

user guide

hp StorageWorks zoning version 3.1.x/4.1.x

Product Version: 3.1.x/4.1.x

Fourth Edition (August 2004)

Part Number: AA-RS26D-TE

This user guide provides an overview of zoning, instructions for activating zoning, and information about configuring and using zoning and QuickLoop zones.



© Copyright 1999-2003 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

BROCADE, the Brocade B weave logo, Brocade: the Intelligent Platform for Networking Storage, SilkWorm, and SilkWorm Express, are trademarks or registered trademarks of Brocade Communications Systems, Inc. or its subsidiaries in the United States and/or in other countries.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

Zoning Version 3.1.x/4.1.x User Guide
Fourth Edition (August 2004)
Part Number: AA-RS26D-TE



contents

About this Guide	7
Overview	8
Intended Audience	8
Related Documentation	8
Conventions	9
Document Conventions	9
Text Symbols	9
Getting Help	10
HP Technical Support	10
HP Storage Website	10
HP Authorized Reseller	11
1 Introducing Zoning	13
Overview	14
Customizing Environments	14
Optimizing Resources	14
License Activation	15
License Activation Using Telnet	16
License Activation Using Web Tools	17
2 Zoning Concepts	19
About Zoning	20
Guidelines to Setting Up Zoning	21
Zone Definitions	22
Zone Objects	22
Selecting Ports on the Core Switch 2/64	23
Zone Objects and Aliases	24
Zone Objects	24
Zone Aliases	24
Zone Configurations	25

Zone Management	26
Commands to Open a Transaction.	26
Commands to Close a Transaction	27
Zoning Schemes	28
Zone Enforcement	28
Implementing Zoning	30
Create and Enable a Basic Zone Configuration.	30
Detailed Zone Configuration Procedures.	30
Review Current Configurations.	31
Create an Alias.	32
Define a Zone	32
Define a Zone Configuration.	33
Analyze the Zone Configuration	33
Enable a Zone Configuration.	33
Review The Enabled Configuration	34
Modifying Configurations	36
Before Merging Zones	36
Adding a New Switch	36
Adding a New Fabric	37
Merging and Segmentation	37
Merging Rules	38
Merging Two Fabrics.	38
Merging with a V4.1 Fabric	38
Merge Conflicts	39
Splitting a Fabric	39
Zone Merging Scenarios.	40
Resolving Zone Conflicts.	42
Rules of Zoning Architecture	43
3 Using QuickLoop Zones.	45
QuickLoop Zones	46
QuickLoop Zoning Advantages	47
Configuring QuickLoop Zones.	48
Create a QuickLoop	48
Define a QuickLoop Zone	48
To Specify by Looplet	48
To Specify by AL_PA	49
To specify a Combination of looplet and AL_PA.	49
Define a QuickLoop Zone Configuration	49

QuickLoop Fabric Assist	50
Fabric Assist Zone Setup	51
Fabric Assist Zone Creation.....	51
Fabric Assist Operation	51
LIP Propagation	51
Fabric Assist Debugging	52
A Zoning Concepts and Guidelines	53
Storage Area Networks.....	54
Zoning.....	55
Zone Management	56
Zoning Implementations.....	57
Host-Based Zoning.....	57
Storage-Based Zoning	57
Fabric-Based Zoning	57
Fabric-Based Zoning Philosophies.....	58
No Fabric Zoning.....	58
Zoning by Application.....	58
Zoning by Operating System	59
Port allocation	59
Single HBA	60
The Effect of Zoning on RSCN Delivery.....	61
Implementing Zoning.....	63
Naming Convention.....	63
Implementing Zoning on an Existing Fabric	64
Hardware-Enforced Zoning in an HP Fabric	65
Fabrics Composed of Only StorageWorks 1 Gb SAN Switch Models	65
Fabrics Composed of StorageWorks 2 Gb SAN Switch and StorageWorks Core Switch Models	66
Fabrics Composed of 1 Gb SAN, 2 Gb SAN, and Core Switch Models	66
Best Practices for Hardware Zone Enforcement	66

B Using Zoning to Administer Security69
Glossary71
Index103
Figures	
1 License activation using telnet.	16
2 Fabric with three zones	20
3 PortZoneShow output.	29
Tables	
1 Document Conventions	9
2 Area and Port Mappings.	23
3 Zone Merging Scenarios	40
4 RSCN Delivery	62



about this guide

This user guide provides information to help you:

- Understand Zoning
- Install Zoning
- Configure and use Zoning and QuickLoop zones
- Contact technical support for additional assistance

“About this Guide” topics include:

- [Overview](#), page 8
- [Conventions](#), page 9
- [Getting Help](#), page 10

Overview

This section covers the following topics:

- [Intended Audience](#)
- [Related Documentation](#)

Intended Audience

This book is intended for use by system administrators who are experienced with the following:

- *HP StorageWorks* Fibre Channel SAN switches
- Fabric Operating System (FOS) V3.1.x or later

Related Documentation

For a list of related documents included with this product, see the “Related Documents” section of the Release Notes that came with your switch.

For the latest information, documentation, and firmware releases, please visit the following StorageWorks website: <http://www.hp.com/country/us/eng/prodserv/storage.html>

For information about Fibre Channel standards, visit the Fibre Channel Association website, located at: <http://www.fibrechannel.org>.

Conventions

Conventions consist of the following:

- [Document Conventions](#)
- [Text Symbols](#)

Document Conventions

The document conventions included in [Table 1](#) apply in most cases.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key and field names, menu items, buttons, and dialog box titles	Bold
File names, application names, and text emphasis	<i>Italics</i>
User input, command and directory names, and system responses (output and messages)	Monospace font COMMAND NAMES are uppercase monospace font unless they are case-sensitive
Variables	<monospace, italic font>
Website addresses	Blue, underlined sans serif font text: http://www.hp.com

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings.



WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.



Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: <http://www.hp.com>.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP website: <http://www.hp.com/support/>. From this website, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: <http://www.hp.com/country/us/eng/prodserv/storage.html>. From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- Elsewhere, see the HP website for locations and telephone numbers:
<http://www.hp.com>.

Introducing Zoning



This chapter provides the following information:

- [Overview](#), page 14
- [License Activation](#), page 15

Overview

A zone in a fabric is a set of devices that have access to one another. All devices connected to a fabric may be configured into one or more zones. Every zone has at least one member. Empty zones are not allowed. Zoning allows partitioning of a Storage Area Network (SAN) into logical groupings of devices that access each other.

Zones can be configured dynamically and can vary in size depending on the number of fabric-connected devices. Devices can also belong to more than one zone. Because zone members can access only other members of the same zone, a device not included in a zone is not available to members of that zone.

Zoning can be used for customizing environments and optimizing resources.

Customizing Environments

Use zones to create logical subsets of the fabric to accommodate closed user groups or to create functional areas within the fabric. For example, include selected devices within a zone for the exclusive use of zone members, or create separate test or maintenance areas within the fabric.

Optimizing Resources

Use zones to consolidate equipment, logically, for IT efficiency, or to facilitate time-sensitive functions. For example, create a temporary zone to back up non-member devices.

License Activation

Before using a feature verify that the specific license is activated. Use the `licenseShow` command to view a list of all licenses activated on your switch, as shown in the example below. If the necessary license is not included in the list, continue with [License Activation Using Telnet](#) on page 16 or [License Activation Using Web Tools](#) on page 17.

1. Log onto the switch by telnet using an account that has administrative privileges.
2. Enter the `licenseshow` command on the telnet command line. A list of all activated licenses on the switch will be generated as shown in [Figure 1](#).

License Activation Using Telnet

```
switch:admin> licenseshow
SdcReRcbSbjedSfa:
    Web license
SdcReRcbSbjedSfb:
    Zoning license
SdcReRcbSbjedSd:
    QuickLoop license
SdcReRcbSbjedSfe:
    Fabric license
SdcReRcbSbjedSff:
    Remote Switch license
SdcReRcbSbjedSfg:
    Remote Fabric license
SdcReRcbSbjedSfh:
    Extended Fabric license
SdcReRcbSbjedSfj:
    Entry Fabric license
SdcReRcbSbVedSfM:
    Fabric Watch license
SdcReRcbSbXedSfO:
    Performance Monitor license
SdcReRcbSbbedSfS:
    Trunking license
SdcReRcbSbjedSfy:
    Security license
switch:admin>
```

Figure 1: License activation using telnet

1. Enter the following on the command line, where the word “*key*” is the license key provided to you, surrounded by double quotes. The license key is case sensitive and must be entered exactly as given.

```
licenseadd "key"
```

2. Verify the license was added by entering the `licenseshow` command, as shown in [Figure 1](#). The feature is now activated and available.

License Activation Using Web Tools

If a Web Tools license is activated, Web Tools can be used to activate additional licenses.

1. Launch a Web browser, enter the switch name or IP address in the **Location/Address** section of the browser, and press **Enter**. Web Tools launches, displaying the Fabric View.
2. Click the **Admin** button on the relevant switch panel. The logon window displays.
3. Enter a logon name and password with administrative privileges and press **Enter**. The Administration View displays. Choose the **License Admin** tab.
4. Enter the license key in the **License Key** field and click **Add**. The feature is now activated.

Zoning Concepts

2

This chapter provides the following information:

- [About Zoning](#), page 20
- [Guidelines to Setting Up Zoning](#), page 21
- [Zone Definitions](#), page 22
- [Zone Management](#), page 26
- [Zoning Schemes](#), page 28
- [Implementing Zoning](#), page 30
- [Zone Merging Scenarios](#), page 40
- [Rules of Zoning Architecture](#), page 43

About Zoning

A zone is a specified group of fabric-connected devices, also called zone objects. Any device, or zone object, connected to the fabric can be included in one or more zones. Each zone object within a zone can communicate only with other zone objects within the same zone; any device outside of a zone cannot communicate with zone objects located inside a zone. Once zoning is enabled, if a device is not explicitly defined in a zone, that device will exist in a zone by itself and be inaccessible by other devices in the fabric.

Zone objects are grouped into zones and zones are grouped in a zone configuration. Zones can overlap; that is, a zone object can belong to more than one zone and a fabric can have multiple zones. A switch can have any number of zone configurations resident; however, only one configuration can be enabled at a time.

Figure 2 illustrates three zones with some overlap. It also contains devices that are not assigned to a zone, and are thus not active in the fabric if zoning is enabled.

Note: Once zoning is enabled, if a device is not defined in a zone, that device will exist in a zone all by itself. The device will be isolated and be inaccessible by other devices in the fabric.

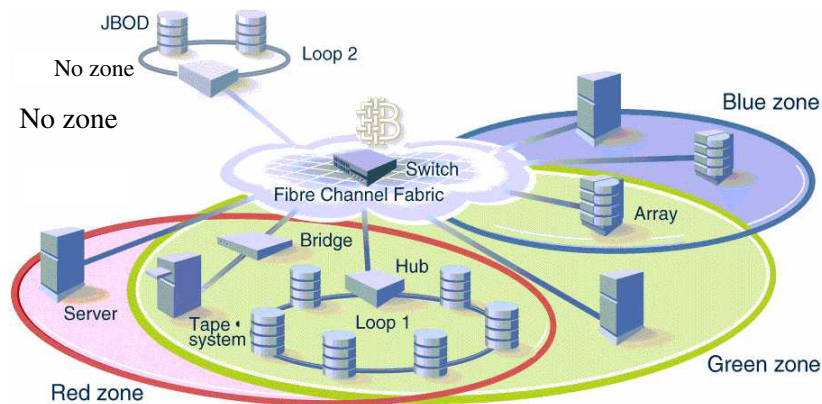


Figure 2: Fabric with three zones

Guidelines to Setting Up Zoning

Below are some guidelines for setting up zoning in your fabric:

- Create a detailed diagram of the fabric, showing all the switches with their inter-switch links (ISLs). The diagram will help to account for every port in the fabric.
- Create an expanded diagram of each switch in the fabric. This diagram will account for every port type on each switch in the fabric (F_Port, FL_Port, E_Port etc.).
- If the fabric is going to contain private loop devices (QuickLoop), then the user will need to account for this. Refer to [Rules of Zoning Architecture](#) on page 43.
- Consider turning off unused ports that have nothing connected to them within zoned fabrics. This is a decision that will affect the security of the fabric. If Secure Fabric OS is utilized, a policy to lock down ports can be implemented.
- For a fabrics with multiple zones enabled within it, it is best to configure one zone at a time and then test it with the Zone Analyzer available in Web Tools. Do not create all the zones at once; it will be more difficult to debug than creating and testing one zone at a time. After the first zone is set up in the fabric, the user may plug in devices and then test the connections to confirm that everything is functioning properly.

Zone Definitions

A Zone in a fabric is a set of devices that have access to one another. All devices connected to a fabric may be configured into one or more zones. Every zone has at least one zone object. Empty zones are not allowed. The zone objects are described by a semicolon-separated list of member definitions.

The memory constraints for zoning are far larger than the number of devices that can be connected to a fabric. The zone size for Fabric OS V4.1 is 128 KB. The zone size for Fabric OS V3.x and V2.x is 96 KB.

Zone definitions and configurations are consistent across reboots and power cycles. If two switches are connected in a fabric, they can become islands unto themselves (for example, due to an ISL failure). When rejoined, they will maintain the same fabric configuration unless one of the switches has had a configuration change.

Zone Objects

A zone object is defined as any of the following:

- Physical port number (area number) on the switch
- Node Worldwide Name
- Port Worldwide name

Zone objects identified by port number or the area number are specified as a pair of decimal numbers “d,area”, where “d” is the Domain ID of the switch and “area” is the port number or area number on that switch. See [Table 2](#) on page 23.

For example, “3,13” specifies port 13 on switch number 3. Another example, “3, 46” specifies port 14 on slot number 3 or area 46. When the physical port number specifies a zone object, then any and all devices connected to that port are in the zone. If this physical port is an arbitrated loop, then all devices on the loop are part of the zone.

World Wide Names (WWNs) are specified as eight hexadecimal numbers separated by colons; for example “10:00:00:90:69:00:00:8a”. When Node Name specifies a zone object, then all ports on that device are in the zone. When Port Name specifies a zone object, then only that single port is in the zone.

The types of zone objects used to define a zone may be mixed and matched. For example, a zone defined with the following zone objects: “2,12; 2,14; 10:00:00:80:33:3f:aa: 11” would contain whatever devices are connected to switch 2, ports 12 and 14, and a device with the WWN (either Node Name or Port Name) “10:00:00:80:33:3f:aa:11” that is connected on the fabric.

Selecting Ports on the Core Switch 2/64

The commands used to administer the Fabric OS V4.1 require specification of the slot and area numbers. These commands use a common specification method. Area numbers distinguish StorageWorks Core switch ports that have the same port number but are on different slots. When specifying a particular slot and port for a command, the slot number operand must be followed by a slash (/), followed by the port number value.

Note: The SAN Switch 2/32 runs Fabric OS V4.1. Because the SAN Switch 2/32 does not implement slots, this portion of the operand is not required.

For example, to enable port 4 on a switch blade in slot 2, specify the following:

```
portEnable 2/4
```

The Core Switch 2/64 switch has a total of 10 slots. Slot numbers 5 and 6 are control processor cards, and slots 1 through 4 and 7 through 10 are switch cards. Each switch card contains 16 ports counted from the bottom 0 to 15. A particular port is represented by both slot number (1 through 10) and port number (0 through 15).

Zoning commands for Fabric OS V4.1 require specifying a port using an area number method, where each port on a particular domain is given a unique area number. Table 2 shows area and port mapping for slots 1 through 10 on a switch.

Table 2: Area and Port Mappings

Slot Number	Area and Port Mappings on a Switch
Slot 1	Area numbers range from 0 to 15 Port numbers range from 0 to 15
Slot 2	Area numbers range from 16 to 31 Port numbers range from 0 to 15
Slot 3	Area numbers range from 32 to 47 Port numbers range from 0 to 15
Slot 4	Area numbers range from 48 to 63 Port numbers range from 0 to 15
Slots 5 and 6	Control Processor Cards
Slot 7	Area numbers range from 0 to 15 Port numbers range from 0 to 15

Table 2: Area and Port Mappings (Continued)

Slot Number	Area and Port Mappings on a Switch
Slot 8	Area numbers range from 16 to 31 Port numbers range from 0 to 15
Slot 9	Area numbers range from 32 to 47 Port numbers range from 0 to 15
Slot 10	Area numbers range from 48 to 63 Port numbers range from 0 to 15

Zone Objects and Aliases

The following sections describe zone objects and zone aliases.

Zone Objects

Zone objects are the devices or ports in a zone. Objects can be categorized as devices that are either part of a fabric zone or of a QuickLoop zone. An object cannot be part of both categories. When zone objects are defined, they are put into zones. One or more zones is a zone configuration.

For example:

Zone Configuration -> Zone -> Zone Objects -> QuickLoop devices/ports or
Fabric devices/ports

```
cfgname -> zonename
```

Zone Aliases

Zone aliases simplify repetitive entry of “zone objects” such as port numbers or World Wide Names. For example, the name “Eng” could be used as an alias for “10:00:00:80:33:3f:aa:11”.

An alias is a name assigned to a device or group of devices. By creating an alias you can assign a familiar name to a device, or you can group multiple devices into a single name. This can simplify cumbersome entries and allow an intuitive naming structure, such as using `NT_Hosts` to define all Windows NT hosts in the fabric.

Zone Configurations

A zone configuration is a group of zones that are enforced whenever that zone configuration is enabled. A zone can be included in more than one zone configuration.

To define a zone configuration, specify the list of zones to be included and assign a zone configuration name. A zone configuration is a set of zones. Zoning may be disabled at any time. When a zone configuration is in effect, all zones that are members of that configuration are in effect.

The set of zone configurations defined in a fabric may not be the same as the configuration that is currently in effect. This may also not be the same as the configurations saved in the flash memory of the switch. The following four terms are used to differentiate between these different configurations:

- **Defined Configuration:** The complete set of all zone objects that have been defined in the fabric.
- **Effective Configuration:** A single zone configuration that is currently in effect. The effective configuration is built when an administrator enables a specified zone configuration. This configuration is “compiled” by checking for undefined zone names, zone alias names, or other issues.
- **Saved Configuration:** A copy of the defined configuration plus the name of the effective configuration which is saved in flash memory by the `cfgSave` command. There may be differences between the “saved configuration” and the “defined configuration” if the system administrator has modified any of the zone definitions and has not saved the configuration.
- **Disabled Configuration:** The effective configuration that is removed from flash memory.

On power up, the switch automatically reloads the “saved configuration”, and if a configuration was in effect when it was saved, the same configuration will be reinstated with an auto run of the `cfgEnable` command.

Zone Management

Zoning may be managed one of three ways: either by logging into the switch via telnet, via Web Tools, or via Fabric Manager. Any switch in the fabric can be used to make changes to the zoning configuration. The changes will be replicated to all the other switches in the fabric only if commands which “close a transaction” are used.

Zoning commands are executed under the transaction model. A working copy of the defined configuration is created at the start of a transaction. Each Zoning command is executed from the working copy.

Note: When a transaction is opened, all new zoning information is placed in a transactional buffer. The new changes are not applied to the fabric until the transaction is closed. A transaction is aborted when another switch closes its transaction or by issuing the command `cfgTransAbort`. When a transaction is closed, all new and existing zoning information is applied to the fabric and saved to flash memory.

Commands to Open a Transaction

The following commands can be issued to open a transaction:

<code>aliAdd</code>	Add a member to a zone alias
<code>aliCreate</code>	Create a zone alias
<code>aliDelete</code>	Delete a zone alias
<code>aliRemove</code>	Remove a member from a zone alias
<code>cfgAdd</code>	Add a member to a configuration
<code>cfgClear</code>	Clear all zone configurations
<code>cfgCreate</code>	Create a zone configuration
<code>cfgDelete</code>	Delete a zone configuration
<code>cfgRemove</code>	Remove a member from a configuration
<code>fazoneAdd</code>	Add a member to a Fabric Assist zone
<code>fazoneCreate</code>	Create a Fabric Assist zone
<code>fazoneDelete</code>	Delete a Fabric Assist zone
<code>fazoneRemove</code>	Remove a member from a Fabric Assist zone
<code>qloopAdd</code>	Add a member to a qloop

<code>qloopCreate</code>	Create a qloop
<code>qloopDelete</code>	Delete a qloop
<code>qloopRemove</code>	Remove a member from a configuration
<code>zoneAdd</code>	Add a member to a zone
<code>zoneCreate</code>	Create a zone
<code>zoneDelete</code>	Delete a zone
<code>zoneRemove</code>	Remove a member from a zone

Commands to Close a Transaction

The following commands close a transaction:

<code>cfgDisable</code>	Disable a zone configuration
<code>cfgEnable</code>	Enable a zone configuration
<code>cfgSave</code>	Save zone configurations in flash

Informative Commands—The following commands do not impact a transaction and are for information only:

<code>aliShow</code>	Print aliases
<code>cfgShow</code>	Print configuration information
<code>zoneShow</code>	Print zone configuration information
<code>qloopShow</code>	Print qloop configuration

Zoning Schemes

Zone schemes are the method in which a zone is established. A zone is established by identifying zone objects by using one or more of the following schemes: the switch and port, World Wide Name (WWN), or AL_PA. The zoning schemes are defined below.

Switch/Port Level Zoning	A zone containing members specified by either domain ID with port number or area number, or aliases of <domain, area>. For information about specifying ports and area numbers, refer to Table 2 on page 23.
WWN Level Zoning	A zone containing members specified only by device World Wide Names (WWNs), or aliases of WWNs.
AL_PA Level Zoning	Members of a QuickLoop are specified by the AL_PA when zoned. Identification other than AL_PAs in a QuickLoop cannot be used.
Mixed Zoning	A zone containing members specified by a combination of WWN and switch port number or area number. Mixed zones are software enforced through the fabric name server only.

Zone Enforcement

Zones are either hardware enforced or software enforced depending on the scheme that is used. When a zone is specified by either port number (area number) or WWN, but not both, it will be a hardware-enforced zone. When a zone is specified by both port number and WWN, it is a software-enforced zone.

Hardware-enforced zoning is enforced at the ASIC level with support from the Name Server. Each ASIC maintains a list of source port IDs that have permission to access any of the ports on that ASIC. Software-enforced zoning is exclusively enforced through selective information presented to end nodes through the fabric Simple Name Server (SNS).

When zoning is disabled, the fabric is in a non-zoning mode, and devices can freely access other devices in the fabric. When zoning is enabled, zoning is enforced throughout the fabric, and devices can communicate only within their zones.

To discern if a zone is hardware-enforced, use either the `portZoneShow` command or `portcamshow` command, as shown in [Figure 3](#).

```

C:\WINNT\System32\cmd.exe - telnet 192.168.188.21
SW3800_CA:admin> portZoneShow

Local Zoning Port-level information:
  0      PORT: 0  enforcement: SOFT      defaultSoftZone: 1      defaultHardZone:
ardZone: 0
  0      PORT: 1  enforcement: HARD PORT      defaultSoftZone: 0      defaultH
ardZone: 0
  0      PORT: 2  enforcement: HARD PORT      defaultSoftZone: 0      defaultH
ardZone: 0
  0      PORT: 3  enforcement: HARD PORT      defaultSoftZone: 0      defaultH
ardZone: 0
  0      PORT: 4  enforcement: HARD PORT      defaultSoftZone: 0      defaultH
ardZone: 0
  0      PORT: 5  enforcement: SOFT      defaultSoftZone: 1      defaultHardZone:
ardZone: 1
  0      PORT: 6  enforcement: HARD PORT      defaultSoftZone: 0      defaultH
ardZone: 0
  0      PORT: 7  enforcement: SOFT      defaultSoftZone: 1      defaultHardZone:
ardZone: 0
  0      PORT: 8  enforcement: HARD PORT      defaultSoftZone: 0      defaultH
ardZone: 0
  0      PORT: 9  enforcement: SOFT      defaultSoftZone: 1      defaultHardZone:
ardZone: 0
  0      PORT: 10 enforcement: HARD PORT      defaultSoftZone: 0      defaultH
ardZone: 0
  0      PORT: 11 enforcement: SOFT      defaultSoftZone: 1      defaultHardZone:
ardZone: 0
  0      PORT: 12 enforcement: SOFT      defaultSoftZone: 1      defaultHardZone:
ardZone: 0
  0      PORT: 13 enforcement: SOFT      defaultSoftZone: 1      defaultHardZone:
ardZone: 0
  0      PORT: 14 enforcement: SOFT      defaultSoftZone: 1      defaultHardZone:
ardZone: 0
  0      PORT: 15 enforcement: SOFT      defaultSoftZone: 1      defaultHardZone:
ardZone: 0

```

Figure 3: PortZoneShow output

Implementing Zoning

Zoning can be implemented and administered from any switch in the fabric that has a Zoning license enabled. When a change in the configuration is saved, enabled, or disabled per the transactional model, it is automatically distributed to all switches in the fabric.

Create and Enable a Basic Zone Configuration

To create and enable a basic zone configuration, follow the procedure below. For a detailed explanation see “[Detailed Zone Configuration Procedures](#)” on page 30.

1. Create a zone: `zoneCreate "zonename", "ports"`
2. Create a zone configuration: `cfgCreate "cfgname", "zonename"`
3. Enable the zone configuration: `cfgEnable "cfgname"`

The following is an example of the above procedure:

```
zonecreate "zone_1", "1,0;1,2"  
cfgcreate "zonecfg_1", "zone_1"  
cfgenable "zonecfg_1"
```

Detailed Zone Configuration Procedures

To implement zoning, perform these procedures, as described in the sections below.

1. Review current configurations, if any.
2. Create an alias.
3. Define the zone.
4. Define the zone configuration.
5. Analyze the zone configuration.
6. Enable the zone configuration.
7. Review the enabled configuration.

Note: Each zone object defined—alias, zone, zone configuration—must have a unique name; that is, an alias cannot have the same name as another alias, zone, or zone configuration.

Review Current Configurations

Use the `cfgShow` command to show all currently defined configurations and the effective configuration.

```
test180_Jr:admin>cfgShow
Defined configuration
  cfg:      cfg1      ql_zone1; al_zone2; fabric_zone1;
fabric_zone2
zone:      fabric_zone1
           Fabric_ServerA; Fabric_StorageA
zone:      fabric_zone2
           Fabric_ServerB; Fabric_StorageB
zone:      ql_zone1
           Private_ServerA; Private_StorageA
zone:      ql_zone2
           Private_ServerB; Private_StorageB
alias: Fabric_ServerA
       50:06:0b:00:00:06:9a:d6
alias: Fabric_ServerB
       50:06:0b:00:00:06:ad:10
alias: Fabric_StorageA
       50:06:04:82:bc:01:0a:1b
alias: Fabric_StorageB
       50:06:04:82:bc:01:9a:1c
alias: Private_ServerA
       1,3
alias: Private_ServerB
       1,4
alias: Private_StorageA
       2,2
alias: Private_StorageB
       2,1
Effective configuration:
  cfg: cfg1
  zone: fabric_zone1
       50:06:0b:00:00:06:9a:d6
       50:06:04:82:bc:01:9a:1b
  zone: fabric_zone2
       50:06:0b:00:00:06:ad:10
       50:06:04:82:bc:01:9a:1c
```

```
zone:    ql_zone1
         1,3
         2,2

zone:    ql_zone2
         1,4
         2,1

test180_Jr:admin>
<END>
```

Create an Alias

An alias must be a unique alpha-numeric string beginning with an alpha character. The underscore character (`_`) is allowed and alias names are case sensitive. For example, `nt_hosts` is not the same name as `NT_Hosts`.

Note: Aliases can greatly simplify the administrative process; however, they are not required to define zones. The alias name may not exceed 64 characters.

Use the `aliCreate` command to create aliases for areas 5 and 29 on switch 7 as shown in this example.

```
test180_Jr:admin> aliCreate "alias by port level", "7, 5: 7, 29"
```

Use the `aliCreate` command to create an alias for a RAID with a known WWN as shown in this example.

```
test180_Jr:admin> aliCreate "RAID_1_NodeName",
"50:06:0b:00:00:06:9a:d6"
```

Define a Zone

Specify the list of zone objects to be included and assign a unique zone name; the zone name must be a unique alpha-numeric string beginning with an alpha character. The underscore character (`_`) is allowed and zone names are case sensitive. For example, `green_zone` is not the same name as `Green_Zone`.

Note: The zone name may not exceed 64 characters.

Zones may be created with or without the use of aliases as shown in the examples below.

Use the `zoneCreate` command to create a zone using the newly created aliases from above as shown in this example.

```
test180_Jr:admin>zoneCreate "fabric_zone1", "RAID_1_NodeName;  
alias by port level"
```

Use the `zoneCreate` command to create a zone without using aliases as shown in this example.

```
test180_Jr:admin>zoneCreate "fabric_zone2",  
"20:06:0b:00:00:06:9a:d6; 20:06:0b:00:00:06:9a:d7"
```

Define a Zone Configuration

To define a zone configuration, specify the list of zones to be included and assign a zone configuration name; the zone configuration name must be a unique alpha-numeric string beginning with an alpha character. The underscore character (`_`) is allowed and zone names are case sensitive. For example, `configuration1` is not the same name as `Configuration1`.

Use the `cfgCreate` command to create your zone configuration.

```
test180_Jr.admin> cfgCreate "cfg1", fabric_zone1; fabric_zone2"
```

Analyze the Zone Configuration

After creating and saving a zone configuration, HP recommends analyzing the zone configuration. Doing this will save time and potential issues.

The Zoning Configuration Analyze screen displays a summary of the saved configuration and warns of zoning conflicts before enabling them. Some potential errors that might be caught are:

- Ports/WWN/Devices that are part of the selected configuration but are not part of the fabric.
- Zones with a single zone object.

To access the Zoning Configuration Analysis screen, click the **Analyze Config** button, in the Zone Administration window in Web Tools.

Enable a Zone Configuration

Use the `cfgEnable` to enable and save your configuration.

```
test180_Jr:admin>cfgEnable "cfg1"  
Setting switch to Fabric mode,  
Committing configuration...done.  
zone config "cfg1" is in effect
```

When a zone configuration is enabled the following detailed list of events occur. Registered State Change Notifications (RSCNs) are sent to all fabric devices within the zone, notifying these devices to re-query the name server to discover available devices that can be accessed. All zones within the configuration are enabled. Once a zone configuration is enabled the following events happen:

1. All aliases are expanded if any are defined in the zone configuration.
2. Inconsistencies are checked. If inconsistencies are discovered, an error occurs and the previous state of the fabric is preserved. (For example, if zoning is disabled, it remains disabled; if an existing configuration is enabled, it remains enabled.)
3. Zone members are loaded.
4. If the steps above were successful, all switches in the fabric are loaded with the zoning information.
5. RSCNs are generated and sent to all devices within the zone.

Review The Enabled Configuration

To review the enabled zone configuration, use the `cfgShow` command.

```
test180_Jr:admin>cfgShow
Defined configuration
  cfg:          cfg1          ql_zone1; al_zone2; fabric_zone1;
fabric_zone2
zone:          fabric_zone1
              Fabric_ServerA; Fabric_StorageA
zone:          fabric_zone2
              Fabric_ServerB; Fabric_StorageB
zone:          ql_zone1
              Private_ServerA; Private_StorageA
zone:          ql_zone2
              Private ServerB; Private StorageB
alias: Fabric_ServerA
              50:06:0b:00:00:06:9a:d6
alias: Fabric_ServerB
              50:06:0b:00:00:06:ad:10
alias: Fabric_StorageA
              50:06:04:82:bc:01:0a:1b
alias: Fabric_StorageB
              50:06:04:82:bc:01:9a:1c
```

```
alias: Private_ServerA
      1,3
alias: Private_ServerB
      1,4
alias: Private_StorageA
      2,2
alias: Private_StorageB
      2,1
Effective configuration:
  cfg: cfg1
  zone: fabric_zone1
        50:06:0b:00:00:06:9a:d6
        50:06:04:82:bc:01:9a:1b
zone:   fabric_zone2
        50:06:0b:00:00:06:ad:10
        50:06:04:82:bc:01:9a:1c
zone:   ql_zone1
        1,3
        2,2
zone:   ql_zone2
        1,4
        2,1
test180_Jr:admin>
<END>
```

Modifying Configurations

To make changes to an existing configuration, add, delete, or remove individual elements to create the desired configuration. Once the changes have been made, save the configuration. This ensures the configuration is permanently saved in the switch, and it also ensures that the configuration is replicated throughout the fabric.

The switch configuration file can also be uploaded to the host for archiving, and it can be downloaded from the host to all switches in the fabric. See the `configupload` and `configdownload` commands in the *HP StorageWorks Fabric OS Version 3.1.x/4.1.x Reference Guide*.

Before Merging Zones

To facilitate merging, check the following before merging switches or fabrics.

- **Zoning licenses**—All switches must have a Zoning license enabled.
- **Native operating mode**—All switches must be in the native operating mode.
- **HP Secure Fabric OS**—If any one switch has HP Secure Fabric OS enabled, all switches in the fabric must have HP Secure Fabric OS. Refer to the *HP StorageWorks Secure Fabric OS Version 1.0 User Guide* for more information.

Adding a New Switch

When a new switch is added to the fabric, it automatically takes on the zone configuration information from the fabric. To add the new switch, attach the E_ports, and the new switch is incorporated into the fabric and the enabled zone configuration. By using the `cfgShow` command, the zoning information displayed will be the same on each switch in the fabric

A new switch is a switch that has not previously been connected to a fabric with a zoning configuration, and has no zone configuration data entered into it. A switch that is configured for zoning may be returned to this new switch state by using the `cfgClear` and `cfgSave` commands before connecting it to the zoned fabric, or by using `cfgClear` and `cfgDisable` if there is an effective configuration.

Adding a New Fabric

Adding a new fabric that has no zone configuration information to an existing fabric is very similar to adding a new switch. All switches in the new fabric inherit the zoning configuration data. If a zone configuration is in effect, then the same configuration becomes the enabled configuration. The `cfgShow` command will display the same information on all switches in the newly formed Fabric. Before the new fabric can merge successfully, it must pass the merging and segmentation criteria listed below.

Merging and Segmentation

The fabric is checked for segmentation during the fabric configure/reconfigure during power-up, when a switch is disabled/enabled, or when a port switches to an F-port.

The entire “Defined Configuration” is merged with adjacent switches, before the Effective Configuration Name is sent, if one exists.

There are two databases used with zoning. The first database is the zone configuration database. This is the data displayed as the “defined configuration” in the `cfgShow` command. It is stored in flash by the `cfgSave` command. This database is a replicated database, which means that all switches in the fabric will have a copy of this database. When a change is made to the defined configuration, the switch where the changes were made must close its transaction for the change to be propagated throughout the fabric.

The second database used with zoning is the N_Port login database. It is stored locally on each switch and is used for translating the World Wide Names into physical port numbers when WWNs are used in zoning. The checking is run locally when the port number can make a match on that switch alone. When the port number is not enough, that switch has to query the remote switches to get the needed login information. This information is cached on the local switch until RSCN renders it stale. There is also a time-out value (usually set from 10 to 15 minutes), after which it will be deleted from the Name Server database.

If debugging is required, the local login data can be viewed using the `portLoginShow pn` command, where “pn” is the port or area number on that switch. The cache of remote logins can be viewed by making a query to the Name Server or using `zoneCheck` with two valid Destination IDs (DIDs), then use the `cfgRemoteShow` command.

Merging Rules

- If the local and adjacent zone database configurations are the same, they will remain unchanged after the merge.
- If there is an effective configuration between two switches, the zone configuration in effect must be the same for the fabrics to merge.
- If a zoning object has the same name in both the local and adjacent defined configurations, the object types and member lists must also be the same. When comparing member lists, the content and order of the members are important.
- If a zoning object appears in an adjacent defined configuration, but not in the local defined configuration, the zoning object is added to the local defined configuration. The modified zone database must be small enough to fit in the flash area allotted for the zone database.
- If a local defined configuration is modified because of a merge, the new zone database is propagated to other switches within the merge request.

Merging Two Fabrics

The simplest scenario for merging two fabrics is when both fabrics have identical zones and the same configuration enabled, the two fabrics will join to make one larger fabric. The same zone configuration will be in effect across this newly created fabric.

If the two fabrics have different zone configurations, then the two sets of information will be merged, or the ISL between the switches will be segmented if the two fabrics cannot join. Refer to [Table 3](#) on page 40 for more information.

Merging with a V4.1 Fabric

If the user has a StorageWorks Core switch-based fabric, or other switches running Fabric OS V4.1, the firmware can operate in the same fabric with StorageWorks SAN switches running Fabric OS V3.0.1a or later firmware. Switches running Fabric OS V4.1 firmware can operate in the same fabric with all StorageWorks 1 Gb SAN switches running V2.6 or later. However, HP recommends that each switch in the SAN run the latest supported firmware for that switch.

Merge Conflicts

When a merge conflict is present, a merge will not take place and the ISL will segment. Below is a list of possible reasons for merge conflicts.

Use the `switchshow` command to obtain additional information about possible merge conflicts, as many non-zone related configuration parameters may cause conflicts

If the fabrics have different zone configuration data, the two sets of zone configuration data are merged if possible. If the zones cannot merge, the interswitch link (ISL) will be segmented. A merge is not possible if any of the following exist:

Configuration mismatch	Zoning is enabled in both fabrics, and the zone configurations that are enabled are different in each fabric.
Type mismatch	The name of a zone object in one fabric is used for a different type of a zone object in the other fabric.
Content mismatch	The definition of a zone object in one fabric is different from the definition of zone object with the same name in the other fabric.

Note: If the order of zoneset members between two switches are not listed in the same order, the configuration is considered a mismatch, resulting in the switches being segmented in the fabric. For example: `cfg1 = z1; z2` is different from `cfg1 = z2; z1`, even though members of the configuration are the same. If zoneset members between two switches have the same name defined in the configuration, make sure zoneset members listed are in the same order.

Splitting a Fabric

If the connections between two fabrics are no longer available, the fabric will segment into two separate fabrics. Each new fabric will retain the same zone configuration.

If the connections between two fabrics are replaced and no changes have been made to the zone configuration in either of the two fabrics, then the two fabrics are guaranteed to merge back into one single fabric. If any changes that cause a conflict have been made to either zone configuration, then the fabrics may segment.

Zone Merging Scenarios

Following are the various Zone Merge scenarios. The “Expected Results” column gives the user an idea of how to do successful merges quickly. The table also gives good guidelines of what to do to avoid merge problems.

Table 3: Zone Merging Scenarios

Description	Switch A	Switch B	Expected Results
<p>Switch A has a defined configuration.</p> <p>Switch B does not have a defined configuration.</p>	<p>defined: cfg1: zone1: ali1; ali2 effective: none</p>	<p>defined: none effective: none</p>	<p>Configuration from Switch A to propagate throughout the fabric in an inactive state, since the configuration is not enabled.</p>
<p>Switch A has a defined and enabled configuration.</p> <p>Switch B has a defined configuration but no effective configuration.</p>	<p>defined: cfg1 zone1: ali1; ali2 effective: cfg1:</p>	<p>defined: cfg1 zone1: ali1; ali2 effective: none</p>	<p>Configuration from Switch A to propagate throughout the fabric.</p>
<p>Switch A and Switch B have the same defined configuration. Neither have an enabled configuration.</p>	<p>defined: cfg1 zone1: ali1; ali2 effective: none</p>	<p>defined: cfg1 zone1: ali1; ali2 effective: none</p>	<p>No change (clean merge).</p>
<p>Switch A and Switch B have the same defined and enabled configuration.</p>	<p>defined: cfg1 zone1: ali1; ali2 effective: cfg1:</p>	<p>defined: cfg1 zone1: ali1; ali2 effective: cfg1:</p>	<p>No change (clean merge).</p>
<p>Switch A does not have a defined configuration.</p> <p>Switch B with a defined configuration.</p>	<p>defined: none effective: none</p>	<p>defined: cfg1 zone1: ali1; ali2 effective: none</p>	<p>Switch A will absorb the configuration from the fabric.</p>

Table 3: Zone Merging Scenarios (Continued)

Description	Switch A	Switch B	Expected Results
Switch A does not have a defined configuration. Switch B has a defined configuration.	defined: none effective: none	defined:cfg1 zone1: ali1; ali2 effective: cfg1	Switch A will absorb the configuration from the fabric, with cfg1 as the effective cfg.
Switch A and Switch B have the same defined configuration. Only Switch B has an enabled configuration.	defined: cfg1 zone1: ali1; ali2 effective: none	defined: cfg1 zone1: ali1; ali2 effective: cfg1	Clean merge, with cfg1 as the effective cfg.
Switch A and Switch B have different defined configurations. Neither has an enabled zone configuration.	defined: cfg2 zone2: ali3; ali4 effective: none	defined: cfg1 zone1: ali1; ali2 effective: none	Clean merge; the new cfg will be a composite of the two— defined: cfg1 zone1: ali1; ali2 cfg2: zone2: ali3; ali4 effective: none.
Switch A and Switch B have different defined configurations. Switch B has an enabled configuration.	defined: cfg1 zone2: ali3; ali4 effective: none	defined: cfg1 zone1: ali1; ali2 effective: cfg1	Clean merge; The new cfg will be a composite of the two, with cfg1 as the effective cfg.
Effective cfg mismatch.	defined: cfg1 zone1: ali1; ali2 effective: cfg1 zone1: ali1; ali2	defined: cfg2 zone2: ali3; ali4 effective: cfg2 zone2: ali3; ali4	Fabric segments due to: Zone Conflictcfg mismatch.
cfg content mismatch.	defined: cfg1 zone1: ali1; ali2 effective: irrelevant	defined: cfg1 zone1: ali3; ali4 effective: irrelevant	Fabric segments due to Zone Conflictcontent mismatch.
	defined: cfg1 zone1: ali1; ali2 effective: irrelevant	defined: cfg1 zone1: ali1; ali4 effective: irrelevant	Fabric segments due to Zone Conflictcontent mismatch.

Table 3: Zone Merging Scenarios (Continued)

Description	Switch A	Switch B	Expected Results
Same content; different effective cfg name.	defined: cfg1 zone1: ali1; ali2 effective: cfg1 zone1: ali1; ali2	defined: cfg2 zone1: ali1; ali2 effective:cfg2 zone1: ali1; ali2	Fabric segments due to Zone Conflictcfg mismatch.
Same content; different zone name.	defined: cfg1 zone1: ali1; ali2 effective: irrelevant	defined: cfg1 zone2: ali1; ali2 effective: irrelevant	Fabric segments due to Zone Conflict content mismatch.
Same content; different alias name.	defined: cfg1:ali1: A; B effective: irrelevant	defined: cfg1:ali2: A; B effective: irrelevant	Fabric segments due to Zone Conflictcontent mismatch.
Same name; different types.	effective: zone1: MARKETING	effective: cfg1: MARKETING	Fabric segments due to Zone Conflicttype mismatch.
Same name; different types.	effective: zone1: MARKETING	effective: alias1: MARKETING	Fabric segments due to Zone Conflicttype mismatch.
Same name; different types.	effective: cfg1: MARKETING	effective: alias1: MARKETING	Fabric segments due to Zone Conflicttype mismatch.

Resolving Zone Conflicts

Zone conflicts can be resolved by using `configupload` and performing a cut and paste operation so the config info matches in both fabrics being merged.

Zone conflicts can also be resolved by performing a `cfgClear` followed by a `cfgDisable` on the segmented fabric that is incorrectly configured. Then do a `portDisable/portEnable` on one of the ISL ports that connects the fabrics. This will cause a merge that will make the fabric consistent with the good configuration. Be careful in using the `cfgClear` command; this command can inadvertently delete the zone configuration in the fabric.

Rules of Zoning Architecture

Here is a list of the rules of zoning architecture.

- Rule 1** Type of Zoning (Hard or Soft)—If security is a priority, then a Hard zoning is recommended.
- Rule 2** The use of aliases is optional with zoning. Using aliases should force some structure when defining zones. Aliases will also aid future administrators of the zoned fabric in understanding the structure and context.
- Rule 3** Evaluate the security requirements of the fabric. Add HP Secure Fabric OS into the fabric if extra security is required.
- Rule 4** Inter-operability Fabric—If the fabric includes a StorageWorks Core switch or StorageWorks 2 Gb SAN switch and the user needs to support a third-party switch product, then that user will only be able to do WWN zoning. Other types of zoning, including QuickLoop zoning, will not be supported.
- Rule 5** Evaluate whether the fabric will have QuickLoop Fabric Assist (QLFA) or QuickLoop (QL) in it. If the user is running HP Fabric OS V4.1, then there are a couple things to consider before creating and setting up QLFA zones:
 - QuickLoop Zoning—QuickLoop/QuickLoop zones cannot run on switches running HP Fabric OS V4.1. HP Fabric OS V4.1 can still manage (create, remove, update) QL zones on any non-V4.1 switch.
 - QuickLoop Fabric Assist—HP Fabric OS V4.1 cannot have a Fabric Assist host directly connected to it. However, HP Fabric OS V4.1 can still be part of a Fabric Assist zone if a Fabric Assist host is connected to a non-V4.1 switch.
- Rule 6** Testing a (new) zone configuration—Before implementing a zone, the user should run the Zone Analyzer from Web Tools to isolate any possible problems. This is especially useful as fabrics increase in size.

- Rule 7** Zone changes in a production fabric can result in a disruption of I/O under conditions where an RSCN is issued as a result of a zone change and the host bus adapter (HBA) is unable to process the RSCN quickly enough. Though RSCNs are a normal part of a functioning SAN, the pause in I/O may not be acceptable. For these reasons, it is recommended to do zone changes only if the resulting behavior is known and acceptable. Changing HBA drivers can rectify the situation.
- Rule 8** After changing or enabling a zone configuration, the user should confirm that nodes and storage are able to see and access one another. Depending on the platform, the user may need to reboot one or more nodes in the fabric with the new changes to the zone.

Using QuickLoop Zones

3

In addition to zoning fabrics, explained in Chapter 2, zoning can also be used to zone QuickLoop, allowing arbitrated loops to be attached to a fabric. The QuickLoop and zoning combination allow a private host to fully participate in a Storage Area Network (SAN). By partitioning selected devices within a QuickLoop into a QuickLoop zone, you can enhance management of a Fibre Channel Arbitrated Loop (FC-AL) in a legacy environment.

Note: Refer to the *HP StorageWorks QuickLoop Fabric Assist Version 3.1.x User Guide* for detailed information about HP QuickLoop.

QuickLoop Zones

QuickLoop zones are hardware enforced. Switch hardware prevents unauthorized data transfer between ports within the zone, allowing devices to be partitioned into zones to restrict system access to selected devices. Once devices are included in a zone, they are visible only to other devices within that zone.

QuickLoop zone members are designated by looplet (port number), or by Arbitrated Loop Physical Address (AL_PA). There are 126 unique AL_PAs per QuickLoop; therefore, a QuickLoop zone can contain no more than 125 devices.

Note: Each QuickLoop port uses one AL_PA.

Fabric zones and QuickLoop zones are independent of each other. Both types of zones can co-exist in the same zone configuration, and QuickLoop devices can be included within a fabric zone configuration. But, while devices within a QuickLoop can be seen by a public host, devices within each QuickLoop are only visible to devices within their own QuickLoop.

In QuickLoop zoning, devices within a QuickLoop can be partitioned off within that QuickLoop to form QuickLoop zones. In other words, a QuickLoop Zone is a subset of a QuickLoop and can include only QuickLoop devices.

Note: QuickLoop is supported in Fabric OS V3.1; however, it is not supported in Fabric OS V4.1.

QuickLoop Zoning Advantages

In addition to the advantages of fabric zoning—security, customized environments, and optimization of IT resources—QuickLoop zoning can protect devices from disruption by unrelated devices during a critical process; for example, during a tape backup session.

In a QuickLoop with zoning enabled, transmission of the loop initialization primitive (LIP) signal and loop initialization are controlled by the switch. The LIP is transmitted only to looplets within the affected zone. Other looplets on the QuickLoop are not affected. In this way, unwanted disruption to devices can be controlled.

Configuring QuickLoop Zones

To configure QuickLoop zoning, perform these steps as described in the following sections.

1. Create a QuickLoop (Only required when zoning by AL_PA.)
2. Define a QuickLoop zone
3. Define a QuickLoop zone configuration

Create a QuickLoop

Refer to the *HP StorageWorks QuickLoop Fabric Assist Version 3.1.x User Guide* for information about creating a QuickLoop.

Define a QuickLoop Zone

A QuickLoop zone is a group of L_ports or AL_PAs that can communicate with each other. These ports and AL_PAs must reside within the same QuickLoop. To be a QuickLoop zone, every member must be either a looplet (L_port) or an AL_PA within a single QuickLoop. QuickLoop zones can overlap looplets, but they must be confined to a single QuickLoop.

QuickLoop zones are hardware enforced, but zones within a single looplet are not enforceable; therefore, it is recommended that you do not partition devices within a looplet into different zones.

To define a QuickLoop zone, first enable and create the necessary QuickLoops. Then specify the list of members to be included and assign a unique zone name. A QuickLoop zone name must be a unique alpha-numeric string beginning with an alpha character. The underscore character (`_`) is allowed and zone names are case sensitive. For example, `Zone1` is not the same name as `zone1`.

To create a QuickLoop zone, specify QuickLoop zone members by looplet, by AL_PA, or by combination of the two.

To Specify by Looplet

Specify the QuickLoop zone name, in quotes, and the physical ports to be included, in quotes. For example:

```
Zonecreate "QLZoneName", "0,0; 0,1; 2,6; 2,7; 2,8"
```

To Specify by AL_PA

Specify the QuickLoop zone name, in quotes, with the QuickLoop name and desired AL_PAs, in quotes. All AL_PAs must be associated with a QuickLoop name. For example:

```
Zonecreate "QLZoneName", "qloop1[01,02,04,e0,e1,e2]"
```

To specify a Combination of looplet and AL_PA

Example:

```
Zonecreate "QLZoneName", "0,2; 0,3; qloop1[ca,cb,e1,e2]"
```

Define a QuickLoop Zone Configuration

To define a QuickLoop zone configuration, assign a zone configuration name and specify the QuickLoop zones to be included, by zone name. The QuickLoop names of the QuickLoop zones must also be included in the zone configuration.

An example of a QuickLoop zone configuration is:

```
cfgname "cfgname", "QLZoneName"
```

For example:

```
cfgname "QLconfig_1", "QLZoneName", "qloop1[01,02,04,e0,e1,e2]"  
cfgenable "QLconfig_1"
```

QuickLoop Fabric Assist

Fabric Assist allows a private host to talk to public/private targets located anywhere within the fabric (if no zoning exists). Private hosts and targets are put into a single Fabric Assist zone, and are identified either by domain and port number or by WWN. Each Fabric Assist zone can have only one private host. The user will need QuickLoop and Zoning licenses to use these features.

Fabric Assist Zone Setup

Zoning commands with the prefix `fazone` that mirror other zoning commands are: `fazoneCreate`, `fazoneAdd`, `fazoneDelete`, `fazoneRemove`, and `fazoneShow`.

Private hosts are indicated within a `fazone` or alias by “H{ }”. Within a single `fazone` or alias, multiple initiators are detected during zone creation process. `CfgEnable` can fail if multiple initiators are found in a single `fazone`.

Fabric Assist Zone Creation

The private host within a `fazone` has its own `AL_PA` domain space. A target that is zoned with multiple hosts may be given different `AL_PAs`. A max of 125 unique targets may be zoned with private hosts on any given switch.

Note: A `fazone` private host must be on a loop by itself. Sharing a loop with other nodes will cause the `fazone` to fail.

Fabric Assist Operation

When “`cfg`” is enabled, `AL_PAs` are created for all zoned targets that are online, on the private host's loop. The private host's loop is re-LIPed so that it may “see” any added `AL_PAs`.

As additional targets join the fabric, if they are within the `fazone`, they will have an `AL_PA` created on the private host's loop. This is triggered off of the RSCN. A target may be zoned with one or more private hosts, and will have a unique `AL_PA` created on each host's loop.

LIP Propagation

LIPs are propagated to all private devices within a `fazone`. They are not sent to public targets in the `fazone`. LIPs are only sent when a `fazone` target comes online. A loop of `fazone` targets that are re-LIPed, but do NOT add any new targets will not propagate a LIP to any private hosts.

Fabric Assist Debugging

The `FaDebugShow` command can help troubleshoot FA issues by displaying internal Fabric Assist tables.

`FaDebugShow`: Displays the internal Fabric Assist tables.

Zoning Concepts and Guidelines



This appendix provides the following information:

- [Storage Area Networks](#), page 54
- [Zoning](#), page 55
- [Zone Management](#), page 56
- [Zoning Implementations](#), page 57
- [Fabric-Based Zoning Philosophies](#), page 58
- [The Effect of Zoning on RSCN Delivery](#), page 61
- [Implementing Zoning](#), page 63
- [Hardware-Enforced Zoning in an HP Fabric](#), page 65

Storage Area Networks

The storage area network brings the connectivity of networks to the SCSI protocol. The Fibre Channel standard provides for up to 16 million devices attached to the network. This change in scale required a new method to discover the devices on the fabric, so that discovery can be accomplished in an acceptable time frame.

The fabric well-known service “nameserver” was implemented to address this need. When a device initially accesses the fabric, it must perform a login process. During this process the device will register with the nameserver. The nameserver records information about the device; that is, protocols supported, World Wide Name (WWN), network address, supported class of service, for example.

When an initiator accesses the network it can query the nameserver for all attached devices and their capabilities. Any initiator can query (probe) the fabric for all targets, and then proceed to initialize the targets and perform I/O. This can be disastrous if another initiator is already utilizing the target and has stored data on it such as with a disk or tape. The process of zoning is utilized to provide a virtual SCSI bus that limits the devices that an initiator can discover and access.

Zoning

Zoning is essentially a filter that is applied by the nameserver against the query from the initiator which limits the information returned by the nameserver to the initiator. A zone contains the WWN of the initiator and the WWN of any devices that it is allowed to access. When an initiator queries the nameserver for accessible devices in the fabric, the nameserver will look for all zones that contain the WWN of the initiator. Then a list is formed from all the members of the zones and is applied to the contents of the nameserver. Only devices that are in the list and in the nameserver are returned to the initiator as accessible devices. The initiator then uses the list of returned devices, along with the access parameters returned and proceeds to further inquire of the devices for specific operational capabilities.

Devices that are not part of the zone are not returned as accessible devices. It is important to note that this process does not prohibit access to the device. If the initiator has prior knowledge of the device, it can access the device. The nameserver does not control access to devices on the fabric. Dependable zoning operation depends on the cooperation of all devices in the fabric to only access devices that are returned in the query from the nameserver. HP fabric switches provide for hardware enforcement of the zoning configuration to prevent unwanted access to devices.

Devices can be listed in more than one zone. Thus, overlapping zones are permitted. A concept of most permissible access is used in zoning. When an initiator requests the list of accessible devices, if at least one zone containing the WWN of the initiator exists then any device in that zone is accessible. If the same device exists in another zone that does not contain the WWN of the initiator, the device is still accessible to the initiator.

Zone Management

Management of the zone information is provided via command line (telnet), Web Tools, and Fabric API via third-party software. There are three components to the zone information: the zone objects, the zone name, and the zone configuration. One or more objects (devices) are placed into a zone and given a zone name. One or more zone names are placed into a zone configuration. One or more configurations are defined. Then one and only one configuration is made the effective configuration for the fabric. The number of aliases, zones, and defined configurations is limited only by the memory available in the HP switch.

It is important to note that zone configuration is managed on a fabric basis. Zoning configuration data is automatically distributed by the Fabric OS to all switches in the fabric, preventing a single point of failure for zone information. The zoning configuration can be administered from any switch.

Zoning Implementations

Zoning can be enabled on the host, in the switch fabric, and in most storage units. Storage units typically implement LUN based zoning, commonly referred to as LUN masking. Fabric switches will implement nameserver-based zoning where the zone members are identified by WWN or port location in the fabric. Host-based zoning can implement WWN or LUN masking.

Host-Based Zoning

Host-based zoning requires the host configuration to be correct in order to avoid zoning conflicts. This provides a greater opportunity for administrative errors to allow conflicting access to targets. The zoning interface varies from host operating systems, even among different HBA vendors. This increases the opportunity for administrative errors to occur. If a host is not configured with the zoning software, it can access all devices in the fabric resulting in the possibility of data corruption.

Storage-Based Zoning

This form of zoning is usually referred to as LUN masking. Its basic function is to limit access to the LUNs on the storage port to specific WWN of the server HBA. This form of zoning is needed in most SANs. It functions during the probe portion of the SCSI initialization. The server will probe the storage port for a list of available LUNs and their properties. The storage system will compare the WWN of the requesting HBA to the defined zone list. It will then return the LUNs that are assigned to the WWN. Any other LUNs on that storage port will not be made available to the server.

Fabric-Based Zoning

This is commonly referred to as nameserver based or soft zoning. With HP switches there may also be additional hardware enforcement of the zone; refer to [Hardware-Enforced Zoning in an HP Fabric](#) on page 65. When a device makes a query to the fabric nameserver, the nameserver determines which zones the device belongs to. It then returns to the requesting device information on all members of the zones that are present in the fabric. Devices in the zone are identified by World Wide Node Name, World Wide Port Name, or Domain/Port of the switch the device is connected to.

Fabric-Based Zoning Philosophies

This is perhaps the most controversial aspect of zoning. There are a number of philosophies for the implementation of fabric zoning. All will work in most cases. However, there are pros and cons to each form. The primary forms are no fabric zoning, single HBA, grouping by operating system, grouping by application, and port allocation.

Note: Refer to the *HP StorageWorks SAN Design Reference Guide* at the following location for general SAN zoning rules and requirements:
<http://h18000.www1.hp.com/products/storageworks/san/documentation.html>

Refer to the *HP StorageWorks Enterprise Backup Solutions Design Guide* at the following location for Enterprise Backup Solution (EBS) zoning recommendations:
<http://h10025.www1.hp.com/ewfrf/wc/manualCategory?lc=en&cc=us&product=406722>

No Fabric Zoning

This is the least desirable zoning option because of the unrestricted access that devices have on the fabric. All devices have full knowledge of the fabric membership and potentially have access to all the devices. Additionally, any device attached to the fabric, intentionally or maliciously, will likewise have unrestricted access to the fabric. This form of zoning should only be utilized in a small and tightly controlled environment, such as when host-based zoning or LUN masking is deployed.

Zoning by Application

In most environments, the concern for availability is by application, not by server, such as in clusters. This method will most likely require zoning multiple operating systems into the same zones. Some operating systems have issues co-existing in the same zone with other operating systems. This method of zoning creates the possibility that a minor server in the application suite potentially has the ability to disrupt a major server, such as a web server being able to disrupt a data warehouse server. Zoning by this method may also result in a zone with a large number of members that would provide a greater opportunity for administrative errors to occur, such as RSCNs going out to a larger group than might be necessary.

Zoning by Operating System

Zoning by operating system allows multiple HBAs of the same operating system type to be grouped with the storage ports being accessed. This grouping helps keep the number of zones to a limited number in a given fabric. In some cases, the zone sizes may become too large; possibly, they can be broken into multiple zones within the operating system type, depending on the application. Zoning by operating system type can limit any disruptions or fabric change notifications (such as RSCNs) to a select few while at the same time retaining the advantage of grouping the HBAs of the same operating system type.

Also, zoning by operating system prevents HBAs of different operating systems from interacting with each other, potentially eliminating any incompatibilities between them.

Zoning by operating system is the preferred method. However, certain situations, such as when configuring for common server access to multiple storage types, may require zoning by HBA. For additional zoning requirement information, refer to the “Best Practices” chapter in the *HP StorageWorks SAN Design Reference Guide* at the following location:

<http://h18000.www1.hp.com/products/storageworks/san/documentation.html>

Port allocation

There is an option to zone based on switch port rather than the WWN of the device. This provides some security to the fabric, but requires very solid processes to prevent the incorrect device from being attached to the wrong ports. This form of zoning should be avoided unless the administration team has very rigidly enforced processes for port and device allocation in the fabric. It does however provide some positive features. For instance, when a storage port, server HBA, or tape drive is replaced, the change of WWN for the new device is of no consequence. As long as the new device is connected to the original port, it will continue to have the same access rights. The ports on the edge switches can be pre-associated to storage ports and control of the fan-in ratio can be established. With this technique, the administrative team could not overload any one storage port by associating too many servers with it.

Single HBA

This method of zoning most closely re-creates the original SCSI bus. Each zone created has only one HBA (initiator) in the zone. Then each of the target devices that the initiator should access is added to the zone. Typically, a zone would be created for the HBA, and the disk storage ports would be added. If the HBA accesses tape devices, a second zone is created with the HBA and associated tape devices in it. In the case of clustered systems, it may be appropriate to have an HBA from each of the cluster members included in the zone. This is equivalent to having a shared SCSI bus between the cluster members. This presumes that the clustering software provides a methodology to manage access to the shared devices.

In a large fabric, this does require the creation of possibly hundreds of zones. However, each zone would contain only a few members. Zone changes would affect the smallest possible number of devices. The impact of an incorrect zone change would be minimized.

The Effect of Zoning on RSCN Delivery

Whenever a change occurs in the nameserver, such as a device addition or removal from the fabric, a registered state change notification (RSCN) is required to be generated. In the absence of zoning, an RSCN is sent to all devices on the fabric. Each device should then query the nameserver to determine how the membership of the fabric has changed. This will happen even if the device change does not affect the other devices. In large fabrics, this can result in a significant amount of traffic being generated, although typically for only short time.

For instance, if a new initiator joins the fabric, there is little purpose in notifying all the other initiators of the change. Initiators do not typically communicate with each other. An equivalent situation exists with targets. As targets generally do not communicate with each other, they have little use in being notified of the addition or removal of another target.

Once zoning is implemented then only affected devices in the changed zone will receive the RSCN. If devices are already aware of their zoned members, then they will not receive an RSCN. Only devices that are affected by the change will receive an RSCN. While all devices are supposed to handle RSCN traffic without affecting normal operation, experience has shown that this is not always the case. Thus, the overall stability of the fabric is increased when zoning is implemented.

Table 4: RSCN Delivery

External Events	HP FOS V2.x up to V2.5	HP FOS V3.0	HP FOS V2.6/3.0.2/ 4.0	HP FOS V3.1/4.1
Fabric reconfigure with no domain change	Fabric RSCN to all devices	Fabric RSCN to all devices	No RSCN	No RSCN
Switch disable	Fabric RSCN to all devices	Fabric RSCN to all devices	Domain RSCN to zoned devices only	No RSCN
Switch enable	Fabric RSCN to all devices	Fabric RSCN to all devices	No RSCN	No RSCN
Device power up	Device RSCN to zoned devices only	Aggregated ¹ RSCN to zoned devices only	Aggregated RSCN to zoned devices only	Aggregated RSCN to affected zoned devices only
Device shutdown	Device RSCN to zoned devices only	Aggregated RSCN to zoned devices only	Aggregated RSCN to zoned devices only	Aggregated RSCN to affected zoned devices only
Zone change	Fabric RSCN to all devices	Fabric RSCN to all devices	Fabric RSCN to all devices	Fabric RSCN to affected devices only
Switchname/IP Address change	Domain RSCN to all devices	Domain RSCN to all devices	Domain RSCN to all devices	Domain RSCN to all devices

1. Aggregated RSCN combines multiple device RSCNs into one.

Implementing Zoning

The first step to implementing zoning is to devise a naming convention. It is important that this convention be consistent, that it produces meaningful names, and that it be used consistently. We will then take a look at implementing zoning in a new fabric and then how to implement it in an existing fabric that does not conform to the single HBA zoning method.

Naming Convention

Typically, there are three types of devices that can have an alias. These are the server HBA, the disk storage device, and the tape device. New devices such as virtualization devices may also require an alias. Any device that acts as either a SCSI initiator or SCSI target will have an alias. A suggested scheme follows.

Each alias has three components: device type, device identifier and port location.

The device type is:

- SRV - for servers
- STO - for storage
- TPE - for tape
- VRA - for virtualization appliance

The device identifier can be the host name for the server, the serial number, or frame identifier for the storage. The port location should allow the administrator to physically find the device port where the fiber is attached. A suggestion would be the PCI slot on a server, the fiber port on the storage frame, or the port on a tape drive. If a unit has only one port then this field can be omitted or identifier “SNG” for single attach used. Some examples:

- SRV_MAILSERVER_SLT5 a server, host name mailserver, in PCI slot 5.
- TPA_LTO9_SNG a tape, LTO drive number 9, and it is single attached.
- STO_DSK3456_5Ca storage unit, serial id 3456 on the fifth card in port C.

The shorter names are easier to remember and less prone to typing errors. Do not sacrifice meaning for shortness.

In a similar manner, zones should be named for the initiator they contain. For the server alias above, the zone would be ZNE_MAILSERVER_SLT5. This clearly identifies the server HBA that is associated with the zone.

Configuration naming is more flexible. In general though there should be one configuration named “PROD fabricname”. Fabricname is the name that the fabric has been designated. The purpose of the PROD configuration is to easily identify the configuration that can be implemented and provide the most generic services. If other configurations are used for specialized purposes, the names such as “BACKUP_A”, “RECOVERY_2”, “TEST_18jun02” may be used.

Implementing Zoning on an Existing Fabric

The fact that zoning is already implemented eliminates the first step of getting a zone and configuration created. The next step of creating aliases and zones and then adding them to the existing configuration is the same. It is acceptable to have overlapping zones. In fact, it would be expected that the single HBA zones overlap one or more of the existing zones. Once the single HBA zones are in place, then the previous zones can be removed. After the previous zones are removed, then the aliases that are no longer needed may also be removed. Carefully executed, this will be non-disruptive to the devices on the fabric. There may be a momentary disruption of data flow when the new zoning configuration is enabled due to the RSCN. Properly configured devices will handle this without issue.

Hardware-Enforced Zoning in an HP Fabric

All zoning employs the nameserver to limit the information returned to an initiator in response to a nameserver query. This is referred to as *soft zoning*. If an initiator has knowledge of the network address of a target device, it does not need to query the nameserver to access it. This allows for undesired access to a target device with the potential for data corruption. HP switches augment the nameserver zoning with hardware enforcement. Nameserver or soft zoning is always active whenever a zone configuration is in effect. However, there are conditions that determine when hardware enforcement will be active.

When hardware enforced or *hard zoning* is active, the HP switch will monitor the communications and block any frames that do not comply with the effective zone configuration. This blocking is performed at the transmit side of the port where the destination device is located. A zone configuration will typically be comprised of many zones, and the hardware enforcement decision is made on a per zone basis. The exact methodology varies on different switch models. The use of hardware enforcement is decided by the Fabric OS whenever the fabric membership or zone configuration changes.

A few definitions are in order before proceeding with this discussion.

- **Domain/Port zone** - All members of this zone are specified with Domain/Port pairs only. Area values may be used when zoning on a StorageWorks Core switch.
- **WWN zone** - All members of this zone are specified with WWN numbers only. They may be Node or Port versions of the WWN.
- **MIXED zone**- This zone contains members specified by either Domain/Port or WWN, and it contains at least one member specified by each method.
- **Overlapping zones** - Two or more zones that contain a common member. The member may be specified by Domain/Port or WWN.

Fabrics Composed of Only StorageWorks 1 Gb SAN Switch Models

The StorageWorks 1 Gb SAN switches enable hardware-enforced zoning only on Domain/Port zones. Any WWN or mixed zones will not be hardware enforced. Any Domain Port zone that overlaps with a mixed or WWN zone will not be hardware enforced. Note that an overlap will occur when a member specified by WWN is connected to a port in a Domain/Port zone. The Domain/Port zone will lose its hardware enforcement, even though a review of the zone configuration would not indicate this.

Fabrics Composed of StorageWorks 2 Gb SAN Switch and StorageWorks Core Switch Models

StorageWorks 2 Gb SAN switches and StorageWorks Core switches enable hardware enforced zoning on Domain/Port zones and WWN zones. Mixed zones will not be hardware enforced. Overlap of like zone types will not result in the loss of hardware enforcement. Overlap with another zone type will result in the loss of hardware enforcement. As in the StorageWorks 1 Gb SAN switches, connecting a device specified by WWN into a port specified in a Domain/Port zone will result in loss of the hardware enforcement in both zones.

Fabrics Composed of 1 Gb SAN, 2 Gb SAN, and Core Switch Models

In mixed fabrics, each switch type continues to enable hardware enforcement of zoning according to the conditions established above. The challenge is that the administrator must now know which switch type the device is attached to, in order to determine if hardware enforcement will be active. This is accomplished using the command `zoneShow`.

Best Practices for Hardware Zone Enforcement

When a site policy has been established requiring hardware enforcement, it certainly is desired that the hardware enforcement always occur. From the preceding paragraphs, it should be clear that there are cases when determining the applicability of hardware enforcement can be difficult. Three basic cases have simple rules for assuring that hardware enforcement is used.

- For StorageWorks 1 Gb SAN switch fabrics, always use Domain/Port identifiers only. Never identify a zone member by WWN.
- For StorageWorks 2 Gb SAN switch and StorageWorks Core switch fabrics, choose to use either WWN or Domain/Port zones. Never use both and never used mixed zones.
- For mixed fabrics always preferably use Domain/Port identifiers. If it is desired to use WWN identifiers, the following methodology may be utilized. Always place targets (disk and tape units) on the StorageWorks 2 Gb SAN switches and StorageWorks Core switches, and use WWN zoning only. If all the targets are on the StorageWorks 2 Gb SAN switches and StorageWorks Core switches, then hardware enforced zoning will be active to protect them. This does not hardware protect the initiators, but in general they do not offer resources anyway and will reject any probe attempt by other initiators.

Hardware enforcement has limitations. Each Quad has 64 SID CAM (Source ID Content Accessible Memory) entries. All four ports on the Quad share these SID CAM entries. When these SID CAM entries are exceeded, then the hardware zoning reverts to SOFT zoning.

For example, a port has taken up 63 SID CAM entries, as it is zoned with 63 devices. Adding two more devices to this zone will cause this port to revert to soft zoning.

Likewise there are 512 DID CAM (Destination ID Content Accessible Memory) entries per quad.

Using Zoning to Administer Security



Zones can be used to provide controlled access to fabric segments and to establish barriers between operating environments, such as to isolate systems with different uses or protect systems in a heterogeneous environment. For example, when Zoning is in secure mode, merge operations do not occur.

HP Zoning is done on the primary Fabric Configuration Server (FCS). The primary FCS switch makes zoning changes and other security-related changes. The primary FCS switch also distributes zoning to all other switches in the secure fabric. All existing interfaces can be used to administer zoning.

Zone management operations must be performed from the primary FCS switch using a zone management interface, such as telnet or Web Tools. A zoning database can be altered, provided you are connected to the primary FCS switch.

When two secure fabrics join, the traditional zoning merge does not occur. Instead, a zoning database is downloaded from the primary FCS switch of the merged secure fabric. When E_ports are active between two switches, the name of the FCS server and a zoning policy set version identifier are exchanged between the switches. If the views of the two secure fabrics are the same, the fabric's primary FCS server downloads the zoning database and security policy sets to each switch in the fabric. If there is a view conflict, the E_ports are segmented as incompatible security data.

Note: Secure Fabric OS requires the activation of an HP security license.

As part of zoning architecture, the user will need to determine which of the two basic zoning architectures will work best for their fabric. With time and planning, the basic hard zone configuration will work for most sites. If a site has additional security needs, the user will need to add the additional layer of Secure Fabric OS to lock down the fabric, in addition to the standard zoning architecture.

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

16-port card

The Fibre Channel port card provided with the StorageWorks Core switch. Contains 16 Fibre Channel ports and the corresponding LEDs indicating port status and speed.

See also port card.

8b/10b Encoding

An encoding scheme that converts each 8-bit byte into 10 bits. Used to balance ones and zeros in high-speed transports.

Access Control List

Enables an organization to bind a specific WWN to a specific switch port or set of ports, preventing a port in another physical location from assuming the identity of a real WWN. May also refer to a list of the Read/Write access of a particular community string.

See also device connection controls.

Account Level Switches

Refers to switches that have four login accounts into the operating system (in descending order): root, factory, admin, and user.

See also root account, factory account, admin account, and user account.

Address Identifier

A 24-bit or 8-bit value used to identify the source or destination of a frame.

Admin Account

A login account intended for use by the customer to control switch operation.

See also account level switches.

AL_PA

Arbitrated Loop Physical Address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

Alias

An alternate name for an element or group of elements in the fabric. Aliases can be used to simplify the entry of port numbers and WWNs when creating zones.

Alias Address Identifier

An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

See also alias.

Alias AL_PA

An AL_PA value recognized by an L_Port in addition to the AL_PA assigned to the port.

See also AL_PA.

Alias Server

A fabric software facility that supports multicast group management.

ANSI

American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API

Application Programming Interface. Defined protocol that allows applications to interface with a set of services.

Arbitrated Loop

A shared 100 or 200 MBps Fibre Channel transport structured as a loop. Can support up to 126 devices and one fabric attachment.

See also topology.

Arbitrating State

The state in which a port has become the loop master. This state is only available from the Open state.

Area Number

A number assigned to each potential port location in the StorageWorks Core switch. Used to distinguish StorageWorks Core switch ports that have the same port number but are on different port blades.

ASIC

Application Specific Integrated Circuit.

ATM

Asynchronous Transfer Mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-negotiate Speed

Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gbps) and functions.

Autosense

Process during which a network device automatically senses the speed of another device.

AW_TOV

Arbitration Wait Time-out Value. The minimum time an arbitrating L_Port waits for a response before beginning loop initialization.

Backup FCS Switch

Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails.

See also FCS switch, primary FCS switch.

Bandwidth

The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a network.

See also throughput.

BB_Credit

Buffer-to-buffer credit. The number of frames that can be transmitted to a directly connected recipient or within an arbitrated loop. Determined by the number of receive buffers available.

See also Buffer-to-buffer Flow Control, EE_Credit.

Beacon

When all the port LEDs on a switch are set to flash from one side of the switch to the other, to enable identification of an individual switch in a large fabric. A switch can be set to beacon by telnet command or through Web Tools.

Beaconing

The state of the switches LEDs when the switch is set to Beacon.

See also Beacon.

Beginning Running Disparity

The disparity at the transmitter or receiver when the special character associated with an ordered set is encoded or decoded.

See also disparity.

BER

Bit Error Rate. The rate at which bits are expected to be received in error. Expressed as the ratio of error bits to total bits transmitted.

See also error.

BISR

Built-In Self Repair. Refers to the range of algorithms and circuit techniques to replace fault elements in a VLSI circuit with redundant fault-free ones.

See also BIST, CMBISR.

BIST

Built-In Self Test. The technique of designing circuits with additional logic which can be used to test proper operation of the primary (functional) logic.

See also BISR, CMBISR.

Bit Synchronization

See BER.

Blade

See 16-port card.

Blind-mate Connector

A two-way connector used in some switches to provide a connection between the motherboard and the power supply.

Block

As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly

A fan that prevents a switch (or individual elements within a switch) from overheating.

Boot Flash

Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor

Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast

The transmission of data from a single source to all devices in the fabric, regardless of zoning.

See also multicast, unicast.

Buffer-to-buffer Flow Control

Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop.

See also BB_Credit.

Cascade

Two or more interconnected Fibre Channel switches. StorageWorks 1 Gb SAN switches (running Fabric OS V2) and later can be cascaded up to 239 switches, with a recommended maximum of seven interswitch links (no path longer than eight switches).

See also fabric, ISL.

Chassis

The metal frame in which the switch and switch components are mounted.

Circuit

An established communication path between two ports. Consists of two virtual circuits capable of transmitting in opposite directions.

See also link.

Class 1

Service that provides a dedicated connection between two ports (also called connection-oriented service), with notification of delivery or non-delivery.

Class 2

Service that provides multiplex and connectionless frame switching service between two ports, with notification of delivery or non-delivery.

Class 3

Service that provides a connectionless frame switching service between two ports, without notification of delivery or non-delivery of data. This service can also be used to provide a multicast connection between the originator and recipients, with notification of delivery or non-delivery.

Class F

Connectionless service for control traffic between switches, with notification of delivery or non-delivery of data between the E_Ports.

Class of Service

A specified set of delivery characteristics and attributes for frame delivery.

CLI

Command line interface. Interface that depends entirely on the use of commands, such as through telnet or SNMP, and does not involve a Graphic User Interface (GUI).

CLS

Close Primitive Signal. Only in an Arbitrated Loop; sent by an L_Port that is currently communicating on the loop, to close communication to an other L_Port.

CMBISR

Central Memory Built-In Self Repair. Test and repair bad cells in the central memory. If a "fail" is reported, inform Tech Support and replace the board.

See also BIST, BISR.

Comma

A unique pattern (either 1100000 or 0011111) used in 8b/10b encoding to specify character alignment within a data stream.

See also K28.5.

Community (SNMP)

A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined.

See also SNMP.

Compact Flash

Flash memory that stores the run-time operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration

How a system is set up. May refer to hardware or software.

- **Hardware:** The number, type, and arrangement of components that make up a system or network.
- **Software:** The set of parameters that guide switch operation. May include general system parameters, IP address information, Domain ID, and other information. Modifiable by any login with administrative privileges.

May also refer to a set of zones.

See also zone configuration.

Connection Initiator

A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient

A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel

Refers to the left-side panel of Web Tools, which accesses fabric-wide functions such as Zoning and Events.

Core Switch

A switch whose main task is to interconnect other switches.

See also SAN switch.

CP Card

Control Processor Card. The central processing unit of the StorageWorks Core switch, which contains two CP Card slots to provide redundancy. Provides Ethernet, serial, and modem ports with the corresponding LEDs.

CRC

Cyclic Redundancy Check. A check for transmission errors included in every data frame.

Credit

As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports.

See also BB_Credit, EE_Credit.

CT_HDR

Common Transport Header. A header that conforms to the Fibre Channel Common Transport (FC_CT) protocol.

CT_IU

Common Transport Information Unit. An information unit that conforms to the Fibre Channel Common Transport (FC_CT) protocol.

Current Fill Word

The fill word currently selected by the LPSM.

See also fill word, LPSM.

Cut-through

A switching technique that allows the route for a frame to be selected as soon as the destination address is received.

See also route.

Data Word

Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words.

See also frame, ordered set, transmission word.

DB-9 connector

A 9-pin version of the RS-232C port interface. May be either the male or female interface.

See also RS-232 port.

dBm

Logarithmic unit of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm. An increase of 10 dBm or represents a 10-fold increase in power.

DCE port

A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2.

See also DTE port, RS-232 port.

Defined Zone Configuration

The set of all zone objects defined in the fabric. May include multiple zone configurations.

See also enabled zone configuration, zone configuration.

Device Connection Controls

Enables organizations to bind an individual device port to a set of one or more switch ports. Device ports are specified by a WWN and typically represent HBAs (servers).

See also access control lists.

Device

A disk, a RAID, or an HBA.

Disparity

The relationship of ones and zeros in an encoded character. “Neutral disparity” means an equal number of each, “positive disparity” means a majority of ones, and “negative disparity” means a majority of zeros.

DLS

Dynamic Load Sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID

As applies to HP StorageWorks switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE port

A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data communications equipment) port. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2 in a 9-pin connector (reversed in 25-pin connectors).

See also DCE port, RS-232 port.

DWDM

Dense Wavelength Multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data onto a different wavelength of light.

E_D_TOV

Error Detect Time-out Value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared.

See also R_A_TOV, RR_TOV.

E_Port

Expansion Port. A type of switch port that can be connected to an E_Port on another switch to create an ISL.

See also ISL.

EE_Credit

End-to-end Credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination.

See also End-to-end Flow Control, BB_Credit.

EIA Rack

A storage rack that meets the standards set by the Electronics Industry Association.

ELWL

Extra Long Wavelength. Laser light with a periodic length greater than 1300 nm (e.g., 1420 or 1550). ELWL lasers are used to transmit Fibre Channel data over distances greater than 10 Km.

Also known as XLWL.

Enabled Zone Configuration

The currently enabled zone configuration. Only one configuration can be enabled at a time.

See also defined zone configuration, zone configuration.

End-to-end Flow Control

Governs flow of class 1 and 2 frames between N_Ports.

See also EE_Credit.

Entry Fabric

Basic HP license that allows one E_Port per switch. Not supported by StorageWorks Core switches.

Error

As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

See also loop failure.

ESD

Electrostatic Discharge.

Exchange

The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in either one or both directions.

Extended Fabric

An HP product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

Extended Fabric is a means of allowing the implementation and management of SANs over extended distances. This is achieved by adjusting the Buffer-to-Buffer Credits to guaranteed allocation of buffers to specific ports.

F_Port

Fabric Port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch.

See also FL_Port, Fx_Port.

Fabric

A Fibre Channel network containing two or more interconnected switches in addition to hosts and devices. May also be referred to as a switched fabric.

See also topology, SAN, cascade.

Fabric Access

An HP product that consists of a set of APIs that allow third party applications to interface with Fabric OS.

Fabric Access allows the application to control the fabric directly for functions such as discovery, access (zoning), management, performance, and switch control. Consists of a host-based library that interfaces the application to switches in the fabric over an out-of-band TCP/IP connection or in-band using an IP-capable Host Bus Adapter (HBA).

Fabric Assist

An HP feature that enables private and public hosts to access public targets anywhere on the fabric, provided they are in the same Fabric Assist zone. This feature is available only when both QuickLoop and Zoning are installed on the switch.

Fabric Assist is a means of allowing private hosts to communicate with public targets across a switched fabric. Fabric Assist also allows private hosts to communicate with private targets that are not resident on the same switch across a switched fabric.

See also QuickLoop.

Fabric Configuration Server

One or more designated HP switches that store and manage the configuration and security parameters for all other switches in the fabric. These switches are designated by WWN, and the list of designated switches is known fabric-wide.

Fabric Manager

An HP product that works in conjunction with Web Tools to provide a graphical user interface for managing switch groups (such as the SAN Switch Integrated/32) as a single unit, instead of as separate switches. Fabric Manager is installed on and run from a computer workstation.

Fabric Name

The unique identifier assigned to a fabric and communicated during login and port discovery.

Fabric OS

The proprietary operating system on HP StorageWorks switches.

Fabric Watch

An HP product that runs on Fabric OS and allows monitoring and configuration of fabric and switch elements.

Allows the SAN manager to monitor key fabric and switch elements, making it easy to quickly identify and escalate potential problems. It monitors each element for out-of-boundary values or counters and provides notification when defined boundaries are exceeded. The SAN manager can configure which elements, such as error, status, and performance counters, are monitored within an HP switch.

See also Fabric Manager.

Factory Account

A login used during manufacturing to initialize and test a switch and is not intended for customer use.

See also account level switches.

Failover

The act that causes control to pass from one redundant unit to another. In the StorageWorks Core switch one may failover from the currently Active Control Processor (CP) to the Standby CP.

FAN

Fabric access notification. Retains the AL_PA and fabric address when loop re-initializes (if the switch supports FAN).

FC-AL-3

The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FC-FLA

The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCIA

Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Among other things, provides oversight of ANSI and industry developed standards.

FCP

Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3

The Fibre Channel Physical and Signaling Interface standards defined by ANSI.

FC-PI

The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA

The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS switch

Fabric configuration server switch. One or more designated HP switches that store and manage the configuration and security parameters for all switches in the fabric. FCS switches are designated by WWN, and the list of designated switches is communicated fabric-wide.

See also backup FCS switch, primary FCS switch.

FC-SW-2

The second generation of the Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of Fibre Channel switches in order to create a multi-switch Fibre Channel fabric.

Fibre Channel Transport

A protocol service that supports communication between Fibre Channel service providers.

See also FSP.

FIFO

First In, First Out. May also refer to a data buffer that follows the first in, first out rule.

Fill Word

An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the Fibre Channel link active.

Firmware Download

Loading firmware down from a server into a switch.

Firmware

The basic operating system provided with the hardware.

FL_Port

Fabric Loop Port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch.

See also F_Port, Fx_Port.

Flash Partition

Two redundant usable areas, called “partitions,” into which firmware can be downloaded in the StorageWorks Core switch.

Flash

Programmable NVRAM memory that maintains its contents.

FLOGI

Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it.

See also PLOGI.

Frame

The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, any optional headers, the data payload, a cyclic redundancy check (CRC), and an end-of-frame delimiter. There are two types of frames: Link control frames (transmission acknowledgements, etc.) and data frames.

See also Data Word.

FRU

Field Replaceable Unit. A component that can be replaced on site.

FS_ACC

Fibre Channel Services Accept. The information unit used to indicate acceptance of a request for a Fibre Channel service.

FS_IU

Fibre Channel Services Information Unit. An information unit that has been defined by a Fibre Channel service.

FS_REQ

Fibre Channel Services Request. A request for a Fibre Channel services function, or notification of a fabric condition or event.

FS_RJT

Fibre Channel Services Reject. An indication that a request for Fibre Channel services could not be processed.

FS

Fibre Channel Service. A service that is defined by Fibre Channel standards and exists at a well-known address. For example, the Simple Name Server is a Fibre Channel service.

See also FSP.

FSPF

Fabric Shortest Path First. HP routing protocol for Fibre Channel switches.

FSP

Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology.

See also FS.

Full Fabric

The HP license that allows multiple E_Ports on a switch, making it possible to create multiple ISL links.

Full-duplex

A mode of communication that allows the same port to simultaneously transmit and receive frames.

See also half-duplex.

Fx_Port

A fabric port that can operate as either an F_Port or FL_Port.

See also F_Port, FL_Port.

G_Port

Generic Port. A port that can operate as either an E_Port or F_Port. A port is defined as a G_Port when it is not yet connected or has not yet assumed a specific function in the fabric.

Gateway

Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC

Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical-level transport for Fibre Channel and gigabit Ethernet. Typically refers only to the SC-form factor transceivers.

See also SFP.

Gbps

Gigabits per second (1,062,500,000 bits/second).

GBps

Gigabytes per second (1,062,500,000 bytes/second).

Half-duplex

A mode of communication that allows a port to either transmit or receive frames at any time, but not simultaneously (with the exception of link control frames, which can be transmitted at any time).

See also full-duplex.

Hard Address

The AL_PA that an NL_Port attempts to acquire during loop initialization.

Hardware Translative Mode

A method for achieving address translation. The following two hardware translative modes are available to a QuickLoop-enabled switch:

- Standard Translative Mode: Allows public devices to communicate with private devices that are directly connected to the fabric.
- QuickLoop Mode: Allows initiator devices to communicate with private or public devices that are not in the same loop.

HBA

Host Bus Adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability

An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically High Availability is identified by the number of nines in that percentage. “Five Nines” means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host

A computer that accesses storage devices over the fabric. May also be referred to as a server.

See also workstation.

Hot Pluggable

A FRU capability that indicates it may be extracted or installed while customer data is otherwise flowing in the chassis.

Hub

A Fibre Channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.

IBTA

The InfiniBand Trade Association (IBTA). The IBTA is an industry consortium of more than 200 companies working together to develop a new common I/O specification designed to bring greater scalability and performance to server I/O. InfiniBand defines a new channel based, switched-fabric technology for server-to-server and server-to-I/O interconnection that is expected to improve scalability and performance over existing PCI Bus technologies.

Idle

Continuous transmission of an ordered set over a Fibre Channel link when no data is being transmitted, to keep the link active and maintain bit, byte, and word synchronization.

InfiniBand

See IBTA.

Initiator

A server or workstation on a Fibre Channel network that initiates communications with storage devices.

See also Target.

Integrated Fabric

The fabric created by a SAN Switch Integrated/32 and SAN Switch Integrated/64, consisting of six SAN Switch 16-EL switches cabled together and configured to handle traffic as a seamless group.

IOD

In-order Delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

IPA

Initial Process Associator. An identifier associated with a process at an N_Port.

Isolated E_Port

An E_Port that is online but not operational due to overlapping Domain IDs or nonidentical parameters (such as E_D_TOVs).

See also E_Port.

ISL

Interswitch Link. a Fibre Channel link from the E_Port of one switch to the E_Port of another.

See also E_Port, cascade, ISL Trunking.

ISL Trunking

An HP feature that enables distribution of traffic over the combined bandwidth of up to four ISLs (between adjacent switches), while preserving in-order delivery. A set of trunked ISLs is called a trunking group; each port employed in a trunking group is called a trunking port.

See also Master Port.

IU

Information Unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

JBOD

Just a Bunch Of Disks. Indicates a number of disks connected in a single chassis to one or more controllers.

See also RAID.

K28.5

A special 10-bit character used to indicate the beginning of a transmission word that performs Fibre Channel control and signaling functions. The first seven bits of the character are the comma pattern.

See also comma.

Kernel Flash

Flash memory that stores the bootable kernel code and is visible within the processor's memory space. Data is stored as raw bits.

Key Pair

In public key cryptography, a pair of keys consisting of an entity's public and private key. The public key can be publicized, but the private key must be kept secret.

L_Port

Loop Port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or non-participating mode.

See also Non-participating Mode, Participating Mode.

Latency

The period of time required to transmit a frame, from the time it is sent until it arrives. Together, latency and bandwidth define the speed and capacity of a link or system.

LED

Light Emitting Diode. Used on HP switches to indicate the status of various switch elements.

Link Services

A protocol for link-related actions.

Link

As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibers.

See also Circuit.

LIP

Loop Initialization Primitive. The signal used to begin initialization in a loop. Indicates either loop failure or resetting of a node.

LIS_HOLD_TIME

Loop Initialization Sequence Hold Time. The maximum period of time for a node to forward a loop initialization sequence.

LM_TOV

Loop Master Time-out Value. The minimum time that the loop master waits for a loop initialization sequence to return.

Login BB_Credit

The number of receive buffers a receiving L_Port has available when a circuit is first established.

See also BB_Credit.

Loop Circuit

A temporary bidirectional communication path established between L_Ports.

Loop Failure

Loss of signal within a loop for any period of time, or loss of synchronization for longer than the time-out value.

See also error.

Loop Initialization

The logical procedure used by an L_Port to discover its environment. Can be used to assign AL_PA addresses, detect loop failure, or reset a node.

Loop_ID

A hex value representing one of the 127 possible AL_PA values in an arbitrated loop.

Looplet

A set of devices connected in a loop to a port that is a member of another loop.

LPSM

Loop Port State Machine. The logical entity that performs arbitrated loop protocols and defines the behavior of L_Ports when they require access to an arbitrated loop.

LWL

Long Wavelength. A type of fiber optic cabling that is based on 1300-nm lasers and supports link speeds of 1.0625 Gbps. May also refer to the type of GBIC or SFP.

See also SWL.

Master Port

As relates to trunking, the port that determines the routing paths for all traffic flowing through the trunking group. One of the ports in the first ISL in the trunking group is designated as the master port for that group.

See also ISL Trunking.

Media

See transceiver.

MIB

Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port

The upper serial port on the CP Card of the StorageWorks Core switch. Can be used to connect the CP Card to a modem with a standard 9-pin modem cable. Consists of a DB-9 connector wired as a RS-232 device, and can be connected by serial cable to a DCE device. A Hayes-compatible modem or Hayes-emulation is required. The device name is ttyS1.

See also DB-9 connector, DCE port, terminal serial port.

Monitoring State

The state in which a port is monitoring the flow of information for data relevant to the port.

Multicast

The transmission of data from a single source to multiple specified N_Ports (as opposed to all the ports on the network).

See also broadcast, unicast.

Multimode

A fiber optic cabling specification that allows up to 500 meters between devices for 1 Gb, or 300 meters between devices for 2 Gb.

N_Port

Node Port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection.

See also NL_Port, Nx_Port.

NAA

Network Address Authority. An identifier that indicates the format of a network address.

Name Server

Frequently used to indicate Simple Name Server.

See also SNS.

Native Address Identifier

A unique, 64-bit address is assigned to each port, and is referred to as its World-Wide Name (WWN). If a port connects to an arbitrated loop, it will also be assigned a dynamic 8-bit address, referred to as its arbitrated loop physical address, or AL_PA. If it connects to a fabric, it will be assigned a dynamic 24-bit address, referred to as its Native Address Identifier.

Negotiate

See auto-negotiate speed and autosense.

NL_Port

Node Loop Port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port.

See also N_Port, Nx_Port.

Node Name

The unique identifier for a node, communicated during login and port discovery.

Node

A Fibre Channel device that contains an N_Port or NL_Port.

Non-participating Mode

A mode in which an L_Port in a loop is inactive and cannot arbitrate or send frames, but can retransmit any received transmissions. This mode is entered if there are more than 127 devices in a loop and an AL_PA cannot be acquired.

See also L_Port, Participating Mode.

Nx_Port

A node port that can operate as either an N_Port or NL_Port.

Open Originator

The L_Port that wins arbitration in an arbitrated loop and sends an OPN ordered set to the destination port, then enters the Open state.

Open Recipient

The L_Port that receives the OPN ordered set from the open originator, and then enters the Open state.

Open State

The state in which a port can establish a circuit with another port. A port must be in the Open state before it can arbitrate.

OPN

Open Primitive Signal.

Ordered Set

A transmission word that uses 8B/10B mapping and begins with the K28.5 character. Ordered sets occur outside of frames, and include the following items:

- Frame delimiters: Mark frame boundaries and describe frame contents.
- Primitive signals: Indicate events.
- Primitive sequences: Indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

Packet

A set of information transmitted across a network.

See also Frame.

Participating Mode

A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions.

See also L_Port, Non-participating Mode.

Path Selection

The selection of a transmission path through the fabric. HP StorageWorks switches use the FSPF protocol.

Performance Monitor

Comprehensive HP tool for monitoring the performance of networked storage resources.

Performance Monitoring

An HP product that provides error and performance information to the administrator and end user for use in storage management.

Phantom Address

An AL_PA value that is assigned to an device that is not physically in the loop.

Also known as phantom AL_PA.

Phantom Device

A device that is not physically in an arbitrated loop, but is logically included through the use of a phantom address.

PLOGI

Port Login. The port-to-port login process by which initiators establish sessions with targets.

See also FLOGI.

Point-to-point

A Fibre Channel topology that employs direct links between each pair of communicating entities.

See also topology.

Port Cage

The metal casing extending out of the optical port on the switch, and in which the SFP can be inserted.

Port Card

A Fibre Channel card that contains optical or copper port interfaces, and acts like a switch module.

See also 16-port card.

Port Module

A collection of ports in a switch.

Port_Name

The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

POST

Power On Self-Test. A series of tests run by a switch after it is turned on.

Primary FCS Switch

Primary fabric configuration server switch. The switch that actively manages the configuration and security parameters for all switches in the fabric.

See also backup FCS switch, FCS switch.

Private Device

A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log into the fabric.

Private Loop

An arbitrated loop that does not include a participating FL_Port.

Private NL_Port

An NL_Port that communicates only with other private NL_Ports in the same loop and does not log into the fabric.

Protocol

A defined method and a set of standards for communication.

PSU

Power Supply Unit.

Public Device

A device that supports arbitrated loop protocol, can interpret 8-bit addresses, and can log into the fabric.

Public Loop

An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port

An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Quad

A group of four adjacent ports that share a common pool of frame buffers.

QuickLoop

An HP StorageWorks product that makes it possible to allow private devices within loops to communicate with public and private devices across the fabric through the creation of a larger loop.

May also refer to the arbitrated loop created using this software. A QuickLoop can contain a number of devices or looplets; all devices in the same QuickLoop share a single AL_PA space.

A means of allowing private hosts to communicate with private targets across a switched fabric.

The QuickLoop/Fabric Assist feature also allows:

- Private hosts to communicate with public targets across a switched fabric
- Private hosts to communicate with private targets that are not resident on the same switch across a switched fabric

See also Fabric Access, fabric assist, and translative mode.

QuickLoop Zoning

Protects devices from disruption by unrelated devices during critical processes; for example, during a tape backup session.

R_A_TOV

Resource Allocation Time-out Value. The maximum time a frame can be delayed in the fabric and still be delivered.

See also E_D_TOV, RR_TOV.

R_RDY

Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID

Redundant Array of Independent Disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking.

See also JBOD.

Remote Fabric

A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fibre Channel over IP.

Remote Switch

Bridges two switches into a SAN as large as 3000KM or more through protocol encapsulation in ATM networks via the Computer Network Technologies (CNT) UltraNet Open Systems Gateway.

Request Rate

The rate at which requests arrive at a servicing entity.

See also service rate.

RLS Probing

Read link status of the AL_PAs.

Root Account

A login used for debugging purposes by HP engineers and is not intended for customer use.

See also account level switches.

Route

As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination.

See also FSPF.

Routing

The assignment of frames to specific switch ports, according to frame destination.

RR_TOV

Resource Recovery Time-out Value. The minimum time a target device in a loop waits after a LIP before logging out a SCSI initiator.

See also E_D_TOV, R_A_TOV.

RS-232 port

A port that conforms to a set of Electrical Industries Association (EIA) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems.

See also DCE port, DTE port.

RSCN

Registered State Change Notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

RX_ID

Responder Exchange Identifier. A 2-byte field in the frame header used by the responder of the Exchange to identify frames as being part of a particular exchange.

SAN

Storage Area Network. A network of systems and storage devices that communicate using Fibre Channel protocols.

See also fabric.

SAN Switch

A switch whose main task is to connect nodes into the fabric.

See also core switch.

SCSI

Small Computer Systems Interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15 - 25 meters.

SDRAM

Synchronous Dynamic Random Access Memory. The main memory for the switch. Used for volatile storage during switch operation.

See also flash.

Sequence

A group of related frames transmitted in the same direction between two N_Ports.

Service Rate

The rate at which an entity can service requests.

See also request rate.

SFF

Small Form Factor.

SFP Cable

The latest innovation in high-speed copper cabling for Fibre Channel and InfiniBand. It incorporates the SFP module directly onto the cable assembly, eliminating the need for a separate SFP copper module and an HSSDC2 cable assembly.

SFP

Small form factor pluggable. A transceiver used on 2 Gbps switches that replaces the GBIC. Refers to the LC-form factor transceiver.

See also GBIC.

SID/DID

Source identifier/Destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode

The fiber optic cabling standard that, when used in conjunction with a 1300 nm laser light, can transfer data up to 10 km between devices. When used in conjunction with a 1550 nm laser light, single mode cabling can transfer data over 10 km.

See also multimode, LWL, ELWL, and XLWL.

SI

Sequence Initiative.

SNMP

Simple Network Management Protocol. An internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols.

See also Community (SNMP).

SNMPv1

The original SNMP, now labeled v1.

SNS

Simple Name Server. A switch service that stores names, addresses, and attributes for up to 15 minutes, and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. May also be referred to as directory service.

See also FS.

StorageWorks SAN switch

The brand name for the HP family of switches.

Switch Name

The arbitrary name assigned to a switch.

Switch Port

A port on a switch. Switch ports can be E_Ports, F_Ports, or FL_Ports.

Switch

Hardware that routes frames according to Fibre Channel protocol and is controlled by software.

SWL

Short Wavelength. A type of fiber optic cabling that is based on 850-nm lasers and supports 1.0625-Gbps link speeds. May also refer to the type of GBIC or SFP.

See also LWL.

Tachyon

A chip developed by Hewlett-Packard, and used in various devices. This chip has FC-0 through FC-2 on one chip.

Target

A storage device on a Fibre Channel network.

See also Initiator.

Tenancy

The time from when a port wins arbitration in a loop until the same port returns to the monitoring state. Also referred to as loop tenancy.

Terminal Serial Port

May also be referred to as the console port. The lower serial port on the CP Card of the StorageWorks Core switch. This port sends switch information messages and can receive commands. Can be used to connect the CP Card to a computer terminal. Has an RS-232 connector wired as a DTE device, and can be connected by serial cable to a DCE device. The connector pins two and three are swapped so that a straight-through cable can be used to connect to a terminal. The device name is ttyS0.

See also DCE port, modem serial port.

Throughput

The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second).

See also bandwidth.

Topology

As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point to point: A direct link between two communication ports.
- Switched fabric: Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop: Multiple NL_Ports connected in a loop.

Transceiver

Device that converts one form of signaling to another for transmission and reception; in fiber optics, it refers to optical and electrical.

Transfer State

The state in which a port can establish circuits with multiple ports without reentering the arbitration cycle for each circuit. This state can only be accessed by an L_Port in the Open state.

Translative Mode

A mode in which private devices can communicate with public devices across the fabric.

Transmission Character

A 10-bit character encoded according to the rules of the 8B/10B algorithm.

Transmission Word

A group of four transmission characters.

See also data word.

Trap (SNMP)

The message sent by an SNMP agent to inform the SNMP management station of a critical error.

See also SNMP.

Trunking

See ISL Trunking.

Tunneling

A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U_Port

Universal Port. A switch port that can operate as a G_Port, E_Port, F_Port, or FL_Port. A port is defined as a U_Port when it is not connected or has not yet assumed a specific function in the fabric.

UDP

User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP_TOV

Upper-level Time-out Value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

ULP

Upper-level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

Unicast

The transmission of data from a single source to a single destination.

See also broadcast, multicast.

user account

A login intended for use by the customer to monitor, but not control, switch operation.

See also account level switches.

VC

Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

Web Tools

An HP product that runs on Fabric OS and provides a graphical interface to allow monitoring and management of individual switches or entire fabrics from a standard workstation running a browser.

Well-known Address

As pertaining to Fibre Channel, a logical address defined by the Fibre Channel standards as assigned to a specific function, and stored on the switch.

Workstation

A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN

World-Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

XLWL

Xtra Long Wave Length. Laser light with a periodic length greater than 1300 nm (e.g., 1420 or 1550). XLWL lasers are used to transmit Fibre Channel data over distances greater than 10 Km.

Also known as ELWL.

Xmitted Close State

The state in which an L_Port cannot send messages, but can retransmit messages within the loop. A port in the XMITTED CLOSE state cannot attempt to arbitrate.

Zone

A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access permission to others in the zone, but are not visible to any outside the zone.

See also Zoning.

Zone Alias

A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

See also alias.

Zone Configuration

A specified set of zones. Enabling a configuration enables all zones in that configuration.

See also defined zone configuration, enabled zone configuration.

Zone Member

A port, node, WWN, or alias, which is part of a zone.

Zone Schemes

The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, AL_PA, or a mixture.

See also zone configuration.

Zone Set

See zone configuration.

Zoning

An HP product that runs on Fabric OS and allows partitioning of the fabric into logical groupings of devices. Devices in a zone can only access and be accessed by devices in the same zone.

See also zone.

A

- adding switches [36](#)
- administering security [69](#)
- aliases [32](#)
- arbitrated loop physical address (AL_PA) [46](#)
- architecture, zoning [43](#)
- audience [8](#)
- authorized reseller, HP [11](#)

C

- configuring
 - QuickLoop zones [48](#)
- conventions
 - document [9](#)
 - text symbols [9](#)
- creating
 - aliases [32](#)
 - QuickLoop zones [48](#)
- customizing environments [14](#)

D

- defining
 - QuickLoop zones [48](#)
 - zones [32](#), [33](#)
- devices [20](#)
- document
 - conventions [9](#)
 - related documentation [8](#)

F

- fabric, devices [20](#)

- Fibre Channel Arbitrated Loop (FC_AL) [45](#)

G

- getting help [10](#)

H

- hardware zones [28](#)
- help, obtaining [10](#)
- HP
 - authorized reseller [11](#)
 - storage website [10](#)
 - technical support [10](#)
- HP Web Tools
 - Fabric Assist [17](#)
 - QuickLoop [17](#)

I

- implementing zoning [30](#)

L

- loop initialization primitive (LIP) [47](#)

M

- mixed zone [28](#)
- modifying configurations [36](#)
- multiple zones [20](#)

O

- optimizing resources [14](#)

Q

QuickLoop

- advantages [47](#)
- configuration [48](#)
- creating [48](#)
- defining [48](#)
- zones [46](#)

R

- related documentation [8](#)

S

- switch adding [36](#)
- symbols in text [9](#)

T

- technical support, HP [10](#)
- text symbols [9](#)

W

- websites
 - HP storage [10](#)
- WWN zone [28](#)

Z

- zone configurations, enabling [33](#)
- zoning
 - architecture [43](#)
 - customization [14](#)
 - defining [32](#)
 - devices [20](#)
 - implementation [30](#)
 - multiple [20](#)
 - Quickloops [45](#)