Heterogeneous Storage Area Networks

COMPAQ STORAGEWORKS

Application Note

EK–SMA30–AN. A01

Visit Our Web Site for the Latest Information

At Compaq, we are continually making additions to our storage solution product line. Please check our web site for more information on our Fibre Channel product line as well as the latest drivers, technical tips, and updates to this application note and other documentation. Visit our web site at:

http://www.compaq.com/storageworks/

Introduction

This application note discusses the *Compaq StorageWorks* Heterogeneous Storage Area Networks (SANs), which connect multiple host servers to multiple shared storage systems through a Fibre Channel fabric using Fibre Channel switches. Smaller SANs that use Fibre Channel hubs are not discussed.

Enterprise Network Storage Architecture (ENSA)

The Compaq Enterprise Network Storage Architecture is key to supporting Compaq's NonStop eBusiness strategy; through ENSA, Compaq leverages industry standards to allow deployment of storage where applications need it. ENSA uses the Compaq StorageWorks product family to deliver the storage solutions that address non-stop computing requirements like availability, reliability, performance, scalability and manageability. ENSA addresses the storage issues that our customers expect to face now and in the future.

Heterogeneous SANs address today's issues including:

- Data protection
- High availability
- Increased distance
- Greater connectivity with high bandwidth
- Multi-vendor platform support
- Economical capacity growth
- Investment protection

Heterogeneous SANs provide dispersed server operation with shared storage access and shared tape library backup across the enterprise.

This application note describes:

- The concept of Heterogeneous SANs.
- The function of a Fibre Channel Switched Fabric.
- How the Compaq StorageWorks Enterprise Storage Array 12000 and RAID Array 8000 storage systems support Heterogeneous and Homogeneous operating system SANs.
- How the Compaq StorageWorks Enterprise Backup Solutions, which protects corporate data against inadvertent or catastrophic loss, provide tape library backup for the complex SAN environment.
- How to configure No-Single-Point-Of-Failure (NSPOF) and Non-NSPOF configurations, including hardware and software requirements.

The presentation of this material is as follows:

1.0 Heterogeneous SAN Concepts

In a multiple-host environment, where each host server or cluster requires exclusive access to its own data, a separate data storage system for each host server or cluster is typically employed. In this scenario, each storage system must be individually configured and maintained, each has its own set of hardware components and each requires its own physical location.

Shared storage, however, provides a better alternative to the complex storage demands of a multiple-host environment. It enables more effective management of storage for a lower total cost. Multiple-host storage needs are consolidated into a few storage systems. There are fewer hardware components and fewer physical locations. Each host server or cluster retains exclusive access to its own data.

A heterogeneous storage area network takes this a step further. It interconnects multiple shared storage environments into a single network. All storage can be managed from a single location or from multiple locations. All of the consolidated storage becomes available to any host server, regardless of physical location.

The storage area network can be configured to offer No-Single-Point-Of-Failure (NSPOF) storage data path protection. In this environment, using multi-path storage software, multiple data paths from the shared storage systems to the server are available. Should the hardware components of one data path fail, the I/O stream is added to another data path. In contrast, a Non-NSPOF configuration enables shared storage using only one data path. NSPOF and Non-NSPOF configurations may be combined in one SAN.

Whether the storage area network is configured for NSPOF, Non-NSPOF or both, it can be configured to support more than one host server operating system. This is called a ***Heterogeneous*** operating system SAN. A storage area network in which all host servers run the same operating system is called a ***Homogeneous*** operating system SAN.

In addition to the interconnected shared storage environments, a SAN can also provide an enterprise level tape library backup for the multiple host servers and multiple shared storage systems. This adds the protection needed against catastrophic loss or inadvertent deletion of corporate data.

A heterogeneous SAN gives a total solution for the increasingly complex and exponentially growing storage needs of the enterprise. It provides more effective centralized management of consolidated Online storage (disks) and Nearline storage (tapes) at a lower total cost.

1.1 Supported Operating Systems

As of the writing of this document, the supported operating systems in a heterogeneous or homogeneous SAN are:

- Compaq OpenVMS V7.2 and V7.2-1
- Compaq Tru64 UNIX V4.0F
- Microsoft Windows NT (Intel) V4.0 with Service Pack 4, or 5
- Sun Solaris V2.6, V2.7 (32-bit) and V2.7 (64-bit)
- HP-UX V10.2 and V11

NOTE

Please consult the host server's operating system Application Notes and other supporting documentation supplied with your storage system for detailed information regarding host server specific configuration requirements, including operating system version and platform maximums. Please refer to Section 7.0 for a listing of related documentation.

1.2 Enterprise Storage Array 12000/RAID Array 8000 Storage Systems

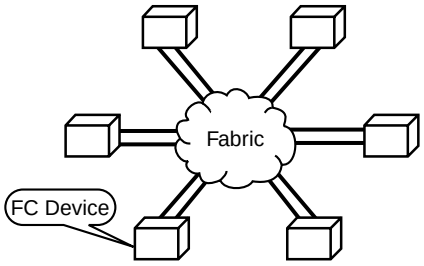
The Enterprise Storage Array 12000 Fibre Channel (ESA12000 FC) and RAID Array 8000 Fibre Channel (RA8000 FC) storage systems use HSG80 controllers. The HSG80 controllers provide storage for multiple hosts, storage protection through the use of multiple RAID levels and storage security through Selective Storage Presentation (SSP).

SSP manages host server access to storage. Each host server is only presented the storage units it is allowed to access; they are never informed the other storage units that belong to other host servers exist. Please refer to Section 4 for more information on SSP.

1.3 Fibre Channel Switched Fabric

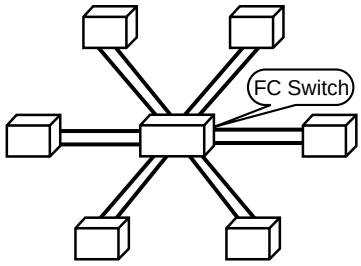
A Fibre Channel switched fabric consists of two or more Fibre Channel devices connected together through one or more interconnected Fibre Channel switches. Each device can establish a connection through the switches to any other device, independent of any other connections that currently exist in the fabric.

Figure 1 Logical View of FC Fabric



SHR-1543

Figure 2 Physical View of FC Fabric



SHR-1544

The Compaq Fibre Channel switches provide the ability to connect Fibre Channel Arbitrated Loop (FC-AL) Private Loop devices to the switch using a feature called QuickLoop. Please refer to Section 5 for more information regarding QuickLoop. The switches also provide device to device communication access control using a feature called Switch Zoning. Please refer to Section 6 for more information regarding Switch Zoning and configurations that require it.

1.4 Enterprise Backup Solutions

The Enterprise Backup Solutions (EBSs) use the Compaq StorageWorks TL895 Tape Library and Legato NetWorker and Legato SmartMedia software to manage and automate the tape library backup-and-restore process for multiple hosts.

As of the writing of this document, the operating systems supported by EBS are:

- Compaq Tru64 UNIX
- Microsoft Windows NT

NOTE
Please consult the *Enterprise Backup Solution for Legato NetWorker, Reference Guide*, and other supporting documentation supplied with your tape library for more information regarding Enterprise Backup Solution configuration requirements. Please refer to Section 7 for a listing of related documentation.

2.0 Heterogeneous SAN Configuration Rules and Building Blocks

This section describes the configuration rules for a supported StorageWorks heterogeneous SAN, which includes:

- Storage Systems
- StorageWorks Command Console (SWCC)
- Host Server Operating Systems and Multi-path software
- Fibre Channel Switches

It also describes recommended SAN configurations called SAN building blocks.

2.1 Storage Systems

The following Compaq StorageWorks Storage Systems are supported in a heterogeneous SAN:

- Compaq StorageWorks Enterprise Storage Array 12000 Fibre Channel (ESA12000 FC)
- Compaq StorageWorks RAID Array 8000 Fibre Channel (RA8000 FC)

Controller Configuration

ESA12000 and RA8000 storage systems use HSG80 controllers with ACS V8.5F or ACS V8.5S firmware. A single controller or dual-redundant controllers may be used. Dual-redundant controllers may be in transparent failover mode or multiple bus failover mode. The controllers may be configured for Fabric (FC-SW) or for Arbitrated Loop (FC-AL) as Private Loop devices.

Single Controller: A single controller provides multiple servers simultaneous access to multiple storage units through two host ports (fabric connections). Host Port 1 presents storage units D0 through D99 and Host Port 2 presents storage units D100 through D199.

Transparent Failover Controllers: Dual-redundant controllers in transparent failover mode provide higher availability and better performance than a single controller does. The top controller's Host Port 1 is active and its Host Port 2 is in standby mode. The bottom controller's Host Port 1 is in standby mode and its Host Port 2 is in active mode. In the unlikely event that one controller should fail, the I/O stream moves immediately to the other controller transparently; the standby mode host port takes over for the failed active host port. The host servers see no interruption in service. The transparent failover controllers both have one active host port and thus split the I/O load. Host Port 1 presents storage units D0 through D99 and Host Port 2 presents storage units D100 through D199.

Multiple Bus Failover Controllers: Dual-redundant controllers in multiple bus failover mode provide higher availability than dual-redundant controllers in transparent failover mode do. They may also provide better performance, depending on how storage access is spread between the controller host ports. Both host ports on both controllers are active. Host servers use multiple independent data paths to access storage systems configured for multiple bus failover mode, a No-Single-Point-Of-Failure (NSPOF) configuration. NSPOF configurations provide the maximum protection from data path failures.

A single data path consists of one Fibre Channel host bus adapter connected to one Fibre Channel switch connected to one storage controller host port. Should any part of a single data path fail, the host server and the storage controllers immediately coordinate moving the I/O stream to be added to another data path. The multiple bus failover controllers each have two active host ports and thus split the I/O load four ways. All four host ports present storage units D0 through D199.

Single controllers and transparent failover controllers cannot be configured for an NSPOF configuration.

Table 1 NSPOF Storage and Non-NSPOF Storage Tradeoffs

	NSPOF Storage Configuration	Non-NSPOF Storage Configuration
Reliability	Highest (completely redundant)	High
Availability	100% (no single point of failure)	High
Performance	Highest (multiple active data paths)	High
Minimum required # of host bus adapters per server	2	1
Minimum required # of Fibre Channel switches	2	1
Maximum # of supported servers per ESA12000 / RA8000	Host operating system and platform dependent	Host operating system and platform dependent
Maximum # of supported ESA12000s / RA8000s per server	Host operating system and platform dependent	Host operating system and platform dependent
For more information, please refer to the platform specific documentation listed in Section 7.		

The HSG80 controllers are configured for SCSI-2 or SCSI-3 mode depending on the requirements of the operating system. If SCSI-3 mode is used, LUN 0 for all host connections is reserved for the Command Console LUN; LUN 0 is not available for addressing a storage unit. Please refer to Section 3.4.

HSG80 controllers can be configured for use as Fabric (FC-SW) devices or Arbitrated Loop (FC-AL) Private Loop devices.

To add Arbitrated Loop (FC-AL) devices to your SAN, use of the switch QuickLoop feature is required. HSG80 controllers used in a QuickLoop must use a host port topology of LOOP_HARD. Currently, HP-UX is the only operating system supported in a QuickLoop. QuickLoop is supported only on specific Fibre Channel switch models. Please refer to Section 5 for more information regarding QuickLoop.

HSG80 controllers configured for Fabric (FC-SW) must use a host port topology of FABRIC. They are used outside of a QuickLoop.

Host servers that are configured for Fabric (FC-SW) can access HSG80 controllers configured for Arbitrated Loop (FC-AL). The QuickLoop feature of the Fibre Channel switches has a translative mode that automatically and transparently provides a loop address to the servers. This allows the servers outside of the QuickLoop to access the loop devices inside the QuickLoop. Servers inside the QuickLoop however, cannot access devices outside of the QuickLoop. If a host server can be configured for either Fabric (FC-SW) or Arbitrated Loop (FC-AL), the recommendation is to configure for Fabric.

OpenVMS: OpenVMS servers are configured only for Fabric (FC-SW). They cannot access devices in a QuickLoop. OpenVMS requires the ESA12000 and RA8000 storage systems to have dual-redundant HSG80 controllers configured for Fabric (FC-SW). It also requires the controllers to be configured for multiple bus failover mode. All OpenVMS host connections must be set for **OPENVMS**.

Tru64 UNIX: Tru64 UNIX servers are configured only for Fabric (FC-SW). They can access devices in the QuickLoop using the QuickLoop translative mode. Tru64 UNIX supports single and dual-redundant HSG80 controllers. The controllers may be configured for Fabric (FC-SW) or Arbitrated Loop (FC-AL); the Loop controllers are accessed using the QuickLoop translative mode. If dual-redundant HSG80 controllers are used, Tru64 UNIX requires they be configured for transparent failover mode. All Tru64 UNIX host connections must be set for **TRU64_UNIX**.

Windows NT: Window NT servers are configured only for Fabric (FC-SW). They can access devices in the QuickLoop using the QuickLoop translative mode. Windows NT supports single and dual-redundant HSG80 controllers. The controllers may be configured for Fabric (FC-SW) or Arbitrated Loop (FC-AL); the Loop controllers are accessed using the QuickLoop translative mode. If dual-redundant HSG80 controllers are used, they can be configured for transparent failover mode or for multiple bus failover mode. All Windows NT host connections must be set for **WINNT**.

Sun Solaris: Sun Solaris servers are configured only for Fabric (FC-SW). They can access devices in the QuickLoop using the QuickLoop translative mode. Sun Solaris supports single and dual-redundant HSG80 controllers. The controllers may be configured for Fabric (FC-SW) or Arbitrated Loop (FC-AL); the Loop controllers are accessed using the QuickLoop translative mode. If dual-redundant HSG80 controllers are used, Sun Solaris requires in a SAN they be configured for transparent failover mode. All Sun Solaris host connections must be set for **SUN**.

HP-UX: HP-UX servers are configured only for Arbitrated Loop (FC-AL) and must be used inside a QuickLoop. They only access devices in the same QuickLoop. HP-UX supports single and dual-redundant HSG80 controllers. HP-UX requires the controllers to be configured only for Arbitrated Loop (FC-AL). If dual-redundant HSG80 controllers are used, HP-UX requires in a SAN they be configured for transparent failover mode. All HP-UX host connections must be set for **HP**.

Fabric Connections

Storage systems can be connected to a fabric (one or more interconnected switches) using:

- 62.5-micron short wave multi-mode optical fibre cables up to 200 meters in length
- 50-micron short wave multi-mode optical fibre cables up to 500 meters in length.

Single controller: ESA12000 and RA8000 storage systems using a single HSG80 controller can have:

1. *One Switch:* Both host ports connected to one switch.
2. *Two Switches:* Each host port connected to a separate switch.

The second connection arrangement provides higher availability and better performance than the first does.

Transparent Failover Mode: ESA12000 and RA8000 storage systems using dual-redundant HSG80 controllers in transparent failover mode can have:

1. *One Switch:* All four host ports connected to one switch.
2. *Two Switches:* Host Port 1 of both controllers connected to one switch and Host Port 2 of both connected to another switch.

The second connection arrangement provides higher availability and better performance than the first does.

Multiple Bus Failover Mode: ESA12000 and RA8000 storage systems using dual-redundant HSG80 controllers in multiple bus failover mode can have:

1. *Two Switches:* Host Port 1 of the top controller and Host Port 2 of the bottom controller connected to one switch. Host Port 2 of the top controller and Host Port 1 of the bottom controller connected to another switch.
2. *Four Switches:* Each host port connected to a separate switch.

Both connection arrangements provide a No-Single-Point-Of-Failure (NSPOF) configuration. The second connection arrangement provides higher availability and better performance than the first does.

Windows NT and NSPOF: In NSPOF configurations, Windows NT servers must use *Compaq Secure Path V2.2*. Secure Path uses a pair of physically separate fabrics or a pair of zones to provide the data path redundancy.

For each Windows NT server, Secure Path only supports connecting to two active host ports on a storage system. Only Host Port 1 of both controllers are connected to the pair of zones or pair of fabrics; each to a separate zone or fabric. Host Port 2 of both controllers cannot be connected to the same pair of zones or pair of fabrics. Host Port 2 of both controllers can be used if they are in a second pair of zones, or are connected to a second pair of redundant fabrics, and they are used by a different set of Windows NT servers running Secure Path.

NOTE

Please consult the *HSG80 Array Controller, ACS Version 8.5, Configuration Guide*, the operating system specific application notes and other supporting documentation supplied with your storage system for more information regarding ESA12000 or RA8000 configuration requirements. Please refer to Section 7 for a listing of related documentation.

2.2 StorageWorks Command Console (SWCC)

StorageWorks Command Console is recommended for setting up and managing the storage systems and the Fibre Channel switches in the SAN. SWCC is a centralized graphical storage management console that allows real-time configuration of the storage environment and delivers reliable, real-time monitoring and notification of storage events.

The SWCC management console runs on Windows NT 4.0 (Alpha and Intel), Windows 98 and Windows 95. It provides a graphical interface for managing the storage systems and the Fibre Channel switches in the SAN.

The SWCC management console uses the SWCC HSG80 Storage Window to communicate over the Ethernet network to a server running an SWCC HS-Series Agent, one Agent for each storage system. The SWCC HS-Series Agent communicates to the storage system on behalf of the SWCC HSG80 Storage Window to manage this storage system. The SWCC HS-Series Agent runs on a host server that can connect with the storage system. It communicates with the storage system over the Fibre Channel fabric.

The SWCC management console uses the SWCC Fabric Window to communicate over the Ethernet network to a server running an SWCC Fibre Channel Switch Agent, one Agent for all Fibre Channel switches. The SWCC Fibre Channel Switch Agent communicates to the Fibre Channel switches on behalf of the SWCC Fabric Window to manage the switches. SWCC Fibre Channel Switch Agent runs on the computer used to manage the SAN or any Windows NT 4.0 server that can communicate with the switches over the Ethernet network.

NOTE

For redundancy in a multiple-host environment, each host may have an SWCC HS-Series Agent installed and each Windows NT host may also have an SWCC Fibre Channel Switch Agent installed. However, only **one** SWCC HS-Series Agent per storage system and only **one** SWCC Fibre Channel Switch Agent may be running at a time in the SAN; the Agents do not have an inter-agent locking mechanism to prevent two users from inadvertently changing the same storage system or same switch simultaneously.

A single SWCC HS-Series Agent gives the Command Console Client complete ability to monitor and control all RAID systems connected to that host server. A single SWCC Fibre Channel Switch Agent gives the Command Console Client complete ability to monitor and control all Fibre Channel switches in the SAN. These single Agents are the primary Agents. The remaining redundant Agents, secondary Agents, will substitute for the primary Agents should they becomes unavailable for any reason.

The secondary Agents must be manually stopped and disabled from starting on boot when they are initially configured. When they become needed, they must be manually started and enable for automatic start on boot.

Table 2 StorageWorks Command Console Supported Versions

SWCC Component	Minimum Version
Command Console	2.1
HSG80ACS85 Storage Window (1)	2.2
HS-Series Agent	2.2
Fabric Window	2.2
Fibre Channel Switch Agent	2.2
Command Line Interface Window	2.0

Table Notes:

(1) There are two storage windows for HSG80 controllers, HSG80 and HSG80ACS85. The HSG80 Storage Window is used for ACS V8.3 and ACS V8.4. The HSG80ACS85 Storage Window is used for ACS V8.5.

NOTE

Please consult the *Command Console, User's Guide* for more information about SWCC. Please refer to Section 7 for a listing of related documentation.

2.3 Host Servers

Host servers may connect to multiple SANs. The number of separate SANs per server is dependent on the operating system, the specific server platforms and the host bus adapters used.

Host servers can be connected to switches using:

- 62.5-micron short wave multi-mode optical fibre cables up to 200 meters in length
- 50-micron short wave multi-mode optical fibre cables up to 500 meters in length.

1. Any operating system that is supported with the ESA12000 or RA8000 storage systems in a switched fabric can be used. As of the writing of this document, the supported operating systems are:
   - Compaq OpenVMS V7.2 with TIMA kit VMS72_HARDWARE-V0100
     (DEC-AXPVMS-VMS72_HARDWARE-V0100--4.PCSI)
     - OR -
     Compaq OpenVMS V7.2-1 with TIMA kit VMS721_FIBRECHAN-V0100
     (DEC-AXPVMS-VMS721_FIBRECHAN-V0100--4.PCSI)
     All versions configured only as Fabric (FC-SW) devices.
   - Compaq Tru64 UNIX V4.0F
     Compaq ASE / TruCluster V1.6 (optional)
     All versions configured only as Fabric (FC-SW) devices.
   - Microsoft Windows NT (Intel) V4.0 with Service Pack 3, 4, or 5
     Microsoft Cluster Server V1.0 (optional)
     All versions configured only as Fabric (FC-SW) devices in a SAN.
   - Sun Solaris V2.6, V2.7 (32 bit) or V2.7 (64 bit)
     VERITAS FirstWatch V2.2.5 (optional)
     VERITAS Cluster Server V1.0 (optional)
     All versions configured only as Fabric (FC-SW) devices in a SAN.
   - HP-UX V10.2 or V11
     HP MC/ServiceGuard V10.10 or V11.0 (optional)
     All versions configured only as Arbitrated Loop (FC-AL) Private Loop devices.
2. For NSPOF configurations, the operating system must provide multiple data access path support and the host servers must be configured to use it.
   - Compaq OpenVMS has multiple path support built-in.
   - Microsoft Windows NT requires Compaq Secure Path V2.2 or newer.

NOTE

In NSPOF configurations, Windows NT servers must use *Compaq Secure Path V2.2*. Secure Path uses a pair of physically separate fabrics or a pair of zones to provide the data path redundancy.

For each Windows NT server, Secure Path only supports connecting to two active host ports on a storage system. Only Host Port 1 of both controllers are connected to the pair of zones or pair of fabrics; each to a separate zone or fabric. Host Port 2 of both controllers cannot be connected to the same pair of zones or pair of fabrics. Host Port 2 of both controllers can be used if they are in a second pair of zones, or are connected to a second pair of redundant fabrics, and they are used by a different set of Windows NT servers running Secure Path.

3. Each server must have the *RA8000/ESA12000 FC Solution Software Kit* for its operating system installed.
4. The host servers can be a mix of cluster servers and standalone servers.
5. Table 3 gives general guidelines for each operating system's supported maximums. The last column is the maximum number of active host connections per storage system for a homogeneous SAN and a heterogeneous SAN.

Table 3 Guidelines for Operating System Supported Maximums

Maximum Supported Number of:	Host Bus Adapters per Server (1)	Targets per HBA (2)	LUNs per HBA Target (2)	HBAs per Server per Switch Zone (2)	Active Controller Host Ports per HBA (2)	Active Host Connections per Storage System (3)
Tru64 UNIX	8	8	8	1	4	8
OpenVMS	4	16	100,000	2	16	8
Windows NT	4	16	8	4	4	16
Sun Solaris	16	16	64	16	4	8
HP-UX	2	16	8	2	4	8
Heterogeneous Access						8

Table Notes:

(1) The actual maximum number of host bus adapters per server is dependent on the specific server platform.

(2) The following are dependent on the specific host bus adapter and the operating system version:

- The maximum number of SCSI targets per host bus adapter, including itself. The maximum number of targets a host bus adapter can address in a SAN may be less.
- The maximum number of LUNs per SCSI target. The maximum number of LUNs per target a host bus adapter can address in a SAN may be less.
- The maximum number of HBAs per server that can be connected to the same switch zone.
- The maximum number of active HSG80 controller host ports a single HBA can simultaneously receive data from.

(3) This column gives the maximum number of active host connections for one storage system in a Homogeneous SAN using the specific operating system. The Heterogeneous Access entry is the maximum total number of active host connections when multiple operating systems are accessing the same storage system.

The maximum number of HBAs communicating with the storage system is dependent on the values in this column and the number of active HSG80 controller host ports:

- ***Two Active Host Ports:*** A single controller or dual-redundant controllers configured for transparent failover mode have two active host ports. Each HBA has one host connection for each host port. This gives two host connections per HBA. The maximum number of HBAs communicating with the storage system is one-half of the value in this column.

  For example, a storage system configured for transparent failover. Two host ports are active. It is being accessed solely by Windows NT servers. It can support 16 active Windows NT host connections. Each HBA has two host connections. The maximum number of HBAs that can communicate with this storage system is 8.

- ***Four Active Host Ports:*** Dual-redundant controllers configured for multiple bus failover mode have four active host ports. Each HBA has one host connection for each host port. This gives four host connections per HBA. The maximum number of HBAs communicating with the storage system is one-quarter of the value in this column.

  For example, one storage system is configured for multiple bus failover. All host ports are active. It is being accessed solely by Windows NT servers. It can support 16 active Windows NT host connections. Each HBA has four host connections. The maximum number of HBAs that can communicate with this storage system is 4.

- ***Zoned Active Host Ports:*** If the active controller host ports are in different zones, the maximum number of HBAs communicating with this storage system is calculated as follows:

  (1) The maximum number of allowed host connections is the value in this column.

  (2) For each HBA in all zones that include the storage system:
  - An HBA uses one host connection for each active host port in the same zone.
  - Subtract the number of host connections used by the HBA from the maximum number of allowed host connections.

  (3) When all of the allowed host connections have been used, the number of HBAs is the maximum number of HBAs that can communicate with this storage system.

  For example, one storage system is configured for multiple bus failover. All host ports are active. It is being accessed solely by Windows NT servers. The maximum number of allowed host connections is 16. Zone #1 has only two controller host ports in it and 2 HBAs. Zone #2 has the other two host ports. We will calculate the maximum number of HBAs that can be added to Zone #2.

  For Zone #1:
  - Each HBA communicates with two active host ports.
  - Four host connections are used by Zone #1.

  For Zone #2:

  (1) 12 host connections remain available for use.

  (2) Each HBA added communicates with two active host ports, thus each uses two host connections.

  (3) 6 HBAs can be added to Zone #2.

NOTE

Please refer to Section 6 for more information regarding switch zoning and the configurations that ***require*** it.

NOTE

Please consult the *RA8000/ESA12000 HSG80 Solution Software V8.5, Installation Reference Guide* for the host server's operating system, the operating system specific application notes and other supporting documentation supplied with your storage system for more information regarding host server configuration requirements, including operating system version. Please refer to Section 7 for a listing of related documentation.

2.4 Fibre Channel Switches

Up to four switches, each with up to sixteen Gigabit Interface Converters (GBIC), are supported for a heterogeneous SAN.

Inter-Switch Links (ISLs), switch to switch connections, can be made using:

- 62.5-micron short wave multi-mode optical fibre cables up to 200 meters in length
- 50-micron short wave multi-mode optical fibre cables up to 500 meters in length.
- 9-micron long wave single-mode optical fibre cables up to 10 kilometers in length

Some applications may not be able to use the longer ISLs.

For example, a configuration has one server and one storage system connected to one switch. Another server and another storage system are connected to another switch. The two switches are connected by a 10 km ISL. The two servers form a cluster. A logical disk is created using host based mirroring of storage on both storage systems. Both servers access this logical disk.

During a write operation the network link between the servers and the ISL are both severed. One mirror member received the write while the other did not; one mirror is now corrupt. Both servers recognize the mirror and cluster both have been broken. Unfortunately, the server that can still access the corrupted mirror is unaware of the corruption. It continues to use the corrupted data as if it were valid.

This scenario requires the two switches to be located in the same data center. A 10 km ISL would not be used.

The Compaq Fibre Channel equipment supported is as follows:

- Compaq 16 port Fibre Channel SAN Switch, firmware V2.0.3A, part # 158223-B21
- Compaq 8 port Fibre Channel SAN Switch, firmware V2.0.3A, part # 158222-B21
- Compaq Fibre Channel Storage Switch 16 (16 ports), firmware V1.6B, part # 380578-B21
- Compaq Fibre Channel Storage Switch 8 (8 ports), firmware V1.6B, part # 380591-B21
- Optical Short Wave GBIC, part # 380561-B21
- Optical Long Wave GBIC, part # 127508-B21
- Fibre Channel Optical Cable, 50-Micron Short Wave Multi-mode, part # 234457-B21/B22/B23/B24/B25 (2/5/15/30/50m)

For longer 50-micron short wave multi-mode optical fibre cables (up to 500 meters) a third party vendor must be contacted. The cables must be duplex tight buffered multi-mode 50/125 µ m (Belcore GR-409 compliant) and the connectors must be SC duplex low metal (NTT-SC Belcore 326, IEC-874-19 SC compliant).

For 9-micron long wave single-mode optical fibre cables (up to 10 kilometers) a third party vendor must be contacted. The cables must be duplex tight buffered single-mode 9/125 µm (Belcore GR-409 compliant) and the connectors must be SC duplex low metal (NTT-SC Belcore 326, IEC-874-19 SC compliant).

NOTE

Please consult the *SAN Switch Fabric Operating System Management Guide* and other supporting documentation supplied with your Fibre Channel SAN switch for more information regarding switch configuration requirements. Please refer to Section 7 for a listing of related documentation.

2.5 Heterogeneous SAN General Configuration Rules

The following are general configuration rules for heterogeneous SANs. They should be used as the base of initial guidelines to start from. The exact configuration used for a specific SAN begins from these guidelines and is modified dependent on operating system specific rules, the server platforms and the applications being run on the SAN. Please consult the documentation and application notes for each storage system, switch and server for specific configuration details. Please refer to Section 7 for a listing of related documentation.

Architecture:

- When possible, devices that exchange the highest amount of data should be connected to the same switch.
- When devices exchanging data are on different switches:
  - For high bandwidth, use a maximum of two controller host ports per switch to switch connection, Inter-Switch Link (ISL).
  - For high throughput, use a maximum of six controller host ports per ISL.
- When possible, the storage system connections should be distributed equally among the switches.
- If future growth of the SAN is anticipated, some ports on each switch should be left unused for later ISL connections to the new SAN components. We recommend reserving Switch Ports 13 and 15 for future growth.

Fabric:

- Up to four switches in a fabric, all interconnected.
- Within a single fabric, each switch must have a unique Domain ID.
- Maximum of one hop under normal operation, maximum of two hops with a single failure.

  Data routing through the fabric is described in terms of hops, where a single hop is the set of Inter-Switch Links (ISLs) between two switches, two switches cascaded. Should the one-hop route fail (all of the ISLs between the two switches fail), the fabric can transparently reroute the I/O traffic to the two-hop path through the fabric. The host servers see no interruption in their I/O flow. Heterogeneous SAN building blocks that provide this rerouting capability are shown in Section 2.6.
- Minimum optical fibre cable length of 2 meters.

- Up to 200 meter connections between Fibre Channel devices when using 62.5-micron short wave multi-mode optical fibre cables and short wave GBICs.
- With 62.5-micron short wave multi-mode fibre cables being used for the ISLs:
  - Up to 600 kilometers total distance from server to storage.
  - Worst case (single fault reroute) distance of 800 meters.
- Up to 500 meter connections between Fibre Channel devices when using 50-micron short wave multi-mode optical fibre cables and short wave GBICs.
- With 50-micron short wave multi-mode fibre cables being used for the ISLs:
  - Up to 1.5 kilometers total distance from server to storage.
  - Worst case (single fault reroute) distance of 2.0 kilometers.
- Up to 10 kilometer connections, only between switches, when using 9-micron long wave single-mode optical fibre cables and long wave GBICs.
- With 9-micron long wave single-mode fibre cables being used for the ISLs:
  - Up to 11 kilometers total distance from server to storage.
  - Worst case (single fault reroute) distance 21 kilometers.

Server/Storage Connectivity:

- Any mix of servers and storage systems based on the maximums given in Section 2.3 and in the operating system specific application notes and documentation. Please refer to Section 7 for a listing of related documentation.
- Any mix of clusters servers and standalone servers.
- Visibility of storage controller host ports to an HBA must be carefully managed. The HBA / operating system combinations have their own limitations on the maximum number of targets they can address. If the number of controller host ports visible to an HBA exceeds this maximum, there is the potential that a specific storage system would not be addressable. A controller host port that is not used may consume a target and prevent a controller host port that was intended to be used from having a target. Please refer to Section 6 on the use of zoning in this case.
- Any required zoning must be configured before connecting the servers and the storage to the SAN. Please refer to Section 6.4 for information on configurations that ***require*** zoning.
- HSG80 controllers use ACS V8.5F or ACS V8.5S.
- If ACS V8.5S is used, the HSG80 controllers cannot participate in a QuickLoop; they cannot be configured for Arbitrated Loop (FC-AL). To participate in a QuickLoop, they must use ACS V8.5F. Please refer to Section 5 for more information on QuickLoop.
- All storage systems must be configured with the appropriate Selective Storage Presentation before the host servers begin using the storage. Please refer to Section 4 for information on Selective Storage Presentation.

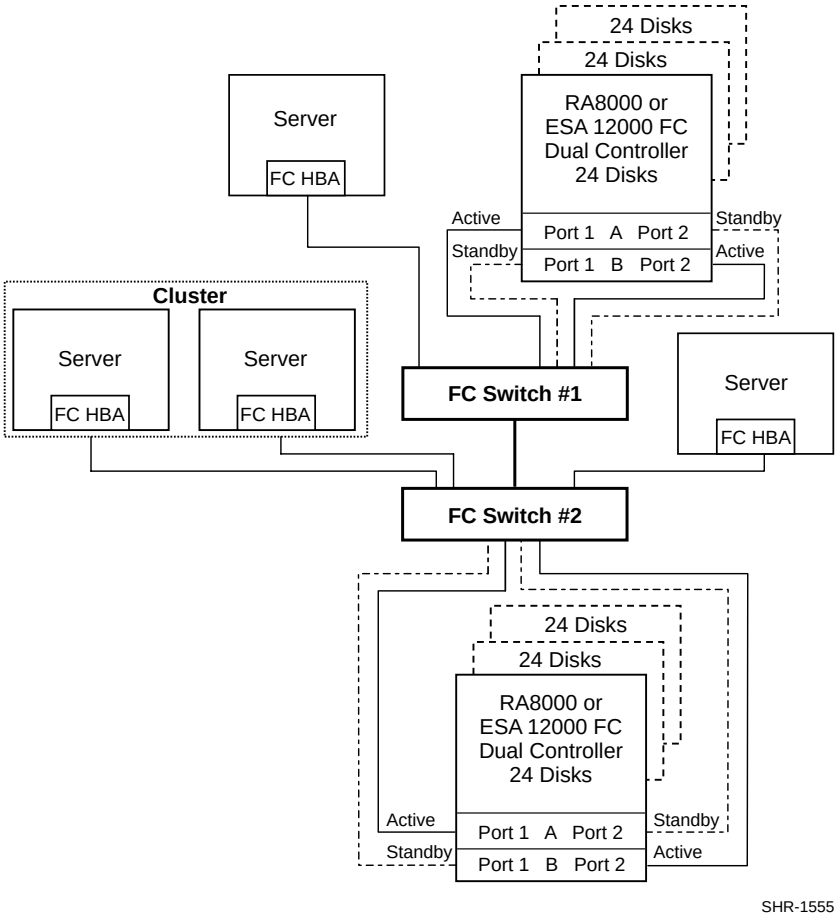
- Host connections to the storage systems must be carefully managed. The HSG80 controllers using ACS V8.5F or ACS V8.5S have a limit of 64 host connections. Exceeding this host connection limit may cause a fatal controller error. Please refer to Section 3.
- All host connections on the storage systems need to indicate the correct operating system.
- The storage must be configured according to the requirements of the specific operating systems. Please consult the operating system specific application notes and documentation; please refer to Section 7 for a listing of related documentation.

2.6 Heterogeneous SAN Building Blocks

The following SAN building blocks have been certified by Compaq and are recommended as SAN layouts.

The fabric topology (switch layout) is the key to each building block. The server and storage system connections shown serve as an example layout. Many possible arrangements of servers and storage systems exist for each building block. To create an appropriate layout for your SAN use the General Configuration Rules given in Section 2.5 and the operating system specific application notes; please refer to Section 7 for a listing of related documentation.

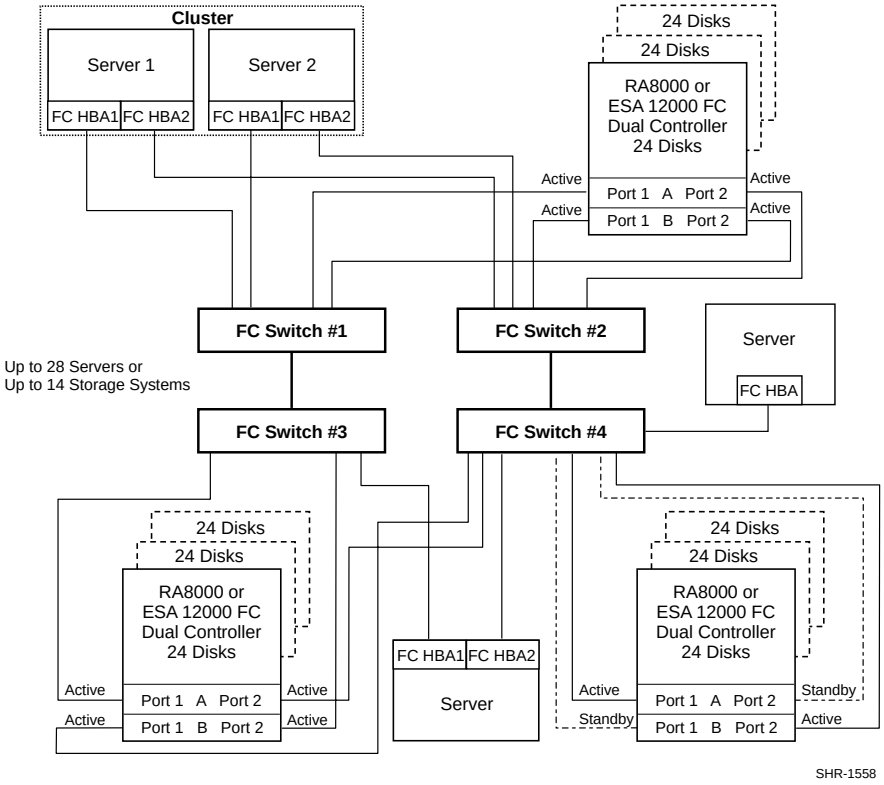
Figure 3 Example General Purpose Fabric 2 Cascaded Switches



The *General Purpose Fabric* SAN building block is the basic building block of SANs. It interconnects multiple servers and multiple storage systems.

Only storage systems configured for transparent failover mode are used in this example. The servers must use operating systems that support HSG80 controllers configured for transparent failover mode.

Figure 4 Example High Availability Storage / Fault Tolerant Fabrics 4 Cascaded Switches



The *High Availability Storage / Fault Tolerant Fabrics* SAN building block combines two physically separate *General Purpose Fabric* SAN building blocks to provide a configuration with No-Single-Point-Of-Failure (NSPOF) high availability (HA).

NSPOF configurations provide the maximum protection from data path failures. A single data path consists of one Fibre Channel host bus adapter connected to one Fibre Channel switch connected to one storage controller. Should any part of a single data path fail, the host server and the storage systems immediately coordinate the move of the I/O stream to another data path.

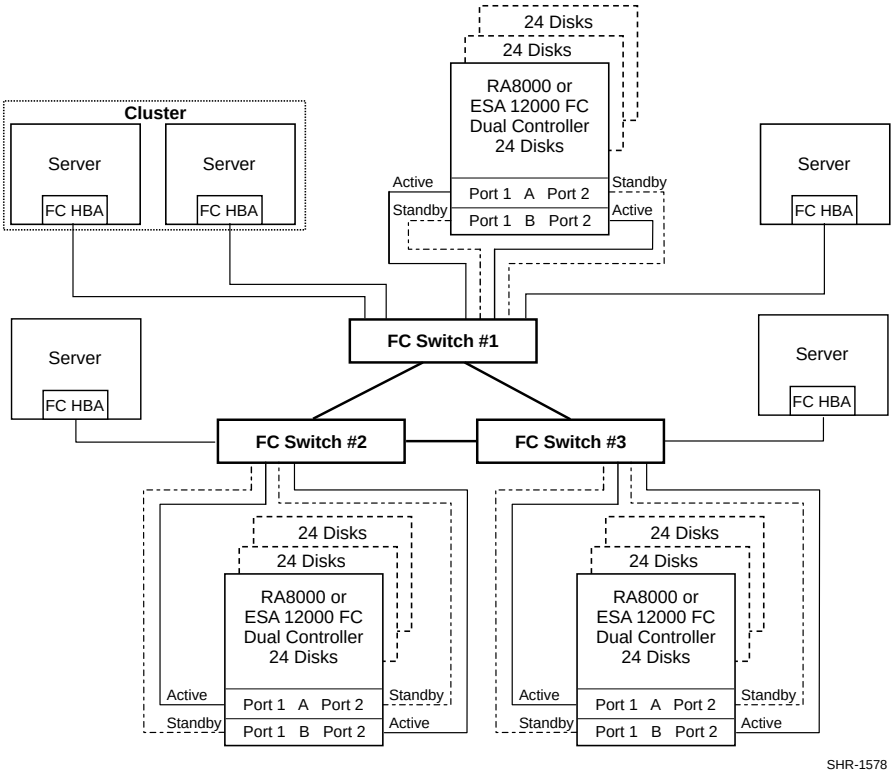
HA requires the host servers to use two Fibre Channel adapters and the storage systems to use dual-redundant controllers in multiple bus failover mode.

The servers configured for NSPOF must use operating systems that support HSG80 controllers configured for multiple bus failover mode.

The example also includes a non-NSPOF configured server and a non-NSPOF configured storage system. They do not use the redundant fabric.

The servers configured for non-NSPOF must use operating systems that support HSG80 controllers configured for transparent failover mode.

Figure 5 Example Meshed Fabric 3 Cascaded Switches



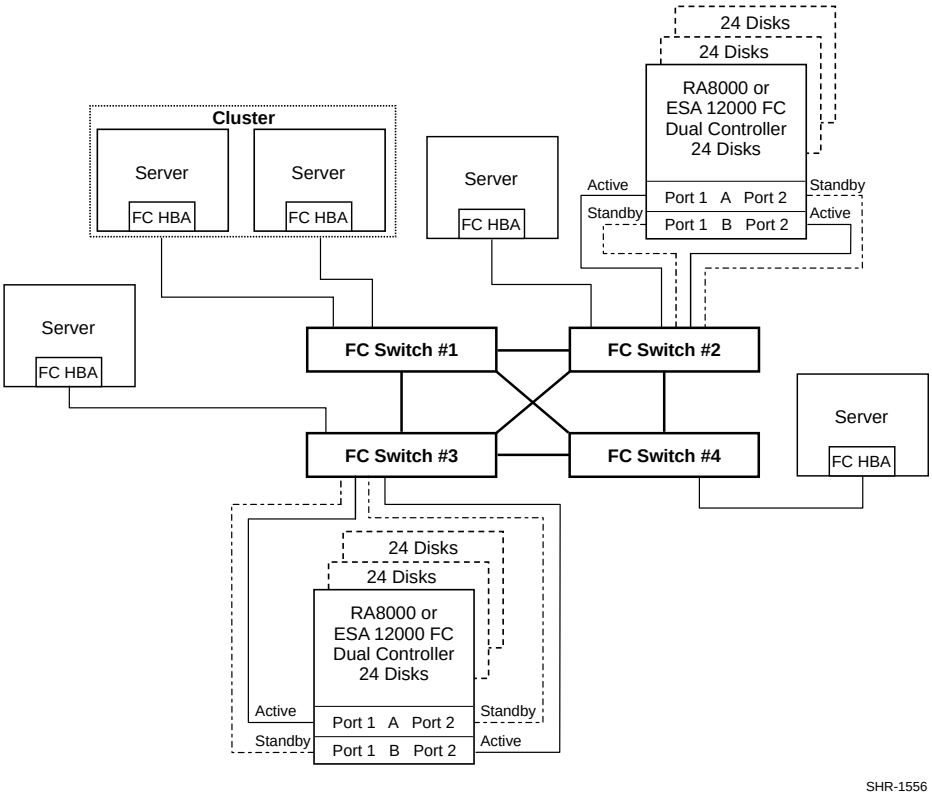
The *Meshed Fabric* SAN building block provides greater connectivity than the *General Purpose Fabric* SAN building block does. It also provides fabric rerouting capability.

Data routing through the fabric is described in terms of hops, where a single hop is the set of Inter-Switch Links (ISLs) between two switches. Should the one-hop route fail (all of the ISLs between the two switches fail), the fabric can transparently reroute the I/O traffic to the two-hop path through the fabric. The host servers see no interruption in their I/O flow.

In the example above, data is being transferred between the standalone server on the left and the top storage system. Should the ISL between FC Switch #1 and FC Switch#2 fail then the fabric would reroute the data through FC Switch #3.

Only storage systems configured for transparent failover mode are used in this example. The servers must use operating systems that support HSG80 controllers configured for transparent failover mode.

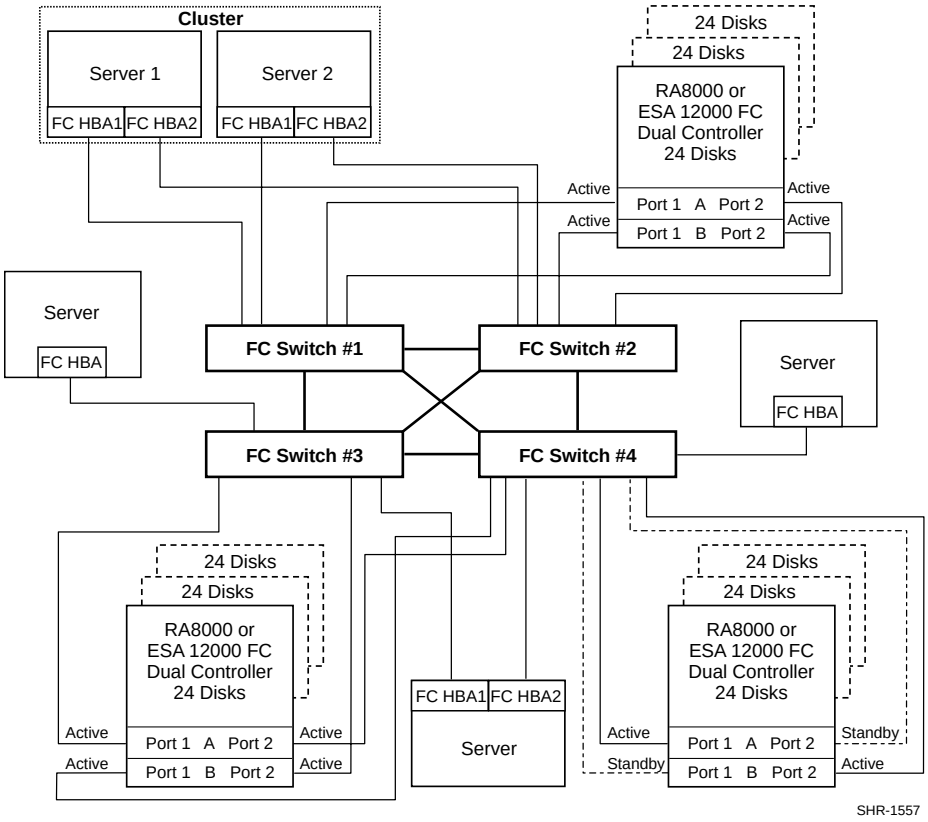
Figure 6 Example Meshed Resilient Fabric 4 Cascaded Switches



The *Meshed Resilient Fabric* SAN building block provides both greater connectivity and a more resilient fabric rerouting capability than the *Meshed Fabric* SAN building block does. Should the one-hop path fail, the fabric transparently can reroute the I/O traffic to a two-hop path. Should this two-hop path fail, the fabric can reroute again to a second two-hop path.

Only storage systems configured for transparent failover mode are used in this example. The servers must use operating systems that support HSG80 controllers configured for transparent failover mode.

Figure 7 High Availability Storage / Meshed Resilient Fabric 4 Cascaded Switches



The *High Availability Storage / Meshed Resilient Fabric* SAN building block provides the advantages of both high availability and fabric resilience. The high availability (HA) capability of the host servers and storage systems are augmented by the resilience of the fabric rerouting capability. Multiple data path failures can be tolerated with this SAN configuration.

This SAN building block's multiple (greater than two) data path capability is supported by the following operating systems:

- OpenVMS V7.2 and V7.2-1

This SAN building block is not supported by operating systems using HA capability that requires two physically separate data paths, two separate fabrics or two separate zones.

Both HA and non-HA configured servers and storage systems can be used in this SAN building block. This example also includes two servers (the middle left and middle right) and a storage system not configured for HA.

The servers configured for HA must use operating systems that support HSG80 controllers configured for multiple bus failover mode. The servers not configured for HA must use operating systems that support HSG80 controllers configured for transparent failover mode.

3.0 Heterogeneous SAN Configuration Procedures

This section gives the configuration procedures for a heterogeneous SAN.

> **NOTE**
>
> It is assumed the reader understands the installation procedure for each specific server platform, storage system, Enterprise Backup Solution (EBS) tape backup system and Fibre Channel switch before these configuration procedures for the SAN are followed. Please consult the documentation and application notes for the servers, storage systems, EBS system and switches for specific details on how to accomplish each of the following steps. Please refer to Section 7 for a listing of related documentation.

This first configuration procedure (Sections 3.1 through 3.7) sets up a new heterogeneous SAN in the following order:

1. Configuration Layout
2. Host Servers
3. Fibre Channel Switches and SAN Connections
4. Storage Systems Initial Set Up and StorageWorks Command Console (SWCC)
5. Storage Systems Configuration
6. Enterprise Backup Solution (EBS) Systems Configuration
7. Host Server Use of the Storage Systems and EBS Systems

The last section gives additional procedures for modifying an existing SAN configuration.

3.1 Configuration Layout

1. Create a SAN topology map that specifies in detail how all of the equipment is to be connected to the SAN. It should detail:

   - The port number of the switch port used to connect to each host bus adapter, each storage controller host port, each EBS tape controller port and each Fibre Channel switch.
   - The Fibre Channel World Wide Name (WWN) of each host bus adapter, each storage controller host port, each EBS tape controller port and each Fibre Channel switch.
   - The storage controller parameters for each storage system; e.g., failover mode. Please refer to Sections 3.5 and 3.6.
   - The unit offset of each server host connection on each storage system. Please refer to Section 4.
   - Which servers will have access to each storage unit on each storage system. Please refer to Section 4.
   - For each storage system, which server will be the primary one to run the SWCC HS-Series Agent to manage that storage system. Plus, which servers will be substitutes if the primary one is unavailable for any reason. Please refer to Section 3.6.

- Whether the Windows NT/98/95 platform that will be used for managing the SAN or one of the Windows NT servers will be the primary one to run the SWCC Fibre Channel Switch Agent. Plus, which of these will be substitutes if the primary one is unavailable for any reason. Please refer to Section 3.6.
- The EBS tape controller parameters for each EBS system; e.g., which servers will be using it.
- The switch domain IDs for each switch.
- Any QuickLoop configurations. Please refer to Section 5.
- Any Switch Zoning configuration. Please refer to Section 6.4 for information on configurations that ***require*** zoning.

2. Create a network topology map that specifies in detail how the equipment is to be connected to the Ethernet network. This may be included on the SAN topology map. It should indicate the TCP/IP address and the network name of each device.

3.2 Host Servers

The following is done for each server for each fabric it will be attached to:

1. If not previously done, install the Fibre Channel host bus adapters in the server.
2. Connect the server to the Ethernet network according to the network topology map.
3. Power on the server.
4. If not already in the operating system, install Fibre Channel support.
5. Install the *RA8000/ESA12000 FC Solution Software Kit*.

NOTE

Please consult the *RA8000/ESA12000 HSG80 Solution Software V8.5, Installation Reference Guide* for the host server's operating system, the operating system specific application notes and other supporting documentation supplied with your storage system for more information regarding host server configuration requirements, including operating system version. Please refer to Section 7 for a listing of related documentation.

6. Install the *StorageWorks Command Console HS-Series Agent*. Configure the Agent to include as a client the Windows NT/98/95 platform that will be used for managing the SAN.
7. Stop the SWCC HS-Series Agent if this server is indicated on the SAN topology map to be a substitute SWCC HS-Series Agent server. Only the primary servers may have the SWCC HS-Series Agent running.
8. Optionally for Windows NT, install the *StorageWorks Command Console Fibre Channel Switch Agent*. Configure the Agent to include as a client the Windows NT/98/95 platform.
9. Stop the SWCC Fibre Channel Switch Agent if this platform is indicated on the SAN topology map to be a substitute for the SWCC Fibre Channel Switch Agent. Only the primary platform may have the SWCC Fibre Channel Switch Agent running.

The following is done for each Windows NT/98/95 platform that will be used for managing each fabric:

10. Optionally, install the *StorageWorks Command Console Fibre Channel Switch Agent*. Configure the Agent to include as a client the Windows NT/98/95 platform.
11. Stop the SWCC Fibre Channel Switch Agent if the SWCC Fibre Channel Switch Agent was installed and if this platform is indicated on the SAN topology map to be a substitute for the SWCC Fibre Channel Switch Agent. Only the primary platform may have the SWCC Fibre Channel Switch Agent running.
12. Install the *StorageWorks Command Console Fabric Window*.
13. Install the *StorageWorks Command Console HSG80ACS85 Storage Window* Client.

NOTE

For redundancy in a multiple-host environment, each host may have an SWCC HS-Series Agent installed and each Windows NT host may also have an SWCC Fibre Channel Switch Agent installed. However, only **one** SWCC HS-Series Agent per storage system and only **one** SWCC Fibre Channel Switch Agent may be running at a time in the SAN; the Agents do not have an inter-agent locking mechanism to prevent two users from inadvertently changing the same storage system or same switch simultaneously.

A single SWCC HS-Series Agent gives the Command Console Client complete ability to monitor and control all RAID systems connected to that host server. A single SWCC Fibre Channel Switch Agent gives the Command Console Client complete ability to monitor and control all Fibre Channel switches in the SAN. These single Agents are the primary Agents. The remaining redundant Agents, secondary Agents, will substitute for the primary Agents should they becomes unavailable for any reason.

The secondary Agents must be manually stopped and disabled from starting on boot when they are initially configured. When they become needed, they must be manually started and enable for automatic start on boot.

NOTE

The servers can be connected to multiple fabrics, each fabric through a separate set of HBAs. The SWCC management platform (Windows NT/98/95 platform) can manage multiple fabrics through the same network or through multiple networks.

3.3 Fibre Channel Switches and SAN Connections

Before the switches are connected to the Ethernet network and before they are interconnected, the following is done for each switch:

1. Power on the switch.
2. Set the Ethernet IP Address and Gateway. Depending on the switch model, use the front panel or a serial line connected to the serial port.
3. Connect the switch to the Ethernet network according to the network topology map.

After all of the switches are connected to the Ethernet network, but before they are interconnected, the following is done:

4. On the Windows NT/98/95 platform that will be used for managing the SAN:
   - Start SWCC.
   - Add the platform that is running the SWCC Fibre Channel Switch Agent.
   - Start the Fabric Window.
   - Add the fabric and all of its switches.

The following is done for each switch:

5. On the Windows NT/98/95 platform that will be used for managing the SAN:
   - In the Fabric Window select the switch.
   - Start its web management window.
6. Click on the **admin** button and log into the administrator account.
7. Set the administrator account's login name and password.
8. Set the Switch Domain ID.
9. If the switch has been previously used:
   - Click on the **telnet** button to start a telnet session with the switch.
   - Log into the administrator account.
   - Disable and delete any zone configuration; use the **cfgClear** switch command.
   - Disable QuickLoop; use the **qlDisable** switch command.
   - Close the telnet session.

If QuickLoop is to be used on this switch:

10. Click on the **telnet** button to start a telnet session with the switch.
11. Log into the administrator account.
12. Enable QuickLoop for each switch port participating in the QuickLoop.
13. If the switch has a QuickLoop partner switch, identify the partner switch by its WWN. QuickLoop is supported only on specific Fibre Channel switch models. Please refer to Section 5 for more information regarding QuickLoop.
14. Close the telnet session.

After the switch has been configured:

15. Close the switch web management windows.
16. Connect the switch to the other configured switches according to the SAN topology map.

If switch zoning is to be used, the following is done on one switch for the entire fabric:

17. From the SWCC Fabric Window on the Windows NT/98/95 platform that will be used for managing the fabric, start the switch web management window for one switch.
18. Click on the **telnet** button to start a telnet session with the switch.
19. Log into the administrator account.
20. If switch zoning is to be used then define, enable and save the zone configuration.

NOTE

- The zone configuration changes will automatically propagate from this switch to the other switches.
- SWCC has a major impact on how zoning is used. Please refer to Section 3.5 for details.
- Please refer to Section 6 for information on zoning and for information on configurations that ***require*** zoning.

21. Close the telnet session.
22. Close the switch web management windows.

After all of the switches are configured and any zoning has been configured:

23. Close the SWCC windows.
24. Connect the host servers to the SAN according to the SAN topology map.

NOTE

Please consult the *SAN Switch Fabric Operating System Management Guide* and other supporting documentation supplied with your Fibre Channel SAN switch for more information regarding switch configuration requirements. Please refer to Section 7 for a listing of related documentation.

3.4 Storage Systems Initial Set Up and Storage Works Command Console (SWCC)

The first part of this section gives the portion of the set up procedure that covers storage systems. The second part gives an explanation how to use storage system's Command Console LUN (CCL) with the SWCC HS-Series Agent running in specific operating systems.

3.4.1 Storage System Initial Set Up

The following is done for each storage system:

1. Install all of the physical components.
2. Power on the storage system.
3. Start a terminal session with the storage system using a serial line connected to the serial port on one storage controller.
4. If not previously done, set the Fibre Channel World Wide Name for the storage system.
5. Set up the HSG80 controllers according to Table 4:

Table 4 HSG80 Controller Set Up

	Failover Mode	Host Port Topology (1)	SCSI mode (2)	Command Console LUN (3)
Tru64 UNIX	Transparent	FABRIC or LOOP_HARD (6)	SCSI-2	Disabled or Enabled
OpenVMS (4)	Multiple Bus	FABRIC	SCSI-3 (8)	Automatically Enabled
Windows NT	Transparent or Multiple Bus (5)	FABRIC or LOOP_HARD (6)	SCSI-2 or SCSI-3 (8)	Disabled or Enabled
Sun Solaris	Transparent	FABRIC or LOOP_HARD (6)	SCSI-2	Disabled or Enabled
HP-UX	Transparent	LOOP_HARD (7)	SCSI-2	Disabled or Enabled

Table Notes:

(1) If the storage controller host ports are configured for a topology of FABRIC, then the host ports connect with the switch ports as Fabric (FC-SW) devices. If the storage controller host ports are configured for a topology of LOOP_HARD, then the host ports connect to the switch ports as Arbitrated Loop (FC-AL) Private Loop devices. These switch ports must be configured for QuickLoop. Please refer to Section 5 for more information regarding QuickLoop.

(2) The SCSI mode is set per storage system; dual-redundant controllers cannot be set to different SCSI modes.

(3) The Command Console LUN is discussed in Section 3.4.2.

(4) OpenVMS requires all Command Console LUNs and storage units to be assigned a device identifier. These identifiers must be unique across all storage systems within a single cluster; e.g., a cluster uses two storage systems, only one device (a storage unit or a Command Console LUN) can use the identifier 2. Devices may have the same identifier if they are not used in the same cluster.

(5) If Windows NT is configured for No-Single-Point-Of-Failure (NSPOF), it must use Compaq Secure Path. The controllers must be configured for multiple bus failover mode.

NOTE

Please note that Secure Path is only supported in a SAN that does not use switch zoning.

For each Windows NT server, Secure Path only supports connecting to two active host ports on a storage system. Only Host Port 1 of both controllers are connected to the pair of fabrics; each to a separate fabric. Host Port 2 of both controllers cannot be connected to the same pair of fabrics. Host Port 2 of both controllers can be used if they are connected to a second pair of redundant fabrics and are used by a different set of Windows NT servers running Secure Path.

(6) A server running any of these operating systems connects to the switch as a Fabric (FC-SW) device. It accesses the storage system, which is connected to the switch as an Arbitrated Loop (FC-AL) device, using the QuickLoop translative feature. Please refer to Section 5 for more information on QuickLoop.

(7) An HP-UX server connects to the switch as an Arbitrated Loop (FC-AL) Private Loop device. All storage systems it accesses must also be Arbitrated Loop devices. The server and storage systems must be in the QuickLoop on the switches. Please refer to Section 5 for more information on QuickLoop.

(8) SCSI-3 mode reserves LUN 0 for the Command Console LUN (CCL) on all host connections; LUN 0 is no longer available for addressing a storage unit. For operating systems that support both SCSI-2 and SCSI-3 modes, use SCSI-2 to gain the use of LUN 0 to address a storage unit.

NOTE

If the CCL is enabled in a storage system configured for SCSI-2 mode, LUN 0 is still unavailable for host connections that have a unit offset of zero. To gain the use of LUN 0 for these host connections, disable the CCL or change the unit offset of each host connections to a non-zero value. Either of these actions affects the ability to use SWCC to manage the storage system. Please refer to Section 3.4.2 for more information on SWCC and the CCL. Please refer to Section 4 for more information on unit offsets.

6. Connect the storage system to the SAN according to the SAN topology map.

NOTE

Please consult the *HSG80 Array Controller, ACS Version 8.5, Configuration Guide* and other supporting documentation supplied with your storage system for more information regarding ESA12000 or RA8000 configuration requirements. Please refer to Section 7 for a listing of related documentation.

3.4.2 SWCC and the Command Console LUN (CCL)

The storage system is configured by creating various types of storage units and associating them with specific IDs called Logical Unit Numbers (LUNs). A host server uses these LUNs to access the underlying storage unit.

The storage system is pre-configured with a virtual LUN located in the controllers at LUN 0. This virtual LUN is the Command Console LUN. It allows the storage system to be recognized by a host server without requiring a storage unit to be created first. The CCL also serves as a communications device for the SWCC HS-Series Agent. The CCL identifies itself to the host server with a unique identification string, returned in response to the SCSI Inquiry command. This identification string is HSG80CCL.

When dual-redundant controllers are configured for transparent failover mode, the CCL is only available through the active controller Host Port 1. If the host server that is running the SWCC HS-Series Agent used to manage the storage system is only connected to controller Host Port 2, it requires access to a storage unit for communication with the storage system; the CCL is not available through Host Port 2.

When dual-redundant controllers are configured for multiple bus failover mode, the CCL is available through all active controller host ports.

When switch zoning is used, every storage system in a zone there must have one server running an SWCC HS-Series Agent that can communicate with the storage system. If this server's SWCC HS-Series Agent can use the storage system's Command Console LUN then the server does not require access to a storage unit on the storage system. Please refer to Section 6 for more information regarding switch zoning.

The following discusses the enabling or disabling of the Command Console LUN (CCL) on a storage system. This depends on which operating system has the server that is running the SWCC HS-Series Agent used to manage the storage system:

Tru64 UNIX: Tru64 UNIX requires the HSG80 controllers to be configured for SCSI-2 mode. When a Tru64 UNIX server is running the SWCC HS-Series Agent:

- If the Tru64 UNIX server does not have access to storage units on the storage system, the CCL must be enabled. In this case, the CCL is the only device on the storage system the Tru64 UNIX SWCC HS-Series Agent can communicate with. The Tru64 UNIX server must also have a host connection with a unit offset of zero; otherwise it cannot access the CCL.
- If the Tru64 UNIX server has access to storage units on the storage system, the CCL can be either enabled or disabled. The Tru64 UNIX SWCC HS-Series Agent can manage the storage system by communicating with the CCL or by communicating through one of the storage units. If the Tru64 UNIX server has a unit offset that is non-zero, it cannot access the CCL; it must communicate through one of the storage units.

OpenVMS: OpenVMS requires the HSG80 controllers to be configured for SCSI-3 mode. This automatically enables the CCL; it cannot be disabled. When an OpenVMS server is running the SWCC HS-Series Agent, it can manage the storage system by communicating with the CCL or by communicating through one of the storage units.

Windows NT: Windows NT supports the HSG80 controllers being configured for either SCSI-2 mode or SCSI-3 mode. All Windows NT servers, regardless of whether they are running the SWCC HS-Series Agent, requires the Command Console LUN (CCL) to be enabled or disabled dependent on the following:

- ***SCSI-2 mode:*** Windows NT requires the CCL to be disabled unless all Windows NT host connections are set to a unit offset that is non-zero. If the Windows NT server is running the SWCC HS-Series Agent, the Windows NT server requires access to a storage unit on the storage system for communication to the storage system. It cannot use the CCL.

NOTE

If one storage system in the SAN is configured for SCSI-2 mode, has the CCL enabled and has a Windows NT host connection with a unit offset of zero, the Windows NT Disk Administrator on that Windows NT server will see the CCL as a disk. It will attempt to write a signature on the CCL, which is a read-only device. The attempt could result in the Disk Administrator having a fatal error. This would prevent that Windows NT server from configuring any of the storage units it has access to on all storage systems in the SAN.

This problem can occur to any Windows NT server, with or without access to a storage unit on the storage system, with or without running the SWCC HS-Series Agent.

On a storage system configured for SCSI-2 mode with the CCL enabled, a non-zero unit offset is required for every Windows NT host connection.

- ***SCSI-3 mode:*** The CCL is automatically enabled and cannot be disabled. Windows NT supports the CCL being enabled in this SCSI mode whether or not the server is running the SWCC HS-Series Agent. If the Windows NT server is running the SWCC HS-Series Agent, the Windows NT server does not require access to a storage unit on the storage system; it can communicate with the CCL.

Sun Solaris: Sun Solaris requires the HSG80 controllers to be configured for SCSI-2 mode. When a Sun Solaris server is running the SWCC HS-Series Agent:

- If the Sun Solaris server does not have access to storage units on the storage system, the CCL must be enabled. In this case, the CCL is the only device on the storage system the Sun Solaris SWCC HS-Series Agent can communicate with. The Sun Solaris server must also have a host connection with a unit offset of zero; otherwise it cannot access the CCL.
- If the Sun Solaris server has access to storage units on the storage system, the CCL can be either enabled or disabled. The Sun Solaris SWCC HS-Series Agent can manage the storage system by communicating with the CCL or by communicating through one of the storage units. If the Sun Solaris server has a unit offset that is non-zero, it cannot access the CCL; it must communicate through one of the storage units.

NOTE

If the CCL is enabled, all Sun Solaris servers that can communicate with the storage system will see the CCL as a disk, whether they are running the SWCC HS-Series Agent or not. During the boot sequence, the Sun Solaris servers will report a warning that the CCL "disk" has not been formatted correctly. This warning can be ignored.

HP-UX: HP-UX requires the HSG80 controllers to be configured for SCSI-2 mode. When an HP-UX server is running the SWCC HS-Series Agent:

- If the HP-UX server does not have access to storage units on the storage system, the CCL must be enabled. In this case, the CCL is the only device on the storage system the HP-UX SWCC HS-Series Agent can communicate with. The HP-UX server must also have a host connection with a unit offset of zero; otherwise it cannot access the CCL.
- If the HP-UX server has access to storage units on the storage system, the CCL can be either enabled or disabled. The HP-UX SWCC HS-Series Agent can manage the storage system by communicating with the CCL or by communicating through one of the storage units. If the HP-UX server has a unit offset that is non-zero, it cannot access the CCL; it must communicate through one of the storage units.

3.5 Storage Systems Configuration

1. If necessary, reboot the host servers running the SWCC HS-Series Agents so that they can find the storage systems.

If the SWCC HS-Series Agent will be used to manage storage systems set for SCSI-2 mode and the CCL is disabled, do the following for each of these storage systems:

2. Start a terminal session with the storage system using a serial line connected to the serial port on one storage controller.
3. Rename the host connection for the server running the SWCC HS-Series Agent to a meaningful name. Each host connection is mapped to the host server by the World Wide Name of the host bus adapter.
4. Create one storage unit to be used by the server.
5. Give the server exclusive access to that storage unit. Please refer to Section 4.
6. If necessary, reboot the server so that it can find the storage unit.

If the Windows NT SWCC HS-Series Agent will be used to manage storage systems set for SCSI-2 mode and the CCL is enabled, do the following for each of these storage systems:

7. Start a terminal session with the storage system using a serial line connected to the serial port on one storage controller.
8. Rename the host connection for the server running the SWCC HS-Series Agent to a meaningful name. Each host connection is mapped to the host server by the World Wide Name of the host bus adapter.
9. Set the unit offset for the Windows NT server host connection to a non-zero value; e.g. a unit offset of 10. Please refer to Section 4 for more information about unit offsets.
10. Create one storage unit to be used by the server.
11. Give the server exclusive access to that storage unit. Please refer to Section 4.

The following is done on the Windows NT/98/95 platform that will be used for managing the SAN:

12. Start SWCC.
13. Add the servers that are running the SWCC HS-Series Agents.

3.5.1 Using the SWCC HSG80ACS85 Storage Window

Either the StorageWorks Command Console (SWCC) HSG80ACS85 Storage Window or the SWCC Command Line Interface (CLI) Window can be used to set up the storage systems. The SWCC HSG80ACS85 Storage Window, a graphical storage management tool, is the recommended approach.

The following is done on the Windows NT/98/95 platform for each storage system:

1. Start the SWCC HSG80ACS85 Storage Window for the storage system.

   Tru64 UNIX SWCC HS-Series Agent: The HSG80ACS85 Storage Window is started using the Command Console LUN (CCL) for the storage controller or the storage unit already assigned to the Tru64 UNIX server.

   OpenVMS SWCC HS-Series Agent: The HSG80ACS85 Storage Window is started using the Command Console LUN (CCL) for the storage controller.

   Windows NT SWCC HS-Series Agent:

   - Managing storage systems set for SCSI-2 mode. The HSG80ACS85 Storage Window is started using the storage unit already assigned to the Windows NT server.
   - Managing storage systems set for SCSI-3 mode. The HSG80ACS85 Storage Window is started using the Command Console LUN (CCL) for the storage controller.

   Sun Solaris SWCC HS-Series Agent: The HSG80ACS85 Storage Window is started using the Command Console LUN (CCL) for the storage controller or the storage unit already assigned to the Sun Solaris server.

   HP-UX SWCC HS-Series Agent: The HSG80ACS85 Storage Window is started using the Command Console LUN (CCL) for the storage controller or the storage unit already assigned to the HP-UX server.

2. Rename all host connections to a meaningful name. Each host connection is mapped to the host server by the World Wide Name of its host bus adapter.
3. Set the correct operating system for each host connection.
4. For storage systems using SCSI-2 mode and with the Command Console LUN enabled, set the unit offset of all host connections for Windows NT servers using the storage system to non-zero values; e.g. a unit offset of 10. Please refer to Section 4 for more information about unit offsets.
5. Set the unit offset for each host connection to avoid addressable LUN ranges that conflict.
6. Create each storage unit and give the appropriate servers exclusive access to that storage unit. Please refer to Section 4.
7. For OpenVMS, all Command Console LUNs and storage units are assigned a device identifier. These identifiers must be unique across all storage systems within a single cluster; e.g., a cluster uses two storage systems, only one device (a storage unit or a Command Console LUN) can use the identifier 2. Devices may have the same identifier if they are not used in the same cluster.

3.5.2 Using the SWCC Command Line Interface (CLI) Window

The following is done on the Windows NT/98/95 platform for each storage system:

1. Start the SWCC CLI Window for the storage system.

   Tru64 UNIX SWCC HS-Series Agent: The CLI Window is started using the Command Console LUN (CCL) for the storage controller or the storage unit already assigned to the Tru64 UNIX server.

   OpenVMS SWCC HS-Series Agent: The CLI Window is started using the Command Console LUN (CCL) for the storage controller.

   Windows NT SWCC HS-Series Agent:

   - Managing storage systems set for SCSI-2 mode. The CLI Window is started using the storage unit already assigned to the Windows NT server.
   - Managing storage systems set for SCSI-3 mode. The CLI Window is started using the Command Console LUN (CCL) for the storage controller.

   Sun Solaris SWCC HS-Series Agent: The CLI Window is started using the Command Console LUN (CCL) for the storage controller or the storage unit already assigned to the Sun Solaris server.

   HP-UX SWCC HS-Series Agent: The CLI Window is started using the Command Console LUN (CCL) for the storage controller or the storage unit already assigned to the HP-UX server.

2. Rename all host connections to a meaningful name. Each host connection is mapped to the host server by the World Wide Name of its host bus adapter.
3. Set the correct operating system for each host connection.
4. If the Command Console LUN was not disabled, set the unit offset of all host connections for Windows NT servers using the storage system to non-zero values; e.g. a unit offset of 10. Please refer to Section 4 for more information about unit offsets.

5. Set the unit offset for each host connection to avoid addressable LUN ranges that conflict.
6. Create each storage unit and give the appropriate servers exclusive access to that storage unit. Please refer to Section 4.
7. For OpenVMS, all Command Console LUNs and storage units are assigned a device identifier. These identifiers must be unique across all storage systems within a single cluster; e.g., a cluster uses two storage systems, only one device (a storage unit or a Command Console LUN) can use the identifier 2. Devices may have the same identifier if they are not used in the same cluster.

> **NOTE**
>
> Please consult the *HSG80 Array Controller, ACS Version 8.5, Configuration Guide* and other supporting documentation supplied with your storage system for more information regarding ESA12000 or RA8000 configuration requirements. Please refer to Section 7 for a listing of related documentation.

3.6 Enterprise Backup Solution (EBS) Systems Configuration

1. Please refer to the *Enterprise Backup Solution for Legato NetWorker, Reference Guide* for details on how to configure the EBS systems. Please refer to Section 7 for a listing of related documentation.
2. Connect the EBS system to the Ethernet network according to the network topology map.
3. Connect the EBS system to the SAN according to the SAN topology map.

3.7 Host Server Use of the Storage Systems and EBS Systems

1. For Windows NT servers set up for an NSPOF configuration, install *Compaq Secure Path*.
2. If necessary, reboot the servers so that they can find the storage units and the EBS systems.
3. On each server, configure the storage units and the EBS systems for use.

3.8 Modifying a SAN Configuration

The following procedures detail the steps for changing a SAN configuration:

3.8.1 Changing a Switch Zone Configuration
3.8.2 Changing a QuickLoop Configuration
3.8.3 Adding a Host Server
3.8.4 Removing a Host Server
3.8.5 Adding a Storage System
3.8.6 Removing a Storage System
3.8.7 Adding an Enterprise Backup Solution (EBS) System
3.8.8 Removing an Enterprise Backup Solution (EBS) System
3.8.9 Adding a Fibre Channel Switch
3.8.10 Removing a Fibre Channel Switch

3.8.1 Changing a Switch Zone Configuration

On the Windows NT/98/95 platform that will be used for managing the SAN:

1. Start SWCC.
2. Start the Fabric Window.
3. Select one switch and start its switch web management window.
4. Click on the telnet button to start a telnet session with the switch.
5. Log into the administrator account.

If new host servers or new storage systems are being added to an existing zone configuration, then do the following for each new switch connection:

6. If new connections are being added to an existing zone alias then use the **aliAdd** switch command; e.g., **`aliAdd "ZoneAlias1", "2,5; 2,6"`**.
7. If new connections are being added to a new zone alias then use the **aliCreate** switch command; e.g., **`aliCreate "ZoneAlias2", "2,5; 2,6"`**.
8. If new connections are being added to an existing zone then add the new aliases and / or new connections themselves using the **zoneAdd** switch command; e.g., **`zoneAdd "Zone2", "ZoneAlias2; 2,7"`**.
9. If new connections are being added to a new zone then add the new aliases and / or new connections themselves using the **zoneCreate** switch command; e.g., **`zoneCreate "Zone4", "ZoneAlias2; 2,7"`**.

If host servers or storage systems are being removed from an existing zone configuration, then do the following for each removed connection:

10. If connections are being removed from an existing zone alias then use the **aliRemove** switch command; e.g., **`aliRemove "ZoneAlias1", "2,5; 2,6"`**.
11. If a zone alias is being removed then use the **aliDelete** switch command; e.g., **`aliDelete "ZoneAlias2"`**.
12. If connections are being removed from an existing zone then use the **zoneRemove** switch command; e.g., **`zoneRemove "Zone2", "ZoneAlias2; 2,7"`**.
13. If a zone is being removed then use the **zoneDelete** switch command; e.g., **`zoneDelete "Zone4"`**.

If a zone is being added to a zone configuration, then do the following for each new zone:

14. If a new zone is being added to an existing zone configuration then add the new zone using the **cfgAdd** switch command; e.g., **`cfgAdd "ZoneCfg", "Zone4"`**.
15. If a new zone is being added to a new zone configuration then add the new zone using the **cfgCreate** switch command; e.g., **`cfgCreate "ZoneCfg2", "Zone4"`**.

If zones are being removed from a zone configuration, then do the following for each removed zone:

16. Use the **cfgRemove** switch command; e.g., **`cfgRemove "ZoneCfg", "Zone4"`**.

If zone configurations are being removed, then do the following for each removed zone configuration:

17. If the zone configuration to be removed is currently enabled and another zone configuration is being enabled in its place, then use the **cfgEnable** switch command with the other zone configuration; e.g., **`cfgEnable "ZoneCfg3"`**. This will disable the current configuration and simultaneously enable the other configuration.
18. If the zone configuration to be removed is currently enabled, other zone configurations exist that will not be removed, but they are not being enabled, then first use the **cfgDisable** switch command with the other zone configuration; e.g., **`cfgDisable "ZoneCfg3"`**. Next use the **cfgDelete** switch command with the zone configuration; e.g., **`cfgDelete "ZoneCfg2"`**.

To enable and save a new or changed zone configuration do the following:

19. Use the **cfgEnable** switch command; e.g., **`cfgEnable "ZoneCfg3"`**. This command disables the currently enabled zone configuration and simultaneously enables the zone configuration identified in the command.
20. Use the **cfgSave** switch command. This command saves the zone configuration changes into the switch's flash memory.

If all zone configurations are being removed, then do the following:

21. Use the **cfgClear** switch command. This command disables the currently enabled zone configuration, deletes all zone configuration information and erases the switch's flash memory of all zoning information.

NOTE

- The zone configuration changes will automatically propagate from this switch to the other switches.
- SWCC has a major impact on how zoning is used. Please refer to Section 3.5 for details.
- Please refer to Section 6 for more information regarding switch zoning.
- Please refer to Section 6.4 for information on configurations that ***require*** zoning.

NOTE

Please consult the *SAN Switch Fabric Operating System Management Guide* and other supporting documentation supplied with your Fibre Channel SAN switch for more information regarding switch configuration requirements. Please refer to Section 7 for a listing of related documentation.

3.8.2 Changing a QuickLoop Configuration

1. On the Windows NT/98/95 platform that will be used for managing the SAN, start a telnet session with the switch. Log into the administrator account.
2. Start SWCC.
3. Start the Fabric Window.

The following is done for each switch being changed in the QuickLoop:

4. Select the switch and start its switch web management window.
5. Click on the telnet button to start a telnet session with the switch.
6. Log into the administrator account.

If switch ports are being added to a QuickLoop configuration, then do the following for each switch port:

7. Use the **qlPortEnable** switch command; e.g., **`qlPortEnable 5`**.

If switch ports are being removed from a QuickLoop configuration, then do the following for each switch port:

8. Use the **qlPortDisable** switch command; e.g., **`qlPortDisable 5`**.

If all switch ports are being added to a QuickLoop configuration, then do the following:

9. Use the **qlEnable** switch command. This command enables QuickLoop for all ports on the switch.

If all switch ports are being removed from a QuickLoop configuration, then do the following:

10. Use the **qlDisable** switch command. This command disables QuickLoop for all ports on the switch.

If a switch is being partnered with another switch in a QuickLoop configuration, then do the following:

11. Use the **qlPartner** switch command; e.g., **`qlPartner "10:00:00:60:44:4d:83:02"`**. This command identifies the switch with the WWN 10000 0060 444d 8302 is the QuickLoop partner for this switch.

If a switch has a QuickLoop partner and the partnership is being removed, then do the following:

12. Use the **qlPartner** switch command; e.g., **`qlPartner 0`**. This command indicates the switch will no longer have a QuickLoop partner.

NOTE

- If switch zoning is being used, update the zoning configuration to accurately reflect the QuickLoop changes. Please refer to Section 6.4 for more information on configurations that ***require*** zoning.
- Please refer to Section 5 for more information regarding QuickLoop.
- Please consult the *SAN Switch Fabric Operating System Management Guide* and other supporting documentation supplied with your Fibre Channel SAN switch for more information regarding switch configuration requirements. Please refer to Section 7 for a listing of related documentation.

3.8.3 Adding a Host Server

Follow the set up procedure given in Sections 3.1 through 3.7 with the following changes.

Before connecting the server to the SAN:

1. Update the SAN topology map and the network topology map.
2. If switch zoning is being used then add the server's switch connections to the appropriate zones. Please refer to Section 6.4 for information on configurations that ***require*** zoning.
3. If the server will participate in a QuickLoop, enable QuickLoop for the switch ports it connects with.
4. Install Fibre Channel support on the server.
5. Install the *RA8000/ESA12000 FC Solution Software Kit*.
6. Install the *StorageWorks Command Console HS-Series Agent*. Configure the Agent to include as a client the Windows NT/98/95 platform that will be used for managing the SAN.
7. Stop the SWCC HS-Series Agent if this server is indicated on the SAN topology map to be a substitute for the SWCC HS-Series Agent server. Only the primary servers may have the SWCC HS-Series Agent running.
8. Optionally for Windows NT, install the *StorageWorks Command Console Fibre Channel Switch Agent*. Configure the Agent to include as a client the Windows NT/98/95 platform.
9. Stop the SWCC Fibre Channel Switch Agent if this platform is indicated on the SAN topology map to be a substitute for the SWCC Fibre Channel Switch Agent. Only the primary platform may have the SWCC Fibre Channel Switch Agent running.

Connect the server to the SAN:

10. Connect the server to the Ethernet network according to the network topology map.
11. Connect the server to the SAN according to the SAN topology map.
12. Create and assign storage units on all storage systems the server will be accessing.
13. Make any changes necessary to the EBS systems for the addition of this server.
14. For Windows NT servers set up for an NSPOF configuration, install *Compaq Secure Path*.
15. If necessary, reboot the server so that it can find the storage units and the EBS systems.

NOTE

Please consult the *RA8000/ESA12000 HSG80 Solution Software V8.5, Installation Reference Guide* for the host server's operating system, the operating system specific application notes and other supporting documentation supplied with your storage system for more information regarding host server configuration requirements, including operating system version. Please refer to Section 7 for a listing of related documentation.

3.8.4 Removing a Host Server

1. Shutdown and power off the server.
2. Disconnect the server from the SAN.
3. Remove its access to all storage units. Optionally, delete the storage units.
4. Make any changes necessary to the EBS systems for the removal of this server.
5. If the server was participating in a QuickLoop, disable QuickLoop for its switch ports.
6. If switch zoning is being used, remove its switch ports from the zones.
7. Update the SAN topology map and the network topology map.

3.8.5 Adding a Storage System

Follow the set up procedure given in Sections 3.1 and 3.7 with the following changes.

Before connecting the storage system to the SAN:

1. Update the SAN topology map.
2. If switch zoning is being used then add the storage system's switch connections to the appropriate zones. Please refer to Section 6.4 for information on configurations that ***require*** zoning.
3. If the storage system will participate in a QuickLoop, enable QuickLoop for the switch ports it connects with.

Connect the storage system to the SAN:

4. Connect the storage system to the SAN according to the SAN topology map.
5. Create storage units for all servers that will be accessing the storage system. When each storage unit is created disable access for all servers. Then assign access to the specific host connections.
6. Make any changes necessary to the EBS systems for the addition of this storage system.
7. If necessary, reboot the servers so that they can find the new storage units.

NOTE
Please consult the *HSG80 Array Controller, ACS Version 8.5, Configuration Guide* and other supporting documentation supplied with your storage system for more information regarding ESA12000 or RA8000 configuration requirements. Please refer to Section 7 for a listing of related documentation.

3.8.6 Removing a Storage System

1. Stop all server I/O to the storage system.
2. On all servers accessing the storage units on the storage system, remove the storage units.
3. Make any changes necessary to the EBS systems for the removal of this storage system.
4. Disconnect the storage system from the SAN.
5. Delete all storage units and all host connections.
6. Shutdown and power off the storage system.
7. If the storage system was participating in a QuickLoop, disable QuickLoop for its switch ports.
8. If switch zoning is being used, remove its switch ports from the zones.
9. Update the SAN topology map.

3.8.7 Adding an Enterprise Backup Solution (EBS) System

Follow the set up procedure given in Sections 3.1 and 3.7 with the following changes.

Before connecting the EBS system to the SAN:

1. Update the SAN topology map and the network topology map.
2. If switch zoning is being used then add the EBS system's switch connections to the appropriate zones. Please refer to Section 6.4 for information on configurations that ***require*** zoning.
3. Please refer to the *Enterprise Backup Solution for Legato NetWorker, Reference Guide* for details on how to configure the EBS systems. Please refer to Section 7 for a listing of related documentation.
4. Connect the EBS system to the Ethernet network according to the network topology map.

Connect the EBS system to the SAN:

5. Connect the EBS system to the SAN according to the SAN topology map.
6. If necessary, reboot the servers so that they can find the new EBS system.

3.8.8 Removing an Enterprise Backup Solution (EBS) System

1. Stop all server I/O to the EBS system.
2. Please refer to the *Enterprise Backup Solution for Legato NetWorker, Reference Guide* for details on how to remove the EBS systems. Please refer to Section 7 for a listing of related documentation.
3. Disconnect the EBS system from the SAN.
4. Shutdown and power off the EBS system.
5. If switch zoning is being used, remove its switch ports from the zones.
6. Update the SAN topology map and the network topology map.

3.8.9 Adding a Fibre Channel Switch

Follow the set up procedure given in Sections 3.1 and 3.7 with the following changes.

Before connecting the Fibre Channel switch to the SAN:

1. Update the SAN topology map and the network topology map.
2. Perform the initial switch set up procedure given in Section 3.3.
3. Make any necessary zoning changes and QuickLoop changes in the SAN. Please refer to Section 6.4 for information on configurations that ***require*** zoning.

Connect the Fibre Channel switch to the SAN:

4. Connect the switch to the SAN.
5. Make any necessary QuickLoop changes to the switch.

NOTE

Please consult the *SAN Switch Fabric Operating System Management Guide* and other supporting documentation supplied with your Fibre Channel SAN switch for more information regarding switch configuration requirements. Please refer to Section 7 for a listing of related documentation.

3.8.10 Removing a Fibre Channel Switch

3. Stop all I/O to all devices attached to the switch.
4. Remove the servers, storage systems and EBS systems from the switch.
5. Power off the switch.
6. Disconnect it from the SAN.
7. Make any necessary zoning changes and QuickLoop changes in the SAN.
8. Update the SAN topology map and the network topology map.

4.0 Selective Storage Presentation (SSP)

Server access control for storage systems in the SAN is provided by the HSG80 controller's selective storage presentation feature. Each storage unit in an ESA12000 FC or RA8000 FC can be selectively presented to specific host servers. This provides each host server or set of host servers with exclusive access to their own data. Selective storage presentation is accomplished by specifying for each storage unit a list of host connections allowed access and by using unit offsets.

4.1 List of Host Connections Allowed Access

A host connection is created when a host bus adapter on the Fibre Channel fabric connects to an HSG80 controller. Each storage system assigns host connection names (e.g., !NEWCON01) to each host bus adapter. These host connection names can be changed to more meaningful names; e.g., SERVER1. The host connections must be set for the correct operating system.

Each storage unit has a list of host connections that are allowed access to it. By default, a storage unit allows access by all host connections. Selective storage presentation occurs by listing a subset of host connections allowed access.

For example, in a configuration there is a storage unit, D24, and three host connections, SERVER1, SERVER2 and SERVER3. If SERVER1 is the only host connection name on the D24's list of host connections allowed access, then D24 is presented only to SERVER1. If SERVER2 is added to D24's list, then D24 is presented to both SERVER1 and SERVER2, but not to SERVER3.

If the storage systems have an active Host Port 1 and an active Host Port 2 connected to the same fabric then each host port will create its own host connection for the same host bus adapter. In other words, each host bus adapter will have associated with it two different host connection names, one assigned by Host Port 1 and the other by Host Port 2. This feature requires careful management of the selective storage presentation. The correct host connection to use is dependent on the storage unit's name and the HSG80 controller's default selective storage presentation feature (described in Unit Offsets below).

4.2 Unit Offsets

The Compaq StorageWorks Fibre Channel storage systems use the SCSI protocol. In multiple bus failover mode, each HSG80 controller host port is mapped to a target SCSI ID. In transparent failover mode, Host Port 1 of both controllers are mapped to one target SCSI ID and Host Port 2 of both controllers are mapped to a second target SCSI ID.

A host server uses these SCSI IDs to address the controllers and uses Logical Unit Numbers (LUNs) to identify the storage units presented by the HSG80 controller. For example, a host server addresses a storage unit using SCSI ID 5, LUN 4. The SCSI ID 5 identifies which HSG80 controller host port is the target of the SCSI message and LUN 4 identifies the storage unit presented by that HSG80 controller host port. The range of LUNs a host server can address is determined by the capability of the host bus adapter it uses.

Unit offsets are a base for addressing storage unit names. The HSG80 controller uses unit offsets to allow multiple host servers to be able to address different storage units using the same SCSI ID and LUN combination. This allows the host servers to be able to use the full range of LUNs their host bus adapters can address without conflicting with another host server's range of addressable LUNs.

Each host connection is assigned a unit offset. In transparent failover mode the HSG80 controller by default assigns a unit offset of 0 (zero) to host connections on Host Port 1 and 100 to host connections on Host Port 2. In multiple bus failover mode the HSG80 controller by default assigns a unit offset of 0 (zero) to host connections on both Host Port 1 and Host Port 2.

Subtracting the host connection's unit offset from the name of the storage unit that is being accessed gives the LUN the server is addressing:

storage unit name – unit offset = server LUN

For example, a host connection, SERVER1, has a unit offset of 100 and it addresses a storage unit by using LUN 3. Subtracting SERVER1's unit offset, 100, from the storage unit name D103 gives LUN 3:

D103 – unit offset 100 = server LUN 3

D103 is seen by SERVER1 as LUN 3.

If multiple host connections have the same unit offset, they all can address the same storage unit using the same LUN. For non-clustered host servers, the range of addressable LUNs is in conflict; they all can address the same storage units and can corrupt each others data. Assigning a different unit offset to a host connection shifts its range of addressable LUNs to a different set of storage units. This prevents the LUN range conflict.

For example, a host connection, SERVER1, and a second host connection, SERVER2, each represents a host bus adapter in two different host servers. Both adapters can only address LUN 0 through LUN 7. SERVER1 is given a unit offset of 20 and SERVER2 is given a unit offset of 10. There exists a storage unit named D24. It is addressable by SERVER1, but not by SERVER2.

D24 is presented to SERVER1 as LUN 4:

D24 – unit offset 20 = LUN 4

D24 is "presented" to SERVER2 as LUN 14, outside the host adapter's addressable range:

D24 – unit offset 10 = LUN 14

The different unit offsets prevent SERVER1 and SERVER2 from having a LUN range conflict.

In the case where D24 needs to be addressable by both SERVER1 and SERVER2 as LUN 4 both host connections must have a unit offset of 20. An example application would be where SERVER1 and SERVER2 are host connections to two host servers in a cluster and both servers must access D24.

The LUN addressing capability of the host bus adapter determines what storage units it can address. For example, if the host bus adapter is only capable of addressing LUN 0 through LUN 7 and its host connection has a unit offset of 50, then only storage units D50 through D57 are addressable.

For ease of understanding the mapping of LUNs to storage unit names, it is recommended that unit offsets be a multiple of 10. Thus, the LUN number matches the last digit of the storage unit name. As in the example above, using a host connection with a unit offset of 20, LUN 4 maps to the storage unit name D24; both the LUN number and the storage unit name have a last digit of 4.

Multiple Bus Failover: For HSG80 controllers configured for multiple bus failover mode, both Host Port 1 and Host Port 2 on both controllers present storage units D0 through D199.

Transparent Failover: HSG80 controllers configured for transparent failover mode have an additional selective storage presentation feature. Host Port 1 only presents storage units D0 through D99 and Host Port 2 only presents storage units D100 through D199.

NOTE

Care must be used in the management of the lists of host connections allowed access and unit offsets.

Host connections: A server can be prevented from accessing its storage units if the correct host connection is left out of the list of host connections allowed access. For example, SERVER1 has two host connections, one for Host Port 1 and one for Host Port 2. On a storage system configured for transparent failover mode, the host connection for Host Port 1 is the connection required to access D24. If the host connection for Host Port 2 is inadvertently put in the list instead, SERVER1 will not be able to access D24.

Unit offsets: A server can be prevented from being able to address its storage units if the incorrect unit offsets are used. For example, SERVER1 is supposed to access D24. Its host connection has a unit offset of 30. This puts D24 outside of SERVER1's addressable LUNs.

NOTE

Please consult the *HSG80 ACS Version 8.5, Configuration Guide* and other supporting documentation supplied with your storage system for more information regarding Selective Storage Presentation. Please refer to Section 7 for a listing of related documentation.

4.3 Configuring Server Access Control for Standalone Servers

To selectively present a storage unit to a single host server, one or both of the following can be used:

- The list of host connections allowed access contains only the host connection name for the standalone host server
- The host connection is given a unique unit offset that puts the storage unit inside the range of LUNs addressable only by the standalone host server

4.4 Configuring Server Access Control for a Cluster

To selectively present a storage unit to the host servers in a cluster, one or both of the following can be used:

- The list of host connections allowed access contains only the host connection names for the host servers in the cluster
- The host connections for the cluster servers are given the same unique unit offset that puts the storage unit inside the range of LUNs addressable only by the cluster servers

5.0 QuickLoop on Fibre Channel Switches

Compaq Fibre Channel switches provide an Arbitrated Loop connectivity feature called QuickLoop. It provides the ability to connect Arbitrated Loop devices to the switch. QuickLoop is used in Private Loop mode only.

Each QuickLoop consists of fabric loop devices connected to specified switch ports on one switch or two switches partnered together. The partnered switches may have intermediate switches between them that do not directly participate in the QuickLoop.

In a configuration where a SAN has both fabric and loop devices connected to it, the switches provide a translative mode which assigns a public loop address to fabric devices communicating with loop devices in the QuickLoop. The fabric devices can access the loop devices in the QuickLoop, but not vice versa.

The maximum number of switches per QuickLoop is two switches. The maximum number of QuickLoops per switch is one QuickLoop.

In a SAN where multiple QuickLoops exist, devices in different QuickLoops cannot communicate with each other.

QuickLoop is supported only on the following models of Fibre Channel switches:

- Compaq 16 port Fibre Channel SAN Switch, part # 158223-B21
- Compaq 8 port Fibre Channel SAN Switch, part # 158222-B21

NOTE

Currently, Fibre Channel hubs are not supported connected to a QuickLoop. Please consult the *SAN Switch QuickLoop Management Guide* and other supporting documentation supplied with your Fibre Channel SAN switch for more information regarding QuickLoop. Please refer to Section 7 for a listing of related documentation.

5.1 QuickLoop Commands

QuickLoop is enabled on a Fibre Channel switch through commands entered in a telnet session logged into a switch account with administrative privileges. If two Fibre Channel switches are partnered in one QuickLoop each switch is configured separately.

QuickLoops are managed with the following commands:

qlEnable, qlDisable
: These are used for configuring an entire switch for QuickLoop.

qlPortEnable, qlPortDisable
: These are used for configuring individual switch ports for QuickLoop.

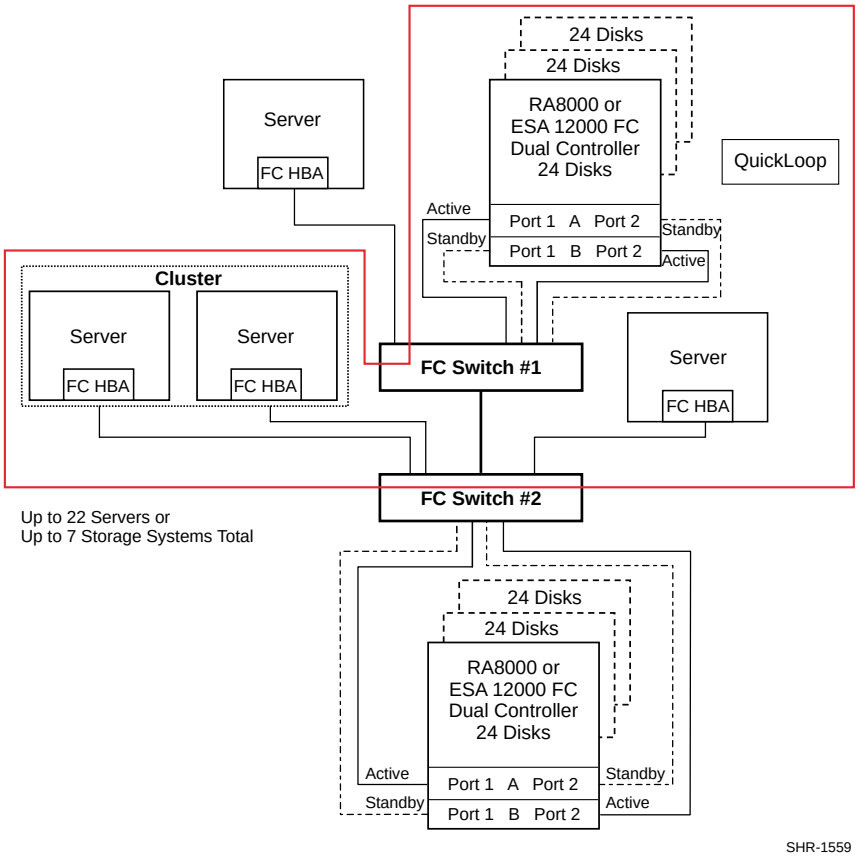
qlPartner
: This is used for partnering two switches into one QuickLoop.

qlShow, qlHelp
: These are used for the management of QuickLoops.

5.2 QuickLoop Example

This example shows how to set up a QuickLoop on two switches.

Figure 8 QuickLoop Example



In Figure 8:

- FC Switch #1 and FC Switch #2 are partnered in a QuickLoop.
- The cluster, the standalone server on the right, and the top storage system are in the QuickLoop.
- The top standalone server and the bottom storage system are outside of the QuickLoop.

- The top standalone server is connected to Port 0 of FC Switch #1.
- The top storage system is connected to FC Switch #1.
  - Host Port 1 of the top controller is connected to Switch Port 4.
  - Host Port 1 of the bottom controller is connected to Switch Port 5.
  - Host Port 2 of the top controller is connected to Switch Port 6.
  - Host Port 2 of the bottom controller is connected to Switch Port 7.
- The cluster is connected to Port 0 and Port 1 of FC Switch #2.
- The standalone server on the right is connected to Port 2 of FC Switch #2.
- The bottom storage system is connected to FC Switch #2.
  - Host Port 1 of the top controller is connected to Switch Port 4.
  - Host Port 1 of the bottom controller is connected to Switch Port 5.
  - Host Port 2 of the top controller is connected to Switch Port 6.
  - Host Port 2 of the bottom controller is connected to Switch Port 7.
- Port 3 of FC Switch # 1 is connected to Port 3 of FC Switch #2.
- FC Switch #1 has a World Wide Name of **`1000 0060 a706 9c4e`**
- FC Switch #2 has a World Wide Name of **`1000 0060 444d 8302`**

The following telnet session log shows the switch commands used to set up the QuickLoop on FC Switch #1 in this example. The user input is in **bold** and explanations are in boxes :

```
switch1:admin> qlPortEnable 4
Setting port 4 to QuickLoop mode,
Committing configuration...done.
Activate looplet 4
switch1:admin> qlPortEnable 5
Setting port 5 to QuickLoop mode,
Committing configuration...done.
Activate looplet 5
switch1:admin> qlPortEnable 6
Setting port 6 to QuickLoop mode,
Committing configuration...done.
Activate looplet 6
switch1:admin> qlPortEnable 7
Setting port 7 to QuickLoop mode,
Committing configuration...done.
Activate looplet 7
```

These enable QuickLoop for Ports 4, 5, 6 and 7 on the switch, for the top storage system.

```
switch1:admin> qlPartner "10:00:00:60:44:4d:83:02"
Setting QuickLoop to dual-switch mode,
Committing configuration...done.
```

This indicates the switch with the WWN 1000 0060 444d 8302 (FC Switch #2) is to be the QuickLoop partner for this switch (FC Switch #1).

The following telnet session log shows the switch commands used to set up the QuickLoop on FC Switch #2:

```
switch2:admin> qlPortEnable 0
Setting port 0 to QuickLoop mode,
Committing configuration...done.
Activate looplet 0
switch2:admin> qlPortEnable 1
Setting port 1 to QuickLoop mode,
Committing configuration...done.
Activate looplet 1
```

These enable QuickLoop for Port 0 and 1 on the switch, for the cluster.

```
switch2:admin> qlPortEnable 2
Setting port 2 to QuickLoop mode,
Committing configuration...done.
Activate looplet 2
```

This enables QuickLoop for Port 2 on the switch, for the standalone server on the right.

```
switch2:admin> qlPartner "10:00:00:60:a7:06:9c:4e"
Setting QuickLoop to dual-switch mode,
Committing configuration...done.
```

This indicates the switch that has the WWN 1000 0060 a706 9c4e (FC Switch #1) is to be the QuickLoop partner for this switch (FC Switch #2).

The following telnet session log shows the QuickLoop configuration on FC Switch #1:

```
switch1:admin> qlShow
Self:    10:00:00:60:a7:06:9c:4e domain 1
Peer:    10:00:00:60:44:4d:83:02 domain 2
State:   Master
Scope:   dual
AL_PA bitmap:    03000000 00000011 00000000 00000000
```

```
Remote AL_PAs
    [021000]:    04
    [021100]:    08
    [021200]:    10
Local AL_PAs
    [011400]:    71
    [011700]:    72
Local looplet states
    Member:     4 5 6 7
    Online:     4 - - 7
    Looplet 4:  online
    Looplet 5:  offline
    Looplet 6:  offline
    Looplet 7:  online
```

This shows the QuickLoop configuration for the switch FC Switch #1.

The following telnet session log shows the QuickLoop configuration on FC Switch #2:

```
switch2:admin> qlShow
Self:    10:00:00:60:44:4d:83:02 domain 2
Peer:    10:00:00:60:a7:06:9c:4e domain 1
State:   Non-Master
Scope:   dual
AL_PA bitmap:    03000000 00000011 00000000 00000000
Remote AL_PAs
    [011400]:    71
    [011700]:    72
Local AL_PAs
    [021000]:    04
    [021100]:    08
    [021200]:    10
Local looplet states
    Member:     0 1 2
    Online:     0 1 2
    Looplet 0:  online
    Looplet 1:  online
    Looplet 2:  online
```

This shows the QuickLoop configuration for the switch FC Switch #2.

The QuickLoop allows the top standalone server to access both the top and bottom storage systems. The cluster and the standalone server on the right can only access the top storage controller.

NOTE

- If switch zoning is being used, update the zoning configuration to accurately reflect the QuickLoop changes. Please refer to Section 6.4 for more information on configurations that ***require*** zoning.
- Please consult the *SAN Switch QuickLoop Management Guide* and other supporting documentation supplied with your Fibre Channel SAN switch for more information regarding QuickLoop. Please refer to Section 7 for a listing of related documentation.

5.3 Heterogeneous Operating Systems Support

Supported operating systems in a QuickLoop:

- HP-UX running on private loop attached servers

Supported operating systems, connected as Fabric devices, accessing a QuickLoop using the translative mode:

- Compaq Tru64 UNIX, Windows NT (Intel) and Sun Solaris running on fabric attached servers

6.0 Switch Zoning

Compaq Fibre Channel switches provide a fabric management feature called switch zoning. It provides the ability to split the fabric into zones; each zone is essentially a virtual fabric. Although it is typically not required in a heterogeneous SAN, switch zoning adds an additional level of information management and data security when used in addition to the Selective Storage Presentation feature of the HSG80 controllers.

Access to one node (Fibre Channel device) is limited to the other nodes that are in the same zone. Any node outside of the zone is unaware of the existence of the nodes inside the zone. Zones can be distinct or they can overlap. If a node is defined to be in the overlap of multiple zones, it is aware of the nodes in all of those zones and all of the nodes in all of those zones are aware of it.

6.1 Using Selective Storage Presentation (SSP) and Switch Zoning Together

Switch zoning and SSP complement each other; they do not replace each other. Switch zoning controls communication access. SSP controls data access.

SSP controls which servers will have access to each storage unit. It does not control which servers can communicate with each storage controller host port, nor does it control which servers can communicate with each other.

Switch zoning controls which servers can communicate with each other and which servers can communicate with each storage controller host port. It does not control what storage units presented at a host port a server can access.

Switch zoning controls access at the storage system level. SSP controls access at the storage unit level. Switch zoning is a higher-level access control than SSP.

6.2 Switch Zoning Commands

Switch zoning is enabled on the SAN through commands entered in a telnet session logged into one switch using a switch account with administrative privileges.

A zone configuration is a list of one or more zones that are enabled together. A zone is a list of one or more zone members. A zone member is any of the following:

- Physical port number
  The physical port number is identified by the switch ID and the port number; e.g., **`1,5`**, where **`1`** is the switch with a domain ID of 1 and **`5`** is port 5 on that switch.
- Node World Wide Name
  The node World Wide Name is the 16 digit hexadecimal identifier of a Fibre Channel device; e.g., **`50:00:00:20:3c:76:df:00`**
- Port World Wide Name
  The port World Wide Name is the 16 digit hexadecimal identifier of a single port on a multi-port Fibre Channel device; e.g., **`50:00:00:20:3c:76:df:01`**
- Zone alias
  A zone alias identifies one or more zone members by a single C-style name; e.g., **`group1`**, which is the name of a list of zone members. A zone alias cannot have a zone alias as one of its zone members.

Compaq Fibre Channel switches allow multiple zone configurations to be defined, of which only one is enabled at a time. Each zone configuration will have multiple zones.

Zone configurations and zones are managed with the following commands:

zoneCreate, zoneDelete, zoneAdd, zoneRemove, zoneShow

These are used for the management of zones.

aliCreate, aliDelete, aliAdd, aliRemove, aliShow

These are used for the management of zone aliases.

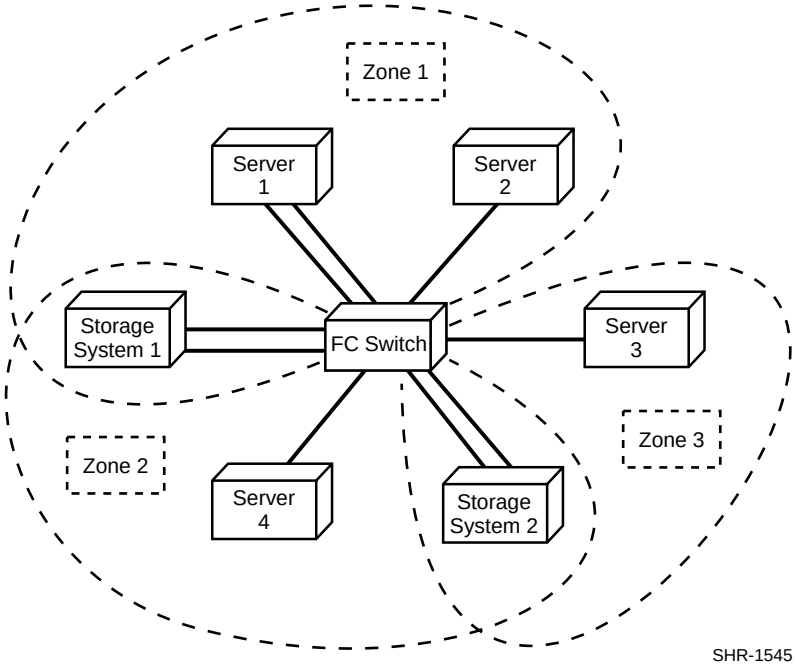
cfgCreate, cfgDelete, cfgAdd, cfgRemove, cfgShow, cfgEnable, cfgDisable, cfgSave, cfgClear

These are used for the management of zone configurations.

6.3 Switch Zoning Example

This example shows how to set up the switch zoning on a switch.

Figure 9 Switch Zoning Example



In Figure 9:

- The FC Switch has a Domain ID of 1.
- Storage System 1 has a Node World Wide Name of: **`5000 0020 3c76 df00`**
  - Host Port 1 is connected to Switch Port 0.
  - Host Port 2 has a Port World Wide Name of: **`5000 0020 3c76 df02`** and is connected to Switch Port 1.
- Storage System 2:
  - Host Port 1 is connected to Switch Port 6
  - Host Port 2 is connected to Switch Port 7
- Server 1 has a Node World Wide Name of: **`1000 0020 3c76 ba05`** and is connected to Switch Port 2.
- Server 2 is connected to Switch Port 3.
- Server 3 is connected to Switch Port 4.
- Server 4 is connected to Switch Port 5.
- Zone 1 consists of Server 1, Server 2 and Storage System 1
- Zone 2 consists of Server 3 and Storage System 2
- Zone 3 consists of Server 4, Storage System 1 and Storage System 2
- Zone Alias 1 identifies a list consisting of Server 1 and Server 2

The following telnet session log shows the switch commands used to set up the zones in this example. The user input is in **bold** and explanations are in boxes :

```
switch:admin> aliCreate "ZoneAlias1", "10:00:00:20:3c:76:ba:05; 1,3"
```

This creates a zone alias `ZoneAlias1` that uses a node World Wide Name zone member for Server 1 and a physical port number zone member for Server 2. The physical port number **`1,3`** identifies Port 3 on the switch with Domain ID 1.

```
switch:admin> zoneCreate "Zone1", "ZoneAlias1; 1,0; 50:00:00:20:3c:76:df:02"
```

This creates a zone `Zone1` that uses the zone alias `ZoneAlias1` zone member for Server 1 and Server 2, a physical port number zone member for Storage System 1's Host Port 1 and a port World Wide Name zone member for Storage System 1's Host Port 2.

```
switch:admin> zoneCreate "Zone2", "1,4; 1,6; 1,7"
```

This creates a zone `Zone2` that uses physical port number zone members for Server 3, Storage System 2's Host Port 1 and Storage System 2's Host Port 2.

```
switch:admin> zoneCreate "Zone3", "1,5; 1,0; 1,1; 1,6; 1,7"
```

This creates a zone `Zone3` that uses physical port number zone members for Server 4, Storage System 1's Host Port 1, Storage System 1's Host Port 2, Storage System 2's Host Port 1 and Storage System 2's Host Port 2.

```
switch:admin> cfgCreate "ZoneCfg", "Zone1; Zone2; Zone3"
```

This creates a zone configuration `ZoneCfg` that consists of the zones `Zone1`, `Zone2` and `Zone3`.

```
switch:admin> cfgEnable "ZoneCfg"
zone config "ZoneCfg" is in effect
```

This enables the zone configuration `ZoneCfg`.

```
switch:admin> cfgShow
Defined configuration:
 cfg:   ZoneCfg Zone1; Zone2; Zone3
 zone:  Zone1   ZoneAlias1; 1,0; 50:00:00:20:3c:76:df:02
 zone:  Zone2   1,4; 1,6; 1,7
 zone:  Zone3   1,5; 1,0; 1,1; 1,6; 1,7
 alias: ZoneAlias1
                10:00:00:20:3c:76:ba:05; 1,3

Effective configuration:
 cfg:   ZoneCfg
 zone:  Zone1
```

```
                ZoneAlias1
                1,0
                50:00:00:20:3c:76:df:02
 zone:  Zone2
                1,4
                1,6
                1,7
 zone:  Zone3
                1,5
                1,0
                1,1
                1,6
                1,7
 alias: ZoneAlias1
                10:00:00:20:3c:76:ba:05
                1,3
```

This displays all zone configurations that have been defined and the one zone configuration that has been enabled on the switch. In this example, there is only one zone configuration defined.

```
switch:admin> cfgSave
Updating flash ...
```

This saves all defined zone configurations into the switch's flash memory. When the switch power is turned on, the switch will automatically reload the saved zone configurations and the enabled zone configuration will be automatically reinstated. Without this command, the zoning information will be lost when the switch power is turned off.

6.4 Configurations Requiring Zoning

Zoning is required in only six situations, but it is not limited to just these situations. The configurations requiring zoning are:

1. Using a SAN configuration where Windows NT is using Secure Path and all four controller host ports of the storage system are connected to the SAN.

   In NSPOF configurations, Windows NT servers must use Compaq Secure Path V2.2. Secure Path uses a pair of physically separate fabrics or a pair of zones to provide the data path redundancy.

   For each Windows NT server, Secure Path only supports connecting to two active host ports on a storage system. Only Host Port 1 of both controllers are connected to the pair of zones or pair of fabrics; each to a separate zone or fabric. Host Port 2 of both controllers cannot be connected to the same pair of zones or pair of fabrics. Host Port 2 of both controllers can be used if they are in a second pair of zones, or are connected to a second pair of redundant fabrics, and they are used by a different set of Windows NT servers running Secure Path.

2. Using a SAN configuration where more than 64 host connections can be made with an ESA12000 / RA8000.

   A host connection is a data path from one host bus adapter to one active controller host port, regardless of whether or not the host connection uses storage units on that storage system. The ESA12000 / RA8000 has a limit of 64 host connections being made. When a 65th connection is attempted, the connection name capacity of the HSG80 controllers will be exceeded which could result in a controller fatal error.

   In transparent failover mode two host ports are active. One host server with one host bus adapter has two data paths, one to each active controller host port. This allows up to 32 servers to have data paths to the HSG80 controllers. In multiple bus failover mode, four host ports are active. One server with two host bus adapters, as in a NSPOF configuration, has eight data paths, four for each host bus adapter. This allows up to 8 servers to have data paths to the HSG80 controllers.

   Switch zoning is used to prevent more than 64 host connections from being made to a single storage system. Thus allowing more servers to be attached to the SAN to use other storage systems.

3. Using a SAN configuration where a host bus adapter (HBA) can communicate with more active storage controller host ports than it has targets for.

   Every storage controller host port on the SAN is a separate target for the HBA. If there are more host ports than it has targets for, it is possible the storage it needs to access will not be given a target by the HBA. For example, a server's HBA can have a maximum of 16 targets. On the SAN there are 3 storage systems configured for transparent failover mode and 2 storage systems configured for multiple bus failover mode. Each of the storage systems configured for transparent failover mode has two active host ports. Each of the storage systems configured for multiple bus failover mode has four active host ports. There are 20 active host ports in the SAN. Four of the host ports cannot be given a target by the HBA.

   Switch zoning is used to prevent the HBA from seeing active host ports that it will not be using. This allows the host ports it will be using to be given targets.

4. Using multiple Tru64 UNIX clusters in a SAN.

   Tru64 UNIX communicates on the SAN in both initiator and target mode. When a Tru64 UNIX server configured for clustering boots, it queries the SAN for all targets it can communicate with. When another Tru64 UNIX server configured for clustering responds, both servers consider each other to be members of the same cluster, when they may actually be in different clusters. Switch zoning is used to avoid this confusion by placing each Tru64 UNIX cluster in separate zones.

5. Using QuickLoop in a SAN where an OpenVMS server is also being used.

   When an OpenVMS server is booted and connected to the SAN, with or without I/O activity, an ESA12000 / RA8000 booting into a QuickLoop will fail to connect to the QuickLoop. It repeatedly attempts to connect without success. Switch zoning is used to isolate the QuickLoop from the OpenVMS server, thus allowing the ESA12000 / RA8000 to successfully connect to the QuickLoop.

6. Using an OpenVMS 7.2 server in a SAN where a Tru64 UNIX server is also being used.

   OpenVMS V7.2 encounters a problem during boot if it finds Compaq Tru64 UNIX V4.0F on the same fabric. As part of the boot process OpenVMS probes the fabric for all devices it can communicate with. A response from a Tru64 UNIX server is handled incorrectly. OpenVMS stops probing for additional devices. This can result in storage units not being found. Switch zoning is used to prevent the OpenVMS and Tru64 UNIX servers from interacting, thus allowing OpenVMS to boot correctly.

   This problem has been fixed starting in Compaq OpenVMS 7.2-1. Zoning is not required with Tru64 UNIX on the same fabric as OpenVMS 7.2-1 or newer.

   NOTE

   Please consult the *SAN Switch Zoning Reference Guide* and other supporting documentation supplied with your Fibre Channel SAN switch for more information regarding switch zoning. Please refer to Section 7 for a listing of related documentation.

7.0 Reference Material

Table 5 lists the documents to reference for further information on the configuration of the Heterogeneous Storage Area Network.

Table 5 Related Configuration Documentation

Topic	Document Title	Order Number
Tru64 UNIX	*RA8000/ESA12000 HSG80 Solution Software V8.5 for Compaq Tru64 UNIX, Installation Reference Guide*	*387389-002 AA-RFAUB-TE*
Tru64 UNIX	*Tru54 UNIX Fibre Channel Switch Application Note*	*EK-SMA33-AN*
OpenVMS	*RA8000/ESA12000 HSG80 Solutions Software V8.5 for OpenVMS, Installation Reference Guide*	*387401-001 AA-RH4BA-TE*
OpenVMS	*OpenVMS Fibre Channel Switch Application Note*	*EK-SMA34-AN*
Windows NT (Intel)	*RA8000/ESA12000 HSG80 Solution Software V8.5 for Windows NT - Intel, Installation Reference Guide*	*387387-003 AA-RFA9C-TE*
Windows NT (Intel)	*RA8000/ESA12000 FC-Fabric SAN Configurations for Windows NT – Intel, Application Note*	*AA-RHH6A-TE*
Sun Solaris	*RA8000/ESA12000 HSG80 Solution Software V8.5 for Sun Solaris, Installation Reference Guide*	*387387-001 AA-RFA9A-TE*
Sun Solaris	*Sun Solaris Fibre Channel Switch Application Note*	*EK-SMA37-AN*
HP-UX	*RA8000/ESA12000 HSG80 Solution Software V8.5 for HP-UX, Installation Reference Guide*	*387387-001 AA-RFA9A-TE*
HP-UX	*HP-UX Fibre Channel Hub Application Note*	*EK-SMA32-AN*
HSG80 Controller	*HSG80 Array Controller, ACS Version 8.5, Configuration Guide*	*165144-001 EK-HSG85-CG*
HSG80 Controller	*HSG80 Array Controller, ACS Version 8.5, CLI Reference Guide*	*165145-001 EK-HSG85-RG*
Enterprise Backup Solution	*Enterprise Backup Solution for Legato NetWorker, Reference Guide*	*161764-001*
Fibre Channel SAN Switch	*SAN Switch Fabric Operating System Management Guide*	*161358-001 EK-P20FF-GA*
Fibre Channel SAN Switch	*SAN Switch Web Management Tools Reference Guide*	*161357-001 EK-P20WW-GA*
Fibre Channel SAN Switch	*SAN Switch QuickLoop Management Guide*	*161360-001 EK-P20QL-GA*
Fibre Channel SAN Switch	*SAN Switch Zoning Reference Guide*	*161361-001 EK-P20ZG-GA*
Fibre Channel Storage Switch, 8 & 16 Port	*StorageWorks Fibre Channel Storage Switch User's Guide*	*135267-001 AA-RHBYA-TE*
StorageWorks Command Console	*Command Console V2.2 (HSG80) for Raid Array 8000/ESA12000, User's Guide*	*387405-004 AA–RFA2D–TE*
StorageWorks Command Console	*Command Console for the SAN Switch Installation Guide*	*136265-002 AA-RHDAB-TE*