]
    queue [option]
    save
    test profile [profile]
```

Operands

`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 operand requires a Callhome Edit session. This operand 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.

NOTE: 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 operand 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 operand, 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]. The Call Home queue statistics parameters are described in Table 6

Table 6 Call Home queue statistics parameters

Parameter	Description
`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.

Operands `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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> callhome list

 Configured Profiles:
 --------------------
 group4
 group5
```

The following is an example of the `callhome list profile` command:

```
8/20q FC Switch #> 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 list` command:

```
8/20q FC Switch #> callhome list

 Configured Profiles:
 --------------------
 group4
 group5
```

The following is an example of the `callhome test profile` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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.
8/20q FC Switch (admin) #>
  Test for Callhome Profile group4 Passed.
```

The following is an example of the `callhome queue clear` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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:

```
8/20q FC Switch #> callhome queue stats
  Callhome Queue Information
  --------------------------
  FileSystemSpaceInUse        534 (bytes)
  EntriesInQueue                3
```

See also profile, page 201

reset, page 206

capture

Description 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 are collected from the switch and sent to recipients specified in the Tech_Support_Center profile.

Authority Admin session and Callhome Edit session. For information about starting a Callhome Edit session, see the `callhome` command.

Syntax

```
capture
    add
    edit
    remove
```

Operands

`add`

Adds data capture instructions to the Tech_Support_Center profile. Table 7 describes the data capture parameters.

Table 7 Data capture configuration parameters

Parameter	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 data-capture 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. See Table 7 for a description of the data capture configuration parameters.

`remove`

Removes the data capture configuration from the Test_Support_Center profile.

Examples The following is an example of the `capture add` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (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.
```

See also profile, page 201

cert_authority

Description Manages certificate authority certificates in the PKI database.

Authority Admin session. 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]
```

Operands

`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 association with the same name.

`list [authority_name]`
Displays certificate authorities on the switch and associated certificate authority certificates.

certificate

Description Creates certificate requests and manages signed certificates in the PKI database.

Authority Admin session

Syntax
```
certificate
    delete local [certificate_name]
    generate request
    import local [certificate_name] [file_name] force
    list local [certificate_name]
```

Operands

`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.

`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.

`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.

Examples The following is an example of a Certificate Generate Request command:

```
8/20q FC Switch (admin) #> admin start
8/20q FC Switch (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)           : key512
   *SubjectDistinguishedName (string, max=128 chars)          : O=HP
    SubjectAlternateName     (may enter up to 16, 1 per line)
            1) enter a hostname, IPv4, IPv6 or Email Address  johndoe@ibm.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
```

See also key, page 196

clone config port

Description 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]
```

Operands `[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]. [source_port_number] can be 0–19. [port_list] can be a list of port numbers or ranges delimited by spaces.

Notes See Table 35 for a description of the port configuration parameters.

Examples The following example configures ports 8–19 based on port 0:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) config edit
8/20q FC Switch (admin) #> clone config port 0 8-19
Port 0 configuration will be cloned to ports 8-19.
  Please confirm (y/n): [n] y
8/20q FC Switch (admin-config)#> config save
8/20q FC Switch (admin)#> config activate
8/20q FC Switch (admin)#> admin end
```

See also set config port, page 221

show config port, page 261

config

Description Manages the Fibre Channel configurations on a switch.

Authority Admin session for all operands 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 import
    save [config_name]
```

Operands

`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 configuration backup file named `configdata`, which contains the system configuration information. This operand does not require an Admin session.

The optional `export` operand creates the configuration backup file and exports it to a remote server prompting you for the server name, 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] from the switch. 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 (version 4 or 6) 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 (version 4 or 6) 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 on the switch. This operand does not require an Admin session.

`restore import`

Restores configuration settings to the switch from a configuration backup file named `configdata`. You can create a backup file using the `config backup` command. Typically, you would upload this backup file from a server using FTP.

The optional `import` operand 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.

After the restore is complete, the switch automatically resets. See "Backing up and restoring a switch configuration" (page 54).

NOTE:

- If the restore process changes the IP address, use the `set setup system` command to return the IP configuration to the values you want. If the IP address is unknown, you must place the switch in maintenance mode and reset the network configuration to restore the default IP address 10.0.0.1. For information about using maintenance mode, see the *HP 8/20q Fibre Channel Switch Installation and Reference Guide*.
- Configuration archive files created with the QuickTools or Enterprise Fabric Management Suite 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 are not restored. Unless you edit the security database and reconfigure the secrets, the switch will be isolated from the fabric.

`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 #, 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 shows an example of how to open and close a Config Edit session:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
   The config named default is being edited.
.
.
8/20q FC Switch (admin-config) #> config cancel
  Configuration mode will be canceled. Please confirm (y/n): [n] y
8/20q FC Switch (admin) #> admin end
```

The following is an example of how to create a backup file (`configdata`) and download the file to the workstation.

```
8/20q FC Switch #> config backup
8/20q FC Switch #> exit

#>ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> get configdata
ftp> 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.

```
#> ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> put configdata
ftp> quit

8/20q FC Switch #> admin start
8/20q FC Switch (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]
8/20q FC Switch (admin) #>
  Alarm Msg: [day month date time year][A1000.0005][SM][The switch is being
reset]
```

See also set config port, page 221

show config port, page 261

set config switch, page 226

show config switch, page 264

create

Description Creates support files for troubleshooting switch problems, and also creates certificates for secure communications for SAN Connection Manager, QuickTools, Enterprise Fabric Management Suite, and SMI-S.

Authority Admin session for the `certificate` operand

Syntax

```
create
    certificate
    support
```

Operands

`certificate`

Creates a security certificate on the switch. The security certificate is required to establish an SSL connection with a management application such as SAN Connection Manager. 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, use the `create certificate` command to create a new one.

NOTE: To insure the creation of a valid certificate, be sure that the switch and the workstation time and date are the same. See also the following commands:

- `date` command for information about setting the time and date
- `set timezone` command for information about setting the time zone on the switch and workstation
- `set setup system` command 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 FTP server, you can proceed with the command prompts to send the file from the switch to a remote host. Otherwise, you can use FTP 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 operand does not require an Admin session.

NOTE: Support files are deleted from the switch during a power-cycle or switch reset.

Examples The following is an example of the `create certificate` command:

```
8/20q FC Switch (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.
```

The following is an example of the `create support` command to download the support file to your workstation. When prompted to send the support file to another machine, you decline, close the Telnet session, and open an FTP session on the switch and log in with the account name `images` and password `images`. You then use the `get` FTP command to transfer the `dump_support.tgz` file in binary mode.

```
8/20q FC Switch (admin) #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): n

8/20q FC Switch (admin) #> quit
>ftp switch_ip_address
user:     images
password: images

ftp>bin
ftp>get dump_support.tgz
    xxxxx bytes sent in xx secs.
ftp> quit
```

The following is an example of the `create support` command when an FTP server is available on the workstation:

```
8/20q FC Switch #> create support
Log Msg:[Creating the support file - this will take several seconds]

FTP the dump support file to another machine? (y/n): y
Enter address of ftp server (hostname, IPv4, or IPv6): 10.20.33.130
Login name: johndoe
Enter remote directory name: bin/support
Would you like to continue downloading support file? (y/n) [n]: y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password:  xxxxxxx

230 User johndoe logged in.
cd bin/support
250 CWD command successful.
lcd /itasca/conf/images
Local directory now /itasca/conf/images
bin
200 Type set to I.
put dump_support.tgz
local: dump_support.tgz remote: dump_support.tgz
227 Entering Passive Mode (10,20,33,130,232,133)
150 Opening BINARY mode data connection for dump_support.tgz.
226 Transfer complete.
43430 bytes sent in 0.292 secs (1.5e+02 Kbytes/sec)
Remote system type is UNIX.
Using binary mode to transfer files.
221-You have transferred 43430 bytes in 1 files.
221-Total traffic for this session was 43888 bytes in 1 transfers.
221 Thank you for using the FTP service on localhost.localdomain.
```

See also date, page 152

set setup system, page 247

set timezone, page 255

date

Description 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]
```

Operands *[MMDDhhmmCCYY]*

Specifies the date by the day, month, time, and year–this requires an Admin session. [MMDDhhmmCCYY] is as follows:

- MM—01 through 12 corresponds to January through December
- DD—01 through 31 corresponds to the day of the month
- hh—00 through 23 corresponds to the hour on a 24-hour clock
- mm—00 through 59 corresponds to the minute
- CC—20 corresponds to the millennium and century
- YY—00 through 99 corresponds to the decade and year

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. To disable the `NTPClientEnabled` parameter, enter the `set setup system` command.

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 To display the date, enter the `date` command, as shown in the following example:

```
8/20q FC Switch #> date
  Mon Apr 07 07:51:24 200x
```

To set the date and time (January 31, 10:15 AM, 2008), enter the `date` command, as shown in the following example:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> date 013110152008
8/20q FC Switch (admin) #> date
  Thu Jan 31 10:15:03 UTC 2008
```

See also set setup system, page 247

exit

Description Closes the switch connection.

Authority None

Syntax `exit`

Notes You can also press **Control-D** to close the switch connection.

fcping

Description Verifies a Fibre Channel connection with another switch or a device and reports status.

Authority None

Syntax
```
fcping destination [address]
    count [number]
    timeout [seconds]
```

Operands

`[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 world wide 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:

```
8/20q FC Switch #> 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
```

See also fctrace, page 155

ping, page 200

fctrace

Description Displays the path from an initiator device port in the fabric to a target device port in the same zone. To trace the path between two initiator ports, you must disable the I/O StreamGuard feature. Use the `set config port` command to change the `IOStreamGuard` parameter.

Path information includes the following:

- Domain IDs
- Inbound port name and physical port number
- Outbound port name and physical port number

Authority None

Syntax `fctrace [port_source] [port_destination] [hop_count]`

Operands `[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 world wide 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 world wide 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], 20 hops is used.

Examples The following is an example of the `fctrace` command:

```
8/20q FC Switch#> 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
```

See also fcping, page 154

ping, page 200

feature

Description Adds license key features to the switch and displays the license key feature log. To order a license key, contact your switch distributor or your authorized reseller. Upgrading a switch is not disruptive, nor does it require a switch reset.

Authority Admin session for `add` operand only

Syntax
```
feature
    add [license_key]
    log
```

Operands

`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.

Notes
- The HP 8/20q Port Activation Upgrade LTU enables additional SFP ports in increments of four on the standard 12-port, single power supply 8/20q Fibre Channel Switch for totals of 16 or 20 ports.

Examples The following is an example of the `feature add` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> feature add 1-LCVXOWUNOJBE6
License upgrade to 20 ports

Do you want to continue with license upgrade procedure? (y/n): [n] y
Alarm Msg:[day mon date time year][A1005.0030][SM][Upgrading Licensed Ports
to 20]
```

The following is an example of the `feature log` command:

```
8/20q FC Switch #> feature log
  Mfg Feature Log:
  ----------------
  Switch Licensed for 8 ports
  Customer Feature Log:
  ---------------------
  1) day month date 19:39:24 year - Switch Licensed for 20 ports
  1-LCVXOWUNOJBE6
```

firmware install

Description 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:

- The file transfer protocol (FTP or TFTP)
- IP address or DNS host name of the remote host
- An account name and password on the remote host (FTP only)
- Pathname for the firmware image file

Authority Admin session

Syntax `firmware install`

Examples The following is an example of the `firmware install` command using FTP:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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 or TFTP     : ftp
  User Account    : johndoe
  IP Address      : 10.0.0.254
  Source Filename : 8.0.x.xx.xx_epc
  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 FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
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 `firmware install` command using TFTP:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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 or TFTP     : tftp
  IP Address      : 10.0.0.254
  Source Filename : 8.0.x.xx.xx_epc
  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 FTP server (Version wu-2.6.1-18) ready.
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.
```

See also image, page 182

group

Description 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. The `list`, `members`, `securitysets`, and `type` operands 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]
```

Operands `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 8, Table 9, and Table 10 respectively. The group name and group type attributes are read-only fields common to all three tables.

Table 8 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`.
`PrimaryHash`	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.
`PrimarySecret`	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
`SecondaryHash`	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 8 ISL group member attributes (continued)

Attribute	Description
SecondarySecret	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 WWN. This option is available only if FabricBindingEnabled is set to True using the set config security command. 0 (zero) specifies no binding.

Table 9 Port group member attributes

Attribute	Description
Member	WWPN for the N_Port device that would attach to the switch. A member cannot belong to more than one group. All loop device WWPNs must be included in the group, otherwise the switch port will be downed, and none of the devices will be able to log in.
Authentication	Enables (Chap) or disables (None) authentication using the Challenge Handshake Authentication Protocol. The default is None.
PrimaryHash	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.
PrimarySecret	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
SecondaryHash	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.
SecondarySecret	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 10 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.

Table 10 MS group member attributes (continued)

Attribute	Description
`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 the new group 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 alphanumeric, _, $, ^, and -. The security database supports a maximum of 16 groups. If you omit [type], ISL is used. Table 11 describes the group type parameters.

Table 11 Group type parameters

Parameter	Description
`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.

`delete [group]`
Deletes the group given by [group].

`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 12.

Table 12 Group member attributes

Attribute	Description
`Authentication` (ISL and Port Groups)	Enables (`Chap`) or disables (`None`) authentication using the Challenge Handshake Authentication Protocol.
`CTAuthentication` (MS Groups)	CT authentication. Enables (`True`) or disables (`False`) authentication for MS group members. The default is `False`.
`PrimaryHash` (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`.

Table 12 Group member attributes (continued)

Attribute	Description
PrimarySecret (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
SecondaryHash (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.
SecondarySecret (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.

Operands `list`
Displays a list of all groups and the security sets of which they are members. This operand is available without an Admin session.

`members [group]`
Displays all members of the group given by [group]. This operand 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 operand is available without an Admin session.

`type [group]`
Displays the group type for the group given by [group]. This operand 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 more information about managing groups in security sets, see the `securityset` command.

Examples The following is an example of the `group add` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> security edit
8/20q FC Switch (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)             [            ]
  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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> security edit
8/20q FC Switch (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:

```
8/20q FC Switch #> group list
  Group       SecuritySet
  -----       -----------
  group1 (ISL)
              alpha
  group2 (Port)
              alpha
```

The following is an example of the `group members` command:

```
8/20q FC Switch #> 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
```

See also security, page 214

hardreset

Description Resets the switch and performs a power-on self test (POST). 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.

Authority Admin session

Syntax `hardreset`

Notes To reset the switch without a power-on self test, see the `reset` command.

To reset the switch without disrupting traffic, see the `hotreset` command.

See also hotreset, page 168

set log, page 231

reset, page 206

help

Description Displays a brief description of the specified command, its operands, and usage.

Authority None

Syntax `help [command] [operand]`

Operands *[command]*

Displays a summary of the command given by [command] and its operands. If you omit [command], the system displays all available commands.

[operand]

Displays a summary of the operand given by [operand] belonging to the command given by [command]. If you omit [operand], the system displays the available operands 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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> 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

Description 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:

```
8/20q FC Switch #> history
   1 show switch
   2 date
   3 help set
   4 history

8/20q FC Switch #> !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

Description 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 firmware upgrades on an operating switch without disrupting data traffic or having to re-initialize attached devices. If the non-disruptive activation fails, you will usually be prompted to try again later. Otherwise, the switch will perform a disruptive activation. Verify that the current firmware version supports the installation and non-disruptive activation of the new firmware version. For information about compatible firmware versions, see the *Firmware Release Notes*.

To ensure a successful non-disruptive activation, you should first satisfy the following conditions:

- No changes are being made to switches in the fabric including installing firmware, powering up, powering down, disconnecting or connecting ISLs, and changing the switch configuration.
- 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.
- No more than two SAN Connection Manager sessions are open.

Ports that change states during the non-disruptive activation are reset. When the non-disruptive activation is complete, SAN Connection Manager sessions, QuickTools sessions, and Enterprise Fabric Management Suite sessions are automatically reconnected. However, Telnet sessions must be restarted manually.

This command clears the event log and all counters.

TIP: After upgrading firmware that includes changes to QuickTools, a QuickTools session that was open during the upgrade may indicate that the new firmware is not supported. To correct this, close the QuickTools session and the browser window, then open a new QuickTools session.

See also hardreset, page 165

reset, page 206

set log, page 231

ike list

Description Displays IKE peer and policy information.

Authority None

Syntax
```
ike list
    active
    configured
    edited
    peer [option]
    policy [option]
```

Operands

`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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch (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
```

See also ike peer, page 171

ike policy, page 176

ike peer

Description 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]
```

Operands

`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.

Table 13 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 from which data originates.
`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 of the following: • 3DES-CBC • AES_CBC_128 • AES_CBC_192 • AES_CBC_256
`Integrity`	Integrity (authentication) algorithm. Integrity can be one of the following: • MD5_96 • SHA1_96 • SHA2_256 • AES_XCBC_96
`DHGroup`	Diffie-Hellman group number. You can specify one or more group numbers: 1, 2, 5, 14, or 24
`Restrict`	Algorithm and DH group restriction. The IKE responder accepts only the configured algorithms and DH groups specified by the IKE initiator (True), or accepts all algorithms and DH groups (False).

Table 13 IKE peer configuration parameters (continued)

Parameter	Description
`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)`	Switch certificate name by which to authenticate the peer. `CertificateName` is a string of up to 32 characters. For more information about certificates, see the `certificate` command.
`SwitchIdentity (Authentication=Pubkey)`	Switch 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 the `subjectAltName` extension in the local certificate.
`PeerIdentity (Authentication=Pubkey)`	Peer 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 the `subjectAltName` extension in the peer certificate.

Operands `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, see Table 13.

`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.

`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:

```
8/20q FC Switch ># admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (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.
8/20q FC Switch (admin-IPSEC) #> ipsec save
```

The following is an example of the `ike peer edit` command:

```
8/20q FC Switch (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:

```
8/20q FC Switch (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              ********
```

See also ike list, page 169

ike policy, page 176

ike policy

Description 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]
```

Operands

`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.

Table 14 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 14 IKE policy configuration parameters (continued)

Parameter	Description
`Protocol (LocalPort=1-65535 or RemotePort=1-65535)`	Transport protocol for which to encrypt 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: • null • 3des_cbc • aes_cbc_128 • aes_cbc_192 • aes_cbc_256 • aes_ctr_128 (not supported on all platforms) • aes_ctr_192 (not supported on all platforms) • aes_ctr_256 (not supported on all platforms)
`Integrity`	One or more authentication algorithms to apply to the policy: • md5_96 • sha1_96 • sha2_256 • aes_xcbc_96
`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.
`Restrict`	Algorithm and DH group restriction. The IKE responder accepts only algorithms and DH groups for an IKE security association (`true`), or accepts any algorithm and DH group (`false`).

Operands `delete [policy]`

Deletes the policy given by [policy] from the IKE database. You must enter the `ipsec save` command afterwards to save your changes.

`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:

```
8/20q FC Switch (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
                          5=null                                 :  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.
8/20q FC Switch (admin-IPSEC) #> ipsec save
```

The following is an example of the `ike policy edit` command:

```
8/20q FC Switch (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
                          5=null                                 :  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.
8/20q FC Switch (admin-IPSEC) #> ipsec save
```

See also ike list, page 169
ike peer, page 171

image

Description Manages and installs switch firmware.

Authority Admin session

Syntax

```
image
    cleanup
    fetch [account_name] [ip_address] [file_source] [file_destination]
    install
    list
    tftp [ip_address] [file_source] [file_destination]
    unpack [file]
```

Operands

`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 FTP and stores it on the switch with the file name given by [file_destination]. [ip_address] can be an IP address (version 4 or 6) or a DNS host name. The image file is retrieved from the host IP address given by [ip_address]. If an account name needs a password to access the FTP 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 or TFTP)
- IP address or DNS host name of the remote host
- An account name and password on the remote host (FTP only)
- Pathname for the firmware image file

`list`
Displays the list of image files that reside on the switch.

`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 (version 4 or 6) 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.

Notes To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

To install firmware when the 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> image 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 or TFTP     : ftp
  User Account    : johndoe
  IP Address      : 10.0.0.254
  Source Filename : 8.x.x.xx.xx_epc
  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 FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
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:

```
8/20q FC Switch (admin) #> image fetch johndoe 10.0.0.254 8.x.x.xx.xx_epc
>ftp 10.0.0.254
user:johndoe
password: ********
ftp>bin
ftp>put 8.x.x.xx.xx_epc
ftp>quit
8/20q FC Switch (admin) $>image list
8/20q FC Switch (admin) $>image unpack 8.x.x.xx.xx_epc
Image unpack command result: Passed
```

See also firmware install, page 157

ipsec

Description 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` operand. The `clear` operand also requires an Ipsec Edit session.

Syntax

```
ipsec
    cancel
    clear
    edit
    history
    limits
    save
```

Operands

`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 operand requires an Ipsec Edit session. The operand 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.

NOTE: The preferred method for deleting the IP security configuration from the switch is the `reset ipsec` command.

`edit`
Opens an Ipsec Edit session in which to create and manage IP security associations and policies, and IKE peers and policies. This keyword requires an Admin session. Ipsec Edit session commands include the `ike peer`, `ike policy`, `ipsec clear`, `ipsec association`, and `ipsec policy` commands. This operand requires an Admin session.

`history`
Displays a history of IP security modifications. This operand 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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> ipsec limits

  Configured (saved) IPsec Information

  IPsec Attribute            Maximum  Current
  ---------------            -------  -------
  MaxConfiguredSAs               512        0
  MaxConfiguredSPs               128        0
  MaxConfiguredIKEPeers           16        0
  MaxConfiguredIKEPolicies       256        0
```

See also ipsec association, page 186

ipsec list, page 189

ipsec policy, page 192

ipsec association

Description 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]
```

Operands

`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 alphanumeric, _, $, ^, 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. Table 15 describes the association configuration parameters.

Table 15 Association configuration parameters

Parameter	Description
`Description`	Description of the association indicating its purpose or the types of connections which it secures.
`SourceAddress`	IP address (version 4 or 6) or DNS host name of the host, switch, or gateway from which data originates
`DestinationAddress`	IP address (version 4 or 6) 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) • Encapsulated Security Payload–RFC 1827 (esp-old) • Authentication Header– RFC 2402 (ah) • Authentication Header–RFC 1826 (ah-old)
`SPI`	Security parameters index number in the range 256–4,294,967,295
`Authentication`	Algorithm to use to authenticate the source or destination. The authentication algorithm can be one of the following: • HMAC-MD5 • HMAC-SHA1 • HMAC-SHA256 • AES-XCBC-MAC
`AuthenticationKey`	Key string to use for authentication such as `"12345678901234567890"`

Table 15 Association configuration parameters (continued)

Parameter	Description
`Encryption`	Algorithm that encrypts outbound data or decrypt inbound data. The encryption algorithm can be one of the following: • DES-CBC • 3DES-CBC • Null • Blowfish-CBC • AES-CBC • Twofish-CBC • AES-CTR (not available on all systems)
`EncryptionKey`	Key string to use in encrypting or decrypting data such as `"12345678901234567890123 4"`
`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

Operands

`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]. For descriptions of the association parameters, refer to Table 15. If the connection is not secure (SSH is disabled), the `AuthenticationKey` and `EncryptionKey` values are masked.

`list` *`[option]`*
Displays the configuration for the policies 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.

Examples The following is an example of the `ipsec association create` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (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)
                         1=des-cbc        (8 byte key)
                         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): "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.
```

See also ipsec, page 184

ipsec list, page 189

ipsec policy, page 192

ipsec list

Description Displays information about IP security associations and policies.

Authority None

Syntax
```
ipsec list
    active
    association [option]
    configured
    edited
    policy [option]
```

Operands

`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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> 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 association` command:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> 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
```

See also ipsec, page 184

ipsec association, page 186

ipsec policy, page 192

ipsec policy

Description 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]
```

Operands

`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 alphanumeric, _, $, ^, 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 16 describes the policy parameters:

Table 16 Policy configuration parameters

Parameter	Description
`Description`	Description of the policy
`SourceAddress`	IP address (version 4 or 6) or DNS host name of the host, switch, or gateway from which data originates
`SourcePort`	Source port number in the range `1—65535`
`DestinationAddress`	IP address (version 4 or 6) 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 in the range `1—65535`
`Protocol`	Protocol or application to which to apply IP security. Enter an operand for one of the following protocols or an integer in the range `0—255`: • Internet Control Message Protocol for IPv4 (ICMP) • Internet Control Message Protocol for IPv6 (ICMP6) • Internet Protocol, version 4 (IPv4) • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • Any protocol
`ICMPv6 Type`	ICMP number (0–255). You are prompted for this parameter only if you specify ICMP6 for the `Protocol` parameter.

Table 16 Policy configuration parameters (continued)

Parameter	Description
`Direction`	Direction of the data traffic to which the policy is to be applied: • In—Data entering the source • 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.
`ProtectionDesired`	Type of IP security protection to apply: • AH—Authentication Header • ESP—Encapsulating Security Payload • Both—Apply both AH and ESP protection
`ahRuleLevel`	Rule level to apply for AH 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 is matched with the policy
`espRuleLevel`	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 is matched with the policy
`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.

Table 16 Policy configuration parameters (continued)

Parameter	Description
`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 is matched with the policy

Operands `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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> ipsec edit
8/20q FC Switch (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      (IPv4, IPv6 or hostname/[PrefixLength])        :
                                                      fe80::2c0:ddff:fe03:d4c1
    SourcePort         (decimal value, 1-65535)                       :
   *DestinationAddress (IPv4, IPv6 or hostname/[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.
```

See also ipsec, page 184

ipsec association, page 186

ipsec list, page 189

key

Description Creates and manages public/private key pairs in the PKI database.

Authority Admin session. 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]
```

Operands

`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:

`512`
Creates a public/private key pair of 512 bits

`1024`
Creates a public/private key of 1,024 bits

`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.

`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.

Examples The following is an example of the `key generate` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #>: key generate key512 size 512
```

The following is an example of the `key list` command for key512:

```
8/20q FC Switch #> key list key512
  Key key512:
    private key with:
    pubkey:    RSA 512 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:

```
8/20q FC Switch #> key list
  Installed Keys:
    key512
    key2048
    key1024
  * indicates key has a matching local certificate
```

See also certificate, page 144

lip

Description Reinitializes the specified loop port.

Authority Admin session

Syntax `lip [port_number]`

Operands `[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:

```
8/20q FC Switch (admin) #> lip 2
```

logout

Description Closes the switch connection.

Authority None

Syntax `logout`

Notes You can also press **Control-D** to close the switch connection.

See also exit, page 153

logout, page 198

passwd

Description Changes a user account's password.

Authority Admin account name and an Admin session to change another account's password; you can change your own password without an Admin session.

Syntax `passwd [account_name]`

Operands `[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 `admin`. 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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.
```

See also user, page 322

ping

Description Initiates an attempt to communicate with another switch over an Ethernet network and reports the result.

Authority None

Syntax
```
ping
    [host_name]
    -ipv4 [host_address]
    -ipv6 [host_address]
```

Operands

`[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 (.).

`-ipv4 [host_address]`

IP address (version 4) or DNS host name of the switch you want to query. Broadcast IP addresses, such as 255.255.255.255, are not valid.

`-ipv6 [host_address]`

IP address (version 6) or DNS host name of the switch you want to query.

Examples The following is an example of a `ping` command that successfully communicated with another switch:

```
8/20q FC Switch #> ping 10.20.11.57
  Ping command issued. Waiting for response...
8/20q FC Switch #>
  Response successfully received from 10.20.11.57.
```

The following is an example of a `ping` command for which there was no response from the other switch:

```
8/20q FC Switch #> ping 10.20.11.57
  Ping command issued. Waiting for response...
  No response from 10.20.11.57. Unreachable.
```

profile

Description 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.

NOTE: The Call Home service provides an e-mail notification capability for the switch. This service has no relationship with the HP Call Home feature, which notifies HP services.

Authority Admin session and a Callhome Edit session. For information about starting a Callhome Edit session, see the `callhome` command.

Syntax

```
profile
    copy [profile_source] [profile_destination]
    create [profile]
    delete [profile]
    edit [profile]
    rename [profile_old] [profile_new]
```

Operands

`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 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 alphanumeric, _, $, ^, and -. The Tech_Support_Center profile name is reserved. The Call Home database supports a maximum of 25 profiles. You must enter the `callhome save` command to save your changes. Table 17 describes the profile configuration parameters.

Table 17 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 it easier to read messages on small display devices such as cell phones. The minimum is 650. The maximum and default is 2,000,000.
`EmailSubject`	Subject of the e-mail; up to 64 characters

Table 17 Profile configuration parameters (continued)

Parameter	Description
RecipientMail	Addresses to send e-mail messages to; maximum of 10 addresses. The address format is account@domain.
CaptureEnabled	Enables (True) or disables (False) the data capture configuration only when creating the Tech_Support_Center profile. The default is False. For more information about the data capture configuration, see the "capture" command.

Operands delete [profile]

Deletes the specified profile given by [profile] from the Call Home database. You must enter the callhome save command 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 descriptions of the profile parameters, see Table 17. 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 to save your changes.

Examples The following is an example of the profile create command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (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)         :
  MaxSize         (decimal value, 650-2000000)      :
  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.

8/20q FC Switch (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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> callhome edit
8/20q FC Switch (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) :
    MaxSize         (decimal value, 650-2000000)      :
    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.

8/20q FC Switch (admin-callhome) #> callhome save
  The CallHome database profiles will be saved and activated.
  Please confirm (y/n): [n] y
```

See also callhome, page 137

capture, page 140

ps

Description Displays current system process information.

Authority None

Syntax `ps`

Examples The following is an example of the `ps` command:

```
8/20q FC Switch #> ps
  PID  PPID %CPU %MEM TIME      ELAPSED    COMMAND
  244   224  0.0  0.3 00:00:04  2-03:02:31 cns
  245   224  0.0  0.3 00:00:06  2-03:02:31 ens
  246   224  0.0  0.3 00:00:09  2-03:02:31 dlog
  247   224  0.0  0.6 00:00:33  2-03:02:31 ds
  248   224  0.3  2.8 00:09:59  2-03:02:31 mgmtApp
  249   224  0.0  0.3 00:00:16  2-03:02:31 sys2swlog
  251   224  0.0  0.4 00:00:06  2-03:02:30 fc2
  252   224  0.0  0.6 00:00:16  2-03:02:30 nserver
  253   224  0.0  0.8 00:00:08  2-03:02:30 PortApp
  254   224  0.0  0.5 00:00:03  2-03:02:30 qfsApp
  255   224  0.0  0.5 00:00:09  2-03:02:30 mserver
  256   224  0.0  0.7 00:00:06  2-03:02:30 eport
  257   224  0.0  0.6 00:00:13  2-03:02:30 zoning
  282   254  0.0  0.5 00:00:00  2-03:02:26 qfsApp
  284   224  0.0  0.6 00:00:08  2-03:02:26 snmpservicepath
  285   282  0.0  0.5 00:00:00  2-03:02:26 qfsApp
  308   224  0.0  0.8 00:00:29  2-03:02:25 cim_server
```

quit

Description Closes the switch connection.

Authority None

Syntax `quit`

Notes You can also press **Control-D** to close the switch connection.

See also exit, page 153
logout, page 198

reset

Description Resets the switch configuration parameters. If you omit the operand, the default is `reset switch`.

Authority Admin session

Syntax

```
reset
    callhome
    config [config_name]
    factory
    ipsec
    port [port_list]
    radius
    security
    services
    snmp
    switch (default)
    system
    zoning
```

Operands

`callhome`
Resets the Call Home database configuration to its default values.

`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 19 through Table 32. 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, zoning configuration, and Call Home configuration to the factory default values as described in Table 19 through Table 32. The switch configuration is activated automatically.

NOTE: Because this operand changes network parameters, the workstation could lose communication with the switch and release the Admin session.

This operand does not affect installed license keys.

`ipsec`
Resets the IP security database and IKE database, removing all associations, policies, and peers.

`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.

`radius`
Resets the RADIUS configuration to the default values as described in Table 24.

`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 25.

`snmp`
Resets the SNMP configuration settings to the factory default values. See Table 23 for SNMP configuration default values.

`switch`

Resets the switch without a power-on self test (POST). 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" (page 231).

To reset the switch with a power-on self test, see the "hardreset" (page 165). To reset the switch without disrupting traffic, see the "hotreset" (page 168).

NOTE: The following files are deleted from the switch during a switch reset:

- Firmware image files that have not been unpacked
- Configuration backup files
- Support files

`system`

Resets the following system configuration settings to the factory default values:

- DNS host (Table 26)
- IPv4 Ethernet (Table 27)
- IPv6 Ethernet (Table 28)
- Event logging (Table 29)
- NTP (Table 30)
- Timers (Table 31)

NOTE: Because this operand changes network parameters, the workstation could lose communication with the switch. This operand does not affect installed license keys.

`zoning`

Clears the zoning database and deactivates the active zone set. The zoning configuration parameters (`MergeAutoSave`, `DefaultZone`, `DiscardInactive`) remain unchanged. See Table 22 for information about the zoning configuration parameters.

Notes The following tables specify the various factory default settings:

- Enter the `show setup callhome` command to display the Call Home database configuration. The default values are shown in Table 18.
- Enter the `show config switch` command to display the switch configuration. The default values are shown in Table 19.
- Enter the `show config port` command to display the port configuration. The default values are shown in Table 20.
- Enter `show config threshold` command to display the port threshold alarm configuration. The default values are shown in Table 21.
- Enter the `show config zoning` command to display the zoning configuration. The default values are shown in Table 22.
- Enter the `show setup snmp` command to display the SNMP configuration. The default values are shown in Table 23.
- Enter the `show setup radius` command to display the RADIUS configuration. The default values are shown in Table 24.
- Enter the `show setup services` command to display the switch service configuration. The default values are shown in Table 25.
- Enter the `show setup system dns` command to display the DNS host configuration. The default values are shown in Table 26.
- Enter the `show setup system ipv4` command to display the IPv4 Ethernet configuration. The default values are shown in Table 27.
- Enter the `show setup system ipv6` command to display the IPv6 Ethernet configuration. The default values are shown in Table 28.
- Enter the `show setup system logging` command to display the event logging configuration. The default values are shown in Table 29.
- Enter the `show setup system ntp` command to display the NTP configuration. The default values are shown in Table 30.
- Enter the `show setup system timers` command to display the timer configuration. The default values are shown in Table 31.
- Enter the `show config security` command to display security configuration. The default values are shown in Table 32.

Table 18 Call Home service configuration defaults

Parameter	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

Table 19 Switch configuration defaults

Parameter	Default
AdminState	Online
Broadcast Enabled	True
InbandEnabled	True
FDMIEnabled	True
FDMIEntries	1,000
DefaultDomainID	1 (0x Hex)
DomainIDLock	False
SymbolicName	8/20q FC Switch
R_A_TOV	10000
E_D_TOV	2000
PrincipalPriority	254
ConfigDescription	Config Default

Table 20 Port configuration defaults

Parameter	Port Defaults
AdminState	Online
LinkSpeed	Auto
PortType	GL
SymbolicName	Port *n*, where *n* is the port number
ALFairness	False
DeviceScanEnabled	True
ForceOfflineRSCN	False
ARB_FF	False
InteropCredit	0
ExtCredit	0
FANEnable	True
AutoPerfTuning	True
LCFEnable	False
MFSEnable	False
MSEnable	True
NoClose	False
IOStreamGuard	Auto
VIEnable	False
PDISCPingEnable	True

Table 21 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

Table 22 Zoning configuration defaults

Parameter	Default
MergeAutoSave	True
DefaultZone	Allow
DiscardInactive	False

Table 23 SNMP configuration defaults

Parameter	Default
SNMPEnabled	True
Contact	<syscontact undefined>
Location	<sysLocation undefined>

Table 23 SNMP configuration defaults (continued)

Parameter	Default
Description	HP 8/20q FC Switch
ObjectID	1.3.6.1.4.1.3873.1.11
AuthFailureTrap	False
ProxyEnabled	True
SNMPv3Enabled	False
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

Table 24 RADIUS configuration defaults

Parameter	Default
DeviceAuthOrder	Local
UserAuthOrder	Local
TotalServers	0
DeviceAuthServer	False
UserAuthServer	False
AccountingServer	False
ServerIPAddress	10.0.0.1
ServerUDPPort	1812
Timeout	2 seconds
Retries	0
SignPackets	False

Table 25 Switch services configuration defaults

Parameter	Default
TelnetEnabled	True
SSHEnabled	False
GUIMgmtEnabled	True
SSLMgmtEnabled	False
EmbeddedGUIEnabled	True
SNMPEnabled	True
NTPEnabled	False
CIMEnabled	True
FTPEnabled	True

Table 25 Switch services configuration defaults

Parameter	Default
MgmtServerEnabled	True
CallHomeEnabled	True

Table 26 DNS host name configuration defaults

Parameter	Default
DNSClientEnabled	False
DNSLocalHostname	<undefined>
DNSServerDiscovery	Static
DNSServer1Address	<undefined>
DNSServer2Address	<undefined>
DNSServer3Address	<undefined>
DNSSearchListDiscovery	Static
DNSSearchList1	<undefined>
DNSSearchList2	<undefined>
DNSSearchList3	<undefined>
DNSSearchList4	<undefined>
DNSSearchList5	<undefined>

Table 27 IPv4 Ethernet configuration defaults

Parameter	Default
EthIPv4NetworkEnable	True
EthIPv4NetworkDiscovery	Static
EthIPv4NetworkIPAddress	10.0.0.1
EthIPv4NetworkIPMask	255.0.0.0
EthIPv4GatewayAddress	10.0.0.254

Table 28 IPv6 Ethernet configuration defaults

Parameter	Default
EthIPv6NetworkEnable	True
EthIPv6NetworkDiscovery	Static
EthIPv6NetworkAddress	<undefined>
EthIPv6GatewayAddress	<undefined>

Table 29 Event logging configuration defaults

Parameter	Default
LocalLogEnabled	True

Table 29 Event logging configuration defaults (continued)

Parameter	Default
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254

Table 30 NTP server configuration defaults

Parameter	Default
NTPClientEnabled	False
NTPServerAddress	10.0.0.254
EmbeddedGUIEnabled	True

Table 31 Timer configuration defaults

Parameter	Default
AdminTimeout	30
InactivityTimeout	0

Table 32 Security configuration defaults

Parameter	Default
AutoSave	True
FabricBindingEnabled	False
PortBindingEnabled	False

See also hardreset, page 165

security

Description Opens a Security Edit session in which to manage the security database on a switch.

Authority Admin session. The operands `active`, `history`, `limits`, and `list` are available without an Admin session.

Syntax

```
security
    active
    cancel
    clear
    edit
    history
    limits
    list
    restore
    save
```

Operands

`active`
Displays the active security set, its groups, and group members. This operand does not require an Admin session.

`cancel`
Closes a Security Edit session without saving changes. To open a Security Edit session, use the `edit` operand.

`clear`
Clears all inactive security sets from the volatile edit copy of the security database. This operand 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.

NOTE: 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 operand 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 operand does not require an Admin session.

`list`
Displays all security sets, groups, and group members in the security database. This operand 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 operand to revert changes to the volatile security database that were propagated from another switch in the fabric through security set activation or merging fabrics. See Table 32 for information about the `AutoSave` parameter.

`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.

Examples The following is an example of the `security active` command:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> 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
```

See also group, page 159

securityset, page 217

securityset

Description 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 . The `active`, `groups`, and `list` operands are available without an Admin session. You must close the Security Edit session before using the `activate` and `deactivate` operands.

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]
```

Operands

`activate [security_set]`
Activates the security set given by [security_set] and deactivates the currently active security set. Close the Security Edit session using the `security save` or `security cancel` command before using this operand.

`active`
Displays the name of the active security set. This operand is available 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, but 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 alphanumeric, _, $, ^, and -. The security database supports a maximum of four security sets.

`deactivate`
Deactivates the active security set. Close the Security Edit session before using this operand.

`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 operand is available without an Admin session.

`list`
Displays a list of all security sets. This operand 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].

Examples The following is an example of the `securityset active` command

```
8/20q FC Switch #> 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

```
8/20q FC Switch #> securityset groups alpha
  Current list of Groups for SecuritySet: alpha
  -------------------------------------
  group1 (ISL)
  group2 (Port)
```

The following is an example of the `securityset list` command

```
8/20q FC Switch #> securityset list
Current list of SecuritySets
----------------------------
  alpha
  beta
```

See also group, page 159

security, page 214

set alarm

Description Controls the display of alarms in the session output stream or clears the alarm log.

Authority Admin session for the `clear` operand. Otherwise, none.

Syntax `set alarm [option]`

Operands `[option]`

Table 33 describes the output stream alarm parameters.

Table 33 Output stream alarm parameters

Parameter	Description
`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:

```
8/20q FC Switch #> set alarm on
```

set beacon

Description Enables or disables the flashing of the Logged-In LEDs for the purpose of locating a switch.

Authority None

Syntax `set beacon [state]`

Operands `[state]`

Table 34 describes the beacon state parameters.

Table 34 Beacon state parameters

Parameter	Description
`on`	Enables the flashing beacon.
`off`	Disables the flashing beacon.

Examples The following is an example of the `set beacon` command:

```
8/20q FC Switch #> set beacon on
```

set config port

Description 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 [port_number]
```

Operands

`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 **Enter** 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 35 describes the port configuration parameters.

`ports [port_number]`

Initiates an editing session in which to change configuration parameters for all ports based on the configuration for the port given by [port_number]. If you omit [port_number], port 0 is used. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets. Enter `q` to end the configuration. Table 35 describes the port configuration parameters.

Table 35 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: 2 Gb/s, 4 Gb/s, 8 Gb/s, or Auto. The default is Auto. 8-Gb/s SFPs do not support the 1-Gb/s setting. Settting a port to 1 Gb/s that has an 8-Gb/s SFP will down the port.
`PortType`	GL, G, F, FL, TR, Donor. The default is GL.
`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.
`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 Registered State Change Notification (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.

Table 35 Port configuration parameters (continued)

Parameter	Description
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.
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.
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	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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
8/20q FC Switch (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]
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, 8=8Gb/s, A=Auto)       [Auto  ]
  PortType         (GL, G, F, FL, TR )                                [GL    ]
  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     ]
  FANEnable        (True / False)                                     [True  ]
  AutoPerfTuning   (True / False)                                     [True  ]
  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.
```

See also config, page 147

show config port, page 261

set config security

Description 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 **Enter** to accept the current value shown in brackets. Enter `q` or `Q` to end the editing session. Table 36 describes the security configuration parameters.

Table 36 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. The default is `False`.

Examples The following is an example of the `set config security` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
8/20q FC Switch (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.
```

See also config, page 147

show config security, page 262

set config security portbinding

Description Configures port binding.

Authority Admin session and a Config Edit session

Syntax `set config security portbinding [port_number]`

Operands `[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 **Enter** to accept the current value shown in brackets. Enter `q` or `Q` to end the editing session. Table 37 describes the `set config security portbinding` parameters.

Table 37 Port binding configuration parameters

Parameter	Description
`PortBindingEnabled`	Enables (`True`) or disables (`False`) port binding for the port given by [port_number]. The default is `False`.
`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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) config edit
8/20q FC Switch (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.
```

See also show config security portbinding, page 263

set config switch

Description 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 **Enter** to accept the current value shown in brackets. Table 38 describes the switch configuration parameters.

Table 38 Switch configuration parameters

Parameter	Description
`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. • `Down`—Disables the ports by removing power from the port lasers.
`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 (FDMI). 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 0–1,000. 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 `8/20q FC Switch`.
`R_A_TOV`	Resource Allocation Timeout Value. The number of milliseconds the switch waits to allow two ports to allocate enough resources to establish a link. The default is `10000`.
`E_D_TOV`	Error Detect Timeout Value. The number of milliseconds a port is to wait for errors to clear. The default is `2000`.
`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 `Config Default`.

Examples The following is an example of the `set config switch` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
8/20q FC Switch (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.

  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)                [8/20q FC Switch]
  R_A_TOV             (decimal value, 100-100000 msec)       [10000         ]
  E_D_TOV             (decimal value, 10-20000 msec)         [2000          ]
  PrincipalPriority   (decimal value, 1-255)                 [254           ]
  ConfigDescription   (string, max=64 chars)                 [Default Config]
```

See also config, page 147

show config switch, page 264

set config threshold

Description 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 a sampling window one line at a time and prompts you for a value. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets. Table 39 describes the port alarm threshold parameters.

Table 39 Port alarm threshold parameters

Parameter	Description
`ThresholdMonitoringEnabled`	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

`RisingTrigger`	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.
`FallingTrigger`	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.
`SampleWindow`	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:

```
8/20q FC Switch #> admin start
8/20q FC Switch  (admin) #> config edit
8/20q FC Switch (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.
```

See also show config threshold, page 265

set config zoning

Description 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 **Enter** to accept the current value shown in brackets. Table 40 describes the zoning configuration parameters.

Table 40 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 for preventing 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.

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> config edit
   The config named default is being edited.
8/20q FC Switch (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.
```

See also config, page 147

show config zoning, page 266

set log

Description 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` operands. You determine what events are automatically displayed on the screen using the `display` operand. 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
```

Operands

`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. Table 41 describes the component event monitoring filter parameters.

Table 41 Component event monitoring filter parameters

Parameter	Description
`All`	Monitors all components. To maintain optimal switch performance, do not use this setting with the `level` operand 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
`Qfs`	Monitors Call Home service 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]. Table 42 describes the event display filter parameters.

Table 42 Event display filter parameters

Parameter	Description
`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. Table 43 describes the severity level monitoring parameters.

Table 43 Severity level monitoring parameters

Parameter	Description
`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. **NOTE:** 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. Table 44 describes the port monitoring parameters.

Table 44 Port monitoring parameters

Parameter	Description
[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` operands 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.

See also show log, page 273

set pagebreak

Description 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]`

Operands `[state]`

Table 45 describes the pagebreak state parameters.

Table 45 Pagebreak state parameters

Parameter	Description
`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:

```
8/20q FC Switch #> set pagebreak on
8/20q FC Switch #> zone list

  Zone         ZoneSet
  ----         -------
  Zone1
               alpha
               beta

  Zone2
               delta
               echo

  Zone3
               sierra
               tango

  Zone4
               gamma
               delta

          Press any key to continue, 'q' to quit ...
```

See also show pagebreak, page 282

set port

Description 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.

Authority Admin session

Syntax

```
set port clear
```

or

```
set port [port_number]
    clear
    speed [transmission_speed]
    state [state]
```

Operands

`[port_number]`
Specifies the port. Ports are numbered beginning with 0.

`clear`
Clears the counters on all ports or the port given by [port_number].

`speed [transmission_speed]`
Specifies the port transmission speed. Table 46 describes the transmission speed parameters.

Table 46 Transmission speed parameters

Parameter	Description
`2Gb/s`	The port speed is 2 Gb/s.
`4Gb/s`	The port speed is 4 Gb/s.
`8Gb/s`	The port speed is 8 Gb/s.
`Auto`	The port speed is automatically detected.

`state [state]`
Specifies the port administrative state. Table 47 describes the port administrative state parameters.

Table 47 Port administrative state parameters

Parameter	Description
`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

Notes QuickTools and Enterprise Fabric Management Suite override any temporary administrative state changes that have been made using the Set Port State command. Therefore, to avoid unexpected results, do not manage port administrative states with QuickTools or Enterprise Fabric Management Suite and the CLI at the same time.

See also show port, page 285

set setup callhome

Description 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 48 describes the Call Home configuration attributes.

Table 48 Call Home service configuration attributes

Parameter	Description
`PrimarySMTPServerAddr`	IP address (version 4 or 6) 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 (version 4 or 6) 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 outgoing e-mail message. The format is `account@domain`. This parameter overrides the `FromEmailAddress` parameter.
`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. The default is `True`.

Notes

- The Callhome service must be active to support Call Home e-mail notification. See the `set setup services` command.
- 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.
- Callhome 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.

Examples The following is an example of the `set setup callhome` command:

```
8/20q FC Switch (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      (hostname, IPv4, or IPv6 Address):
  PrimarySMTPServerPort      (decimal value)                  :
  PrimarySMTPServerEnable    (True / False)                   :
  SecondarySMTPServerAddr    (hostname, IPv4, or IPv6 Address):
  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):
```

See also callhome, page 137

profile, page 201

set setup services, page 241

set setup radius

Description Configures RADIUS servers on the switch.

Authority Admin session

Syntax
```
set setup radius
    common
    server [server_number]
```

Operands `common`

Prompts you in a line-by-line fashion to configure attributes that are common to all RADIUS servers. To configure common and server-specific attributes, omit the operand. Table 49 describes the common RADIUS server configuration attributes.

Table 49 Common RADIUS server configuration attributes

Attribute	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. • `RadiusLocal`: Authenticate devices using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
`UserAuthOrder`	Authenticator priority for user accounts: • `Local`: Authenticate users using only the local security database. This is the default. • `Radius`: Authenticate users using only the security database on the RADIUS server. • `RadiusLocal`: Authenticate users using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
`TotalServers`	Number of RADIUS servers to configure during this session. Setting TotalServers to `0` disables all RADIUS authentication. The default is `0`.

Operands `server [server_number]`

Prompts you in a line-by-line fashion to configure attributes for the RADIUS server given by [server_number]. [server_number] is a positive integer. To configure common and specific RADIUS server parameters, omit the operand. Table 50 describes the server-specific RADIUS server configuration attributes.

Table 50 Server-specific RADIUS server configuration attributes

Attribute	Description
`ServerIPAddress`	IP address (version 4 or 6) or DNS host name 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`.

Table 50 Server-specific RADIUS server configuration attributes

Attribute	Description
`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`.
`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 (the default is `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`	22-byte ASCII string (1–63 characters) used as a password for authentication purposes between the switch and the RADIUS server.

Examples The following is an example of the `set setup radius common` command:

```
8/20q FC Switch (admin) #> set setup radius 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 attributes
  for the server 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.

  PLEASE NOTE:
  -----------
  * SSL must be enabled in order to configure RADIUS User Authentication
    SSL can be enabled using the 'set setup services' command.

  Current Values:
    DeviceAuthOrder  Local
    UserAuthOrder    Local
    TotalServers     1

  New Value (press ENTER to not specify value, 'q' to quit):
    DeviceAuthOrder  1=Local, 2=Radius, 3=RadiusLocal :
    UserAuthOrder    1=Local, 2=Radius, 3=RadiusLocal :
    TotalServers     decimal value, 0-5               :

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

The following is an example of the `set setup radius server` command:

```
8/20q FC Switch (admin) #> set setup radius server 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 attributes
  for the server 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.

  PLEASE NOTE:
  -----------
  * SSL must be enabled in order to configure RADIUS User Authentication
    SSL can be enabled using the 'set setup services' command.

Server 1 Current Values:
  ServerIPAddress    10.20.11.8
  ServerUDPPort      1812
  DeviceAuthServer   True
  UserAuthServer     True
  AccountingServer   False
  Timeout            10
  Retries            0
  SignPackets        False
  Secret             **********

New Server 1 Value (press ENTER to accept current value, 'q' to skip):
  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+)      :

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

See also show setup radius, page 293

set setup services

Description Configures services on the switch.

Authority Admin session

Syntax `set setup services`

This command prompts you in a line-by-line fashion to enable or disable switch services. Table 51 describes the switch service parameters. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets.

IMPORTANT: Be mindful when disabling `TelnetEnabled` and `GUIMgmtEnabled`; it is possible to disable all Ethernet access to the switch.

Table 51 Switch services settings

Parameter	Description
`TelnetEnabled`	Enables (`True`) or disables (`False`) the ability to manage the switch over a Telnet connection. Disabling this service is not recommended. The default is `True`.
`SSHEnabled`	Enables (`True`) or disables (`False`) Secure Shell (SSH) 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 `False`.
`GUIMgmtEnabled`	Enables (`True`) or disables (`False`) out-of-band management of the switch with SAN Connection Manager, Enterprise Fabric Management Suite, SNMP, and SMI-S. If this service is disabled, the switch can only be managed inband or through the serial port. The default is `True`.
`SSLEnabled`	Enables (`True`) or disables (`False`) secure SSL connections for management applications including SAN Connection Manager, QuickTools, Enterprise Fabric Management Suite, and SMI-S. The default is `False`. • SAN Connection Manager version 1.0 does not support the SSL service. If SSL is enabled, you will be unable to manage the switch using this version of SAN Connection Manager. • This service must be enabled to authenticate users through a RADIUS server. • Enabling SSL automatically creates a security certificate on the switch. • To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation. • To disable SSL when using a user authentication RADIUS server, the RADIUS server authentication order must be local.
`EmbeddedGUIEnabled`	Enables (`True`) or disables (`False`) the QuickTools embedded switch management application. QuickTools enables you to point at a switch with an internet browser and manage the switch. This parameter is the master control for the `set setup system` command parameter, `EmbeddedGUIEnabled`. The default is `True`.

Table 51 Switch services settings (continued)

Parameter	Description
SNMPEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). This parameter is the master control for the set setup snmp command parameter, SNMPEnabled. 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. The default is True.
FTPEnabled	Enables (True) or disables (False) FTP for transferring files rapidly between the workstation and the switch. The default is True.
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. **NOTE:** The 8/20q Fibre Channel Switch Call Home service provides an e-mail notification capability for the switch. This service has no relationship with the HP Call Home feature, which notifies HP services.

Examples The following is an example of the `set setup services` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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.

  TelnetEnabled       (True / False)   [True ]
  SSHEnabled          (True / False)   [False]
  GUIMgmtEnabled      (True / False)   [True ]
  SSLEnabled          (True / False)   [False]
  EmbeddedGUIEnabled  (True / False)   [True ]
  SNMPEnabled         (True / False)   [True ]
  NTPEnabled          (True / False)   [False]
  CIMEnabled          (True / False)   [False]
  FTPEnabled          (True / False)   [True ]
  MgmtServerEnabled   (True / False)   [True ]
  CallHomeEnabled     (True / False)   [True ]

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

See also show setup services, page 294

set setup snmp

Description Configures SNMP on the switch.

Authority Admin session

Syntax
```
set setup snmp
    common
    trap [trap_number]
```

Operands `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 common operand. Table 52 describes the common SNMP configuration parameters.

Table 52 Common SNMP configuration parameters

Parameter	Description
`SNMPEnabled`	Enables (`True`) or disables (`False`) SNMP on the switch. The default is `True`.
`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`.
`TrapCommunity`	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`.
`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`.
`SNMPv3Enabled`	Enables (`True`) or disables (`False`) SNMP version 3. The default is `False`.

Operands `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 `trap` operand. Table 53 describes the trap parameters.

Table 53 SNMP trap configuration parameters

Parameter	Description
`Trap [1-5] Address`	Specifies the workstation IP address 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 [1-5] Port`	Specifies the workstation port to which SNMP traps are sent. Valid workstation port numbers are 1–65535. The default is `162`.
`Trap [1-5] Severity`	Specifies the severity level to use when monitoring trap events. The default is `Warning`.
`Trap [1-5] Version`	Specifies the SNMP version (`1` or `2`) to use in formatting traps. The default is `2`.
`Trap [1-5] Enabled`	Specifies whether traps (event information) are enabled (`True`) or disabled (`False`). The default is `False`.

Examples The following is an example of the `set setup snmp common` command:

```
8/20q FC Switch (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:
    SnmpEnabled      True
    Contact          <sysContact undefined>
    Location         <sysLocation undefined>
    ReadCommunity    public
    WriteCommunity   private
    AuthFailureTrap  False
    ProxyEnabled     True
    SNMPv3Enabled    False

  New Value (press ENTER to not specify value, 'q' to quit):
    SnmpEnabled      (True / False)         :
    Contact          (string, max=64 chars) :
    Location         (string, max=64 chars) :
    ReadCommunity    (string, max=32 chars) :
    WriteCommunity   (string, max=32 chars) :
    AuthFailureTrap  (True / False)         :
    ProxyEnabled     (True / False)         :
    SNMPv3Enabled    (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:

```
8/20q FC Switch (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
    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)                           :
    Trap1Community  (string, max=32 chars)            :

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

See also show setup snmp, page 295

set setup system

Description 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
```

Operands `dns`

Prompts you in a line-by-line fashion to change DNS host name configuration parameters described in Table 54. To configure all system parameters, omit the operand. For each parameter, enter a new value or press **Enter** to accept the current value.

Table 54 DNS host name configuration parameters

Parameter	Description
`DNSClientEnabled`	Enables (`True`) or disables (`False`) the DNS client. The default is `False`.
`DNSLocalHostname`	Name of local DNS server
`DNSServerDiscovery`	DNS server boot method: • 1—Static • 2—DHCP (Dynamic Host Configuration Protocol) • 3—DHCP version 6 The default is `Static`.

`DNSServer1Address`
`DNSServer2Address`
`DNSServer3Address`
	IP addresses (version 4 or 6) of up to three DNS servers.

`DNSSearchListDiscovery`	DNS search list discovery method: • Static • DHCP for IPv4 • DHCP for IPv6 The default is `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 55. To configure all system parameters, omit the operand. For each parameter, enter a new value or press **Enter** to accept the current value.

NOTE: Changing the IP address will terminate all Ethernet management sessions.

Table 55 IPv4 Ethernet configuration parameters

Parameter	Description
`EthIPv4NetworkEnable`	Enables (`True`) or disables (`False`) the IPv4 interface. The default is `True`.
`EthIPv4NetworkDiscovery`	Ethernet boot method: • `1`—Static • `2`—Bootp (Bootstrap Protocol) • `3`—DHCP (Dynamic Host Configuration Protocol) • `4`—RARP (Reverse Address Resolution Protocol) The default is `1-Static`.
`EthIPv4NetworkAddress`	Ethernet IP address. The default is `10.0.0.1`.
`EthIPv4NetworkMask`	Ethernet subnet mask address. The default is `255.0.0.0`.
`EthIPv4GatewayAddress`	Ethernet IP address gateway. The default is `10.0.0.254`

Operands `ipv6`

Prompts you in a line-by-line fashion to change the switch IPv6 Ethernet configuration parameters described in Table 56. To configure all system parameters, omit the operand. For each parameter, enter a new value or press **Enter** to accept the current value.

NOTE: Changing the IP address will terminate all Ethernet management sessions.

Table 56 IPv6 Ethernet configuration parameters

Parameter	Description
`EthIPv6NetworkEnable`	Enables (`True`) or disables (`False`) the IPv6 interface. The default is `True`.
`EthIPv6NetworkDiscovery`	Ethernet boot method: • 1—Static • 2—DHCPv6 (Dynamic Host Configuration Protocol) • 3—NDP (Neighbor Discovery Protocol) The default is `Static`.
`EthIPv6NetworkAddress`	Ethernet IP address
`EthIPv6GatewayAddress`	Ethernet IP address gateway.

Operands `logging`

Prompts you in a line-by-line fashion to change the event logging configuration parameters described in Table 57. To configure all system parameters, omit the operand. For each parameter, enter a new value or press **Enter** to accept the current value.

Table 57 Event logging configuration parameters

Parameter	Description
`LocalLogEnabled`	Enables (`True`) or disables (`False`) the saving of log information on the switch. The default is `True`.
`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 (version 4 or 6) 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`.

Operands `ntp`

Prompts you in a line-by-line fashion to change the NTP server configuration parameters described in Table 58. To configure all system parameters, omit the operand. For each parameter, enter a new value or press **Enter** to accept the current value.

Table 58 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`	NTP boot method: • 1—Static • 3—DHCP (Dynamic Host Configuration Protocol) • 3—DHCP version 6 The default is `Static`.
`NTPServerAddress`	The IP address (version 4 or 6) 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`.

Operands `timers`

Prompts you in a line-by-line fashion to change the timer configuration parameters described in Table 59. To configure all system parameters, omit the operand. For each parameter, enter a new value or press **Enter** to accept the current value.

Table 59 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 Telnet command line interface session. Zero (0) disables the time out threshold. The default is 0, the maximum is 1440.

Examples The following is an example of the `set setup system dns` command:

```
8/20q FC Switch (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:

```
8/20q FC Switch (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)             :
    EthIPv4NetworkMask      (dot-notated IP Address)             :
    EthIPv4GatewayAddress   (dot-notated IPv4 Address)           :

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

The following is an example of the `set setup system ipv6` command:

```
8/20q FC Switch (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:

```
8/20q FC Switch (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:
    LocalLogEnabled         True
    RemoteLogEnabled        False
    RemoteLogHostAddress    10.0.0.254

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    LocalLogEnabled         (True / False)                    :
    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:

```
8/20q FC Switch (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

  New Value (press ENTER to accept current value, 'q' to quit, 'n' for none):
    NTPClientEnabled        (True / False)                    :
    NTPServerDiscovery      (1=Static, 2=Dhcp, 3=Dhcpv6)      :
    NTPServerAddress        (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 timers` command:

```
8/20q FC Switch (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]
```

See also show setup system, page 296

set switch state

Description Changes the administrative state for all ports on the switch. The previous `set config switch` command settings are restored after a switch reset or a reactivation of a switch configuration.

Authority Admin session

Syntax `set switch state [state]`

Operands `[state]`

Table 60 describes the switch administrative state parameters.

Table 60 Switch administrative state parameters

Parameter	Description
`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.

Notes QuickTools and Enterprise Fabric Management Suite will override any temporary administrative state changes that have been made using the Set Switch State command. Therefore, to avoid unexpected results, do not manage switch administrative states with QuickTools or Enterprise Fabric Management Suite and the CLI at the same time.

Examples The following is an example of the `set switch` command:

```
8/20q FC Switch #>admin start
8/20q FC Switch (admin) #>set switch state offline
```

See also show switch, page 299

set timezone

Description Specifies the time zone for the switch and the workstation. The default is Universal Time (UTC), also known as Greenwich Mean Time (GMT). This command prompts you to choose a region, then a subregion to specify the time zone. Changing the time zone converts the time to the time in the new time zone.

Authority Admin session

Syntax `set timezone`

Examples The following is an example of the `set timezone` command:

```
8/20q FC Switch (admin) #> set timezone
  Africa                                America
  Antarctica                            Asia
  Atlantic                              Australia
  Europe                                Indian
  Pacific                               UTC
        Press ENTER for more options or 'q' to make a selection.

  America/Grenada                       America/Guadeloupe
  America/Guatemala                     America/Guayaquil
  America/Guyana                        America/Halifax
  America/Havana                        America/Hermosillo
  America/Indiana                       America/Indianapolis
  .
  .
  .
  America/Monterrey                     America/Montevideo
  America/Montreal                      America/Montserrat
  America/Nassau                        America/New_York
  America/Nipigon                       America/Nome
  America/Noronha                       America/North_Dakota
  America/Panama                        America/Pangnirtung

        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
```

See also date, page 152

show timezone, page 304

show about

Description Displays introductory information about the operational attributes of the switch. This command is equivalent to the `show version` command.

Authority None

Syntax `show about`

Table 61 describes the information returned by the `show about` command.

Table 61 Show about display entries

Attribute	Description
`SystemDescription`	Description of the switch system
`HostName`	DNS host name
`EthIPv4NetworkAddress`	IP address, IPv4
`EthIPv6NetworkAddress`	IP address, IPv6
`MacAddress`	Media Access Control (MAC) address of the switch
`WorldWideName`	Worldwide name of the switch
`ChassisSerialNumber`	Serial number of the switch
`SymbolicName`	Symbolic name of the switch
`ActiveSWVersion`	Firmware version
`ActiveTimestamp`	Date and time that the firmware was activated
`POSTStatus`	Results of the power-on self test
`LicensedPorts`	Number of licensed ports
`SwitchMode`	`Full Fabric` indicates that the switch operates with the standard Fibre Channel port types: G, GL, F, FL, E, TR

Examples The following is an example of the `show about` command:

```
8/20q FC Switch #> show about
       ************************************************
       *                                              *
       *       Command Line Interface SHell  (CLISH)  *
       *                                              *
       ************************************************

       SystemDescription         HP 8/20q Fibre Channel Switch
       HostName                  <undefined>
       EthIPv4NetworkAddress     10.20.11.192
       EthIPv6NetworkAddress     ::
       MACAddress                00:c0:dd:00:71:ee
       WorldWideName             10:00:00:c0:dd:00:71:ed
       SerialNumber              FAM033100024
       SymbolicName              8/20q FC Switch
       ActiveSWVersion           V8.0.4.xx.xx
       ActiveTimestamp           day month date time year
       POSTStatus                Passed
       LicensedPorts             20
       SwitchMode                Full Fabric
```

See also show version, page 307

show alarm

Description Displays the alarm log and session output stream display setting.

Authority None

Syntax `show alarm`
`settings`

Operands *`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` command:

```
8/20q FC Switch #> show alarm
  [1][Fri Jan 19 13:50:26.508 UTC 2007][A][1004.000F][Port: 4][Eport
Isolating
due to Merge Zone Failure]
  [2][Fri Jan 19 13:50:26.513 UTC 2007][A][1004.0030][Topology change, lost
route to switch with domain ID 1]
  [3][Sun Jan 21 07:59:28.677 UTC 2007][A][1004.0030][Topology change, lost
route to switch with domain ID 99]
  [4][Sun Jan 21 07:59:29.367 UTC 2007][A][1004.0030][Topology change, lost
route to switch with domain ID 101]
```

The following is an example of the `show alarm settings` command:

```
8/20q FC Switch #> show alarm settings

  Current settings for alarm
  --------------------------
  display  ON
```

show broadcast

Description 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:

```
8/20q FC Switch #> show broadcast

  Group Member Ports ISL Ports
  ----- ------------ ---------
  0     3            16
        15
        16
```

show chassis

Description Displays chassis component status and temperature.

Authority None

Syntax `show chassis`

Examples The following is an example of the `show chassis` command.

```
8/20q FC Switch #> show chassis
   Chassis Information
  -------------------
  BoardTemp (1) - Degrees Celsius   26
  BoardTemp (2) - Degrees Celsius   31
  BoardTemp (3) - Degrees Celsius   31
  PowerSupplyStatus (1)             Good
  HeartBeatCode                     1
  HeartBeatStatus                   Normal
```

show config port

Description Displays configuration parameters for one or more ports.

Authority None

Syntax `show config port [port_number]`

Operands *[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 port 3:

```
8/20q FC Switch #> show config port 3

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

  Port Number: 3
  ------------
  AdminState          Offline
  LinkSpeed           Auto
  PortType            GL
  SymbolicName        Port3
  ALFairness          False
  DeviceScanEnabled   True
  ForceOfflineRSCN    False
  ARB_FF              False
  InteropCredit       0
  ExtCredit           0
  FANEnabled          True
  AutoPerfTuning      True
  MSEnabled           True
  NoClose             False
  IOStreamGuard       Auto
  PDISCPingEnable     True
```

See also set config port, page 221

show config security

Description Displays the security database configuration parameters.

Authority None

Syntax `show config security`

Examples The following is an example of the `show config security` command:

```
8/20q FC Switch #> show config security

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

  Switch Security Configuration Information
  -----------------------------------------
  FabricBindingEnabled  False
  AutoSave              True

  Port  Binding Status  WWN
  ----  --------------  ---
  0       True          10:20:30:40:50:60:70:80
  1       True          10:20:30:40:50:60:70:80
  2       False         No port binding entries found.
  3       True          10:20:30:40:50:60:70:80
  4       True          10:20:30:40:50:60:70:80
  5       False         No port binding entries found.
  6       True          10:20:30:40:50:60:70:81
  7       False         No port binding entries found.
  8       True          10:20:30:40:50:60:70:80
  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.
  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.
```

See also set config security, page 224

show config security portbinding

Description Displays the port binding configuration for one or more ports.

Authority None

Syntax `show config security portbinding [port_number]`

Operands *[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:

```
8/20q FC Switch #> show config security portbinding

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

  Port    Binding Status   WWN
  ----    --------------   -----------------------
  0       True             10:20:30:40:50:60:70:80
  1       True             10:20:30:40:50:60:70:80
  2       False            No port binding entries found.
  3       True             10:20:30:40:50:60:70:80
  4       True             10:20:30:40:50:60:70:80
  5       False            No port binding entries found.
  6       True             10:20:30:40:50:60:70:81
  7       False            No port binding entries found.
  8       True             10:20:30:40:50:60:70:80
  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.
  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.
```

See also set config security portbinding, page 225

show config switch

Description Displays the switch configuration parameters.

Authority None

Syntax `show config switch`

Examples The following is an example of the `show config switch` command:

```
8/20q FC Switch #> show config switch
 Configuration Name: default
 -------------------
  Switch Configuration Information
  --------------------------------
  AdminState            Online
  BroadcastEnabled      False
  InbandEnabled         True
  FDMIEnabled           False
  FDMIEntries           10
  DefaultDomainID       19 (0x13)
  DomainIDLock          True
  SymbolicName          8/20q FC Switch
  R_A_TOV               10000
  E_D_TOV               2000
  PrincipalPriority     254
  ConfigDescription     Default Config
  ConfigLastSavedBy     admin@OB-session5
  ConfigLastSavedOn     day month date time year
  InteropMode           Standard
```

See also set config switch, page 226

show config threshold

Description 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:

```
8/20q FC Switch #> 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
```

See also set config threshold, page 228

show config zoning

Description 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:

```
8/20q FC Switch #> show config zoning

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

  Zoning Configuration Information
  --------------------------------
  MergeAutoSave         True
  DefaultZone           Allow
  DiscardInactive       False
```

See also set config zoning, page 230

show domains

Description Displays list of each domain and its WWN in the fabric.

Authority None

Syntax `show domains`

Examples The following is an example of the `show domains` command:

```
8/20q FC Switch #> 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

Description 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:

```
8/20q FC Switch #> show donor

  Port    Config Ext Credit Max Credit Donated Member of   Valid Groups to
  Number  Type   Requested  Available  to Port Donor Group Extend Credit
  ------  ------ ---------- ---------- ------- ----------- ---------------
  0       GL     0          16         None    0           0
  1       GL     0          16         None    0           0
  2       GL     0          16         None    0           0
  3       GL     0          16         None    0           0
  4       GL     0          16         None    0           0
  5       GL     0          16         None    0           0
  6       GL     0          16         None    0           0
  7       GL     0          16         None    0           0
  8       GL     0          16         None    0           0
  9       GL     0          16         None    0           0
  10      GL     0          16         None    0           0
  11      GL     0          16         None    0           0
  12      GL     0          16         None    0           0
  13      GL     0          16         None    0           0
  14      GL     0          16         None    0           0
  15      GL     0          16         None    0           0
  16      G      0          16         None    0           0
  17      GL     0          16         None    0           0
  18      GL     0          16         None    0           0
  19      G      0          16         None    0           0
  Donor Group  Credit Pool
  -----------  -----------
  0            0
```

show env

Description Displays temperature and voltage information.

Authority None

Syntax `show env`

Examples The following is an example of the `show env` command:

```
8/20q FC Switch #? show env
Temperature(C) Sensors:

 Sensor  Description  Status  Current  High Warn  High Alarm
 ------  -----------  ------  -------  ---------  ----------
      0  BOARD        Normal       24         65          70
      1  DS1780       Normal       28        n/a         n/a
      2  MAX1617      Normal       31         65          70
      3  ASIC         Normal       49         95         100

 Voltage Sensors:

 Sensor  Description  Status  Current  Low Alarm  High Alarm
 ------  -----------  ------  -------  ---------  ----------
      0  2.5V         Good       2.50       2.20        2.80
      1  1.25V        Good       1.24       1.00        1.50
      2  3.3V         Good       3.32       3.02        3.58
      3  12V          Good      12.00      10.00       13.31
      4  1.2V         Good       1.26       1.04        1.38
      5  1.5V         Good       1.50       1.31        1.68
      6  1.8V_ANALOG  Good       1.78       1.58        2.02
      7  1.8V         Good       1.79       1.60        1.99
      8  2.5V_ANALOG  Good       2.40       2.08        2.84
```

See also show temp, page 302

show voltage, page 309

show fabric

Description Displays list of each domain, symbolic name, worldwide name, node IP address, and port IP address in the fabric.

Authority None

Syntax `show fabric` *`brief`*

Operands `brief`

Displays a table of switches in the fabric including domain ID, WWN, and symbolic name. If you omit the `brief` operand, the command displays information for the local switch only.

Examples The following is an example of the `show fabric` command:

```
8/20q FC Switch #> show fabric
  Domain           *133(0x85)
  WWN              10:00:00:c0:dd:0d:53:91
  SymbolicName     8/20q FC Switch
  HostName         <undefined>
  EthIPv4Address   10.20.116.133
  EthIPv6Address   <undefined>

  * indicates principal switch
```

The following is an example of the `show fabric brief` command:

```
8/20q FC Switch #> 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

Description Displays detailed information about the device host bus adapter.

Authority None

Syntax `show fdmi` *[port_wwn]*

Operands *[port_wwn]*

The device WWPN 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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> show fdmi 21:00:00:e0:8b:09:3b:17
  FDMI Information
  ----------------
  Manufacturer            QLogic Corporation
  SerialNumber            [04202
  Model                   QLA2342
  ModelDescription        QLogic QLA2342 PCI Fibre Channel Adapter
  PortID                  610000
  NodeWWN                 20:00:00:e0:8b:07:aa:bc
  HardwareVersion         FC5010409-10
  DriverVersion           8.2.3.10 Beta 2 (W2K VI)
  OptionRomVersion        1.21
  FirmwareVersion         03.02.13.
  OperatingSystem         SunOS 5.8
  MaximumCTPayload        2040
  NumberOfPorts           1

  Port  21:01:00:e0:8b:27:aa:bc

  SupportedFC4Types       FCP
  SupportedSpeed          2Gb/s
  CurrentSpeed            2Gb/s
  MaximumFrameSize        2048
  OSDeviceName
  HostName
```

show interface

Description Displays the status of the active network interfaces.

Authority None

Syntax `show interface`

Examples The following is an example of the `show interface` command:

```
8/20q FC Switch #> show interface
eth0      Link encap:Ethernet  HWaddr 00:C0:DD:00:00:27
          inet addr:10.20.116.131  Bcast:10.20.116.255  Mask:255.255.255.0
          inet6 addr: fd70:c154:c2df:116:2c0:ddff:fe00:27/64 Scope:Global
          inet6 addr: fe80::2c0:ddff:fe00:27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:137168 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2194 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:47764214 (45.5 Mb)  TX bytes:328639 (320.9 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3887 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3887 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:272461 (266.0 Kb)  TX bytes:272461 (266.0 Kb)
```

show log

Description Displays the contents of the log or the parameters used to create and display entries in the log. The log contains a maximum of 1,200 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
```

Operands

`[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 62 describes the log monitoring components.

Table 62 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
QFS	Call Home service 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].Table 63 describes the event log display filter parameters.

Table 63 Event log display filter parameters

Parameter	Description
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 severity level settings for event logging setting and the setting for the display level.

`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.

`port`
Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but is 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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> show log level
   Current settings for log
   ------------------------
   FilterLevel       Info
   DisplayLevel      Critical
```

The following is an example of the `show log options` command:

```
8/20q FC Switch #> show log options
  Allowed options for log
  -----------------------
   FilterComponent
All,None,NameServer,MgmtServer,Zoning,Switch,Blade,Port,Eport,Snmp,CLI,Qfs
   FilterLevel       Critical,Warn,Info,None
   DisplayLevel      Critical,Warn,Info,None
```

The following is an example of the `show log` command:

```
8/20q FC Switch #> show log
   [327][day month date time year][I][Eport Port:0/8][Eport State=
   E_A0_GET_DOMAIN_ID]
   [328][day month date time year][I][Eport Port: 0/8][FSPF PortUp state=0]
   [329][day month date time year][I][Eport Port: 0/8][Sending init hello]
   [330][day month date time year][I][Eport Port: 0/8][Processing EFP, oxid=
0x8]
   [331][day month date time year][I][Eport Port: 0/8][Eport State =
E_A2_IDLE]
   [332][day month date time year][I][Eport Port: 0/8][EFP,WWN=
0x100000c0dd00b845,
   len= 0x30]
   [333][day month date time year][I][Eport Port: 0/8][Sending LSU
oxid=0xc:type=1]
   [334][day month date time year][I][Eport Port: 0/8][Send Zone Merge
Request]
   [335][day month date time year][I][Eport Port: 0/8][LSDB Xchg timer set]
```

See also set log, page 231

show lsdb

Description Displays link state database information,

Authority None

Syntax `show lsdb`

Examples The following is an example of the `show lsdb` command:

```
8/20q FC Switch #> 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

Description Displays transceiver operational and diagnostic information for one or more ports.

Authority None

Syntax
```
show media
    [port_number]
    all
    installed
```

Operands

`[port_number]`
The port for which to display transceiver information. [port_number] can be 0–19.

`all`
Displays transceiver information for all ports.

`installed`
Displays transceiver information for all ports that have transceivers installed.

Notes Table 64 describes the transceiver information in the `show media` display.

Table 64 Transceiver information

Entry	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 one 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`	Vendor 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 laser 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.
`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:

```
8/20q FC Switch #> show media 4
Port Number: 4
-------------
MediaType           800-MX-SN-S
MediaVendor         FINISAR CORP.
MediaPartNumber     FLTF8528P2BNV
MediaRevision       A
MediaSerialNumber   P6G22RL
MediaSpeeds         2Gb/s, 4Gb/s, 8Gb/s

                       Temp      Voltage      Tx Bias      Tx Pwr      Rx Pwr
                        (C)          (V)          (mA)        (mW)        (mW)
                 ----------- ----------- ------------ ----------- -----------
       Value           37.32        3.33         7.30       0.373       0.000
       Status         Normal HighWarning       Normal      Normal    LowAlarm
       HighAlarm       95.00        3.90        17.00       0.637       1.264
       HighWarning     90.00        3.70        14.00       0.637       0.791
       LowWarning     -20.00        2.90         2.00       0.082       0.028
       LowAlarm       -25.00        2.70         1.00       0.073       0.019
```

show mem

Description Displays information about memory activity.

Authority None

Syntax `show mem [count]`

Operands *[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.

> **NOTE:** This operand 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:

```
8/20q FC Switch #> show mem

procs -----------memory---------- ---swap-- -----io---- --system-- ----cpu----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in    cs us sy id wa
 1  0      0 334464  55932  18728    0    0     1     0  401    57  1  2 97  0

Filesystem space in use: 41138/53188 KB (77%)
```

show ns

Description Displays the WWNs for devices in the fabric.

Authority None

Syntax `show ns [option]`

Operands *[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. Table 65 describes the name server display options.

Table 65 Name server display parameters

Parameter	Description
`all`	Displays WWNs for all switches and ports in the fabric
[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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch #> show ns 1301e1
  Port ID: 1301e1
  --------
  PortType          NL
  PortWWN           21:00:00:20:37:73:13:69
  SymbolicPortName  (NULL)
  NodeWWN           20:00:00:20:37:73:13:69
  SymbolicNodeName  (NULL)
  NodeIPAddress     diskarray7.anycompany.com
  ClassOfService    3
  PortIPAddress     ::
  FabricPortName    20:01:00:c0:dd:00:bc:56
  FC4Type           FCP
  FC4Desc           (NULL)
```

show pagebreak

Description Displays the current pagebreak setting.

Authority None

Syntax `show pagebreak`

Operands The pagebreak setting limits the display of information to 20 lines (`ON`) or allows the continuous display of information without a break (`OFF`).

Examples The following is an example of the `show pagebreak` command:

```
8/20q FC Switch #> show pagebreak

  current setting: ON
```

See also set pagebreak, page 234

show perf

Description Displays port performance in frames/second and bytes/second. If you omit the operand, the command displays data transmitted (`out`), data received (`in`), and total data transmitted and received in frames/second and bytes/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]
```

Operands

[port_list]
Displays the instantaneous performance data for up to sixteen 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. 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 up to sixteen 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. If you omit [port_list], the command displays performance data for ports 0–15. Type `q` and press **Enter** 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. For example, `0 2 10-15` specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type q and press **Enter** 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. For example, `0 2 10-15` specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type q and press **Enter** 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. For example, `0 2 10-15` specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type `q` and press **Enter** 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. For example, `0 2 10-15` specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type `q` and press **Enter** 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. For example, `0 2 10-15` specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type `q` and press **Enter** 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. For example, `0 2 10-15` specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type `q` and press **Enter** to stop the display.

Examples The following is an example of the `show perf` command:

```
8/20q FC Switch #> show perf
  Port    Bytes/s     Bytes/s     Bytes/s     Frames/s    Frames/s    Frames/s
  Number    (in)        (out)     (total)       (in)        (out)     (total)
  ------ -------     -------     -------     --------    --------    --------
  0       7K          136M        136M        245         68K         68K
  1       58K         0           58K         1K          0           1K
  2       0           0           0           0           0           0
  3       0           0           0           0           0           0
  4       0           0           0           0           0           0
  5       0           0           0           0           0           0
  6       0           7K          7K          0           245         245
  7       136M        58K         136M        68K         1K          70K
  8       7K          136M        136M        245         68K         68K
  9       58K         0           58K         1K          0           1K
  10      0           0           0           0           0           0
  11      0           0           0           0           0           0
  12      0           0           0           0           0           0
  13      0           0           0           0           0           0
  14      0           7K          7K          0           245         245
  15      136M        58K         136M        68K         1K          70K
  16      47M         23K         47M         23K         726         24K
  17      0           0           0           0           0           0
  18      23K         47M         47M         726         23K         24K
  19      0           0           0           0           0           0
```

The following is an example of the `show perf byte` command:

```
8/20q FC Switch #> show perf byte
Displaying bytes/sec (total)...  (Press any key to stop display)

  0    1    2    3    4    5    6    7    8    9    10   11   12   13   14   15

-------------------------------------------------------------------------------
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    8K   136M
  0    0    0    0    0    0    0    0    135M 58K  0    0    0    0    7K   135M
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    7K   136M
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    8K   136M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    7K   136M
```

show port

Description Displays operational information for one or more ports.

Authority None

Syntax `show port`

Table 66 describes the information returned by the `show port` command.

Table 66 Show port display entries

Parameter	Description
`AdminState`	Administrative state
`AIinit`	Number of times the port begins arbitrated loop initialization
`AIinitError`	Number of times the port entered initialization and the initialization failed
`AsicNumber`	Application-specific integrated circuit (ASIC) number
`AsicPort`	ASIC port number
`BadFrames`	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 Receiver_Ready (R_RDY) primitives 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
`ConfigType`	Configured port type: `G`, `GL`, `F`, `FL`, `TR`, or `Donor`
`DecodeError`	Number of decode errors detected
`POSTFaultCode`	Fault code from the most recent power-on self test
`POSTStatus`	Status from the most recent power-on self test
`DownstreamISL`	Downstream ISL state. `True` indicates a connection to another switch that is not the principal switch.
`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 fabric busy (F_BSY) frame because the Class 2 frame could not be delivered within ED_TOV time; or the number of class 2 and class 3 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.

Table 66 Show port display entries (continued)

Parameter	Description
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
LinkFailures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or a loss of signal while online. 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, Arbitrated Loop Source Address (AL_PS) Loop Initialization Primitives (LIPs), or Arbitrated Loop Destination Address (AL_PD) (vendor specific) resets performed
LIP_F7_AL_PS	Number of LIP frames that reinitialized 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	Number of LIP frames indicating a loop failure detected by the L_Port identified by AL_PS
LIP_F7_F7	Number of LIP frames that acquire a valid Arbitrated Loop Physical Address (AL_PA)
LIP_F8_F7	Number of LIP frames indicating that a loop failure has been detected at the receiver
Login	Number of device logins that have occurred on the port
LoginStatus	Device login status for the port: LoggedIn or NotLoggedIn
Logout	Number of device logouts that have occurred on the port
LongFramesIn	Number of incidents when one or more frames that are greater than the maximum size were received
LoopTimeouts	A two second timeout, as specified by FC-AL-2
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by the receipt of an invalid transmission word.
LostFrames	Number of incidents of lost frames
LostRRDYs	Number of incidents of lost Receiver_Ready (R_RDY) primitives
MaxCredit	Maximum number of port buffer credits
MediaSpeeds	Possible transmission speeds for the port
MediaPartNumber	Transceiver vendor part number
MediaRevision	Transceiver revision number

Table 66 Show port display entries (continued)

Parameter	Description
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
LinkFailures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or a loss of signal while online. 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, Arbitrated Loop Source Address (AL_PS) Loop Initialization Primitives (LIPs), or Arbitrated Loop Destination Address (AL_PD) (vendor specific) resets performed
LIP_F7_AL_PS	Number of LIP frames that reinitialized 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	Number of LIP frames indicating a loop failure detected by the L_Port identified by AL_PS
LIP_F7_F7	Number of LIP frames that acquire a valid Arbitrated Loop Physical Address (AL_PA)
LIP_F8_F7	Number of LIP frames indicating that a loop failure has been detected at the receiver
Login	Number of device logins that have occurred on the port
LoginStatus	Device login status for the port: LoggedIn or NotLoggedIn
Logout	Number of device logouts that have occurred on the port
LongFramesIn	Number of incidents when one or more frames that are greater than the maximum size were received
LoopTimeouts	A two second timeout, as specified by FC-AL-2
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by the receipt of an invalid transmission word.
LostFrames	Number of incidents of lost frames
LostRRDYs	Number of incidents of lost Receiver_Ready (R_RDY) primitives
MaxCredit	Maximum number of port buffer credits
MediaSpeeds	Possible transmission speeds for the port
MediaPartNumber	Transceiver vendor part number
MediaRevision	Transceiver revision number

Table 66 Show port display entries (continued)

Parameter	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.
MediaVendor	Transceiver manufacturer
MediaVendorID	Transceiver manufacturer identifier
OperationalState	Operational state
PerfTuningMode	AutoPerfTuning status
PortID	Fibre Channel port address
PortWWN	Worldwide port name
PrimSeqErrors	Number of primitive sequence errors detected
RunningType	Operational port type: F, FL, E, TR, or Unknown
RxLinkResets	Number of link reset primitives received from an attached device.
RxOfflineSeq	Number of offline sequences (OLSs) 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 that are less than the minimum size were received
SymbolicName	Symbolic name of the port
SyncStatus	Synchronization status: SyncAcquired, SyncLost
TestFaultCode	Fault code from the most recent port test
TestStatus	Status from the most recent port test: Passed, Failed, NeverRun
TotalErrors	Total number of errors detected on the port since the last port or switch reset
TotalLinkResets	Total number of link resets since the last port or switch reset
TotalLIPsRecvd	Number of loop initialization primitive frames received by this port
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: True, False.

Examples The following is an example of the `show port` command:

```
8/20q FC Switch #> show port 1
  Port Number: 1
  ------------
  AdminState       Online              OperationalState Offline
  AsicNumber       0                   PerfTuningMode   Normal
  AsicPort         2                   PortID           3a0100
  ConfigType       GL                  PortWWN          20:01:00:c0:dd:0d:4f:08
  POSTFaultCode    00000000            RunningType      Unknown
  POSTStatus       Passed              MediaPartNumber  FTLF8528P2BCV
  DownstreamISL    False               MediaRevision    A
  EpConnState      None                MediaType        800-MX-SN-S
  EpIsoReason      NotApplicable       MediaVendor      FINISAR CORP.
  IOStreamGuard    Disabled            MediaVendorID    00009065
  Licensed         True                SymbolicName     Port1
  LinkSpeed        Auto                SyncStatus       SyncLost
  LinkState        Inactive            TestFaultCode    00000000
  LoginStatus      NotLoggedIn         TestStatus       NeverRun
  MaxCredit        16                  UpstreamISL      False
  MediaSpeeds      2Gb/s, 4Gb/s, 8Gb/s  XmitterEnabled   True

  ALInit             1                   LIP_F8_F7          0
  ALInitError        0                   LinkFailures       0
  BadFrames          0                   Login              0
  BBCR_FrameFailures 0                   Logout             0
  BBCR_RRDYFailures  0                   LongFramesIn       0
  Class2FramesIn     0                   LoopTimeouts       0
  Class2FramesOut    0                   LossOfSync         0
  Class2WordsIn      0                   LostFrames         0
  Class2WordsOut     0                   LostRRDYs          0
  Class3FramesIn     0                   PrimSeqErrors      0
  Class3FramesOut    0                   RxLinkResets       0
  Class3Toss         0                   RxOfflineSeq       0
  Class3WordsIn      0                   ShortFramesIn      0
  Class3WordsOut     0                   TotalErrors        0
  DecodeErrors       0                   TotalLinkResets    0
  EpConnects         0                   TotalLIPsRecvd     0
  FBusy              0                   TotalLIPsXmitd     2
  FlowErrors         0                   TotalOfflineSeq    0
  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       0
  LIP_F7_F7          0                   TxOfflineSeq       0
  LIP_F8_AL_PS       0
```

See also set port, page 235

show postlog

Description Displays the power-on self test log, which contains results from the most recently failed power-on self test (POST).

Authority None

Syntax `show postlog`

or

`show post log`

Examples The following is an example of the `show postlog` command:

```
8/20q FC Switch #> 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 setup callhome

Description Displays the Call Home database configuration.

NOTE: The 8/20q Fibre Channel Switch Call Home service provides an e-mail notification capability for the switch. This service has no relationship with the HP Call Home feature, which notifies HP services.

Authority None

Syntax `show setup callhome`

Examples The following is an example of the `show setup callhome` command:

```
8/20q FC Switch (admin) #> 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
```

See also set setup callhome, page 236

show setup mfg

Description Displays manufacturing information about the switch.

Authority None

Syntax `show setup mfg`

Examples The following is an example of the `show setup mfg` command:

```
8/20q FC Switch #> show setup mfg
  Manufacturing Information
  -------------------------
  BrandName                HP
  BuildDate                Tuesday, September 25, 2007 11:23
  ChassisPartNumber        HSTNM-N015
  ChassisSerialNumber      0729C00137
  CPUBoardSerialNumber     0729c00137
  LicensedPorts            20
  MACAddress               00:c0:dd:0d:53:e7
  PlanarPartNumber         31894-00  A
  SwitchSymbolicName       8/20q FC Switch
  SwitchWWN                10:00:00:c0:dd:0d:53:e7
  SystemDescription        HP 8/20q Fibre Channel Switch
  SystemObjectID           1.3.6.1.4.1.3873.1.11
```

show setup radius

Description Displays RADIUS server information.

Authority None

Syntax
```
show setup radius
    common
    server [server_number]
```

Operands

`common`
Displays the configuration parameters that are common for all RADIUS servers. To display common and server-specific information, omit the operand. See Table 49 for a description of the common configuration parameters.

`server [server_number]`
Displays the configuration parameters for the RADIUS server given by [server_number]. [server_number] is an integer corresponding to a configured server. To display common and server-specific information, omit the operand. Refer to Table 50 for a description of the server-specific configuration parameters.

Examples The following is an example of the `show setup radius common` command:

```
8/20q FC Switch #> show setup radius common
  Radius Information
  ------------------
  DeviceAuthOrder   Local
  UserAuthOrder     Local
  TotalServers      2
```

The following is an example of the `show setup radius server` command:

```
8/20q FC Switch #> show setup radius server 2
  Radius Information
  ------------------
  Server: 2

  ServerIPAddress   bacd:1234:bacd:1234:bacd:1234:bacd:1234
  ServerUDPPort     1812
  DeviceAuthServer  True
  UserAuthServer    True
  AccountingServer  True
  Timeout           2
  Retries           0
  SignPackets       False
  Secret            ********
```

See also set setup radius, page 238

show setup services

Description Displays switch service status information.

Authority None

Syntax `show setup services`

Examples The following is an example of the `show setup services` command:

```
8/20q FC Switch #> show setup services
System Services
---------------------------
TelnetEnabled             True
SSHEnabled                False
GUIMgmtEnabled            True
SSLEnabled                False
EmbeddedGUIEnabled        True
SNMPEnabled               True
NTPEnabled                True
CIMEnabled                True
FTPEnabled                True
MgmtServerEnabled         True
CallHomeEnabled           True
```

See also set setup services, page 241

show setup snmp

Description Displays the current SNMP settings.

Authority None

Syntax
```
show setup snmp
    common
    trap [trap_number]
```

Operands

`common`
Displays SNMP configuration parameters that are common to all traps. To display common and trap-specific parameters, omit the operand. See Table 52 for descriptions of the common configuration parameters.

`trap [trap_number]`
Displays SNMP configuration parameters for the trap given by [trap_number]. To display common and trap-specific parameters, omit the operand. See Table 53 for descriptions of the trap-specific configuration parameters.

Examples The following is an example of the `show setup snmp common` command:

```
8/20q FC Switch #> show setup snmp common
  SNMP Information
  ----------------
  SNMPEnabled           True
  Contact               <sysContact undefined>
  Location              <sysLocation undefined>
  Description           HP 8/20q FC Switch
  ObjectID              1.3.6.1.4.1.3873.1.11
  AuthFailureTrap       True
  ProxyEnabled          True
  SNMPv3Enabled         False
```

The following is an example of the `show setup snmp trap` command:

```
8/20q FC Switch #> show setup snmp trap 1
  SNMP Information
  ----------------
  Trap1Enabled          False
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Version          2
```

See also set setup snmp, page 244

show setup system

Description Displays network, logging, NTP server, and timer parameters on the switch.

Authority None

Syntax

```
show setup system
    dns
    ipv4
    ipv6
    logging
    ntp
    timers
```

Operands

`dns`
Displays DNS host name configuration parameters. To display all system configuration parameters, omit the operand. See Table 54 for descriptions of the DNS host name configuration parameters.

`ipv4`
Displays switch IPv4 Ethernet configuration parameters. To display all system configuration parameters, omit the operand. See Table 55 for descriptions of the IPv4 Ethernet configuration parameters.

`ipv6`
Displays switch IPv6 Ethernet configuration parameters. To display all system configuration parameters, omit the operand. See Table 56 for descriptions of the IPv6 Ethernet configuration parameters.

`logging`
Displays event logging configuration parameters. To display all system configuration parameters, omit the operand. See Table 57 for descriptions of the event logging configuration parameters.

`ntp`
Displays NTP server configuration parameters. To display all system configuration parameters, omit the operand. See Table 58 for descriptions of the NTP server configuration parameters.

`timers`
Displays timer configuration parameters. To display all system configuration parameters, omit the operand. See Table 59 for descriptions of the timer configuration parameters.

Examples The following is an example of the `show setup system dns` command:

```
8/20q FC Switch #> 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 is an example of the `show setup system ipv4` command:

```
8/20q FC Switch #> show setup system ipv4

  System Information
  ------------------
  EthIPv4NetworkEnable         True
  EthIPv4NetworkDiscovery      Static
  EthIPv4NetworkAddress        10.20.11.32
  EthIPv4NetworkMask           255.255.252.0
  EthIPv4GatewayAddress        10.20.8.254
```

The following is an example of the `show setup system ipv6` command:

```
8/20q FC Switch #> show setup system ipv6

  System Information
  ------------------
  EthIPv6NetworkEnable         False
  EthIPv6NetworkDiscovery      Static
  EthIPv6NetworkAddress        2001::1/64
  EthIPv6GatewayAddress        fe80::1
```

The following example of the `show setup system logging` command:

```
8/20q FC Switch #> show setup system logging

  System Information
  ------------------
  LocalLogEnabled          True
  RemoteLogEnabled         False
  RemoteLogHostAddress     10.0.0.254
```

The following is an example of the `show setup system ntp` command:

```
8/20q FC Switch #> show setup system ntp

  System Information
  ------------------
  NTPClientEnabled         False
  NTPServerDiscovery       Static
  NTPServerAddress         51.68.85.102
```

The following example of the `show setup system timers` command:

```
8/20q FC Switch #> show setup system timers

  System Information
  ------------------
  AdminTimeout            30
  InactivityTimeout       0
```

See also set setup system, page 247

show steering

Description Displays the routes that data takes in the fabric.

Authority None

Syntax `show steering` *[domain_id]*

Operands *[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:

```
8/20q FC Switch #> 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

Description Displays switch operational information.

Authority None

Syntax `show switch`

Notes Table 67 describes the switch operational parameters.

Table 67 Switch operational parameters

Parameter	Description
SymbolicName	Descriptive name for the switch
SwitchWWN	Switch worldwide name
BootVersion	Programmable Read-only Memory (PROM) boot version
CreditPool	Number of port buffer credits available to recipient ports
DomainID	Switch domain ID
FirstPortAddress	Fibre Channel 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 switch test
TestStatus	Status from the most recent switch test
BoardTemp (1) - Degrees Celsius	Internal switch temperature at circuit board sensor 1
SwitchTemperatureStatus	Normal, warning, failure

Examples The following is an example of the `show switch` command:

```
8/20q FC Switch #> show switch
 Switch Information
 ------------------
 SymbolicName                        8/20q FC Switch
 SwitchWWN                           10:00:00:c0:dd:00:bc:56
 BootVersion                         Vx.x.x.x-0 (day month date time year)
 CreditPool                          0
 DomainID                            19 (0x13)
 FirstPortAddress                    130000
 FlashSize - MBytes                  128
 LogFilterLevel                      Critical
 MaxPorts                            20
 NumberOfResets                      15
 ReasonForLastReset                  PowerUp
 ActiveImageVersion - build date     Vx.x.x.0 (day month date time year)
 PendingImageVersion - build date    Vx.x.x.0 (day month date time year)
 ActiveConfiguration                 default
 AdminState                          Online
 AdminModeActive                     False
 BeaconOnStatus                      Off
 OperationalState                    Online
 PrincipalSwitchRole                 False
 POSTFaultCode                       00000000
 POSTStatus                          Passed
 TestFaultCode                       00000000
 TestStatus                          NeverRun
 BoardTemp (1) - Degrees Celsius     32
 SwitchTemperatureStatus             Normal
```

See also set config switch, page 226

set switch state, page 254

show system

Description 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:

```
8/20q FC Switch #> show system

  Assigned System Network Information
  -----------------------------------
  Hostname                <undefined>
  EthIPv4NetworkAddress   10.20.116.133
  EthIPv6NetworkAddress   <undefined>
  DNSServer1              <undefined>
  DNSSearchList1          <undefined>
  IPv4GatewayList1        10.20.116.1
  IPv6GatewayList1        <undefined>
  NTPServer               10.20.10.10
```

See also set setup system, page 247

show setup system, page 296

show temp

Description Displays temperature information.

Authority None

Syntax `show temp`

Examples

```
8/20q FC Switch #? show temp
Temperature(C) Sensors:

  Sensor  Description  Status  Current  High Warn  High Alarm
  ------  -----------  ------  -------  ---------  ----------
       0  BOARD        Normal       24         65          70
       1  DS1780       Normal       28        n/a         n/a
       2  MAX1617      Normal       31         65          70
       3  ASIC         Normal       49         95         100
```

See also show env, page 269

show voltage, page 309

show testlog

Description 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:

```
8/20q FC Switch #> 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

Description Displays the current time zone setting.

Authority None

Syntax `show timezone`

Examples The following is an example of the `show timezone` command:

```
8/20q FC Switch #> show timezone

  America/Chicago
```

See also set timezone, page 255

show topology

Description Displays all connected devices.

Authority None

Syntax `show topology [port_number]`

Operands `[port_number]`
Displays the devices connected to the port given by [port_number].

Examples The following is an example of the `show topology` command:

```
8/20q FC Switch #> show topology
Unique ID Key
-------------
A = ALPA,  D = Domain ID,  P = Port ID
Port   Local Local                    Remote  Remote                     Unique
Number Type  PortWWN                  Type    NodeWWN                    ID
------ ----- -------                  ------  -------                    ------
5      F     20:05:00:c0:dd:00:bd:ec   N      20:00:00:00:c9:22:1e:93   010500 P
10     E     20:0a:00:c0:dd:00:bd:ec   E     10:00:00:c0:dd:00:80:21   4(0x4) D
```

The following is an example of the `show topology` command for port 1:

```
8/20q FC Switch  #> show topology 1
  Local Link Information
  ----------------------
  PortNumber             1
  PortID                 650100
  PortWWN                20:01:00:c0:dd:00:91:11
  PortType               F

  Remote Link Information
  -----------------------
  Device                 0
  NodeWWN                50:80:02:00:00:06:d5:38
  PortType               NL
  Description            (NULL)
  IPv4Address            0.0.0.0
  IPv6Address            fc00:1234:5678:9abc:def0:1234:5678:9abc

  Device                 1
  NodeWWN                20:00:00:20:37:2b:08:c9
  PortType               NL
  Description            (NULL)
  IPv4Address            0.0.0.0
  IPv6Address            fc00:1234:5678:9abc:def0:1234:5678:9efg
```

show users

Description Displays a list of logged-in users. This is equivalent to the `user list` command.

Authority None

Syntax `show users` *brief*

Operands `brief`

Displays just the account name and client.

Examples The following is an example of the `show users` command:

```
8/20q FC Switch #> show users
  User             cim@OB-session1
  Client           cim
  Logged in Since  Tue Apr  8 05:22:47 2008

  User             snmp@IB-session2
  Client           Unknown
  Logged in Since  Tue Apr  8 05:22:55 2008

  User             snmp@OB-session3
  Client           Unknown
  Logged in Since  Tue Apr  8 05:22:55 2008

  User             admin@OB-session5
  Client           10.33.21.27
  Logged in Since  Thu Apr 10 04:14:11 2008
```

The following is an example of the `show users brief` command:

```
8/20q FC Switch #> show users brief
  User                          Client
  ----                          ------
  cim@OB-session1               cim
  snmp@IB-session2              Unknown
  snmp@OB-session3              Unknown
  admin@OB-session5             10.33.21.27
```

See also user, page 322

show version

Description Displays introductory information about the operational attributes of the switch. This command is equivalent to the `show about` command.

Authority None

Syntax `show version`

Notes Table 68 describes the information returned by the `show version` command.

Table 68 Show version display entries

Attribute	Description
`SystemDescription`	Description of the switch system
`HostName`	DNS host name
`EthIPv4NetworkAddress`	Switch IP address, version 4
`EthIPv6NetworkAddress`	Switch IP address, version 6
`MacAddress`	Media Access Control (MAC) address of the switch
`WorldWideName`	Worldwide name of the switch
`ChassisSerialNumber`	Serial number of the switch
`SymbolicName`	Symbolic name of the switch
`ActiveSWVersion`	Firmware version
`ActiveTimestamp`	Date and time that the firmware was activated
`POSTStatus`	Results of the power-on self test
`LicensedPorts`	Number of licensed ports
`SwitchMode`	`Full Fabric` indicates that the switch operates with the standard Fibre Channel port types: G, GL, F, FL, E, TR

Examples The following is an example of the `show version` command.

```
8/20q FC Switch #> show version
       ****************************************************
       *                                                  *
       *       Command Line Interface SHell  (CLISH)      *
       *                                                  *
       ****************************************************

       SystemDescription     HP 8/20q Fibre Channel Switch
       HostName              <undefined>
       EthIPv4NetworkAddress 10.20.11.192
       EthIPv6NetworkAddress ::
       MACAddress            00:c0:dd:00:71:ee
       WorldWideName         10:00:00:c0:dd:00:71:ed
       SerialNumber          FAM033100024
       SymbolicName          8/20q FC Switch
       ActiveSWVersion       V8.0.4.xx.xx
       ActiveTimestamp       day month date time year
       POSTStatus            Passed
       LicensedPorts         20
       SwitchMode            Full Fabric
```

See also show about, page 256

show voltage

Description Displays voltage information.

Authority None

Syntax `show voltage`

Examples

```
8/20q FC Switch #? show voltage
  Voltage Sensors:

Sensor  Description  Status  Current  Low Alarm  High Alarm
------  -----------  ------  -------  ---------  ----------
     0  2.5V         Good       2.50       2.20        2.80
     1  1.25V        Good       1.24       1.00        1.50
     2  3.3V         Good       3.32       3.02        3.58
     3  12V          Good      12.00      10.00       13.31
     4  1.2V         Good       1.26       1.04        1.38
     5  1.5V         Good       1.50       1.31        1.68
     6  1.8V_ANALOG  Good       1.78       1.58        2.02
     7  1.8V         Good       1.79       1.60        1.99
     8  2.5V_ANALOG  Good       2.40       2.08        2.84
```

See also show env, page 269

show temp, page 302

shutdown

Description Terminates all data transfers on the switch at convenient points and closes the switch connection. Always power-cycle the switch after entering this command.

Authority Admin session

Syntax `shutdown`

Notes When the shutdown is complete, the Heartbeat LED is extinguished.

snmpv3user

Description Manages SNMP version 3 user accounts on the switch.

Authority Admin session except for the `list` operand

Syntax
```
snmpv3user
    add
    delete [account]
    edit
    list
```

Operands `add`

Creates an SNMP version 3 user account, prompting you for the parameters that are described in Table 69.

Table 69 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`.
`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. The default is `DES`.
`PrivPhrase`	Privacy phrase
`Confirm PrivPhrase`	Privacy phrase confirmation. Re-enter the phrase.

Operands `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 a description of the SNMP version 3 user account parameters, see Table 69.

`list`

Displays SNMP version 3 user accounts, group, authentication type, and privacy type. This operand does not require an Admin session.

Examples The following is an example of the `snmpv3user add` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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)            [MD5       ] : 1
  AuthPhrase      (8-32 chars)                          : ***********
  Confirm AuthPhrase                                    : ***********
  Privacy         (True/False)              [False     ] : t
  PrivType        (1=DES)                   [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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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 edit` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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] y

  SNMPV3 user account edited and activated.
```

The following is an example of the `snmpv3user list` command:

```
8/20q FC Switch #> snmpv3user list

  Username                         Group           AuthType   PrivType
  --------                         -----           --------   --------
  snmpuser1                        ReadWrite       MD5        DES
```

See also set setup snmp, page 244

show setup snmp, page 295

test cancel

Description Cancels a port test that is in progress.

Authority Admin session

Syntax
```
test cancel
    port [port_number]
```

Operands
`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:

```
8/20q FC Switch (admin) #> test cancel port 15
```

See also test port, page 315

test status, page 317

test port

Description Tests individual ports using an offline or online test.

Authority Admin session

Syntax
```
test port [port_number]
    offline [loopback_type]
    online
```

Operands `[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. Table 70 describes the offline port test parameters.

Table 70 Offline port loopback types

Parameter	Description
`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. Online testing of TR_Ports is not allowed. This test does not disrupt communication on the port.

Notes 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.

Table 71 describes the port test parameters.

Table 71 Port 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.

Examples The following example performs an online test on port 1:

```
8/20q FC Switch #> admin start
8/20q FC Switch (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)    [429496729]
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.

8/20q FC Switch (admin) #>
  Test for port 1 Passed.
```

See also test cancel, page 314

test status, page 317

test switch, page 319

test status

Description Displays the status of a test in progress, or if there is no test in progress, the status of the last test that was executed.

Authority None

Syntax
```
test status
    port [port_number]
    switch
```

Operands

`port [port_number]`
Display test status for the port given by [port_number]. [port_number] can be 0–19.

`switch`
Display test status for the switch: `Passed`, `Failed`, `NeverRun`.

Examples The following is an example of the `test status port` command:

```
8/20q FC Switch (admin) #> test status port 1
Port               Test                Test                Loop      Test
Num      Port      Type                Status             Count  Failures
----     --------  ----                ------             -----  --------
1        1         Offline Internal    Passed                12         0
```

The following is an example of the `test status switch` command:

```
8/20q FC Switch #> test status switch

  Test    Test                  Test                Loop      Test
  Level   Type                  Status             Count  Failures
  -----   ----                  ------             -----  --------
  Switch  Offline internal      Passed                 4         0

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

See also test cancel, page 314

test port, page 315

test switch, page 319

test switch

Description 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
```

Operands

`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. Table 72 describes the connectivity loopback types.

Table 72 Connectivity loopback types

Parameter	Description
`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. Table 73 describes the offline loopback types.

Table 73 Offline loopback types

Parameter	Description
`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 port-to-device connections for all ports that are online. This test does not disrupt communication on the ports. The online test excludes TR_Ports.

Notes 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.

Table 74 describes the switch test parameters.

Table 74 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

Table 74 Switch test parameters (continued)

Parameter	Description
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.

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

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #>set switch state diagnostics
8/20q FC Switch (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
```

See also test cancel, page 314

test status, page 317

test switch, page 319

uptime

Description Displays the elapsed up time since the switch was last reset and the 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:

```
8/20q FC Switch #> uptime

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

user

Description Administers and displays user accounts.

Authority Admin account name and an Admin session. The `accounts` and `list` operands are available to all account names without an Admin session.

Syntax

```
user
    accounts
    add
    delete [account_name]
    edit
    list brief
```

Operands

`accounts`
Displays all user accounts that exist on the switch. This operand 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. An account name can be up to 15 characters: the first character must be alphanumeric; the remaining characters must be ASCII characters excluding semicolon (;), comma (,), #, and period (.).
- 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 (2,000 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 operand 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:

```
8/20q FC Switch (admin) #> user accounts

    Current list of user accounts
-----------------------------
images       (admin authority = False, never expires)
admin        (admin authority = True , never expires)
chuckca      (admin authority = False, expires in < 50 days)
gregj        (admin authority = True , expires in < 100 days)
fred         (admin authority = True , never expires)
```

The following is an example of the `user add` command:

```
8/20q FC Switch (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 delete` command:

```
8/20q FC Switch (admin) #> user del user3

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

The following is an example of the `user edit` command:

```
8/20q FC Switch (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 list` command:

```
8/20q FC Switch #> 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
```

See also passwd, page 199

show users, page 306

whoami

Description Displays the account name, session number, and switch domain ID for the Telnet session.

Authority None

Syntax `whoami`

Examples The following is an example of the `whoami` command:

```
8/20q FC Switch #> whoami

User name       : admin@session2
Switch name     : HP 8/20q Fibre Channel Switch
Switch domain ID: 21 (0x15)
```

zone

Description Manages zones and zone membership on a switch.

Authority Admin session and a Zoning Edit session. See the `zoning edit` command. The `list`, `members`, and `zonesets` operands are available without an Admin session.

Syntax

```
zone
    add [zone] [member_list]
    list
    members [zone]
    orphans
    remove [zone] [member_list]
    rename [zone_old] [zone_new]
    zonesets [zone]
```

Operands

`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 2,000 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 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. You must enter the `zoning save` command to save your changes.

`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]. You must enter the `zoning save` command to save your changes.

`create [zone]`

Creates a zone with the name given by [zone]. A zone name must begin with a letter and be no longer than 64 characters. Valid characters are alphanumeric, _, $, ^, and -. The zoning database supports a maximum of 2,000 zones. You must enter the `zoning save` command to save your changes.

`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. You must enter the `zoning save` command to save your changes.

`list`

Displays a list of all zones and the zone sets of which they are components. This operand does not require an Admin session.

`members [zone]`

Displays all members of the zone given by [zone]. This operand does not require an Admin session.

`orphans`

Displays a list of zones that are not members of any zone set.

`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 WWPN with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

You must enter the `zoning save` command to save your changes.

`rename [zone_old] [zone_new]`

Renames the zone given by [zone_old] to the zone given by [zone_new]. You must enter the `zoning save` command to save your changes.

`zonesets [zone]`

Displays all zone sets of which the zone given by [zone] is a component. This operand does not require an Admin session.

Examples The following is an example of the `zone list` command:

```
8/20q FC Switch #> zone list

  Zone        ZoneSet
  ----        -------
  wwn_b0241f
              zone_set_1

  wwn_23bd31
              zone_set_1

  wwn_221416
              zone_set_2

  wwn_2215c3
              zone_set_2

  wwn_0160ed
              zone_set_3
```

The following is an example of the `zone members` command:

```
8/20q FC Switch #> 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 orphans` command:

```
8/20q FC Switch #> zone orphans
Current list of orphan zones
---------------------------
zone3
zone4
```

The following is an example of the `zone zonesets` command:

```
8/20q FC Switch #> zone zonesets zone1

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

See also zoneset, page 328

zoning edit, page 335

zoneset

Description Manages zone sets and component zones across the fabric.

Authority Admin session and a Zoning Edit session. See the `zoning edit` command. The `active`, `list`, and `zones` operands are available without an Admin session. You must close the Zoning Edit session before using the `activate` and `deactivate` operand.

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]
```

Operands

`activate [zone_set]`
Activates the zone set given by [zone_set]. This operand deactivates the active zone set. Close the Zoning Edit session before using this operand.

`active`
Displays the name of the active zone set. This operand 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]. You must enter the `zoning save` command to save your changes.

`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]. You must enter the `zoning save` command to save your changes.

`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 alphanumeric, _, $, ^, and -. The zoning database supports a maximum of 256 zone sets. You must enter the `zoning save` command to save your changes.

`deactivate`
Deactivates the active zone set. Close the Zoning Edit session before using this operand.

`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. You must enter the `zoning save` command to save your changes.

`list`
Displays a list of all zone sets. This operand 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. You must enter the `zoning save` command to save your changes.

`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. You must enter the `zoning save` command to save your changes.

`zones [zone_set]`

Displays all zones that are components of the zone set given by [zone_set]. This operand 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:

```
8/20q FC Switch #> zoneset active

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

The following is an example of the `zoneset list` command:

```
8/20q FC Switch #> zoneset list

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

The following is an example of the `zoneset zones` command:

```
8/20q FC Switch #> zoneset zones ssss

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

See also zoning edit, page 335

zoning save, page 342

zoning active

Description 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` operand.

Syntax
```
zoning active
    capture
```

Operands *capture*

Saves the active zone set to the non-volatile zoning data base.

Examples The following is an example of the `zoning active` command:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch (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.
```

See also zone, page 325

zoneset, page 328

zoning cancel

Description 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
.
.
.
8/20q FC Switch (admin-zoning) #> zoning cancel
  Zoning edit mode will be canceled.  Please confirm (y/n): [n] y
```

See also zoning edit, page 335

zoning clear

Description Clears all inactive zone sets from the volatile edit copy of the zoning database. This operand requires a zoning edit session. This operand 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.

TIP: The preferred method for clearing the zoning database from the switch is the `reset zoning` command.

Authority Admin session and a Zoning Edit session.

Syntax `zoning clear`

Examples The following is an example of the `zoning clear` command:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #> zoning clear
8/20q FC Switch (admin-zoning) #> zoning save
```

See also zoning save, page 342

zoning configured

Description 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:

```
8/20q FC Switch #> 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

Description 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning delete orphans
   This command will remove all zonesets, zones, and aliases
   that are not currently active.
Please confirm (y/n): [n] y
8/20q FC Switch (admin) #> zoning save
```

zoning edit

Description Opens a Zoning Edit session for the non-volatile zoning database or merged zone set in which to create and manage zone sets and zones.

Authority Admin session

Syntax `zoning edit` *`[database]`*

Operands *`[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. Table 75 describes the zoning database parameters

Table 75 Zoning database parameters

Parameter	Description
`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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #>
.
.
8/20q FC Switch (admin-zoning) #> zoning save
  The changes have been saved; however, they must be activated
   before they can take effect -- see Zoneset Activate command.
```

See also zone, page 325

zoneset, page 328

zoning cancel, page 331

zoning edited

Description 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:

```
8/20q FC Switch (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
```

See also zoning configured, page 333

zoning history

Description Displays a history of zoning modifications. This operand 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:

```
8/20q FC Switch #> 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

Description 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
```

Operands *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 operand, the display includes a membership breakdown for each zone. Table 76 describes the zoning database limits.

Table 76 Zoning database limits

Limit	Description
MaxZoneSets	Maximum number of zone sets is 256.
MaxZones	Maximum number of zones is 2,000.
MaxAliases	Maximum number of aliases is 2,500.
MaxTotalMembers	Maximum number of zone and alias members that can be stored in the switch's zoning database is 10,000. Each instance of a zone member or alias member counts toward this maximum.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets, excluding those in the orphan zone set, that can be stored in the switch's zoning database is 2,000. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone is 2,000.
MaxMembersPerAlias	Maximum number of members in an alias is 2,000.

zoning list

Description 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:

```
8/20q FC Switch #> 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
```

See also zoning edited, page 336

zoning configured, page 333

zoning merged

Description 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` operand.

Syntax
```
zoning merged
    capture
```

Operands *capture*

Saves the merged zone set to the non-volatile zoning database. You must enter the `zoning save` command to save your changes. If you omit this operand, this command displays the contents of the merged zone set.

Examples The following is an example of the `zoning merged` command:

```
8/20q FC Switch #> 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:

```
8/20q FC Switch (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.
```

See also zoning configured, page 333

zoning edited, page 336

zoning list, page 339

zoning restore

Description Restores the volatile zoning database with the contents of the non-volatile zoning database. If the `MergeAutoSave` parameter is `False` (see Table 22), 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

Description 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:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> zoning edit
8/20q FC Switch (admin-zoning) #>
.
.
8/20q FC Switch (admin-zoning) #> zoning save
  The changes have been saved; however, they must be activated
   before they can take effect -- see zoneset activate command.
```

See also zoning edit, page 335

14 Support and Other Resources

Document conventions and symbols

Table 77 Document conventions

Convention	Element
Medium blue text: Figure 1	Cross-reference links and email addresses
Medium blue, underlined text (http://www.hp.com)	Website addresses
Bold font	• Keys that are pressed • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italics font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of monospace text, including file and directory names, system output, code, and text typed at the command line

WARNING! Indicates that failure to follow directions could result in bodily harm or death.

CAUTION: Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

Contacting HP

HP contact information

For HP technical support:

- In the United States, see the Contact HP United States webpage: (http://welcome.hp.com/country/us/en/contact_us.html). To contact HP by phone, call: 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
- In other locations, see the Contact HP worldwide (in English) webpage: (http://www.hp.com/country/us/en/wwcontact.html).
- For worldwide technical support information, see the HP support website: http://www.hp.com/support/.

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website: http://www.hp.com/go/e-updates. After registering, you will receive an e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, send a message to storagedocs.feedback@hp.com. Include the document title and manufacturing part number. All submissions become the property of HP.

New and changed information in this edition

The following additions and changes have been made for this edition:

- Added support for the Enterprise Fabric Management Suite fabric management application

Related information

Documents

In addition to this guide, see the following documents for this product:

- *HP 8/20q and SN6000 Fibre Channel Switch Quick Start Installation Instructions*
- *HP 8/20q and SN6000 Fibre Channel Switch Rack Mount Kit Quick Start Installation Instructions*
- *HP SAN Connection Manager User Guide*
- *HP 8/20q Fibre Channel Switch Installation and Reference Guide*
- *HP 8/20q Fibre Channel Switch QuickTools Switch Management User Guide*
- *HP 8/20q and SN6000 Fibre Channel Switch CLI Quick Reference Guide*
- *HP 8/20q and SN6000 Enterprise Fabric Management Suite User Guide*
- *HP 8/20q and SN6000 Fibre Channel Switch Event Messages Reference Guide*
- *HP 8/20q and SN6000 Fibre Channel Switch Simple Network Management Protocol Reference Guide*
- *HP 8/20q and SN6000 Fibre Channel Switch CIM Agent Reference Guide*

For the latest product information, including firmware, documentation, and supported SAN configurations, see the following HP website: http://www.docs.hp.com/go/8Gb-SSC.

Other HP websites

For additional information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.docs.hp.com
- http://www.hp.com/go/sandesignguide

Customer self repair

HP products are designed with many Customer Self Repair parts to minimize repair time and allow for greater flexibility in performing defective parts replacement. If during the diagnosis period HP (or HP service providers or service partners) identifies that the repair can be accomplished by the use of a Customer Self Repair part, HP will ship that part directly to you for replacement. There are two categories of Customer Self Repair parts:

- Mandatory—Parts for which Customer Self Repair is mandatory. If you request HP to replace these parts, you will be charged for the travel and labor costs of this service.
- Optional—Parts for which Customer Self Repair is optional. These parts are also designed for customer self repair. If, however, you require that HP replace them for you, there may or may not be additional charges, depending on the type of warranty service designated for your product.

NOTE:

Some HP parts are not designed for Customer Self Repair. In order to satisfy the customer warranty, HP requires that an authorized service provider replace the part. These parts are identified as No in the Illustrated Parts Catalog.

Based on availability and where geography permits, Customer Self Repair parts will be shipped for next business day delivery. Same day or four-hour delivery may be offered at an additional charge where geography permits. If assistance is required, you can call the HP Technical Support Center and a technician will help you over the telephone. HP specifies in the materials shipped with a replacement Customer Self Repair part whether a defective part must be returned to HP. In cases where it is required to return the defective part to HP, you must ship the defective part back to HP within a defined period of time, normally five (5) business days. The defective part must be returned with the associated documentation in the provided shipping material. Failure to return the defective part may result in HP billing you for the replacement. With a Customer Self Repair, HP will pay all shipping and part return costs and determine the courier/carrier to be used.

For more information about the HP Customer Self Repair program, contact your local service provider. For the North American program, visit the HP website (http://www.hp.com/go/selfrepair).

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z