53-1001964-01
October 1, 2010

8/4Gbps FC SAN Module

Administrator's Guide

53-1001964-01

Notes, Cautions, and Warnings

NOTE
A NOTE indicates important information that helps you make better use of your computer.

CAUTION
A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

DANGER
A DANGER indicates a potential for property damage, personal injury, or death.

Contents

Tables

About this Document

How this document is organized

This document is a procedural guide to help SAN administrators configure and manage the Dell 8/4Gbps FC SAN Module, hereafter identified as the FC SAN Module.

This preface contains the following components:

- Chapter 1, "NPIV Basic Concepts" describes NPIV function and an overview of key the FC SAN Module key features.
- Chapter 2, "Configuring Ports on the FC SAN Module" describes how to configure ports in FC SAN Module mode.
- Chapter 3, "Managing Policies and Features" describes how to enable policies on the FC SAN Module. It also provides information on how to set up Failover and Failback.
- Chapter 4, "Fabric Configuration with the Dell FC SAN Module" describes how to connect multiple devices using the FC SAN Module.
- Appendix A, "Troubleshooting" provides symptoms and troubleshooting tips to resolve issues.
- Appendix B, "Command Reference" provides a reference for CLI commands used for module configuration and information.

Document conventions

This section describes text formatting conventions and important notices formats.

Text formatting

The narrative-text formatting conventions that are used in this document are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI

italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
code text	Identifies CLI output Identifies syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive. The **ficonCupSet** and **ficonCupShow** commands are an exception to this convention.

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are printed in bold.
--**option, option**	Command options are printed in bold.
-**argument,** arg	Arguments.
[ ]	Optional element.
variable	Variables are printed in italics. In the help pages, values are underlined or enclosed in angled brackets < >.
...	Repeat the previous element, for example “member[;member...]”
value	Fixed values following arguments are printed in plain font. For example, --**show** WWN
|	Boolean. Elements are exclusive. Example: --**show** -**mode** egress | ingress

Notes, cautions, and warnings

The following notices appear in this document.

NOTE
A note provides a tip, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Brocade Corporation	Brocade
Dell Corporation	Dell, 8/4Gbps FC SAN Module
Cisco Systems, Inc.	Cisco
Sun Microsystems, Inc.	Sun, Solaris
Netscape Communications Corporation	Netscape
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover
Emulex Corporation	Emulex
QLogic Corporation	QLogic

Key terms

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at: *http://www.snia.org/education/dictionary*.

The following terms are used in this manual.

FC SAN Module
: Port aggregation I/O module that reduces SAN (storage area network) deployment complexity by leveraging NPIV (N_Port ID Virtualization).

Edge switch
: A fabric switch that connects host, storage, or other devices, such as the FC SAN Module, to the fabric.

F_Port A fabric port. A switch port that connects a host, HBA (host bus adaptor), or storage device to the SAN. On the FC SAN Module, the internal port (F_Port) connects to an HBA on an individual blade server.

Mapping On the FC SAN Module, the configuration of internal port (F_Port) to external port (N_Port) routes.

N_Port A node port. A Fibre Channel host or storage port in a fabric or point-to-point connection. On the FC SAN Module, the external port (N_Port connects to the Edge switch.

NPIV N_Port ID Virtualization. Allows a single Fibre Channel port to appear as multiple, distinct ports providing separate port identification and security zoning within the fabric for each operating system image as if each operating system image had its own unique physical port.

Preferred Secondary N_Port On the FC SAN Module, the preferred secondary external port (N_Port) refers to the secondary path to which an internal port (F_Port) fails over if the primary external port goes offline.

Additional information

This section lists additional industry-specific documentation that you might find helpful.

Industry resources

For additional information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

http://www.fibrechannel.org

Getting technical help

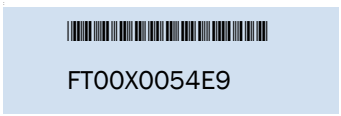
Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. General Information
    - Dell Service Tag
    - Technical Support contract number, if applicable
    - FC SAN Module model
    - FC SAN Module operating system version
    - Error numbers and messages received

- **supportSave** command output
- Detailed description of the problem and specific questions
- Description of any troubleshooting steps already performed and results
- Serial console and Telnet session logs
- syslog message logs

2. 8/4Gbps FC SAN Module Serial Number

   The FC SAN Module serial number and corresponding bar code are provided on the serial number label attached to the module. Following is an example of a serial number and barcode:

3. World Wide Name (WWN). Use the CLI **wwn** or **switchShow** commands to display the WWN.
4. Software licenses. Use the CLI **licenseShow** command to display the list of licenses available on the unit.

Chapter

1 NPIV Basic Concepts

In this chapter

NPIV overview

With the FC SAN Module, your Enterprise fabric can handle additional external ports (N_Ports) instead of domains. You do this by configuring internal ports (F_Ports) to connect to the fabric as external ports, which increases the number of device ports you can connect to a single fabric.

Because the Dell (Fibre Channel) FC SAN Module functions as an NPIV port aggregator, it is compatible with Brocade Fabric OS, M-EOS v9.1 or v9.6 and later, and Cisco-based fabrics v3.0 (1) or later and v3.1 (1) and later. This document describes configurations using the CLI commands.

Since the FC SAN Module operates using NPIV it is logically transparent to the host and the fabric. You can increase the number of blade servers that have access to the fabric without increasing the number of switches. This simplifies configuration and management in a large fabric by reducing the number of domain IDs and ports. Figure 1 shows how the FC SAN Module connects to blade servers (Hosts) and fabrics.

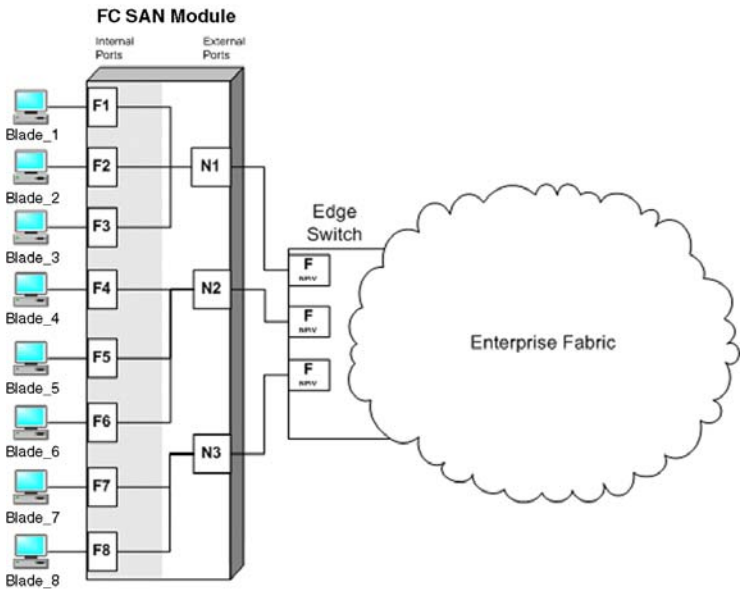


FIGURE 1 **FC SAN Module connection**

FC SAN Module port types

The Dell NPIV Switch FC SAN Module differs from a typical fabric switch because it is a port aggregator rather than a switch; instead, it connects to the fabric using node ports (N_Ports). Typically fabric switches connect to the fabric using ISL (InterSwitch Link) ports, such as E_Ports.

Following are the Fibre Channel (FC) ports that the FC SAN Module uses:

- **F_Port -** internal fabric port that connects a blade server (HBA).
- **N_Port -** external node port that connects to a switch.

FC SAN Module limitations

The limitations of the FC SAN Module are as follows:

- The maximum number of devices that can be connected to a fabric switch through the FC SAN Module depends on the maximum number of local devices supported by the fabric.
- Loop devices are not supported.
- Port groups cannot be overlapped. This means that an N_Port cannot belong to two different groups.
- Direct connections to SAN target devices are not supported.
- Management Platform Services is not supported.
- Name Services is not supported.
- Zoning is not supported; security enforcement is done using the ADS policy.

Chapter

2

Configuring Ports on the FC SAN Module

In this chapter

Port state description

The following table describes the possible port states.

TABLE 1 Port state description

State	Description
No _Card	No interface card present
No _Module	No module (GBIC or other) present
Mod_Val	Module validation in process
Mod_Inv	Invalid module
No_Light	The module is not receiving light
No_Sync	Receiving light but out of sync
In_Sync	Receiving light and in sync
Laser_Flt	Module is signaling a laser fault
Port_Flt	Port marked faulty
Diag_Flt	Port failed diagnostics
Lock_Ref	Locking to the reference signal
Testing	Running diagnostics
Offline	Connection not established (only for virtual ports)
Online	The port is up and running

Port mapping

The FC SAN Module uses port-mapped pre-provisioned routes to direct traffic from the blade server (HBAs) to the fabric. When you first turn on the module, by default, the internal ports (F_Ports) are mapped to a set of predefined external ports (N_Ports). For the default port mapping, see Table 3 on page 5. See t "Remapping ports" on page 5 if you want to change the default mapping. Figure 2 shows a mapping with eight internal ports (F_Ports) evenly mapped to four external ports (N_Ports). External ports connect to the same fabric through different Edge switches.

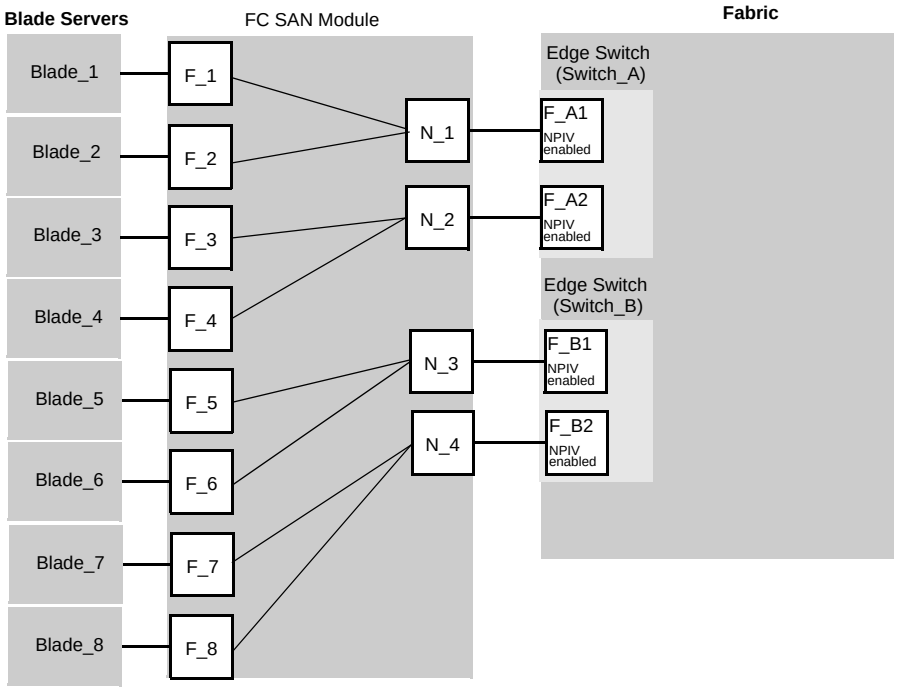


FIGURE 2 **Example NPIV port mapping**

Table 2 provides a description of the port mapping in Figure 2.

TABLE 2 Description of port mapping in preceding figure

NPIV Switch		**Fabric**	
F_Port	**N_Port**	**Edge switch**	**F_Port**
F_1, F_2	N_1	Switch_A	F_A1
F_3, F_4	N_2	Switch_A	F_A2
F_5, F_6	N_3	Switch_B	F_B1
F_7, F_8	N_4	Switch_B	F_B2

Default port mapping

Table 3 shows the default port mapping. By default, Failover and Failback policy are enabled on all external ports (N_Ports).

TABLE 3 FC SAN Module default F_Port-to-N_Port mapping

Total Ports	Server Ports (F_Ports)	External Ports (N_Ports)	Default F_ to N_Port Mapping
24	1-16	0, 17-23	1, 2 mapped to 17 3, 4 mapped to 18 5, 6 mapped to 19 7, 8 mapped to 20 9, 10 mapped to 21 11, 12 mapped to 22 13, 14 mapped to 23 15, 16 mapped to 0

The FC SAN Module ships with 12 active ports and two installed SFP+ optical transceivers. A port upgrade license is available to activate 12 additional ports and includes two additional SFP+ transceivers. Additional single SFP+ transceivers are also available for maximum bandwidth and redundancy.

By default, port licensing on the FC SAN Module is dynamic, so port licenses are flexibly assigned from the pool of available licenses. Ports 17 and 18 are licensed at the factory (and align with the two included SFP+ transceivers). The remaining ten licenses are assigned to active ports as required, making port licensing more flexible.

If no additional SFP+ transceivers are used to enable additional external ports on the FC SAN Module and your M1000e blade chassis contains more than four blade servers, you should make modifications to the default port mapping to ensure connectivity for all servers to the SAN.

Remapping ports

You can modify the default port mapping by adding internal ports (F_Ports) to an external port (N_Port). Doing so, routes that traffic to and from the fabric through the specified external port.

You can assign an internal port to only one primary external port at a time. If the internal is already assigned to an external port, you must remove it from the external port before you can add it to a different port.

Use the following steps to add an internal port (F_Port) to an external port (N_Port).

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the command with the **--mapadd** *n_portnumber "f_port1;f_port2;... "*operand to add the list of internal to the external port.

   The *f_portlist* can contain multiple internal ports (F_Ports) numbers separated by semicolons, for example "17;18".

```
switch:admin> ag --mapadd 13 "6;7"
F-Port to N-Port mapping has been updated successfully
```

3. Enter the **ag --mapshow** command and specify the port number to display the list of mapped internal ports (F_Ports). Verify that the added internal ports (F_Ports) appear in the list.

```
switch:admin> ag --mapshow 13

        N_Port                          : 13
        Failover(1=enabled/0=disabled) : 1
        Failback(1=enabled/0=disabled) : 1
        Current F_Ports                 : None
        Configured F_Ports              : 6;7
        PG_ID                           : 0
        PG_Name                         : pg0
```

Removing internal ports (F_Ports) from external ports (N_Ports)

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --mapdel** command to remove the internal port from the external port.

   The *f_portlist* can contain multiple internal port numbers separated by semicolons, for example “17;18”.

```
switch:admin> ag --mapdel 17;18
F-Port to N-Port mapping has been updated successfully
```

3. Enter the **switchshow** command to verify that the internal port is free (unassigned).

   Unassigned F_Port status is Disabled (No mapping for internal port). See port 6 in the following example.

```
switch:admin> switchshow
switchName:     fsw534_4016
switchType:     45.0
switchState:    Online
switchMode:     Access Gateway Mode
switchWwn:      10:00:00:05:1e:02:1d:b0
switchBeacon:   OFF

Area Port Media Speed State     Proto
====================================
  0   0   cu    AN   No_Sync
  1   1   cu    AN   No_Sync          Disabled (N-Port Offline for F-Port)
  2   2   cu    AN   No_Sync          Disabled (N-Port Offline for F-Port)
  3   3   cu    AN   No_Sync          Disabled (N-Port Offline for F-Port)
  4   4   cu    AN   No_Sync          Disabled (N-Port Offline for F-Port)
  5   5   cu    AN   No_Sync          Disabled (N-Port Offline for F-Port)
  6   6   cu    AN   No_Sync          Disabled (No mapping for F-Port)
  7   7   cu    AN   No_Sync
  8   8   cu    AN   No_Sync
  9   9   cu    AN   No_Sync
 10  10   --    N4   No_Module
 11  11   --    N4   No_Module
 12  12   --    N4   No_Module
 13  13   id     N4   Online          N-Port  10:00:00:05:1e:35:10:1e 0x5a0a00
 14  14   id     N4   Online          N-Port  10:00:00:05:1e:35:10:1e 0x5a0900
 15  15   id     N4   Online          N-Port  10:00:00:05:1e:35:10:1e 0x5a0800
```

Chapter

3

Managing Policies and Features

In this chapter

Policies overview

This chapter provides detailed information on the following policies.

- Advanced Device Security policy (ADS)
- Automatic Port Configuration policy (APC)
- Port Grouping policy (PG)
- Persistent ALPA policy

These policies can be used to control various advanced features, such as Failover, and Failback.

Displaying current policies

You can run the following command to display policies that are currently enabled or disabled on a FC SAN Module.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --policyshow** command.

```
switch:admin> ag --policyshow
Policy_Description       Policy_Name   State
-------------------------------------------------
Port Grouping            pg            Enabled
Auto Port Configuration  auto          Disabled
Advanced Device Security ads           Enabled
```

FC SAN Module policy enforcement matrix

The following table shows which combinations of policies can co-exist with each other.

TABLE 4 Policy enforcement matrix

Policies	Auto Port Configuration	Port Grouping	ADS Policy
Auto Port Configuration	N/A	Cannot co-exist	Can co-exist
N_Port Grouping	Mutually exclusive	N/A	Can co-exist
ADS Policy	Can co-exist	Can co-exist	N/A

Advanced Device Security policy

The Advanced Device Security (ADS) is disabled by default for the FC SAN Module. ADS is a security policy that restricts access to the fabric at the to a set of authorized devices. Unauthorized access is rejected and the system logs a RASLOG message. You can configure the list of allowed devices for each internal port (F_Port) by specifying their Port WWN (PWWN). The ADS policy secures virtual and physical connections to the SAN.

How the ADS policy works

When you enable this policy, it applies to all internal ports (F_Ports) on the FC SAN Module. By default, all devices have access to the fabric on all ports. You can restrict the fabric connectivity to a particular set of devices where FC SAN Module maintains a per-port allow list for the set of devices whose PWWN you define to log in through an internal port. You can view the devices with active connections to an internal port using the **ag –show** command.

NOTE
The **ag --show** command only displays the Core FC SAN Module, such as the modules that are directly connected to fabric. The **agshow --name** *name* command displays the internal ports of both the Core and Edge modules.

Enabling and disabling the Advanced Device Security policy

By default, the ADS policy is disabled. When you manually disable the ADS policy, all of the allow lists (global and per-port) are cleared. Before disabling the ADS policy, you should save the configuration using the **configupload** command in case you need this configuration again.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --policyenable ads** command to enable the ADS policy.

```
switch:admin> ag --policyenable ads
The policy ADS is enabled
```

3. Enter the **ag --policydisable ads** command to disable the ADS policy.

```
switch:admin> ag --policydisable ads
The policy ADS is disabled
```

NOTE
Use the **ag –policyshow** command to determine the current status of the ADS policy.

Setting the list of devices allowed to log in

You can determine which devices are allowed to log in by internal (F_Port) by specifying the device's port WWN (PWWN). Lists must be enclosed in double quotation marks. List members must be separated by semicolons. The maximum number of entries in the allowed device list is twice the per port maximum log in count. Replace the WWN list with an asterisk (*) to indicate all access on the specified internal port list. Replace the internal port list with an asterisk (*) to add the specified WWNs to all the internal ports' allow lists. A blank WWN list ("") indicates no access. The ADS policy must be enabled for this command to succeed.

NOTE
Use an asterisk enclosed in quotation marks,"*", to set the Allow list to "All Access" to all internal ports; use a pair of double quotation marks ("") to set the Allow list to "No Access".

Note the following characteristics of the Allow List:

- The maximum device entries allowed in the Allow List is twice the per port max login count.
- Each port can be configured to "not allow any device" or "to allow all the devices" to log in.
- If the ADS policy is enabled, by default, every port is configured to allow all devices to log in.
- The same Allow List can be specified for more than one internal port.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --adsset** command with the appropriate operands to set the list of devices allowed to log into specific ports. In the following example, ports 1, 10, and, 13 are set to "all access."

```
switch:admin> ag--adsset"1;10;13""*"
WWN list set successfully as the Allow Lists of the F_Port[s]
```

Setting the list of devices not allowed to log in

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --adsset** command with the appropriate operands to set the list of devices not allowed to log into specific ports. In the following example, ports 11 and 12 are set to "no access."

```
switch:admin > ag --adsset "11;12" ""
WWN list set successfully as the Allow Lists of the F_Port[s]
```

Removing devices from the list of allowed devices

Use the **ag --adsdel** command to delete the specified WWNs from the list of devices allowed to log in to the specified internal ports (F_Ports). Lists must be enclosed in double quotation marks. List members must be separated by semicolons. Replace the internal port list with an asterisk (*) to remove the specified WWNs from all the internal ports' allow lists. The ADS policy must be enabled for this command to succeed.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --adsdel** command to remove one or more devices from the list of allowed devices.

   Use the following syntax:

   ```
   ag--adsdel "F_Port [;F_Port2;...]" "WWN [;WWN2;...]"
   ```

   In the following example, two devices are removed from the list of allowed devices (for ports 3 and 9).

   ```
   switch:admin> ag --adsdel "3;9"
   "22:03:08:00:88:35:a0:12;22:00:00:e0:8b:88:01:8b"
   WWNs removed successfully from Allow Lists of the F_Port[s]Viewing F_Ports
   allowed to login
   ```

Adding new devices to the list of allowed devices

You can add the specified WWNs to the list of devices allowed to log in to the specified internal ports (F_Ports). Lists must be enclosed in double quotation marks. List members must be separated by semicolons. Replace the internal port list with an asterisk (*) to add the specified WWNs to all the internal ports' allow lists. The ADS policy must be enabled for this command to succeed.

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **ag –adsadd** command with appropriate operands to add one or more new devices to the list of allowed devices.

   Use the following syntax:

   ```
   ag--adsadd "F_Port [;F_Port2;...]" "WWN [;WWN2;...]"
   ```

   In the following example, two devices are added to the list of allowed devices (for ports 3 and 9).

   ```
   switch:admin> ag --adsadd "3;9"
   "20:03:08:00:88:35:a0:12;21:00:00:e0:8b:88:01:8b"
   WWNs added successfully to Allow Lists of the F_Port[s]
   ```

Displaying the list of allowed devices on the FC SAN Module

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --adsshow** command.

   ```
   switch:admin> ag --adsshow
     F_Port                WWNs Allowed
   ------------------------------------------------------------------------------
     1                     ALL ACCESS
     3                     20:03:08:00:88:35:a0:12
                           21:00:00:e0:8b:88:01:8b
     9                     20:03:08:00:88:35:a0:12
                           21:00:00:e0:8b:88:01:8b
     10                    ALL ACCESS
     11                    NO ACCESS
     12                    NO ACCESS
     13                    ALL ACCESS
   ------------------------------------------------------------------------------
   ```

ADS policy considerations

The ADS policy can be enabled or disabled independent of status of other policies.

Automatic Port Configuration policy

The automatic Port Configuration (APC) policy is disabled by default. APC provides the ability to automatically discover port types (host vs. fabric) and dynamically update the routing maps when a new connection is detected. This policy is intended for a complete hands-off operation. APC dynamically maps internal ports (F_Ports) to available external ports (N_Ports) so they are evenly distributed. For example, when a port on the module is connected to a fabric switch, the module configures the port as an external port. If a host is connected to a port on the FC SAN Module, then it determines that it is connected and configures the port as an internal port and automatically maps it to an existing external port with the least number of internal ports mapped to it.

How the APC policy works

When the APC policy is enabled, it applies to all ports on the switch. Enabling the APC policy is disruptive and erases all existing port mappings. Therefore, before enabling the APC policy, you must disable the FC SAN Module. When you disable the APC policy, the external port (N_Port) configuration and the port mapping revert back to the default factory configurations for that platform. It is recommended that you save the current configuration file using the **configupload** command in case you might need this configuration again.

Enabling and disabling the APC policy

Use the following steps to enable and disable Automatic Port Configuration policy.

Enabling APC policy

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **switchdisable** command to ensure that the module is disabled.
3. Enter the **configupload** command to save the module's current configuration.
4. Enter the **ag --policyenable auto** command to enable the APC policy.

```
switch:admin> ag --policyenable auto
All Port related Access Gateway configurations will be lost.
Please save the current configuration using configupload.
Do you want to continue? (yes, y, no, n): [no] y
```

5. At the command prompt, type **Y** to enable the policy.

   The switch is ready; a reboot is not required.

Disabling APC policy

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **switchdisable** command to ensure that the module is disabled.
3. Enter the **configupload** command to save the module's current configuration.

4. Enter the command **ag --policydisable auto** to disable the APC policy.
5. At the command prompt, type **Y** to disable the policy.

```
switch:admin> ag --policydisable auto
Default factory settings will be restored.
Default mappings will come into effect.
Please save the current configuration using configupload.
Do you want to continue? (yes, y, no, n): [no] y
Access Gateway configuration has been restored to factory default
```

6. Enter the **switchenable** command to enable the module.

Automatic Port Configuration policy considerations

Following are the considerations for the Automatic Port Configuration policy:

- The APC and the PG policies cannot be enabled at the same time.
- You cannot manually map ports with this policy enabled.

Port Grouping policy

The Port Grouping (PG) policy is enabled by default. Use the PG policy to partition the fabric and host ports within a module into independently operated groups. Use the PG policy in the following situations:

- When connecting the module to multiple physical or virtual fabrics.
- When you want to isolate specific hosts to specific fabric ports for performance, security, or other reasons.

How port groups work

Create port groups using the **ag --pgcreate** command. This command groups external ports (N_Ports) together as “port groups.” Any internal ports (F_Ports) mapped to the external ports belonging to a port group will become members of that port group. Port grouping fundamentally restricts failover of internal ports to the external ports that belong to that group. For this reason an external ports cannot be member of two port groups. The default PG0 group contains all external ports that do not belong to any other port groups.

Figure 3 on page 13 shows that.if you have created port groups and then an external port (N_Port) goes offline, the internal ports (F_Ports) being routed through that port will fail over to any of the external ports that are part of that port group and are currently active. For example, if external port 4 goes offline then internal ports 7 and 8 are routed through to external port 3 as long as external port 3 is online because both external ports 3 and 4 belong to the same port group, PG2. If no active external ports are available, the internal ports are disabled. The internal ports belonging to a port group do not fail over to external ports belonging to another port group.

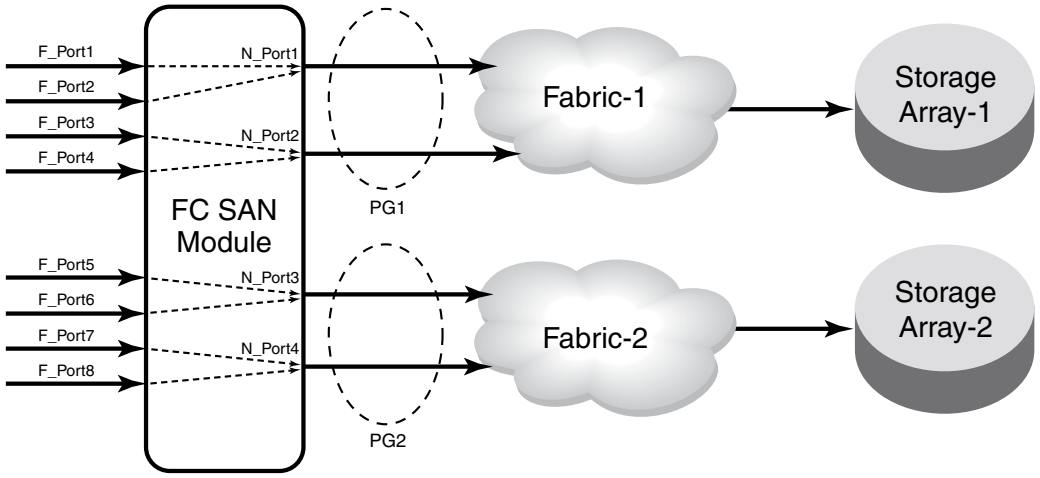


FIGURE 3 **Port grouping behavior**

When a dual redundant fabric configuration is used, internal ports (F_Ports) connected to a FC SAN Module can access the same target devices from both of the fabrics. In this case, you must group the external ports (N_Ports) connected to the redundant fabric into a single port group. It is recommended to have paths fail over to the redundant fabric when the primary fabric goes down. Refer to Figure 4.

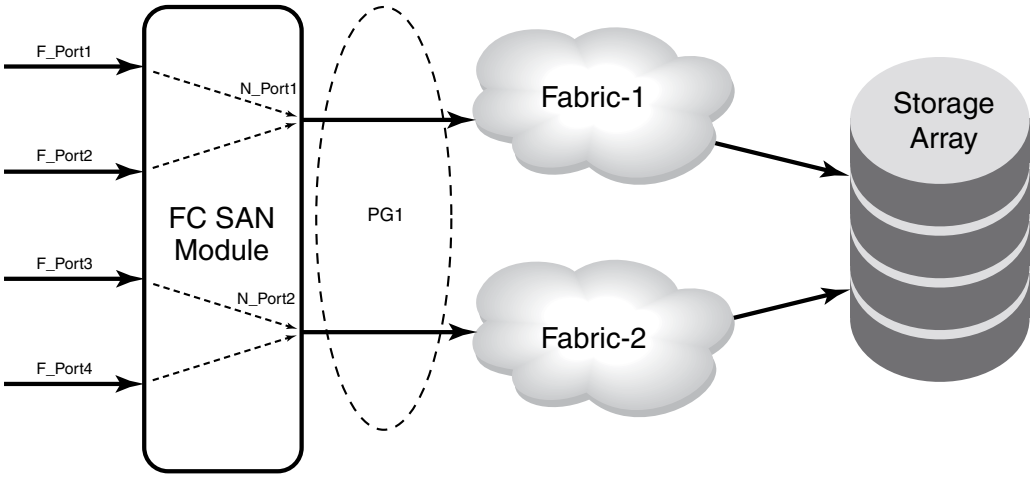


FIGURE 4 **Port group 1 (pg1) setup**

Adding an external port (N_Port) to a port group

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --pgadd** command with the appropriate operands to add an external port (N_Port) to a specific port group. In the following example external port 14 is added to port group 3.

   Note that if you add more than one external ports, you must separate them with a semicolon.

```
switch:admin> ag --pgadd 3 14
N_Port[s] are added to the port group 3
```

Deleting an external port (N_Port) from a port group

Before deleting an external port (N_Port), all internal ports (F_Ports) mapped to that external port must be remapped before that external port is deleted from a port group.

If an external port is deleted from a port group enabled for Login Balancing, the internal ports mapped to that external port stay with the port group as long as there are other external ports in the group. Only the external port is removed from the port group. This is because the internal ports are logically associated with the port groups that are enabled for Login Balancing. This is not the case for port groups not enabled for Login Balancing. When you delete an external port from one of these port groups, the internal port that are mapped to the external port move to PG0 along with the external port. This is because the internal ports are logically associated with the external ports in port groups not enabled for Login Balancing.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --pgdel** command with the appropriate operands to delete an external port (N_Port) from a specific port group. In the following example, external port 13 is removed from port group 3.

   ```
   switch:admin> ag --pgdel 3 13
   N_Port[s] are deleted from port group 3
   ```

3. Enter the command **ag --pgshow** to verify the external port was deleted from the specified port group.

   ```
   switch:admin> ag --pgshow
   PG_ID PG_Name      PG_Mode  N_Ports   F_Ports
   -----------------------------------------------
   0     pg0          lb,mfnm  1;3       10;11
   2     SecondFabric    -     0;2       4;5;6
   -----------------------------------------------
   ```

Removing a port group

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --pgremove** command with appropriate operands to remove a port group. In the following example, port group 3 us removed.

   ```
   switch:admin> ag --pgremove 3
   Port Group 3 has been removed successfully
   ```

Renaming a port group

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --pgrename** command with appropriate operands to rename port group. In the following example, port group pgid 2 is renamed to MyEvenFabric.

   ```
   switch:admin> ag --pgrename 2 MyEvenFabric
   Port Group 2 has been renamed as MyEvenFabric successfully
   ```

Disabling the Port Grouping policy

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **ag --policydisable** command.

```
switch:admin> ag --policydisable pg
.
```

Port Grouping policy modes

You can modify certain default behavior such as the following within a port group:

- **Login Balancing (LB)**

  If login balancing mode is enabled for a port group and an internal port (F_Port) goes offline, logins in the port group are redistributed among the remaining internal ports. Similarly, if an external port (N_Port) comes online, port logins in the PG are redistributed to maintain a balanced external-to-internal port ratio. Please note the following facts about LB mode:

  - LB is disruptive. However, you can minimize disruption by disabling or enabling rebalancing of internal ports on internal-port-offline or external-port-online events.
  - You must be explicitly enable LB on a port group.
  - Internal ports can be directly added to port groups that have Login Balancing mode enabled.

- **Managed Fabric Name Monitoring (MFNM)**

  Fabric Name Monitoring mode automatically detects whether all the external ports (N_Ports) within a port group are physically connected to the same physical or virtual fabric. Once a misconnection is detected there are two methods to handle it, depending on the operating mode. For “default” mode a message is logged into RASLOG. For “managed” mode (MFNM), automatic failover disables on all external ports within the external port group.

  In both default and managed mode, the system queries the fabric name once every 120 seconds to detect inconsistencies such as a port group being connected to multiple fabrics. You can configure the monitoring timeout value to something other than 120 seconds using the **ag –pgfnmtov** command. Refer to “Setting the current fabric name monitoring timeout value” on page 17.

Creating a port group and enabling login balancing mode

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --pgcreate** command with appropriate operands to create a port group. In the following example, a port group named “FirstFabric” is created that includes external ports (N_Ports) 1 and 3 and has login balancing enabled.

```
switch:admin> ag --pgcreate 3 “1;3” -n FirstFabric1 -m “lb”
Port Group 3 created successfully
```

3. Enter the **ag --pgshow** command to verify the port group was created.

```
switch:admin> ag --pgshow
PG_ID PG_Name      PG_Mode  N_Ports   F_Ports
-------------------------------------------------
0     pg0          lb,mfnm  none      none
```

```
2     SecondFabric    -     0;2       4;5;6
3     FirstFabric    lb     1;3       10;11
```

Rebalancing internal ports (F_Ports)

To minimize disruption that could occur once internal ports (F_Ports) go offline or when additional external ports (N_Ports) are brought online you can modify the default behavior of the automatic login balancing feature by disabling or enabling rebalancing of internal ports when internal port or external port online events occur.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **agautomapbalance --enable** command with appropriate operands to enable automatic login redistribution of internal ports (F_Ports). In the following example, rebalancing of internal ports in port group 1 in the FC SAN Module is enabled when an internal-port-online event occurs.

   ```
   switch:admin> agautomapbalance --enable -fport -pg 1
   ```

3. Enter the **agautomapbalance --disable - all** command with appropriate operands to disable automatic login distribution of external ports (N_Ports) for all PGs in the FC SAN Module when an external port online event occurs.

   ```
   switch:admin> agautomapbalance --disable -nport -all
   ```

4. Enter the **agautomapbalance --disable - all** command with appropriate operands to disable automatic login distribution of internal ports for all port groups in the FC SAN Module when an internal port online event occurs.

   ```
   switch:admin> agautomapbalance --disable -fport -all
   ```

5. Enter the **agautomapbalance --show** command to display the automatic login redistribution settings for port groups. In the following example, there are two port groups, 0 and 1.

   ```
   switch:admin> agautomapbalance --show

   AG Policy: pg
   ----------------------------------------
   PG_ID LB mode nport fport
   ----------------------------------------
   0 Enabled     Enabled    Disabled
   1 Disabled        -          -
   ----------------------------------------
   ```

   This command also displays the automatic login redistribution settings for external ports (N_Ports) and internal ports (F_Ports) as shown in the following example.

   ```
   switch:admin> agautomapbalance --show

   ------------------------------------------------
   AG Policy: Auto
   ------------------------------------------------
   automapbalance on N_Port Online Event: Disabled
   automapbalance on F_Port Offline Event: Enabled
------------------------------------------------
   ```

Enabling Managed Fabric Name Monitoring mode

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **ag --pgsetmodes** command with appropriate operands to enable MFNM mode. In the following example, MFNM mode is enabled for port group 3.

```
switch:admin> ag --pgsetmodes 3 "mfnm"
Managed Fabric Name Monitoring mode has been enabled for Port Group 3
```

Disabling Managed Fabric Name Monitoring mode

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --pgdelmodes** command with appropriate operands to disable MFNM mode. In the following example, MFNM mode is disabled for port group 3.

```
switch:admin> ag --pgdelmodes 3 "mfnm"
Managed Fabric Name Monitoring mode has been disabled for Port Group 3
switch:admin> ag --pgshow
PG_ID PG_Name PG_Mode N_Ports F_Ports
-----------------------------------------------
0 pg0 lb,mfnm 0;2 4;5;6
3 FirstFabric lb 1;3 10;11
-----------------------------------------------
```

Displaying the current fabric name monitoring timeout value

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --pgfnmtov** command.

```
switch:admin> ag --pgfnmtov

Fabric Name Monitoring TOV: 120 seconds
```

Setting the current fabric name monitoring timeout value

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --pgfnmtov** command, followed by a value.

```
switch:admin> ag --pgfnmtov 100
```

This sets the timeout value to 100 seconds.

Port Grouping policy considerations

Following are the considerations for the Port Grouping policy:

- A port cannot be a member of more than one port group.
- The PG policy is enabled by default. A default port group “0” (PG0) is created, which contains all ports on the FC SAN Module.
- APC policy and PG policy are mutually exclusive. You cannot enable these policies at the same time.
- If an external port (N_Port) is added to a port group or deleted from a port group and login balancing is enabled or disabled for the port group, the external port maintains its original failover or failback setting. If an external port is deleted from a port group, it automatically gets added to port group 0.
- When specifying a preferred secondary external port (N_Port) for a port group, the second port must be from the same group. If you specify an external port as a preferred secondary port and it already belongs to another port group, the operation fails. Therefore, it is recommended to form groups before defining the preferred secondary path.
- If the PG policy is disabled while the FC SAN Module is online, all the defined port groups are deleted, but the port mapping remains unchanged. Before disabling the PG policy, you should save the configuration using the **configupload** command in case you might need this configuration again.
- If external ports (N_Ports) connected to unrelated fabrics are grouped together, external port failover within a port group can cause the internal ports (F_Ports) to connect to a different fabric and the ports may lose connectivity to the targets they were connected to before the failover, thus causing I/O disruption as shown in Figure 4 on page 13. Ensure that the port group mode is set to Managed Fabric Name Monitoring (MFNM) mode. This monitors the port group to detect connection to multiple fabrics and disables failover of the external ports in the port group. For more information on MFNM, refer to “Enabling Managed Fabric Name Monitoring mode” on page 17.

Failover

Failover ensures maximum uptime for the servers. Failover is enabled by default and is enforced during power-up. Failover allows internal ports (F_Ports) to automatically remap to an online external port (N_Port) if the primary external port goes offline. If multiple external ports are available for failover, failover evenly distributes the internal ports to available internal ports belonging to the same external port group. If no other external is available, failover does not occur.

The Dell FC SAN Module provides an option to specify a secondary failover external port for an internal port. This external port is called the preferred secondary port for failover. If you specify a preferred secondary external port for any of the internal ports, and if the primary mapped external port goes offline, the internal ports will fail over to the preferred secondary external port (if it is online), then re-enable.

The preferred secondary external port (N_Port) that you specify must be online; otherwise, the internal ports (F_Ports) will become disabled. The preferred secondary port is defined per internal port. For example, if two internal ports are mapped to a primary external port 1, you can define a secondary port for one of those internal ports and not define a secondary port for the other internal port. Refer to “Adding a preferred secondary external port (N_Port)” on page 21 for more information.

Failover configurations

The following sequence describes how a failover event occurs:

- An external port (N_Port) goes offline.
- All internal ports (F_Ports) mapped to that external port are disabled.
- If the external port Failover configuration is enabled and a preferred secondary port is specified for the internal port (and that external port is online), the internal port fails over to the secondary external port, then re-enables. If the preferred port is not set, then the internal port fails over to any available external port in the port group. Otherwise the internal ports will be evenly distributed among available online external ports that are part of the same port group.

Example: Failover configuration

The example in "Example 1 and 2 Failover behavior" on page 20 shows the failover behavior in a scenario where two fabric ports go offline, one after the other. Note that this example assumes that no preferred secondary external port (N_Port) is set for any of the internal ports (F_Ports).

- First the Edge switch F_A1 port goes offline, as shown in Figure 5 on page 20 Example 1 (left), causing the corresponding N_1 port to be disabled.

  The ports mapped to N_1 fail over; F_1 fails over to N_2 and F_2 fails over to N_3.

- Next the F_A2 port goes offline, as shown in Figure 5 on page 20 Example 2 (right), causing the corresponding N_2 port to be disabled.

  The ports mapped to N_2 (F_1, F_3, and F_4) fail over to N_3 and N_4. Note that the internal ports are evenly distributed to the remaining online external ports and that the F_2 port did not participate in the failover event.

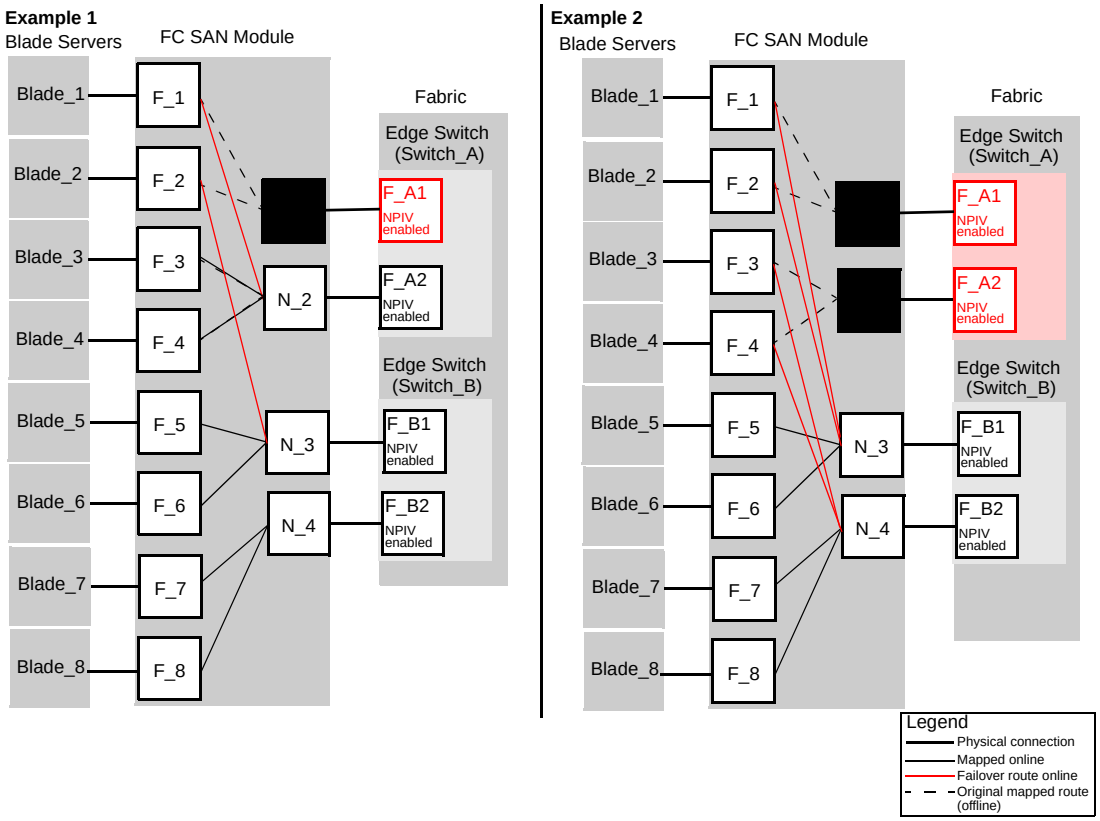


FIGURE 5 **Example 1 and 2 Failover behavior**

Enabling and disabling Failover on an external port (N_Port)

Use the following steps to enable or disable failover policy on an external port.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --failovershow** *n_portnumber* command to display the failover setting.

```
switch:admin> ag --failovershow 13
Failover on N_Port 13 is not supported
```

3. Enter the **ag --failoverenable** *n_portnumber* command to enable failover.

```
switch:admin> ag --failoverenable 13
Failover policy is enabled for port 13
```

4. Enter the **ag --failoverdisable** *n_portnumber* command to disable failover.

```
switch:admin> ag --failoverdisable 13
Failover policy is disabled for port 13
```

Enabling and disabling Failover for a port group

Failover policy can be enabled on a port group. To enable or disable use the following steps to enable or disable failover on all the external ports (N_Ports) belonging to the same port group.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --failoverenable -pg** *pgid* command to enable failover.

```
switch:admin> ag --failoverenable -pg 3
Failover policy is enabled for port group 3
```

3. Enter the **ag --failoverdisable -pg** *pgid* command to disable failover.

```
switch:admin> ag --failoverdisable -pg 3
Failover policy is disabled for port group 3
```

Adding a preferred secondary external port (N_Port)

Internal ports (F_Ports) automatically fail over to any available external port. Alternatively, you can specify a preferred secondary external port for mapping in case the primary external port has failed. The internal ports must have a primary external port mapping before a secondary external port can be configured.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --prefset** command with the *"F_Port1;F_Port2; ..." N_Port* operands to add the preferred secondary internal ports to the specified external port.

   The internal ports must be enclosed in quotation marks and the port numbers must be separated by a semicolon, for example:

```
switch:admin> ag --prefset "3;9" 4
Preferred N_Port is set successfully for the F_Port[s]
```

NOTE
Preferred mapping is not allowed when login balancing mode is enabled for a port group, so there is no preferred secondary external port. All external ports are the same when login balancing is enabled.

Deleting internal ports from a preferred secondary external port

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --prefdel** command with the "F_Port1;F_Port2;..." External port (N_Port) operands to delete internal ports (F_Ports) from an external port.

   The list of internal ports must be enclosed in quotation marks. Port numbers must be separated by a semicolon. In the following example, internal ports 3 and 9 are deleted from preferred secondary external port 4.

```
switch:admin> ag --prefdel  "3;9" 4
Preferred N_Port is deleted successfully for the F_Port[s]
```

Failback

Failback policy provides a means for ports that have failed over to move back to their intended external ports (N_Ports) when these ports come back online. When Failback is enabled, all internal ports (F_Ports) automatically reroute back to these primary-mapped external ports. Failback is an external port parameter and is enabled by default.

Only the originally mapped internal ports fail back. In the case of multiple external port failures, only internal ports that were mapped to the recovered external port experience failback. The remaining internal ports are not redistributed among the online external ports during the failback.

Failback configurations in the FC SAN Module

The following sequence describes how a failback event occurs:

- When an external port comes back online, with Failback enabled, the internal ports that were originally mapped to it are disabled.
- The internal port is rerouted to the primary mapped external port, and then re-enabled.
- The host establishes a new connection with the fabric.

Example: Failback configuration

In Example 3, described in Figure 6 on page 23, N_1 remains disabled because the corresponding F_A1 port is offline. However, N_2 comes back online. See Figure 5 on page 20 for the original fail over scenario.

The ports F_1 and F_2 are mapped to N_1 and continue routing to N_3. Ports F_3 and F_4, which were originally mapped to N_2, are disabled and rerouted to N_2, and then enabled.

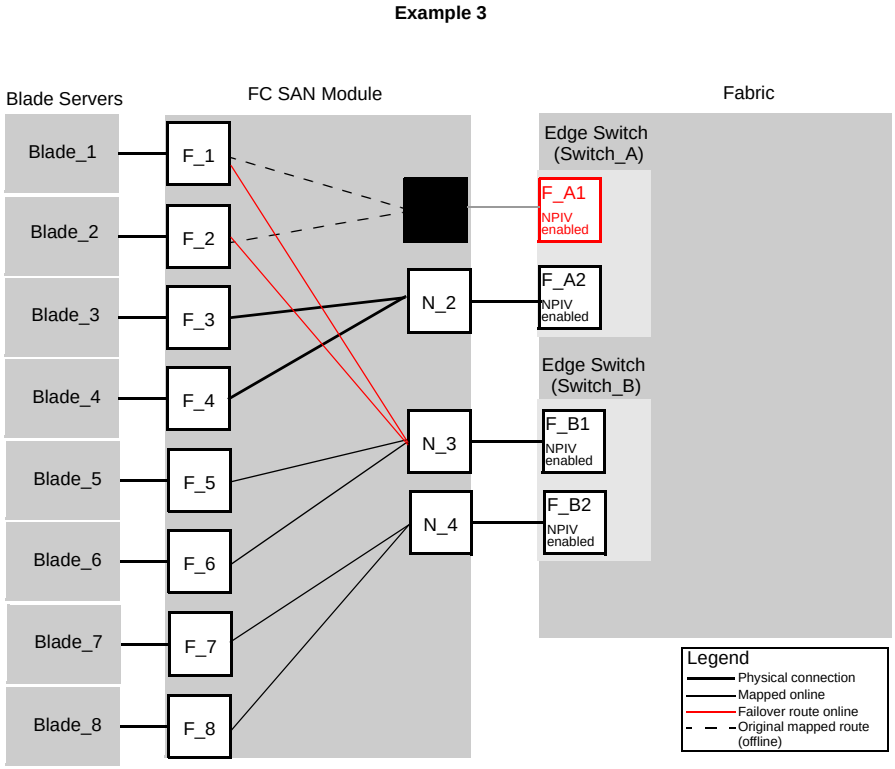


FIGURE 6 Failback behavior

Enabling and disabling Failback on an external port (N_Port)

Use the following steps to enable or disable Failback on external ports.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Enter the **ag --failbackshow** *n_portnumber* command to display the failover setting.

```
switch:admin> ag --failbackshow 13
Failback on N_Port 13 is not supported
```

3. Use the following commands to enable or disable Failback:
   - Enter the **ag --failbackenable** *n_portnumber* command to enable failback.

```
switch:admin> ag --failbackenable 13
Failback policy is enabled for port 13
```

   - Enter the **ag –failbackdisable** n_portnumber command to disable failback.

```
switch:admin> ag --failbackdisable 13
Failback policy is disabled for port 13
```

Enabling and disabling Failback for a port group

Use the following steps to enable or disable Failback policy on all the external ports (N_Ports) belonging to the same port group.

1. Connect to the FC SAN Module and log in using an account assigned to the admin role.
2. Use the following commands to enable or disable Failback for a port group:
   - Enter the **ag --failbackenable pg** *pgid* command to enable failback on a port group.

     ```
     switch:admin> ag --failbackenable -pg 3
     Failback policy is enabled for port group 3
     ```

   - Enter the **ag --failbackdisable pg** *pgid* command to disable failback on a port group.

     ```
     switch:admin> ag --failbackdisable -pg 3
     Failback policy is disabled for port group 3
     ```

Chapter

Fabric Configuration with the Dell FC SAN Module 4

In this chapter

Connectivity of multiple devices overview

This chapter describes how to connect multiple FC SAN Modules to a switch, discusses Edge switch compatibility, port requirements, NPIV HBA, and interoperability.The FC SAN Module does not support daisy chaining when two such devices are connected to each other in a loop configuration. The Dell FC SAN Module can connect to third-party fabrics with the following firmware versions:

- McDATA M-EOSc v9.6.2 or later and M-EOSn v9.6 or later.
- Cisco MDS Switches with SAN OS v3.1.
- Brocade Fabric OS

The FC SAN Module does not support loop devices and FICON channels/control unit connectivity. It can connect to NPIV-enabled HBAs, or NPIV-aware internal ports (F_Ports). It supports NPIV industry standards per FC-LS-2 v1.4.

Fabric and Edge switch configuration

To connect devices to the fabric, configure the fabric and Edge switches within the fabric that will connect to the FC SAN Module using the following parameters. These parameters apply to Brocade Fabric OS, M-EOS, and Cisco-based fabrics:

- Install and configure the external switch as described in the switch's Hardware Reference manual before performing these procedures.
- Verify that the interop mode parameter is set to Native mode.
- Configure the internal ports (F_Ports) on the Edge switch to which FC SAN Module is connected as follows:
  - Enable NPIV.
  - Disable long distance mode.
  - Allow multiple logins for M-EOS switches. The recommended fabric login setting is the maximum allowed per port and per switch.
- Use only WWN zoning for devices functioning behind NPIV mode.

- If DCC security is being used on Edge switches that directly connect to the FC SAN Module, make sure to include the module WWN or the port WWN of the external ports (N_Ports). Also include the HBA WWNs that will be connected to internal ports (F_Ports) to the ACL list in the ACL policy. It is recommended to use FC SAN Module ADS policy instead of the DCC policy on the Edge switch.
- Allow inband queries for forwarded fabric management requests from the hosts. Add the FC SAN Module WWN to the access list if inband queries are restricted.

Before connecting the FC SAN Module to Brocade switches, disable the Brocade Fabric OS Management Server Platform Service to get accurate statistical and configuration fabric data,

Verifying the switch mode

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the **switchShow** command to display the current switch configuration.

   The following example shows a switch in the Fabric OS Native mode where **switchMode** displays as Native.

```
switch:admin> switchshow
switchName:     switch
switchType:     43.2
switchState:    Online
switchMode:     Native
switchRole:     Principal
switchDomain:   1
switchId:       fffc01
switchWwn:      10:00:00:05:1e:03:4b:e7
zoning:         OFF
switchBeacon:   OFF

Area Port Media Speed State     Proto
==================================
  0   0   --    N4   No_Module
  1   1   cu    N4   Online          F-Port  50:06:0b:00:00:3c:b7:32
  2   2   cu    N4   Online          F-Port  10:00:00:00:c9:35:43:f5
  3   3   cu    AN   No_Sync
  4   4   cu    AN   No_Sync          Disabled (Persistent)
  5   5   cu    N4   Online          F-Port  50:06:0b:00:00:3c:b4:3e
  6   6   cu    N4   Online          F-Port  10:00:00:00:c9:35:43:f3
  7   7   cu    AN   No_Sync          Disabled (Persistent)
  8   8   cu    AN   No_Sync
  9   9   cu    AN   No_Sync          Disabled (Persistent)
 10  10   cu    AN   No_Sync          Disabled (Persistent)
 11  11   cu    AN   No_Sync          Disabled (Persistent)
 12  12   cu    AN   No_Sync          Disabled (Persistent)
 13  13   cu    AN   No_Sync          Disabled (Persistent)
 14  14   cu    AN   No_Sync          Disabled (Persistent)
 15  15   cu    AN   No_Sync          Disabled (Persistent)
 16  16   cu    AN   No_Sync          Disabled (Persistent)
 17  17   --    N4   No_Module
 18  18   --    N4   No_Module
 19  19   --    N4   No_Module
 20  20   --    N4   No_Module
 21  21   id    N4   Online          E-Port  segmented,(zone conflict)(Trunk
master)
 22  22   id    N4   Online          E-Port  (Trunk port, master is Port 21 )
```

```
23  23   id    N4   Online          E-Port  (Trunk port, master is Port 21 )
```

See Table 1 on page 3 for a description of the port state.

If the switch is in Native mode, you can enable NPIV mode; otherwise, set the switch to Native mode, and then reboot the switch.

Enabling NPIV on M-EOS switches

1. Connect to the switch and log in as admin on the M-EOS McDATA switch.
2. Enable the MS services by entering the following command:

   ```
   config OpenSysMs setState <osmsState>
   ```

   where

   osmsState — Can be *enable* or *1* for the enabled state or *disable* or *0* for the disabled state.

3. Enable NPIV functionality on the Edge fabric ports so that multiple logins are allowed for each port. Enter the following command on the M-EOS switch to enable NPIV on the specified ports.

   ```
   config NPIV
   ```

   Your M-EOS switch is now ready to connect.

NOTE
When connected to Brocade FOS-based switches, you can run the **agshow** command to display information registered with the fabric.

Connectivity to Cisco Fabrics

When connecting an FC SAN Module to a Cisco fabric, make sure that NPIV function is enabled on the Cisco switch ports connected to the Dell 8/4Gbps FC SAN Module. NPIV is enabled by default on Cisco MDS switches with SAN OS 3.1 or higher. For additional information, refer to Dell technical brief: *Connecting Dell PowerEdge M-Series Blades to a Cisco SAN Fabric*.

Enabling NPIV on a Cisco switch

1. Log in as admin on the Cisco MDS switch.
2. Enter the **show version** command to determine that you are using the correct SAN-OS version and to see if NPIV is enabled on the switch.
3. Enter the following commands to enable NPIV:

   ```
   conf t
   enable npiv
   ```

4. Press **Ctrl-Z** to exit.

5. Enter the following commands to save the MDS switch connection:

   `copy run start`
   Your Cisco switch is now ready to connect to a Dell FC SAN Module.

Appendix

Troubleshooting

A

This appendix provides troubleshooting instructions.

TABLE 5 Troubleshooting

Problem	Cause	Solution
NPIV disabled on Edge switch ports	Inadvertently turned off	On the Edge switch, enter the **portCfgShow** command. Verify that NPIV status for the port to which FC SAN Module is connected is ON. If the status displays as "--" NPIV is disabled. Enter the **portCfgNpivPort** *port_number* command with the **1** operand to enable NPIV. Repeat this step for each port as required.
LUNs are not visible	Zoning on fabric switch is incorrect. Port mapping on the NPIV Switch is incorrect. Cabling not properly connected.	Verify zoning on the Edge switch. Verify that internal ports (F_Ports) are mapped to an online external port (N_Port). Perform a visual inspection of the cabling, check for issues such as wrong ports, twisted cable, or bent cable. Replace the cable and try again. Ensure the internal port on the FC SAN Module is enabled and active.
Failover is not working	Failover disabled on external port (N_Port).	Verify that the failover and failback policies are enabled, as follows: Enter the **ag --failoverShow** command with the *port_number* operand. Enter the **ag --failbackShow** command with the *port_number* operand. Command returns "Failback (or Failover) on N_Port *port_number* is supported." If it returns, "Failback (or Failover) on N_Port *port_number* is not supported." See "Adding a preferred secondary external port (N_Port)" on page 21.

A Troubleshooting

Appendix

Command Reference

B

Understanding role-based access control

The FC SAN Module commands use Role-Based Access Control (RBAC) to control access to all FC SAN Module OS operations.

Seven roles are supported, as defined in Table 6. Role definitions are guided by perceived common operational situations and the operations and effects a role is permitted to have on a fabric and individual fabric elements.

TABLE 6 Role definitions

Role Name	Definition
User	Non-administrative use, such as monitoring system activity. In OS v6.2.0 and later, the user account gains access to Fabric ID 128. This is the default Logical Fabric after a firmware upgrade.
Operator	A subset of administrative tasks typically required for routine maintenance operations.
SwitchAdmin	Administrative use excluding security, user management, and zoning.
ZoneAdmin	Zone management only.
FabricAdmin	Administrative use excluding user management and Admin Domain management.
BasicSwitchAdmin	A subset of administrative tasks, typically of a more limited scope and effect.
Admin	May perform all administrative tasks, including encryption and chassis commands.
SecurityAdmin	Administrative use including admin, encryption, security, user management, and zoning.

Additional command restrictions apply depending on whether Virtual Fabrics or Admin Domains are enabled in a fabric.

NOTE
Virtual Fabrics and Admin Domains are mutually exclusive and are not supported at the same time on a switch. To use Admin Domains, you must first disable Virtual Fabrics; to use Virtual Fabrics, you must first delete all Admin Domains. Use **ad --clear -f** to remove all Admin Domains.

Understanding Virtual Fabric restrictions

In OS v6.2.0 and later, all commands are subject to additional RBAC enforcement with regard to Virtual Fabric contexts and switch types. Commands can be executed in one or more of the contexts described in Table 7. Execution of chassis commands requires chassis permissions.

TABLE 7 Virtual Fabric contexts

Context type	Definition
Switch context	Command applies to the current logical switch only, or to a specified logical switch.
Chassis context	Command applies to the chassis on which it is executed.
Switch and Chassis context	Command can be executed in a logical switch context or in a chassis context.
Disallowed	Command is not supported in Virtual Fabric mode.

Switch commands are further defined by the switch type restrictions as described in Table 8. Switch type restrictions are not applicable to commands that require chassis permissions.

TABLE 8 Switch Types

Switch Type	Definition
All Switches	Command can be executed in any switch context.
Base Switch Only	Command can be executed only on the base switch.
Default Switch Only	Command can be executed only on the default switch.
N/A	Command is a chassis command or not supported in Virtual Fabric mode.

In a Virtual Fabric environment where contexts are enforced, the following Virtual Fabric restrictions apply to the RBAC permissions specified in Table 6. Refer to **userConfig** help for more information on configuring user account access permissions in a Virtual Fabric environment.

- Any given role is allowed to execute all switch commands to which the role is authorized in the account's home context. The default home context is the default logical fabric FID 128.
- You can change an account's home context to a specified FID and configure the account permissions to access additional Logical Switches specified in the user's Fabric ID list.
- Accounts with user or admin permissions can be granted chassis permissions. A user account with the chassis role can execute chassis-level commands at the user RBAC access level. An admin account with the chassis role can execute chassis-level commands at the admin RBAC access level.

Understanding Admin Domain restrictions

A subset of commands is subject to Admin Domain restrictions that may be in place. In order to execute an AD-restricted command on a switch or device, the switch or device must be part of a given Admin domain, and the user must be logged into that Admin Domain.

Six Admin Domain types are supported, as defined in Table 9.

TABLE 9 AD types

AD Type	Definition
Allowed	Allowed to execute in all ADs.
PhysFabricOnly	Allowed to execute only in AD255 context (and the user should own access to AD0-AD255 and have admin RBAC privilege).
Disallowed	Only allowed to execute in AD0 or AD255 context, not allowed in AD1-AD254 context.
PortMember	All control operations allowed only if the port or the local switch is part of the current AD. View access allowed if the device attached to the port is part of current AD.
AD0Disallowed	Allowed to execute only in AD255 and AD0 (if no ADs are configured).
AD0Only	Allowed to execute only in AD0 when ADs are not configured.

Using the command line interface

This appendix describes using the command line interface (accessed via Telnet, SSH, or serial console) to manage the Dell 8/4Gbps FC SAN Module. The command line interface (CLI) enables an administrator to monitor and manage the FC SAN Module from a standard workstation.

Selected commands must be issued from a secure Telnet or SSH session, as indicated in the command description in this manual. Access is controlled by a switch-level password for each access level. The commands available through the CLI are based on the user's login role and the license keys used to unlock certain features.

The documentation for each command includes a synopsis of its syntax, a description of command use, and a set of examples. The same information can be accessed by issuing help command for the module. This command displays the help page for the specified command. For example, to display the help page for ad, type:

```
switch:admin> help ad
```

Commands

Commands are provided in alphabetical order.

configUpload

Uploads system configuration data to a file.

Synopsis **configupload**

configupload [**-all**] [**-p ftp** | **-ftp**] [*"host","user","path",["passwd"]]

configupload [**-all**] [**-p scp**| **-scp**] [*"host","user","path"*]

configupload [**-all**] [**-force**] [**-local** | **USB** |**-U**] [*"file"*]

configupload [**-fid** *FID* | **-chassis** | **-all**] [**-p ftp** | **-ftp**] [*"host","user","path",["passwd"]*]

configupload [**-fid** *FID* | **-chassis** | **-all**] [**-p scp**| **-scp**] [*"host","user","path"*]

configupload [**-fid** *FID* | **-chassis** | **-all**] [**-force**] [**-local** | **USB** |**-U**] [*"file"*]

configupload [**-vf**] [**-p ftp** | **-ftp**] [*"host","user","path",["passwd"]*]

configupload [**-vf**] [**-p scp**| **-scp**] [*"host","user","path"*]

configupload [**-vf**] [**-force**] [**-local** | **USB** |**-U**] [*"file"*]

Description This command uploads configuration data to a file. Two types of configuration files can be uploaded with this command: Virtual Fabric configuration parameters and system configuration parameters.

Use the **-vf** option to upload Virtual Fabric configuration parameters. The Virtual Fabric configuration includes logical switch definitions, Virtual Fabric status (enabled or disabled), and the internal port (F_Port) trunking ports. The file should be named switch-conf_xx.txt to distinguish it from the regular system configuration (config.txt). The xx indicates the platform ID. The platform ID is the same as the first two digits of the "switchType" parameter displayed by **switchShow**. Virtual Fabric configuration data can only be shared between switches that belong to the same platform type and share the same platform ID. Refer to **configDownload** for more information on the Virtual Fabric configuration.

The system configuration data is uploaded separately. It is grouped into chassis information and switch information. Each configuration type is managed separately and the behavior of **configUpload** depends on the environment in which the command is executed and which part of the system configuration you wish to upload.

- In a Virtual Fabric environment, when executed without chassis permissions, this command uploads the current logical switch configuration only. An Admin user with chassis permissions can use additional parameters to perform the following selective configuration uploads:
  - Upload the switch configuration of a specified logical switch (**-fid** *FID*).
  - Upload the chassis configuration only (**-chassis**).
  - Upload the entire system configuration including the data for all logical switches and for the chassis (**-all**).

  The interactive version of the command (no operands) prompts for input on only the parameters the user is allowed to execute.

- In a non-Virtual Fabric environment, this command by default uploads the switch configuration only. Additional options support uploading the chassis configuration (**-chassis**) or all of the system's configuration data, including chassis and switch configurations (**-all**). Chassis permissions are required. The **-fid** option is not valid.

You can use FTP or SCP to upload configuration files to an external host, or you can save the configuration in a predetermined directory on the local chassis or on an attached USB device. If the specified file already exists, this command prompts you to overwrite the file. Specify **-force** to overwrite the file without confirmation. When the local chassis is chosen as the destination, the resulting file is written to both primary and secondary partitions, and on enterprise-class platforms, to both Active and Standby Control Processors (CPs).

Notes The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 and "Understanding Admin Domain restrictions" on page 33 for details.

Do not manually edit a configuration or a switch-conf.xx file after uploading the file and before downloading the file to a switch. Manual editing bypasses sanity checks for some configuration parameters and results in unpredictable system behavior

Operands The following operands are supported:

-p ftp | **-ftp** or **-p scp** | **-scp**
: Specifies the data transmission protocol as either File Transfer Protocol (FTP) or Secure Copy Protocol (SCP). If no protocol is specified, the protocol defaults to FTP.

-vf
: Uploads the Virtual fabric configuration to a file. You must specify a filename when uploading this file. It is recommended to name this file switch-conf_xx.txt (where xx indicates the platform ID) to distinguish this file from the system configuration (config.txt). Use **switchShow** to determine the platform ID of the system. The platform ID in the header of the configuration file is the same as the first two digits of the switchType parameter in the **switchShow** output. You cannot use the **-vf** option with any of the regular configuration upload options (**-fid**, **-chassis**, **-all**).

-fid *FID*
: Uploads switch configuration data from a logical switch specified by its fabric ID. This parameter is valid only in a Virtual Fabric environment and requires chassis permissions.

-chassis
: Uploads chassis configuration only.

-all
: Uploads all system configuration data including chassis and switch configuration for all logical switches.

"*host***"**
: Specifies the name or the IP address of the external host to which to upload the configuration. To be able to mention the FTP server by name, you need to set up one or more DNS servers with **dnsConfig**. Quotation marks are optional.

"*user***"**
: Specifies the login name for the external host. Quotation marks are optional.

"*path***"**	Specifies the file name and path of the configuration file. Absolute path names may be specified using a forward slash (/). Relative path names upload the file to the login account's home directory on UNIX hosts and into the directory on which the FTP server is running on Windows hosts. This operand is valid only when the file is uploaded to an external host. Quotation marks are optional.
"*passwd***"**	Specifies the account password when you use the FTP protocol. Quotation marks are optional.
-local	Uploads a specified configuration file to a predetermined directory on the local chassis. This option requires a file name.
-USB | **-U**	Uploads a specified configuration file to a predetermined directory on an attached USB device. This option requires a file name.
"*file*"	Specifies the file name. Quotation marks are optional. This parameter is valid only with the **-local** or **-USB** options, each of which stores files in a predetermined directory on the local chassis or on an attached USB device. Therefore, subdirectories and absolute path names are not permitted.
-force	Overwrites an existing file without confirmation. This parameter is valid only with the **-local** or **-USB** options.

When invoked without operands or without "*host*" or "file" parameters, **configUpload** runs in interactive mode. When invoked without any of the parameters **-all**, **-fid**, or **-chassis**, only the switch configuration for the current logical switch is uploaded.

Examples To upload the switch configuration interactively from a switch that is not enabled for Virtual Fabrics:

```
switch:admin> configupload
Protocol (scp, ftp, local) [ftp]:
Server Name or IP Address [host]: 192.168.38.245
User Name [user]: jdoe
File Name [<home dir>/config.txt]:
Password:

configUpload complete: All config parameters are uploaded
```

To upload the switch configuration that belongs to a logical switch with FID 100:

```
switch:admin> configupload
Protocol (scp, ftp, local) [ftp]:
Server Name or IP Address [host]: 10.32.220.100
User Name [user]: jdoe
File Name [<home dir>/config.txt]: config.fid100.txt
Section (all|chassis|FID# [all]): 100
Password:

configUpload complete: All config parameters are uploaded
```

To upload the configuration for the entire chassis to a local file from the command line forcing an overwrite:

```
switch:admin> configupload -chassis -local -force config.txt

configUpload complete: All config parameters are uploaded
```

To upload the configuration for the current logical switch to an external FTP server:

```
switch:admin> configupload -ftp 192.168.38.245,jdoe,config.txt,password
```

To upload all system configuration data to an external FTP server:

```
switch:admin> configupload -all -ftp 192.168.38.245,jdoe,config.txt,password
```

To upload the system configuration file for a logical switch with FID 8 to an attached USB device:

```
switch:admin> configupload -fid 8 -ftp -USB config.txt
```

To upload the Virtual Fabric configuration of the current platform to an external FTP server:

```
switch:admin> configupload -vf -p ftp 10.32.248.119,jdoe,/temp/switch-conf.66.txt,password
```

Diagnostics The configuration upload might fail for one or more of the following reasons:

- The host name is not known to the switch.
- The host IP address cannot be contacted.
- The user does not have permission on the host.
- The FTP server is not running on the host.

configDownload

Downloads configuration data to the system.

Synopsis **configdownload**

configdownload [**- all**] [**-p ftp** | **-ftp**] [*"host"*,*"user"*,*"path"* [,*"passwd"*]]

configdownload [**- all**] [**-p scp**| **-scp**] [*"host"*,*"user"*,*"path"*]

configdownload [**- all**] [**-local** | **-USB** | **-U** [*"file"*]]

configdownload [**-fid** *-FID* [**-sfid** *FID*] | **-chassis** |**- all**] [**-p ftp** | **-ftp**] [*"host"*,*"user"*,*"path"* [,*"passwd"*]]

configdownload [**-fid** *-FID* [**-sfid** *FID*] | **-chassis** |**- all**] [**-p scp**| **-scp**] [*"host"*,*"user"*,*"path"*]

configdownload [**-fid** *-FID* [**-sfid** *FID*] | **-chassis** |**- all**] [**-local** | **-USB** | **-U** [*"file"*]]

configdownload [**-vf**] [**-p ftp** | **-ftp**] [*"host"*,*"user"*,*"path"* [,*"passwd"*]]

configdownload [**-vf**] [**-p scp**| **-scp**] [*"host"*,*"user"*,*"path"*]

configdownload [**-vf**] [**-local** | **-USB** | **-U** [*"file"*]]

Description This command downloads configuration parameters to the local system. Two types of configuration files can be downloaded with this command: Virtual Fabric configuration parameters and system configuration parameters. You must download both types of configuration data for the system to behave as expected. You can use FTP or SCP to download configuration files from a remote host, or you can retrieve the configuration files from a predetermined directory on the local system, or from an attached USB device.

Use the **-vf** option to download the Virtual Fabric configuration parameters. The Virtual Fabric configuration file includes logical switch definitions for a specific platform, the platform ID, Virtual Fabric status (enabled or disabled), and internal port (F_Port) trunking ports. The file should be named switch-conf_xx.txt to distinguish it from the regular system configuration (config.txt). The xx

indicates the platform ID. Virtual Fabric configuration data can only be shared between switches that belong to the same platform type and share the same platform ID. If the platform ID contained in the header of the configuration file does not match the platform ID of the system to which it is downloaded, **configDownload** fails. When you download a switch-conf_xx.txt file, all attributes defined in this file are downloaded to the system and take effect with the exception of LISL ports. The LISL ports on the system are not affected by this download.

The system configuration data is downloaded separately. It is grouped into chassis information and switch information. Each configuration type is managed separately and the behavior of **configDownload** depends on the environment in which the command is executed and which part of the system configuration you wish to download.

- In a Virtual Fabric environment, when executed without chassis permissions, this command downloads the switch configuration to the current logical switch only. An Admin user with chassis permissions can use additional parameters to perform the following selective configuration downloads:
  - Download the switch configuration to a specified logical switch (**-fid** *FID*).
  - Download the switch configuration from a specified logical switch source (**-sfid** *FID*) to a specified logical switch target (**-fid** *FID*).
  - Download the chassis configuration only (**-chassis**).
  - Download the entire configuration including the data for all logical switches and for the chassis (**-all**).

  The interactive version of the command (no operands) prompts for input on only the parameters the user is allowed to execute.
- In a non-Virtual Fabric environment, this command by default downloads the switch configuration. Additional options support downloading the chassis configuration (**-chassis)** or all of the system's configuration data, including chassis and switch configurations (**-all**). Chassis permissions are required. The **-fid,** and **-sfid** options are not valid.

Configuration management supports download of v6.1 or v6.2+ configuration files to a switch running v6.2 firmware, but a v6.2 configuration file is not accepted by a switch running pre-v6.2 firmware. A v6.1 configuration downloaded to a 6.2 system is applied only to the default switch or chassis.

The switch must be disabled for configuration download of all parameters with the exception of SNMP and Fabric Watch.

The following rules apply to configuration download in Virtual Fabric mode:

- When downloading the chassis configuration, the number of logical switches defined in the configuration download must match the number of logical switches currently defined on the switch.
- When downloading the switch configuration, the target FID must be defined in both the configuration download and the current system.
- When downloading the switch configuration from a specified source FID to a target FID, the target FID must be defined on the switch and the source FID and associated configuration must be defined in the configuration download. **In addition, downloading an SFID configuration resets the target FID ports without warning. Caution is advised when using this option.**
- When downloading all configuration parameters, the number of switches defined in the downloaded configuration file must match the number of switches currently defined on the switch. In addition, the following restrictions apply:
  - The switches must be disabled unless you only wish to download SNMP parameters.

- Downloading a configuration file from a system that is not Virtual Fabric-capable to a system in Virtual Fabric mode is not recommended. The configuration is applied to the default switch only, and only to the ports that are part of the default switch.

If an FCS policy is enabled, the following rules and restrictions apply:

- Both [Defined Security Policies] and [Active Security Policies] sections must exist and contain the FCS_POLICY.
- In the [Defined Security Policies] section, at least one member of the FCS_POLICY must be the same as a member in the previous FCS_POLICY.
- In the [Active Security Policies] section, the FCS_POLICY must be exactly the same as the previous FCS_POLICY. Order of members must be maintained.
- If either security policies section has an RSNMP_POLICY, then that section must have a WSNMP_POLICY.
- After the switch is enabled, if the switch is the primary FCS, then its security and zoning information is propagated to all other switches in the fabric.
- After the switch is enabled, if the switch is a non-FCS or a backup FCS, then its security and zoning information will be overwritten by the primary FCS.

Security parameters and the switch's identity cannot be changed by **configDownload**. Parameters such as the switch name and IP address are ignored; they are lines in the configuration file that begin with "boot". Security parameters and version stamp are ignored; they are the lines in the configuration file that begin with "sec".

[License] is only accepted if the boot.mac parameter matches the license ID (WWN) of the switch performing the download; otherwise, it is ignored.

The configuration parameters R_A_TOV, E_D_TOV, WAN_TOV, and MAX_HOPS are interrelated. Assigning a specific value to one or more of these parameters might change the range of allowed values that can be assigned to the other parameters. As a result, you may not be able to set all the values within the range displayed for each parameter. This command validates the modified values of these four parameters and terminates the download operation, if the validation check fails.

This is particularly important when downloading a zoning configuration. Since the new zoning information is added to the current configuration, there might not be any conflicts. If the current zoning configuration is to be replaced, the keyword "clear:" should be inserted into the configuration file immediately before the zoning lines (starting at the line "[Zoning]").

If the configuration file contains the keyword "enable:" followed by a *zone_configuration*, that zoning configuration is enabled in the fabric. If there is no "enable:" keyword in the configuration file or no zoning configuration by that name exists, or if enable fails for any reason (such as dangling aliases), then the following conditions apply:

- The effective configuration remains as it was prior to the configuration download. The "enable:" action is ignored.
- The Defined Configuration changes to reflect the new zoning configuration.

Notes The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to *"Understanding Virtual Fabric restrictions"* on page 32 *and* *"Understanding Admin Domain restrictions"* on page 33 for details.

Do not manually edit a configuration file after uploading the file and before downloading the file to a switch. Manual editing bypasses sanity checks for some configuration parameters and results in unpredictable system behavior.

Operands This command has the following operands:

-p ftp | **-ftp** or **-p scp** | **-scp**

Specifies the data transmission protocol as either File Transfer Protocol (FTP) or Secure Copy Protocol (SCP). If no protocol is specified, the protocol defaults to FTP.

-vf Downloads the Virtual Fabric configuration (switch-conf_xx.txt) instead of the regular system configuration. The switch-con_xx.txt file contains a listing of logical switches configured on the platform specified by the platform ID (xx) and other Virtual Fabric parameters. You cannot use the **-vf** option with any of the system configuration upload options (**-fid**, **-chassis, -all**).

-all Downloads all configuration data, including chassis and switch configuration data.

-fid *FID* Downloads the switch configuration to a logical switch specified by its fabric ID. This operand is valid only in a Virtual Fabric environment and requires chassis permissions. The following optional parameter is supported with the **-fid** operand:

-sfid *FID* Specifies an alternate source switch configuration to be downloaded to the target logical switch specified by **-fid**. When no source FID is specified, the configuration file corresponding to the logical switch **-fid** *FID* is downloaded. When a source FID is specified, the configuration corresponding to the logical switch specified by the source FID is downloaded instead. This parameter allows you to effectively swap logical switch configurations. **Note that all ports in the FID are reset to the default state when downloading data from the source FID.**

-chassis Downloads the chassis configuration only.

"*host***"** Specifies the name or the IP address of the external host, from which to download the configuration. IPv4 and IPv6 addresses are supported. To be able to mention the FTP server by name, you need to set up two DNS servers with **dnsConfig**. Quotation marks are optional.

"*user***"** Specifies the login name for the external host. Quotation marks are optional.

"*path***"** Specifies the file name and path of the configuration file. Absolute path names may be specified using a forward slash (/). Relative path names search for the file in the login account's home directory on UNIX hosts and in the directory on which the FTP server is running on Windows hosts. This operand is valid only when the file is downloaded from an external host. Quotation marks are optional.

"*passwd***"** Specifies the login password when you use the FTP protocol. Quotation marks are optional.

-local Downloads a specified configuration file from a predetermined directory on the local chassis.

-USB | **-U** Downloads a specified configuration file from a predetermined directory on an attached USB device.

"file" A file name in quotation marks, for example, "config.txt". This parameter can be used only with the **-local** or **-USB** option, each of which retrieves files from a predetermined directory on the local chassis or on an attached USB device. Therefore, subdirectories and absolute path names are not permitted.

Examples To download the switch configuration file interactively to the current logical switch from a local directory (no chassis permissions):

```
switch:admin> configdownload
Protocol (scp, ftp, local) [ftp]:
Server Name or IP Address [host]: 192.168.163.233
User Name [user]: admin
Path/Filename [<home dir>/config.txt]:
Section (all|chassis|FID# [all]):

                          *** CAUTION ***

  This command is used to download a backed-up configuration
  for a specific switch.  If using a file  from a  different
  switch, this file's configuration  settings will  override
  any current switch settings.   Downloading a configuration
  file, which was uploaded  from a different type of switch,
  may cause this switch to fail.  A switch reboot might be
  required for some parameter changes to take effect.

  configDownload operation may take several minutes
  to complete for large files.

  Do you want to continue [y/n]: y
    Password:
Activating configDownload: Switch is disabled

configDownload complete: All config parameters are downloaded
```

To download the switch configuration data to the current logical switch from an external FTP server (no chassis permissions):

```
switch:admin> configdownload -ftp 192.168.38.245,jdoe,config.txt,password
```

To download all system configuration data for the chassis and all logical switches (requires chassis permissions):

```
switch:admin> configdownload -all -ftp 192.168.38.245,jdoe,config.txt,password
```

To download the switch configurations to a logical switch with FID 8 from an attached USB device (requires chassis permissions):

```
switch:admin> configdownload -fid 8 -USB config.txt
```

To download the switch configurations belonging to a logical switch with FID 4 to a logical switch with FID 8 from an attached USB device (requires chassis permissions):

```
switch:admin> configdownload -fid 8 -sfid 4 -USB config_fid8.txt
```

To download the Virtual Fabric configuration file using FTP:

```
switch:admin> configdownload -vf -p ftp 10.32.248.119,jdoe,/temp/switch-conf_66.txt,mypassword
```

Diagnostics The configuration download may fail for one or more of the following reasons:

- The switch has not been disabled. Disabling the switch is not necessary for configuration files containing only certain SNMP or Fabric Watch parameters. You may wish to attempt **configDownload** first without disabling the switch, and if there is at least one changed parameter outside of Fabric Watch or SNMP, you are prompted to disable the switch before proceeding.
- The host name is not known to the switch.
- The host IP address cannot be contacted.
- You do not have permission on the host.
- You are running a script that prints something at login.
- The file does not exist on the host.
- The file is not a switch configuration file.
- The FTP server is not running on the host.
- The configuration file contains errors.
- The configuration file's logical switch definitions do not match the definitions on the target switch.

firmwareDownload

Downloads firmware from a remote host, a local directory, or a USB device.

Synopsis To invoke the command in interactive mode:

firmwaredownload

To download FOS firmware over a network:

firmwaredownload [**-s** [**-b** | **-n**]] [**-p ftp** | **scp**] [**-c**] [**-o**] *host*, *user*, *pfile*, *passwd*

To download SAS/SA firmware over a network:

firmwaredownload -a sas | dmm | *application* [**-t** *slotnumber(s)*] [**-p ftp** | **scp**] [**-c**] [**-o**] *host*, *user*, *pfile*, *passwd*

To download SAS firmware over a network and remove the existing SA firmware at the same time:

firmwaredownload -a sas [**-t** *slotnumber(s)*] [**-p ftp** | **scp**] [**-c**] [**-o**] [**-e**] *host*, *user*, *pfile*, *passwd*

To download FOS firmware from a USB device:

firmwaredownload [**-s** [**-b** | **-n**]] [**-U**] [**-c**] [**-o**] *pfile*

To download SAS/SA firmware from a USB device:

firmwaredownload -a sas | dmm | *application* [**-t** *slotnumber(s)*] [**-U**] [**-c**] [**-o**] *pfile*

To download SAS firmware from a USB device and remove the existing SA firmware at the same time:

firmwaredownload -a sas [**-t** *slotnumber(s)*] [**-U**] [**-c**] [**-o**] [**-e**] *pfile*

Description Use this command to download switch firmware from an FTP or SSH server or local NFS directory to nonvolatile storage. Switch firmware can also be downloaded from an external USB device on platforms that support USB.

The new firmware is downloaded in the form of RPM packages. Package names are defined in *pfile* along with other firmware information (time stamp, platform code, version, etc.). These packages are made available periodically to add features or to remedy defects. Contact customer support to obtain information about available firmware versions.

On enterprise-class platforms, this command, by default, downloads the firmware image to both CPs in rollover mode to prevent disruption to application services. This operation depends on High Availability (HA) support. If HA is not available, use the **-s** option to upgrade the CPs one at a time.

All systems supported by this firmware have two partitions of nonvolatile storage (primary and secondary) to store two firmware images. This command always downloads the new image to the secondary partition and then swaps partitions so the secondary partition becomes the primary.

By default, **firmwaredownload** then reboots the system and activates the new image. Finally, it performs a **firmwareCommit** automatically to copy the new image to the other partition. In systems with blade processors (BPs), after the new CP firmware is downloaded to the system and activated, the BP firmware is downloaded to the BP processors if there is a mismatch between the BP and CP firmware.

By default, **firmwareDownload** performs a full install, auto reboot, and auto commit. These modes are selectable only in single CP (**-s**) mode, in which case auto reboot is OFF by default.

For each standalone switch in your fabric, complete all firmware download changes before issuing the **firmwareDownload** command on the next switch to ensure a nondisruptive download.

If **firmwareDownload** is interrupted due to an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another **firmwareDownload**.

Notes

Firmware download procedures may vary depending on which OS version you are migrating from.

The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 and "Understanding Admin Domain restrictions" on page 33 for details.

Operands

The following operands are optional. When invoked without operands, the command goes into interactive mode.

-U Downloads the firmware from an attached USB device. This option is valid only on platforms that support a USB port. Refer to your specific *Hardware Reference Guide* for details. The USB device must be enabled prior to firmware download with the **usbStorage** command. Firmware must be stored under the /firmware directory in the USB file system. On a dual-CP chassis, the USB device must be attached to the active CP. When downloading firmware from a USB device, the **-p** option is ignored.

-s Enables single-CP mode. This mode supports selectively enabling or disabling a full install, auto reboot, and auto commit on bladed and non-bladed systems. On enterprise-class platforms, this mode supports upgrading a single CP. When downloading the main OS firmware, this option disables auto reboot, unless overridden by the **-b** option.

-b Enables auto reboot mode. When single CP mode is enabled and this operand is not specified, **reboot** must be run manually to activate the downloaded image. If auto reboot mode is enabled, the switch reboots automatically after the firmware has been downloaded.

-n	Disables auto commit mode. When auto commit mode is disabled, the **firmwareCommit** command must be executed manually to propagate the downloaded image to both partitions of the storage device.
host	Specify a valid FTP or SSH server name or IP address. IPV4 and IPv6 addresses are supported. The firmware is downloaded from the specified host. If a host is not specified, the firmware is considered accessible on a local directory. To mention an FTP server by name, a DNS server must first be set up with the **dnsConfig** command. If DNS is enabled and a server name is specified, **firmwareDownload** automatically determines whether IPv4 or IPv6 should be used.
user	Specify a user name for FTP or SSH server access. This operand can be omitted, if the firmware is accessible on a local directory, a USB device, or by anonymous FTP server access. A user name other than “anonymous” is required for SSH server access.
pfile	Specify a fully qualified path for the firmware *pfile*. Absolute path names may be specified using forward slashes (/).
passwd	Specify a password. This operand can be omitted, if the firmware is accessible through a local directory or an attached USB device, or if no password is required by the FTP server. This operand is required when accessing an SSH server**.**
-p scp|ftp	Specify the file transfer protocol. Valid values are **ftp** and **scp**. The values are not case-sensitive. If **-p** is not specified, **firmwareCommit** determines the protocol automatically by checking the config.security parameter. When using the USB option, these parameters, if specified, are ignored.
-a fos |*sas*| any *application*	Specify the type of firmware to be downloaded. Accepted values are **fos**, **sas,** or any valid application name. Values are not case-sensitive.
-t *slot_number(s)*	Specify the target slots for the firmware download. Valid values are a list of slot numbers separated by comma.
-c	Disables version compatibility checking. By default, **firmwareDownload** checks if the firmware being downloaded is compatible with other running firmware images in the system. If the firmware version is not compatible, **firmwareDownload** fails. If this option is specified, version compatibility checking is disabled.
-e	Removes all of the installed SA images in the system during SAS firmware download. By default, downloading a SAS image does not remove the installed SA images. If this option is specified, the installed SA images are removed. This option is only valid with the **-a sas** option.
-o	Bypasses the checking of Coordinated HotCode Load (HCL). On single CP systems in interop fabrics, the HCL protocol is used to ensure data traffic is not disrupted during firmware upgrades. This option allows **firmwareDownload** to continue even if HCL is not supported in the fabric or the protocol fails. Using this option may cause traffic disruption for some switches in the fabric.

Examples To download the firmware to an HA switch over a network:

```
switch:admin> firmwaredownload 192.168.166.30,johndoe,/pub/dist/release.plist,12345
The following BP blades are installed in the system.

Slot Name      Versions              Scope of Impact
-----------------------------------------------------------------
  2  FR4-18i   v5.3.0               GigE/FC Fast-write
  7  FR4-18i   v5.3.0               GigE/FC Fast-write
  9  FA4-18    v5.3.0               Virtualization

This command will upgrade both CPs and all BP blade above. If
you want to upgrade a single CP only, use the -s option.

You can run firmwaredownloadstatus to get the status of this
command.

This command will cause the active CP to reset and will require
that existing telnet, secure telnet or SSH sessions be restarted.

Do you want to continue [Y]: y

The firmware is being downloaded to the Standby CP. It may take up to 10
minutes.
```

To download the firmware to both CPs on a dual-CP chassis with an attached USB device (You would execute the same command on a single-CP switch with USB support. Output may vary depending on platform.):

```
switch:admin> firmwaredownload -U v6.2.0

Checking system settings for firmwaredownload...
Protocol selected: USB
Trying address-->AF_INET IP: 127.1.1.8, flags : 2
System settings check passed.

Checking version compatibility...
Version compatibility check passed.

This command will upgrade the firmware on both CP blades. If you want
to upgrade firmware on a single CP only, please use -s option.

You may run firmwaredownloadstatus to get the status of this command.

This command will cause a warm/non-disruptive boot on the active CP,
but will require that existing telnet, secure telnet or SSH sessions
sessions be restarted.
```

To download SAS firmware interactively:

```
switch:admin> firmwaredownload
Type of Firmware (FOS, SAS, or any application) [FOS]:SAS
Target Slots (all, or slot numbers) [all]:
Server Name or IP Address: 192.168.32.10
Network Protocol (1-auto-select, 2-FTP, 3-SCP) [1]:
User Name: userfoo
File Name: /home/userfoo/dist/release.plist
Password:
```

To download SAS firmware without version compatibility checking:

Note that in interactive mode, the options **-a, -p**, and **-t** are invalid and defaults are used. When specified, these options are overridden.

```
switch:admin> firmwaredownload -c
Type of Firmware (FOS, SAS, or any application name) [FOS]: SAS
Targeted Slots (slot numbers): 8
Server Name or IP Address: 192.168.126.250
Network Protocol (1-auto-select, 2-FTP, 3-SCP) [1]:
User Name: userfoo
File Name: /home/userfoo/dist/release.plist
Password:

Verifying the system parameters for firmwaredownload...
System parameters checking passed.

Checking version compatibility...
Version compatibility checking DISABLED.

This command will reboot the selected blades and disrupt the
virtualization applications on these blades.

WARNING: YOU HAVE ELECTED TO DISABLE THE VERSION COMPATIBILITY
CHECKING FEATURE. THIS CAN CAUSE THE VIRTUALIZATION SERVICES
TO STOP WORKING. If you want to  check the version compatibility,
please exit and re-enter this command without the "-c" option.
Do you want to continue [Y]: y
```

To download SAS firmware and remove the installed SA image at the same time:

```
switch:admin> firmwaredownload -a sas -e 192.168.126.250,\
    userfoo,/home/userfoo/dist/release.plist

This command will download "sas" and at the same time, it will
remove all of the installed SA images on the switch.

Do you want to continue [Y]: y
```

Diagnostics

The command checks the network connection and other system parameters before initiating **firmwareDownload**. It may fail if at least one of the following conditions is encountered:

- The host is not reachable from the switch.
- The user does not have permission on *host.*
- The *password* is not specified correctly.
- Indicated firmware does not exist on the host, or is not in the right format, or is corrupted.
- The FTP or SSH service is not running on *host.*
- The platform is not supported by the firmware indicated.
- The USB device may not be plugged in correctly. On standalone switches, the device must be plugged into the switch USB port. On enterprise-class platforms, the USB device must be plugged into the Active CP
- The USB device is not enabled. Use the **usbStorage** command on the switch to enable the USB device. On enterprise-class platforms, the command must be run on the Active CP to enable the USB device.

- The switch is a single-CP switch in an interop fabric and does not support Coordinated HotCode Load.

firmwareDownloadStatus

Displays the status of a firmware download.

Synopsis **firmwaredownloadstatus**

Description Use this command to display an event log that records the progress and status of events during FOS, SAS, and SA **firmwaredownload**. The event log is created by the current **firmwaredownload** command and is kept until another **firmwaredownload** command is issued. There is a timestamp associated with each event.

When downloading SAS or SA in systems with two control processor (CP) cards, you can only run this command on the active CP. When downloading FOS, the event logs in the two CPs are synchronized. This command can be run from either CP.

Note The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 and "Understanding Admin Domain restrictions" on page 33 for details.

Operands none

Examples The following example shows the status of the **firmwaredownload** for an SAS image to the blades in slot 2 and 7.

```
switch:admin> firmwaredownloadstatus
[1]: Thu Jul 28 00:30:49 2007
Slot 2 (SAS): Firmware is being downloaded to the blade. It may take up to 30
minutes.

[2]: Thu Jul 28 00:30:49 2007
Slot 7 (SAS): Firmware is being downloaded to the blade. It may take up to 30
minutes.

[3]: Thu Jul 28 00:37:42 2007
Slot 2 (SAS): Firmware has been downloaded successfully to the blade.

[4]: Thu Jul 28 00:37:42 2007
Slot 7 (SAS): Firmware has been downloaded successfully to the blade.

[5]: Thu Jul 28 00:37:50 2007
Slot 2 (SAS): Blade is rebooting.

[6]: Thu Jul 28 00:37:50 2007
Slot 7 (SAS): Blade is rebooting.

[7]: Thu Jul 28 00:37:50 2007
Slot 2 (SAS): Firmware commit is started.

[8]: Thu Jul 28 00:37:50 2007
Slot 7 (SAS): Firmware commit is started.

[9]: Thu Jul 28 00:37:50 2007
Slot 2 (SAS): Firmware commit has completed.
```

```
[10]: Thu Jul 28 00:37:50 2007
Slot 7 (SAS): Firmware commit has completed.
```

To display the status of a firmware download on a switch:

```
switch:admin> firmwaredownloadstatus
[1]: Fri Feb 15 22:17:03 2007
Firmware is being downloaded to the switch. This step may take up to 30
minutes.

[2]: Fri Feb 15 22:20:54 2007
Firmware has been downloaded to the secondary partition of the switch.

[3]: Fri Feb 15 22:22:19 2007
The firmware commit operation has started. This may take up to 10 minutes.

[4]: Fri Feb 15 22:22:51 2007
Switch is relocating an internal firmware image.

[5]: Fri Feb 15 22:25:15 2007
The commit operation has completed successfully.

[6]: Fri Feb 15 22:25:46 2007
The internal firmware image is relocated successfully.

[7]: Fri Feb 15 22:25:46 2007
Firmwaredownload command has completed successfully. Use firmwareshow to
verify the firmware versions.
```

To display the status of a firmware download on a chassis:

```
switch:admin> firmwaredownloadstatus
[1]: Mon Dec 19 18:40:19 2007
Slot 6 (CP1, active): Firmware is being downloaded to standby CP. This step
may take up to 30 minutes.

[2]: Mon Dec 19 18:46:18 2007
Slot 6 (CP1, active): Firmware has been downloaded successfully to Standby CP.

[3]: Mon Dec 19 18:46:25 2007
Slot 6 (CP1, active): Standby CP is going to reboot with new firmware.

[4]: Mon Dec 19 18:47:45 2007
Slot 6 (CP1, active): Standby CP booted successfully with new firmware.

[5]: Mon Dec 19 18:47:56 2007
Slot 8 (FR4-18i): Firmware is being downloaded to the blade. This step may
take up to 10 minutes.

[6]: Mon Dec 19 18:48:50 2007
Slot 5 (CP0, active): Forced failover succeeded. New Active CP is running new
firmware

[7]: Mon Dec 19 18:48:57 2007
Slot 5 (CP0, active): Firmware is being download to standby CP. This step may
take up to 30 minutes.

[8]: Mon Dec 19 18:49:28 2007
```

```
Slot 8 (FR4-18i): Firmware has been downloaded successfully. Blade is
rebooting with the new firmware.

[9]: Mon Dec 19 18:50:12 2007
Slot 8 (FR4-18i): Firmware commit has started on the blade. This may take up to
10 minutes.

[10]: Mon Dec 19 18:50:51 2007
Slot 8 (FR4-18i): The commit operation has completed successfully.

[11]: Mon Dec 19 18:55:39 2007
Slot 5 (CP0, active): Firmware has been downloaded successfully on Standby CP.

[12]: Mon Dec 19 18:55:46 2007
Slot 5 (CP0, active): Standby CP reboots.

[13]: Mon Dec 19 18:57:06 2007
Slot 5 (CP0, active): Standby CP booted successfully with new firmware.

[14]: Mon Dec 19 18:57:10 2007
Slot 5 (CP0, active): Firmware commit operation has started on both active and
standby CPs.

[15]: Mon Dec 19 19:01:38 2007
Slot 5 (CP0, active): Firmware commit operation has completed successfully on
active CP.

[16]: Mon Dec 19 19:01:39 2007
Slot 5 (CP0, active): Firmwaredownload command has completed successfully. Use
firmwareshow to verify the firmware versions.
```

firmwareShow

Displays the OS versions on all firmware partitions in the system.

Synopsis **firmwareshow**

Description Use this command to display the OS, SAS, and SA firmware versions. The command shows the firmware versions on both the primary and secondary partitions of the storage device.

Note The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 and "Understanding Admin Domain restrictions" on page 33 for details.

Operands none

Examples To display the firmware version on a switch:

```
switch:admin> firmwareshow
Appl     Primary/Secondary Versions
------------------------------------------
FOS      v6.1.1
         v6.1.1
SAS      v3.0.0
         v3.0.0
DMM      v3.0.0
         v3.0.0
```

licenseShow

Displays current license keys.

Synopsis **licenseshow**

Description Use this command to display current license keys, along with a list of licensed products enabled by these keys. Depending on the type of license, this command displays the following information:

Permanent licenses

- License key
- Associated product

Temporary and universal time-based licenses

- License key
- Associated product
- Expiration date or expiration notice if the license has expired

Slot-based licenses

- License key
- Associated product
- Capacity (number of slots purchased)
- Consumed (number of slots configured to use the license)
- Configured Blade Slot Positions (slot numbers of the configured blade slots)

When no licenses are installed, the message "No license installed on this switch" is displayed.

Note The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. "Understanding Virtual Fabric restrictions" on page 32 and "Understanding Admin Domain restrictions" on page 33 for details.

Operands none

Examples To display the license keys on a switch with permanent licenses installed:

```
switch:admin> licenseshow
        S9bddb9SQbTAceeC:
             Fabric license
          eezeRRySff0fSe:
             Remote Switch license
          bzbzRcbcSc0c0SY:
             Remote Fabric license
          dSeR9RcSeeTfSAq:
             Extended Fabric license
          RyeSzRScycTzfT09:
             Entry Fabric license
          RyeSzRScycUzfT0A:
             Fabric Watch license
          RyeSzRScycazfT0G:
             Trunking license
          RyeSzRScycS0fT09:
             4 Domain Fabric license
```

To display the license keys on a switch with temporary (expired) licenses installed:

```
switch:admin> licenseShow
 7QmYFYJrmDgE9tTS4AYXB9trYSGtMtrQZSTK4ZSC7FC9ZAYAgE:
    Integrated Routing license
    Expiry Date 01/16/2008
    License is expired
33YBfZfKZ3tQKrRJJRtgmS3JDtCL99P4fYrJYQP7GffS4ASmNE:
    Enterprise Bundle license
    Expiry Date 01/16/2008
    License is expired
```

To display the license keys on a switch with universal time-based and slot-based licenses installed (the first two examples show time-based, the third one shows a slot-based license):

```
switch:admin> licenseshow
DAmHTPgQ7KDtKrEYQC7X7STF9HJDL7TmTWRmZPmSTSE49AEfaE:
    Trunking license
    Expiry Date 11/11/2008
    License is expired
H47CFSa93aKgKJM9NWMYEMaLrATQWDHCgHfZftWGGgNCYAJaBA:
    High-Performance Extension over FCIP/FC license
    Expiry Date 12/20/2008
KBrttggRJ4TEBBAt4CrXWRgSCgCJrKZNRFYS9A74ZG:
     10 Gigabit Ethernet (FTR_10G) license
    Capacity 4
    Consumed 2
    Configured Blade Slots 1,3.
```

licenseAdd

Adds a license key to a switch.

Synopsis **licenseadd** *license*

Description Use this command to add a license key to a switch.

Some features of the switch and the fabric to which it is connected are optional, licensed products. Without a valid license installed for such products, their services are not available.

A license key is a string of any length consisting of upper- and lowercase letters and numbers. License keys are case-sensitive. The license must be entered exactly as issued. The system may accept an incorrectly entered license, but the licensed products will not function. After entering the license, use the **licenseShow** command to validate the product associated with the license. If no licensed products are shown, the license is invalid.

After you enter a license, the licensed product is generally available immediately without requiring a system reboot. The following exceptions apply:

- When adding a fabric license to a switch that lacks a fabric license, you must reboot the switch to activate the license.
- When adding a trunking license is added to the switch, you must refresh the trunk ports to activate the trunking license. Depending on your system, use **portDisable**/**portEnable**, **switchDisable/switchEnable** or **chassisDisable/chassisEnable** to refresh the trunk ports.

Note The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 snf "Understanding Admin Domain restrictions" on page 33 for details.

Operands This command has the following operand:

license Specifies the license key to be installed. This operand is required.

Examples To add a license key to the switch:

```
    switch:admin> licenseadd DXXtN3LmRSMWCSW3XmfSBPfrWKLZ3HMTN73rP9GANJMA
adding license-key [DXXtN3LmRSMWCSW3XmfSBPfrWKLZ3HMTN73rP9GANJMA]
```

portCfgShow

Displays port configuration settings.

Synopsis **portcfgshow**

portcfgshow [*slot/*]*port*

portcfgshow *option* [*slot/*] [*arguments*] [*optional_arguments*]

Description Use this command to display the current configuration of a port. The behavior of this command is platform-specific; output varies depending on port type and platform, and not all options are supported on all platforms.

"Non-GbE port displays" on page 52

If no operand is specified, this command displays port configuration settings for all ports on a switch, except Gigabit Ethernet (GbE) ports.

Non-GbE port displays

The following information is displayed when the command is issued for all ports or for a specific port:

Area Number Displays the port area number. This field is displayed only when **portCfgShow** is executed for a specific port.

Speed Displays Auto for auto speed negotiation mode, or a specific speed of 1, 2, 4, or 8 Gbps. This value is set by the **portCfgSpeed** command.

Fill Word Displays 0(Idle-Idle) or 1(arbff-arbff). This parameter is set by the **portcfgFillword** command.

AL_PA Offset 13 Displays (...) or OFF when the arbitrated loop physical address (AL_PA) on the port is configured to use a 0x0 AL_PA address (default). Displays ON when the address configuration is 0x13 AL_PA. This value is set by the **portCfgAlpa** command.

Trunk Port Displays ON when port is set for trunking. Displays (..) or OFF when trunking is disabled on the port. This value is set by the **portCfgTrunkPort** command.

Long Distance Displays (..) or OFF when long distance mode is off; otherwise, displays long distance levels as follows:

LE The link is up to 10 km.

LM The link is up to 25 km.

L1 The link is up to 50 km.

L2 The link is up to 100 km.

LD The distance is determined dynamically.

LS The distance is determined statically by user input.

This value is set by the **portCfgLongDistance** command.

VC Link Init Displays (..) or OFF when the long distance link initialization option is turned off. Displays ON when it is turned on for long distance mode. This value is set by the **portCfgLongDistance** command.

Locked L_Port Displays ON when the port is locked to L_Port only. Displays (..) or OFF when L_Port lock mode is disabled and the port behaves as a U_Port). This value is set by the **portCfgLport** command.

Locked G_Port Displays ON when the port is locked to G_Port only. Displays (..) or OFF when G_Port lock mode is disabled and the port behaves as a U_Port. This value is set by the **portCfgGport** command.

Disabled E_Port Displays ON when the port is not allowed to be an E_Port. Displays (..) or OFF when the port is allowed to function as an E_Port. This value is set by the **portCfgEport** command.

ISL R_RDY Mode Displays ON when ISL R_RDY mode is enabled on the port. Displays (..) or OFF when ISL R_RDY mode is disabled. This value is set by the **portCfgISLMode** command.

RSCN Suppressed

Displays ON when RSCN suppression is enabled on the port. Displays (..) or OFF when RSCN suppression is disabled. This value is set by the **portCfg rscnsupr** command.

Persistent Disable Displays ON when the port is persistently disabled; otherwise displays (..) or OFF. This value is set by the **portCfgPersistentDisable** command.

NPIV capability Displays ON when N_Port ID Virtualization (NPIV) is enabled on the port (default). Displays (..) or OFF when NPIV capability is disabled. This value is set by the **portCfgNPIVPort** command.

QOS E_Port Displays ON when Quality of Service (QoS) is enabled on the E_Port (or EX_Port) when QoS is enabled in an FCR deployment scenario. Displays (..) or OFF when QoS is disabled. By default, QoS is enabled if sufficient buffers are available. Displays AE when QOS is configured as Auto Enabled. In the AE state, QoS is enabled based on the availability of buffers. Use **islShow** to determine the current status of QoS (on or off) in the AE state. This value is set by the **portCfgQos** command.

EX_port. Displays ON when the port is configured as an EX_Port. Otherwise displays (..) or OFF. This value is set by the **portCfgExPort** command.

Mirror Port Displays ON when Mirror Port is enabled on the port. Displays (..) or OFF when Mirror Port is disabled. This value is set by the **portCfg mirrorport** command.

FC Fastwrite	Displays ON when FC Fastwrite is enabled on the port or (..) or OFF when disabled. Fastwrite is disabled by default. This value is set by the **portCfg fastwrite** command.
Rate Limit	Displays ON when ingress rate limit is set on the port or (..) or OFF when the ingress rate limiting feature is disabled. This value is set by the **portCfgQos --setratelimit** command. The default value is OFF.
Credit Recovery	Displays ON when Credit Recovery is enabled on the port. Displays (..) or OFF when the feature is disabled. This value is set by the **portCfgCreditRecovery** command. The credit recovery feature is enabled by default, but only ports configured as long distance ports can utilize this feature.
Port Auto Disable	Displays On when the Auto Disable feature is enabled on a port. Displays (..) or OFF when the feature is disabled. This feature causes ports to become disabled when they encounter an event that would cause them to reinitialize. This feature is enabled by the **portCfgAutoDisable** command. The feature is disabled by default.
F_Port Buffers	Displays the number of configured internal port (F_Port) buffers. Displays (..) or OFF if no buffers are configured. The buffer value is set by the **portCfgfPortbuffers** command.

Notes The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 snf "Understanding Admin Domain restrictions" on page 33 for details.

Operands This command supports the following operands:

slot	For bladed systems only, specifies the slot number of the port to be configured, followed by a slash (/).
port	Specifies the number of the port to be displayed, relative to its slot for bladed systems.

Use **portCfgshow** with one of the following options and optional arguments to display specific FCIP-related parameters configured for a GbE port:

Examples To display the configuration settings for a single port on a switch with NPIV mode enabled:

```
switch:admin> portcfgshow 8
Area Number:              8
Speed Level:              AUTO(HW)
Fill Word:                0(Idle-Idle)
Trunk Port                ON
Locked N_Port             OFF
Persistent Disable        OFF
NPIV capability           ON
QOS Port                  AE
Port Auto Disable:        OFF
Rate Limit                OFF
F_Port Buffers            OFF
```

To display the configuration settings for all ports on a switch with NPIV Mode enabled:

```
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Fill Word          0  0  0  0    0  0  0  0    0  0  0  0    0  0  0  0
```

```
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Locked N_Port     ON ON .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
NPIV capability   ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
QOS Port          AE AE AE AE   AE AE AE AE   AE AE AE AE   AE AE AE AE
Rate Limit        .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Fport Buffers     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Port Auto Disable .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..

Ports of Slot 0   16 17 18 19   20 21 22 23   24 25 26 27   28 29 30 31
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Fill Word          0  0  0  0    0  0  0  0    0  0  0  0    0  0  0  0
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Locked N_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
NPIV capability   ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
QOS Port          AE AE AE AE   AE AE AE AE   AE AE AE AE   AE AE AE AE
Rate Limit        .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Fport Buffers     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Port Auto Disable .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..

Ports of Slot 0   32 33 34 35   36 37 38 39
-----------------+--+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN
Fill Word          0  0  0  0    0  0  0  0
Trunk Port        ON ON ON ON   ON ON ON ON
Locked N_Port     ON ON ON ON   ON ON ON ON
Persistent Disable.. .. .. ..   .. .. .. ..
NPIV capability   ON ON ON ON   ON ON ON ON
QOS Port          AE AE AE AE   AE AE AE AE
Rate Limit        .. .. .. ..   .. .. .. ..
Fport Buffers     .. .. .. ..   .. .. .. ..
Port Auto Disable .. .. .. ..   .. .. .. ..

                where AE:QoSAutoEnable, AN:AutoNegotiate, ..:OFF, ??:INVALID,


switch:admin>
```

To display the QoS configuration for an EX_Port (QoS over FCR deployment):

```
switch:admin> switchshow | grep EX-Port
 16  16   id    N4   Online      FC  EX-Port  10:00:00:05:1e:41:4a:45 "Tom_100"
(fabric id = 25 )(Trunk master)

switch:admin> portcfgshow 16
Area Number:              11
Speed Level:              AUTO(HW)
Fill Word:                0(Idle-Idle)
AL_PA Offset 13:          OFF
Trunk Port                ON
Long Distance             OFF
VC Link Init              OFF
Locked L_Port             OFF
Locked G_Port             OFF
Disabled E_Port           OFF
ISL R_RDY Mode            OFF
RSCN Suppressed           OFF
Persistent Disable        OFF
```

```
NPIV capability          ON
QOS E_Port               AE
Port Auto Disable:       OFF
Rate Limit               OFF
EX Port                  ON
Mirror Port              OFF
Credit Recovery          ON
F_Port Buffers           OFF
```

portCfgSpeed

Configures the speed for a single port.

Synopsis **portcfgspeed** [*slotnumber*/]*portnumber*, *speed*

Description Use this command to set the speed on a specified port. This command disables and then re-enables the port, and the port comes online with the new speed setting. The configuration is saved in nonvolatile memory and is persistent across switch reboots or power cycles.

Use the **portShow** command to display actual port speed levels. Use the **portCfgShow** command to display user-specified speed settings.

Notes This configuration cannot be set on VE/VEX_Ports. For a virtual FC port, the speed is always 10 GbE and port speed auto-negotiation is not possible.

The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 and "Understanding Admin Domain restrictions" on page 33 for details.

Operands This command has the following operands:

slotnumber	For bladed systems only, specifies the slot number of the port to be configured, followed by a slash (/).
portnumber	Specifies the port to be configured, relative to its slot for bladed systems. Use **switchShow** for a listing of valid ports.
speed_level	Specifies the speed of a port. This operand is required. Valid values are one of the following:
0	Auto-sensing mode (hardware). The port automatically configures for maximum speed.
ax	Auto-sensing mode (hardware). The port automatically configures for maximum speed with enhanced retries.
s	Auto-sensing mode (software). The port automatically configures for maximum speed with enhanced retries.
1	The port is set at a fixed speed of 1 Gbps.
2	The port is set at a fixed speed of 2 Gbps.
4	The port is set at a fixed speed of 4 Gbps.
8	The port is set at a fixed speed of 8 Gbps.

Examples To set the speed of a port to 4 Gbps:

```
switch:admin> portcfgspeed 2/3, 4
```

portShow

Displays status and configuration parameters for ports and GbE ports.

Synopsis **portshow** [*slot/*][**ge**]*port*

portshow *option* [*slot/*]*ge_port* [*optional_args*]

portshow *option* [**all** |*ve_port*] *arguments* [*optional_arguments*]

portshow *option* [**all** |*ge_port*] *arguments* [*optional_arguments*]

Description Use this command to display general port status and specific configuration parameters for a specified port, GbE port, or VE_Port.

If this command is executed for a specified port with no additional options, it displays general status and configuration for that port. .

You must use this command in a manner that honors the platform-specific differences in command syntax and behavior. Some command options are not available on all platforms. Others behave differently depending on the platform on which they are executed. To display command usage on the switch, use **portShow** [*action*].

Notes The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 and "Understanding Admin Domain restrictions" on page 33 for details.

Some of the features supported by this command may require a license.

In an AD context, if one of the L_Ports or NPIV ports is a part of the current AD, the complete device information attached to the port is shown in the output.

Function **General port status display commands (supported on all platforms)**

Synopsis **portshow** [*slot/*][**ge**]*port*

Description Use this command to display general port status and configuration parameters for the specified port. This command is valid on all platforms, but the output is platform-specific and not all fields are displayed on all platforms.

The following general information is displayed when the command is issued for a non-GbE port without additional arguments:

portName	Name assigned to the port by the **portName** command.
Authentication	Authentication type and associated parameters (ifapplicable) used on the port at port online.
None	No authentication was performed.
FCAP	FCAP authentication was performed.
DHCHAP	DHCHAP authentication was performed. Also displays DH group and hash type used for authentication.

portDisableReason
: Provides an explanation for the port's disabled status, if it has not been disabled by **portDisable** or **portCfgPersistentDisable**.

portCFlags
: Port control flags.

portFlags
: A bit map of port status flags, including information on the type of port, whether it is fully online, and whether logins have been accepted.

portType
: The port's type and revision numbers.

portState
: The port's SNMP state:

  - Online: Up and running.
  - Offline: Not online, see **portPhys** for more detail.
  - Testing: Running diagnostics.
  - Faulty: Failed diagnostics.
  - Persistently Disabled: Persistently disabled.

Protocol
: Protocol used by the port: FC or FCoE.

portPhys
: The port's physical state:

  - No_Card: No interface card present.
  - No_Module: No module (GBIC or other) present.
  - No_Light: Module is not receiving light.
  - Mod_Inv: Incompatible vendor or module speed mismatch.
  - No_Sync: Receiving light but out of sync.
  - In_Sync: Receiving light and in sync.
  - Laser_Flt: Module is signaling a laser fault.
  - Port_Flt: Port marked faulty.
  - Diag_Flt: Port failed diagnostics.
  - Lock_Ref: Locking to the reference signal.

portScn
: The port’s last State Change Notification.

port generation number
: The port’s generation number for the last offline state change.

portId
: The port’s 24-bit port ID.

portIfId
: The user port’s interface ID.

portWwn
: The port’s world wide name.

portWwn of devices(s) connected
: The World Wide Port Names of connected devices.

Distance
: The port's long-distance level. In the case of LD mode, the user configured distance and actual distance also are displayed. See **portCfgLongDistance** for information on long distance levels.

Port part of other AD
Yes or No.

portSpeed The port's fixed speed (1, 2, 4, or 8 Gbps) or negotiated speed (N1 Gbps, N2 Gbps, N4 Gbps, N8 Gbps or AN).

LE domain The LE domain ID.

FC Fastwrite The status of FC Fastwrite (ON or OFF).

If the port is configured as an EX_Port, the following additional port information is displayed:

EX_Port Mode The port is configured as an EX_Port.

Fabric ID The fabric ID assigned to this EX_Port; this is the fabric ID of the edge fabric attached to this EX_Port.

Front Phantom Information on the front phantom domain presented by this EX_Port. Includes the preferred (if not active) or actual (if active) domain ID for the front domain and the WWN of the front domain.

Pr Switch Info Information on the principal switch of the edge fabric attached to this EX_Port. Includes the domain ID and WWN of the principal switch.

BB XLate Information on the xlate (translate) phantom domain presented at this port. Includes the preferred (if not active) or actual (if active) domain ID for the xlate phantom domain and the WWN of the xlate phantom domain. The xlate phantom domain connected at this port is in the same fabric as the router and represents the edge fabric connected to the EX_Port.

Authentication Type
Displays NONE or DH-CHAP. DH-CHAP is the only authentication type supported on EX_Ports.

DH Group Displays DH group [0-4] if DH-CHAP authentication is used. Otherwise displays N/A.

Hash Algorithm Displays hash type (MD5 or SHA-1) if DH-CHAP authentication is used. Otherwise, displays N/A.

Edge fabric's primary WWN
If the EX_Port is connected to an edge switch with FCS policy enforcement, the WWN of the primary FCS is displayed when the edge fabric is secure and the primary FCS is online. Otherwise, displays "No Primary".

Edge fabric's version stamp
If the EX_PORT is connected to an edge switch with FCS policy enforcement, the version of the security database is displayed. Otherwise displays N/A.

If the port is configured as a VE_Port, the command shows FC and Physical layer attributes of the underlying port, as well as status information regarding the underlying FCIP link for those logical FC ports that are instantiated over a physical 1/10GbE port. Refer to the example section for an illustration.

Following the general information, the command displays three columns of counters. The first column shows interrupt statistics:

Interrupts Total number of interrupts.

Unknown Interrupts that are not counted elsewhere.

Lli	Low-level interface (physical state, primitive sequences).
Proc_rqrd	Frames delivered for embedded N_Port processing.
Timed_out	Frames that have timed out.
Rx_flushed	Frames requiring translation.
Tx_unavail	Frames returned from an unavailable transmitter.
Free_buffer	Free buffer available interrupts.
Overrun	Buffer overrun interrupts.
Suspended	Transmission suspended interrupts.
Parity_err	Central memory parity errors.
2_parity_err	Secondary transmission parity errors.
CMI_bus_err	Control message interface errors.

The second column displays link error status block counters.

The third column shows the number of F_RJTs and F_BSYs generated. For L_Ports, the third column also displays the number of loop initialization protocols (LIPs) received, number of LIPs transmitted, and the last LIP received.

Examples To display the current state of a port:

```
switch:admin> portshow 6
portName:

Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x1000490b    PRESENT ACTIVE E_PORT T_PORT T_MASTER G_PORT U_PORT
LOGICAL_ONLINE LOGIN LED
portType:  18.0
portState: 1    Online
Protocol: FC
portPhys:  6    In_Sync        portScn:   16   E_Port    Trunk master port Flow
control mode 4
port generation number:    10
portId:    d70600
portIfId:    43020012
portWwn:   20:06:00:05:1e:55:63:05
portWwn of device(s) connected:

Distance:  normal
portSpeed: N8Gbps

LE domain: 0
FC Fastwrite: OFF
Interrupts:        0          Link_failure: 0          Frjt:         0
Unknown:           0          Loss_of_sync: 9          Fbsy:         0
Lli:               53         Loss_of_sig:  10
Proc_rqrd:         9525       Protocol_err: 0
Timed_out:         0          Invalid_word: 588
Rx_flushed:        0          Invalid_crc:  0
Tx_unavail:        0          Delim_err:    0
Free_buffer:       0          Address_err:  0
Overrun:           0          Lr_in:        8
```

```
Suspended:          0          Lr_out:       0
Parity_err:         0          Ols_in:       0
2_parity_err:       0          Ols_out:      4
CMI_bus_err:        0

Port part of other ADs: No
switch:admin>
```

supportSave

Saves RASLOG, TRACE, supportShow, core file, FFDC data, and other support information

Synopsis **supportsave**

supportsave [**-n**] [**-c**] [**-k**] [**-u** *user_name* **-p** *password* **-h** *host_ip* **-d** *remote_dir* **-l** *protocol*]

supportsave [**-R**]

supportsave [**-U -d** *remote_dir*]

Description Use this command to collect RASLOG, TRACE, **supportShow**, core file, FFDC data and other support information to a remote FTP location. On platforms that support USB, the information can also be stored on an attached USB device. On a dual-CP system, information is saved for the local and the remote CP. **SupportShow** information is available on Active and Standby CPs. To reduce the chance of missing the correct trace dump, **supportSave** retrieves old (the dump created prior to the current one) and new (the dump triggered by the command) trace dumps.

The files generated by this command are compressed before being sent off the switch. The core files and panic dumps remain on the switch after the command is run. The FFDC data are removed after the command has finished.

This command accepts IPv4 and IPv6 addresses. If the configured IP address is in IPv6 format, the RAS auto file transfer and event notification to syslog will not work in the case where the FC SAN Module OS version is downgraded. It is required to reconfigure auto file transfer and syslog with IPv4 IP addresses.

In a Virtual Fabric environment, **supportSave** saves all chassis-based information and iterates through the defined switch-based information for all logical switches. Chassis permissions are required to execute this command.

System-wide **supportSave** is supported on platforms running FC SAN Module OS v6.2.0 or later. The command collects support data from the Active CP (and its Co-CPU), the standby CP (and its Co-CPU), and all AP blades.

Note The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 and "Understanding Admin Domain restrictions" on page 33 for details.

Operands When invoked without operands, this command goes into interactive mode. The following operands are optional:

-n Does not prompt for confirmation. This operand is optional; if omitted, you are prompted for confirmation.

-c	Uses the FTP or SCP parameters saved by the **supportFtp** command. This operand is optional; if omitted, specify the FTP or SCP parameters through command line options or interactively. To display the current FTP parameters, run **supportFtp** (on a dual-CP system, run **supportFtp** on the active CP). The **-c** option is mutually exclusive with **-u**, **-p**, **-h**, and **-d**.
-k	Specifies that the **supportFtp** auto file transfer configuration transfer only core and FFDC files in non-interactive mode.
-u *user_name*	Specifies the user name for the FTP or SCP server. This operand is optional; if omitted, anonymous FTP is used.
-p *password*	Specifies the password for the FTP or SCP server. This operand is optional with FTP; if omitted, anonymous FTP is used.
-h *host_ip*	Specifies the IPv4 or IPv6 address for the remote server.
-d *remote_dir*	Specifies the remote directory to which the file is to be transferred. When saving to a USB device, the predefined `/support` directory must be used.
-R	Removes all core files on the CP and BP. This option cannot be used with any other options.
-l *protocol*	Specifies the transfer protocol. Valid values are FTP or SCP. If you plan to use secure copy (SCP) to transfer files, it is important to test the **supportSave** command prior to its use with various SCP-mode services. Because the **supportSave** command makes several access requests to copy files, it is important that the SCP-mode service be configured so that passwords are not required for each attempted transfer by the **supportSave** command. Failure to configure the service correctly may result in significant delays in obtaining transferred output from the **supportSave** command. When using secure copy (SCP), **supportSave** may create a directory specified by the **-d** option if it does not already exist and the parent directory has the appropriate permissions. Use of FTP requires the directory to exist on the remote server.
-U	Saves support data to an attached USB device. When using this option, a target directory must be specified with the **-d** option.

Examples To save RASLOG, TRACE, supportShow, and other support information to an FTP server in interactive mode:

```
switch:admin> supportsave
This command will collect RASLOG, TRACE, supportShow, core file, FFDC data
and other support information and then transfer them to a FTP/SCP server
or a USB device. This operation can take several minutes.
NOTE: supportSave will transfer existing trace dump file first, then
automatically generate and transfer latest one. There will be two trace dump
files transfered after this command.
OK to proceed? (yes, y, no, n): [no] y

Host IP or Host Name: 192.168.126.115
User Name: admin
Password:
Protocol (ftp or scp): ftp
Remote Directory: /temp/support
```

```
Saving support information for chassis:HL_5100_66, module:RAS...
Saving support information for chassis:HL_5100_66, module:TRACE_OLD...
Saving support information for chassis:HL_5100_66, module:TRACE_NEW...
Saving support information for chassis:HL_5100_66, module:FABRIC...
Saving support information for chassis:HL_5100_66, module:CORE_FFDC...
Saving support information for chassis:HL_5100_66, module:DIAG...
Saving support information for chassis:HL_5100_66, module:RTE...
Saving support information for chassis:HL_5100_66, module:ISCSID_DBG...
Saving support information for chassis:HL_5100_66, module:AGDUMP...
Saving support information for chassis:HL_5100_66, module:SSHOW_PLOG...
Saving support information for chassis:HL_5100_66, module:SSHOW_OS...
Saving support information for chassis:HL_5100_66, module:SSHOW_EX...
Saving support information for chassis:HL_5100_66, module:SSHOW_FABRIC...
Saving support information for chassis:HL_5100_66, module:SSHOW_SERVICE...
Saving support information for chassis:HL_5100_66, module:SSHOW_SEC...
Saving support information for chassis:HL_5100_66, module:SSHOW_NET...
......(output truncated)
```

supportShow

Displays switch information for debugging purposes.

Synopsis **supportshow** [[*slotnumber/*]*portnumber1-portnumber2*] [*lines*]

Description Use this command to display support information from groups of preselected FC SAN Module OS and Linux commands and other support and debugging information. You can specify the range of ports for which to display this information. These commands are organized by groups, but note that the order of the groups listed below is not the same as executed by the command.

SupportShow executes commands in the following command groups. Use **supportShowCfgenable** or **supportShowCfgDisable** to modify the settings for each group.

os	OS group commands, enabled by default.
exception	Exception group commands, enabled by default.
port	Port group commands, enabled by default.
fabric	Fabric group commands, enabled by default.
services	Service group commands, enabled by default.
security	Security group commands, enabled by default.
network	Network group commands, enabled by default.
portlog	Portlog group commands, enabled by default.
system	System group commands, enabled by default.
extend	Extend group commands, disabled by default.
filter	Filter group commands, disabled by default.
perfmon	Performance Monitor group commands, disabled by default.
ficon	FICON group commands, disabled by default.
iswitch	FC Router group commands, disabled by default.
asic_db	ASIC DB group commands, disabled by default.

iscsi	iSCSI group commands, disabled by default.
fcip	FCIP group commands, disabled by default.
ag	Access Gateway group commands, disabled by default.
dce_hsl	DCE group commands, enabled by default.
crypto	Encryption group commands, disabled by default.

Notes The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 and "Understanding Admin Domain restrictions" on page 33 for details.

This is a diagnostic command and should only be run for diagnostic support.

Output generated by this command may vary by switch configuration and platform. Output may change without notice.

Operands This command has the following operands:

slotnumber	On bladed systems only, specifies a slot number, followed by a slash (/).
portnumber1-portnumber2	Specifies the range of ports for which to display **supportShow** information. If a port range is not specified, the command displays information for all ports.
lines	Specifies the number of lines for the **portLogDump** output. This parameter is valid only with the *slotnumber/portnumber* parameters.

Examples To display debugging information:

```
switch:admin> supportshow
VF
======================
Date:
Wed Oct 22 09:31:41 UTC 2008

Time Zone:
Time Zone Hour Offset: 0
Time Zone Minute Offset: 0

Version:
Kernel:     2.6.14.2
Fabric OS:  v6.2.0_main_bld26
Made on:    Mon Oct 20 10:10:30 2008
Flash:      Mon Oct 20 16:04:18 2008
BootProm:   1.0.6

supportshow groups enabled:
 os         enabled
 exception  enabled
 port       enabled
 fabric     enabled
 services   enabled
 security   enabled
 network    enabled
 portlog    enabled
 system     enabled
 extend     disabled
 filter     disabled
```

```
 perfmon    disabled
 ficon      disabled
 iswitch    enabled
 asic_db    enabled
 iscsi      enabled
 fcip      enabled
 ag         enabled
 crypto    disabled

**** Begin start_port_log_cmd group ****
Wed Oct 22 09:31:44 UTC 2008
portlogdump:
portlogdump:
CURRENT CONTEXT -- 0 , 128
/fabos/cliexec/portlogdump        :
time         task       event   port cmd  args
-----------------------------------------------
Tue Oct 21 07:32:21 2008
07:32:21.887 FCPH       read      0   40
02fffffd,00fffffd,f4000000,00000000,1a
731af5
07:32:21.887 FCPH       seq       0   28
22380000,1a731af5,000007c4,0000001c,00
000000
07:32:30.131 FCPH       write     0   40
00fffffd,00fffffd,00000000,00000000,00
000000
07:32:30.131 FCPH       seq       0   28
00300000,00000000,00000834,00020182,00
000000
07:32:30.131 PORT       Tx        0   40  02fffffd,00fffffd,1af6ffff,14000000
07:32:30.131 PORT       Rx        0    0  c0fffffd,00fffffd,1af61a74,00000001
07:32:41.887 PORT       Rx        0   40  02fffffd,00fffffd,1a75ffff,14000000
07:32:41.887 PORT       Tx        0    0  c0fffffd,00fffffd,1a751af7,00000001
07:32:41.887 FCPH       read      0   40
02fffffd,00fffffd,f5000000,00000000,1a
751af7

(output truncated)
```

version

Displays firmware version information.

Synopsis **version**

Description Use this command to display firmware version information and build dates.

The command output includes the following:

Kernel	The version of switch kernel operating system.
Fabric OS	The version of switch OS.
Made on	The build date of firmware running in switch.
Flash	The build date of firmware stored in flash proms.
BootProm	The version of the firmware stored in the boot PROM

Usually the Made on and Flash dates are the same, because the switch starts running flash firmware at power-on. However, in the time period between **firmwareDownload** and the next **reboot**, the dates can differ.

Operands none

Examples To display the firmware version information in a switch:

```
switch:admin> version
Kernel:     2.6.14.2
Fabric OS:  v6.1.0
Made on:    Wed Feb 13 06:59:17 2008
Flash:      Thu Feb 14 18:38:31 2008
BootProm:   4.6.6
```

wwn

Displays the world wide name (WWN) and serial number of the switch.

Synopsis **wwn** [**-sn**]

Description Use this command to display the WWN associated with a switch and to display the switch serial number. The switch WWN is a 64-bit number that has eight colon-separated fields each consisting of one or two hexadecimal digits between 0 and ff. The switch WWN is a factory-set parameter that cannot be changed by the end user. The WWN is used as the license ID in many cases, but the only official string to be used for requesting licenses is the **licenseidShow** output. Alternately, use **switchShow** to display the switch WWN.

In addition to the WWN, all switches have a unique 24-bit Fibre Channel address that is used for communicating with the switch. Use **farbricShow** to display the FC address in addition to the WWN.

Note The execution of this command is subject to Virtual Fabric or Admin Domain restrictions that may be in place. Refer to "Understanding Virtual Fabric restrictions" on page 32 and "Understanding Admin Domain restrictions" on page 33 for details.

Operands This command has the following operands:

-sn	Displays the switch serial number following the current WWN. This operand is optional; if omitted, this command displays only the current WWN.

Examples To display the switch WWN:

```
switch:admin> wwn
10:00:00:05:1e:41:5c:c1
```

To display the switch WWN and serial number:

```
switch:admin:admin> wwn -sn

WWN: 10:00:00:05:1e:41:5c:c1
SN:  ALK0343C00Y
```

To display the license ID:

```
switch:admin>licenseidshow
10:00:00:05:1e:41:5c:c1
```

To display the WWN and the Fibre Channel address:

```
switch:admin> fabricshow
Switch ID   Worldwide Name         Enet IP Addr FC IP Addr Name
-------------------------------------------------------------------
 66:fffc42 10:00:00:05:1e:41:5c:c1 10.32.228.66  0.0.0.0 "Spir6"
200:fffcc8 10:00:00:05:1e:39:d8:5a 10.32.228.200 0.0.0.0 "DCX2"

The Fabric has 2 switches
```

Index

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Z